Basic System Operations Guide

SmartEdge OS

Release 5.0.3
Part Number 220-0583-01

Corporate Headquarters
Redback Networks Inc.
300 Holger Way
San Jose, CA 95134-1362
USA
http://www.redback.com
Tel: +1 408 750 5000

Rights and Restrictions

All statements, specifications, recommendations, and technical information contained are current or planned as of the date of publication of this document. They are reliable as of the time of this writing and are presented without warranty of any kind, expressed or implied. In an effort to continuously improve the product and add features, Redback Networks Inc. ("Redback") reserves the right to change any specifications contained in this document without prior notice of any kind.

Redback shall not be liable for technical or editorial errors or omissions which may occur in this document. Redback shall not be liable for any indirect, special, incidental or consequential damages resulting from the furnishing, performance, or use of this document.

Third Party Software

The following third party software may be included with this Software and is subject to the following terms and conditions:

The OpenLDAP Version 2.0.1 © 1999 The OpenLDAP Foundation; OpenSymphony Software License, Version 1.1 2001-2004 © The OpenSymphony Group; TOAD © 2004 Quest Software, Inc.; NuSOAP Web Services Toolkit for PHP © 2002 NuSphere Corporation; The PHP License, versions 2.02 and 3.0 © 1999 - 2002 The PHP Group; The OpenSSL toolkit Copyright © 1998-2003 The OpenSSL Project; Apache HTTP © 2000 The Apache Software Foundation; Java © 2003 Sun Microsystems, Inc.; ISC Dhcpd 3.0pl2 © 1995, 1996, 1997, 1998, 1999 Internet Software Consortium - DHCP; IpFilter © 2003 Darren Reed; Perl Kit © 1989-1999 Larry Wall; SNMP Monolithic Agent © 2002 SNMP Research International, Inc.; VxWorks © 1984-2000, Wind River Systems, Inc.; Point-to-Point Protocol (PPP) © 1989, Carnegie-Mellon University; Dynamic Host Configuration Protocol (DHCP) © 1997, 1998 The Internet Software Consortium; portions of the Redback SmartEdge Operating System use cryptographic software written by Eric Young (eay@cryptsoft.com); Redback adaptation and implementation of the UDP and TCP protocols developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. © 1982, 1986, 1988, 1990, 1993, 1995 The Regents of the University of California. All advertising materials mentioning features or use of this Software must display the following acknowledgment: "This product includes software developed by the University of California, Berkeley and its contributors."

This Software includes software developed by Sun Microsystems, Inc., Internet Software Consortium, Larry Wall, the Apache Software Foundation (http://www.apache.org/) and their contributors. Such software is provided "AS IS," without a warranty of any kind. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE HEREBY EXCLUDED. LICENSORS AND ITS CONTRIBUTORS SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THIS SOFTWARE OR ITS DERIVATIVES. IN NO EVENT WILL LICENSOR OR ITS CONTRIBUTORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE THIS SOFTWARE, EVEN IF THE LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see http://www.apache.org/. Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign. The portions of this Software developed by Larry Wall may be distributed and are subject to the GNU General Public License as published by the Free Software Foundation.

FCC Notice

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

1. MODIFICATIONS

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Redback could void the user's authority to operate the equipment.

2. CABLES

Connection to this device must be made with shielded cables with metallic RFI/EMI connector hoods to maintain compliance with FCC Rules and Regulations. (This statement only applies to copper cables, Ethernet, DS-3, E1, T1, and so forth. It does not apply to fiber cables.)

3. POWER CORD SET REQUIREMENTS

The power cord set used with the System must meet the requirements of the country, whether it is 100-120 or 220-264 VAC. For the U.S. and Canada, the cord set must be UL Listed and CSA Certified and suitable for the input current of the system.

For DC-powered systems, the installation instructions need to be followed.

VCCI Class A Statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

European Community Mark

CE

The marking on this product signifies that it meets all relevant European Union directives.

Safety Notices

1. Laser Equipment:

CAUTION! Use of controls or adjustments of performance or procedures other than those specified herein may result in hazardous radiation exposure.

Class 1 Laser Product—Product is certified by the manufacturer to comply with DHHS Rule 21 Subchapter J.

CAUTION! Invisible laser radiation when an optical interface is open.

2. Lithium Battery Warnings:

It is recommended that, when required, Redback replace the lithium battery.

WARNING! Do not mutilate, puncture, or dispose of batteries in fire. The batteries can burst or explode, releasing hazardous chemicals. Discard used batteries according to the manufacturer’s instructions and in accordance with your local regulations.

Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type as recommended by the manufacturer’s instructions.

VARNING Eksplosionsfara vid felaktigt batteribyte. Använd samma batterityp eller en ekvivalent typ som rekommenderas av apparattillverkaren. Kassera använt batteri enligt fabrikantens instruktion.

ADVARSEL! Lithiumbatteri—Eksplosionsfare ved fejlagtig håndtering. Udskiftning må kun ske med batteri af samme fabrikat og type. Levér det brugte batteri tilbage tilleverandøren.

VARIOTUS Paristo voi räjähtää, jos se on virheellisesti asennettu. Vaihda paristo ainoastaan valmistajan suosittelemaan tyyppiin. Hävitä käytetty paristo valmistajan ohjeiden mikaisesti.

ADVARSEL Eksplosjonsfare ved feilaktig skifte av batteri. Benytt samme batteritype eller en tilsvarende type anbefait av apparatfabrikanten. Brukte batterier kasseres i henhold til fabrikantens instruksjoner.

WAARSCHUWING! Bij dit produkt zijn batterijen geleverd. Wanneer deze leeg zijn, moet u ze niet weggooien maar inleveren als KCA.

Contents

Part 4: Appendixes

About This Guide

This guide describes the tasks and commands used to monitor, administer, and troubleshoot the SmartEdge® OS features described in the *Basic System Configuration Guide* for the SmartEdge OS; commands include all **clear**, **debug**, **monitor**, **process**, and **show** commands that monitor and test system-wide functions and features, such as software processes.

This preface includes the following sections:

- Related Publications
- Intended Audience
- Organization
- Conventions
- Ordering Documentation

Related Publications

In parallel with this guide, use the *Basic System Configuration Guide* for the SmartEdge OS, which describes the tasks and commands used to configure the SmartEdge OS basic system features.

Use this guide and the *Basic System Configuration Guide* for the SmartEdge OS, in conjunction with the following publications:

- *Ports, Circuits, and Tunnels Configuration Guide* for the SmartEdge OS

  Describes the tasks and commands to use the command-line interface CLI and manage SmartEdge OS releases and configuration files; describes the tasks and commands used to configure the following SmartEdge OS features: traffic cards, their ports, channels, and subchannels, and Automatic Protection Switching (APS); circuits, including clientless IP service selection (CLIPS) circuits and link aggregation; bridging and cross-connections between circuits; Generic Routing Encapsulation (GRE) tunnels (including IP Version 6 [IPv6] over GRE tunnels), Layer 2 Tunneling Protocol (L2TP) tunnels, and overlay tunnels (IPv6 over IP Version 4 [IPv4]); static and dynamic bindings between ports, channels, subchannels, and circuits to interfaces, either directly or indirectly.

- *Routing Protocols Configuration Guide* for the SmartEdge OS

  Describes the tasks and commands used to configure the following SmartEdge OS features: static IP routing; dynamically verified static routing (DVSR); Virtual Router Redundancy Protocol (VRRP); Routing Information Protocol (RIP) and RIP next generation (RIPng); Open Shortest Path First (OSPF) and OSPF Version 3 (OSPFv3); Border Gateway Protocol (BGP); BGP/Multiprotocol Label Switching Virtual Private Networks (BGP/MPLS VPNs); Intermediate System-to-Intermediate System (IS-IS); Bidirectional Forwarding Detection (BFD); IP multicast, including Internet Group Management Protocol (IGMP), Multicast Source Discovery Protocol (MSDP), and Protocol Independent Multicast (PIM); routing policies; MPLS; Layer 2 Virtual Private Networks (L2VPNs); Virtual Private LAN Services (VPLS); and Label Distribution Protocol (LDP). BGP, OSPFv3, RIPng, and routing policies include tasks and commands that provide limited support for IPv6 routing.

- *IP Services and Security Configuration Guide* for the SmartEdge OS

  Describes the tasks and commands used to configure the following SmartEdge OS features: Address Resolution Protocol (ARP), Neighbor Discovery (ND) protocol for IPv6 routers, Dynamic Host Configuration Protocol (DHCP), Network Time Protocol (NTP), Domain Name System (DNS), HTTP redirect, access control lists (ACLs), forward policies, Network Address Translation (NAT) policies, service policies, quality of service (QoS) policies, authentication, authorization, and accounting (AAA), Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+), key chains, and lawful intercept (LI).

- *Ports, Circuits, and Tunnels Operations Guide* for the SmartEdge OS

  Describes the tasks and commands used to monitor, administer, and troubleshoot the SmartEdge OS features described in the *Ports, Circuits, and Tunnels Configuration Guide*; commands include all **clear**, **debug**, **monitor**, and **show** commands, along with other operations-based commands, such as device management and on-demand diagnostics.

- *Routing Protocols Operations Guide* for the SmartEdge OS

  Describes the tasks and commands used to monitor, administer, and troubleshoot the SmartEdge OS features described in the *Routing Protocols Configuration Guide*; commands include all **clear**, **debug**, **monitor**, **process**, and **show** commands, along with other operations-based commands.

- *IP Services and Security Operations Guide* for the SmartEdge OS

  Describes the tasks and commands used to monitor, administer, and troubleshoot the SmartEdge OS features described in the *IP Services and Security Configuration Guide*; commands include all **clear**, **debug**, and **show** commands, along with other operations-based commands.

- *SmartEdge 800 Router Hardware Guide*

  Describes the SmartEdge 800 hardware and provides site preparation information and installation, monitoring, and maintenance procedures for the chassis and cards.

- *SmartEdge 400 Router Hardware Guide*

  Describes the SmartEdge 400 hardware and provides site preparation information and installation, monitoring, and maintenance procedures for the chassis and cards.

Intended Audience

This publication is intended for system and network administrators experienced in access and internetwork administration.

Organization

This guide is organized as follows:

- Part 1, “Introduction”

  This part describes the SmartEdge OS operations and tasks for basic features and functions.

- Part 2, “Getting Started”

  This part describes the SmartEdge OS operations functions, tasks and displays the command history used to access and navigate the SmartEdge OS CLI, and administer file storage and releases.

- Part 3, “Basic System Operations”

  This part describes the SmartEdge OS operations functions, tasks, and commands used to monitor, administer, and troubleshoot sessions; system clock and services; and monitor and test system-wide functions and features, such as software processes, and so on.

- Part 4, “Appendixes”

  This part describes the SmartEdge OS boot loader functions, tasks, and commands used to perform system recovery and system upgrade operations, including the alarm conditions and their probable causes.

Note There are two indexes in this guide: an index of tasks and features and an index of commands.

Conventions

This guide uses special conventions for the following elements:

- Command Modes and Privilege Levels
- Command Syntax
- Examples
- Task Tables
- Online Navigation Aids

Command Modes and Privilege Levels

You enter commands (in exec mode) or in one of many configuration modes. By default, the majority of commands in exec mode have a privilege level of 3, while commands in any configuration mode have a privilege level of 10. Exceptions are noted in parentheses ( ) in the "Command Mode" section in any command description; for example, "exec (15)".

For a hierarchy list of commands, see the "Operations Commands" section in the "Overview" chapter.

For detailed information about command modes, prompts, and privilege levels, see the "User Interface" section in the "Overview" chapter.

Command Syntax

Table 1 lists the descriptions of the elements used in a command syntax terminology.

Table 1 Command Syntax Terminology

Syntax Element	Definition	Example Fragment
Argument	An item for which you must supply a value.	*slot*
Construct	A combination of: • A keyword and its argument. • Two or more keywords that cannot be specified independently. • Two or more arguments that cannot be specified independently.	 • **min-wait** *seconds* • **line fdl ansi** • *dest dest-wildcard*
Keyword	An optional or required item that must be entered exactly as shown.	**all**

Table 2 describes the separator characters in a command syntax.

Table 2 Separator Characters in Command Syntax

Character	Use	Example Fragment
@	Separates the prefix name from the suffix name.	*sub-name*@*ctx-name*
/	Separates slot from port, IP address from prefix length, and separates fields in URLs.	*slot*[**/***port*] {*ip-addr* | **/***prefix-length*} **/***device*[**/***directory*]**/***filename***.***ext*
:	Separates port from channel and channel from subchannel.	*port*[**:***chan-num*] *ds3-chan-num*[**:***ds1-chan-num*]
-	Separates starting value from ending value.	*start***-***end*
|	Separates output modifiers from keywords and arguments in **show** commands[1].	**show configuration | include port**

1. For more information about the use of the pipe (**|**) character, see Chapter 2, "Using the CLI."

The following guidelines apply to separator characters in Table 2:

- The separator character between the prefix and suffix names in a structured username is configurable; the @ character is the default and is used in command syntax throughout this guide.
- Separator characters act as one-character keywords; therefore, they are always shown in bold.

Table 3 lists the characters and formats used in command syntax statements.

Table 3 Text Formats and Characters in Command Syntax

Convention	Example
Commands and keywords are indicated in **bold**.	**no ip unnumbered**
Arguments for which you must supply the value are indicated in *italics.*	**banner login** *delimited-text*
Square brackets ([ ]) indicate optional arguments, keywords, and constructs within scripts or commands.	**show clock** [**universal**] **enable** [*level*]
Alternative arguments and keywords within commands are separated by the pipe character (|).	**public-key** {**DSA** | **RSA**} [**after-key** *existing-key* | **position** *key-position*] {*new-key* | **ftp** *url*}
Alternative, but required arguments and keywords, are shown within grouped braces ({ }), and are separated by the pipe character (|).	**debug ssh** {**all** | **ssh-general** | **sshd-detail** | **sshd-general**} **ip address** *ip-addr* {*netmask* | */prefix-length*} [**secondary**]
Optional and required arguments, keywords, and constructs can be nested with grouped braces and square brackets, where the syntax requires such format.	**enable authentication** {**none** | *method* [*method* [*method*]]}

Examples

Examples use the following conventions:

- System prompts are of the form `[context]hostname(mode)#, [context]hostname#`, or `[context]hostname>`.

  In this case, `context` indicates the current context, `hostname` represents the configured name of the SmartEdge system, and `mode` indicates the string for the current configuration mode, if applicable.

  Whether the prompt includes the # or the > symbol depends on the privilege level. For further information about privilege levels, see Chapter 1, “Overview.”

  For example, the prompt in the `local` context on the system `Redback` in `context` configuration mode is:

  ```
  [local]Redback(config-ctx)#
  ```

- Information displayed by the system is in `Courier` font.
- Information that you enter is in **`Courier bold`** font.

Task Tables

Tasks to monitor, administer, and troubleshoot features are described in task tables under the “Operations Tasks” section in each chapter. The command syntax displays only the root command, which is hyperlinked to the location where the complete command syntax is described in the “Command Descriptions” section of the chapter. Table 4 displays an example of an operations task table.

Table 4 Operations Task Table

Task	Command
Enable the generation of debug messages for all configured interfaces in the current context.	**debug if**

Table 4 Operations Task Table *(continued)*

Task	Command
Display information about interfaces, including the interface bound to the Ethernet management port on the controller card.	**show ip interface**
Display status of the IP address pool for the specified interface.	**show ip pool**

Online Navigation Aids

To aid in accessing information in the online format for this guide, the following types of cross-references are hyperlinks:

- Cross-references to chapters, sections, tables, and figures in the text
- Lists of section headings within a chapter or appendix
- Commands listed in the "Related Commands" section at the end of each command description
- Entries in the table of contents
- Entries in indexes

Note Hyperlinks in PDF files appear the same as regular text; however, your cursor changes from an open hand icon to a pointing finger icon when you move your cursor over a hyperlink.

Ordering Documentation

Redback® documentation is available on CD-ROM, which ships with Redback products. The appropriate CD-ROMS are included with your products as follows:

- SMS™ product
- SmartEdge router product
- NetOp™ product (includes NetOp Element Manager System [EMS] and NetOp Policy Manager [PM])

To order additional copies of the appropriate CD-ROM or printed, bound books, perform the following steps:

1. Log on to the Redback Networks Support web site at http://www.redback.com and enter a username and password.

   If you do not have a logon username and password, contact your Redback Networks support representative, or send an e-mail to supportlogin@redback.com with a copy of the **show hardware** command output, your contact name, company name, address, and telephone number. For detailed information on the **show hardware** command, see the "Hardware Operations" chapter, in the *Ports, Circuits, and Tunnels Operations Guide* for the SmartEdge OS.

2. On the Redback Networks Support web site, select one of the Redback Networks product line tabs at the bottom of the web page, click **Documentation** on the navigation bar, and then click **To Order Books** on the navigation bar.

To electronically provide feedback on our documentation, perform the following steps:

1. On the Documentation web page, click **Feedback** on the navigation bar.
2. Complete and submit the documentation feedback form.

We appreciate your comments.

Part 1

Introduction

This part describes the SmartEdge® OS operations and tasks for basic features and functions, and consists of Chapter 1, “Overview.”

Overview

The edge of the network is a highly demanding environment due to the large number of access terminations and the need to perform in-service upgrades to handle new feature deployments.

The SmartEdge® router hardware and software products provide multiservice optical platforms that enable the next generation of services in the new access network. The SmartEdge router products are edge routing platforms that provide:

- High-performance—The SmartEdge router product architecture enables line-rate packet forwarding.
- Robustness—The SmartEdge router products enable packet reliability, meeting rigorous uptime and availability requirements.
- Scalability—The SmartEdge router products support a large number of access terminations.
- Flexibility—The SmartEdge router products provide platforms that can support multiple services.

This chapter describes the SmartEdge OS tools you can use to manage the SmartEdge router; topics include:

- SmartEdge OS Overview
- Operations Tasks
- Operations Commands

SmartEdge OS Overview

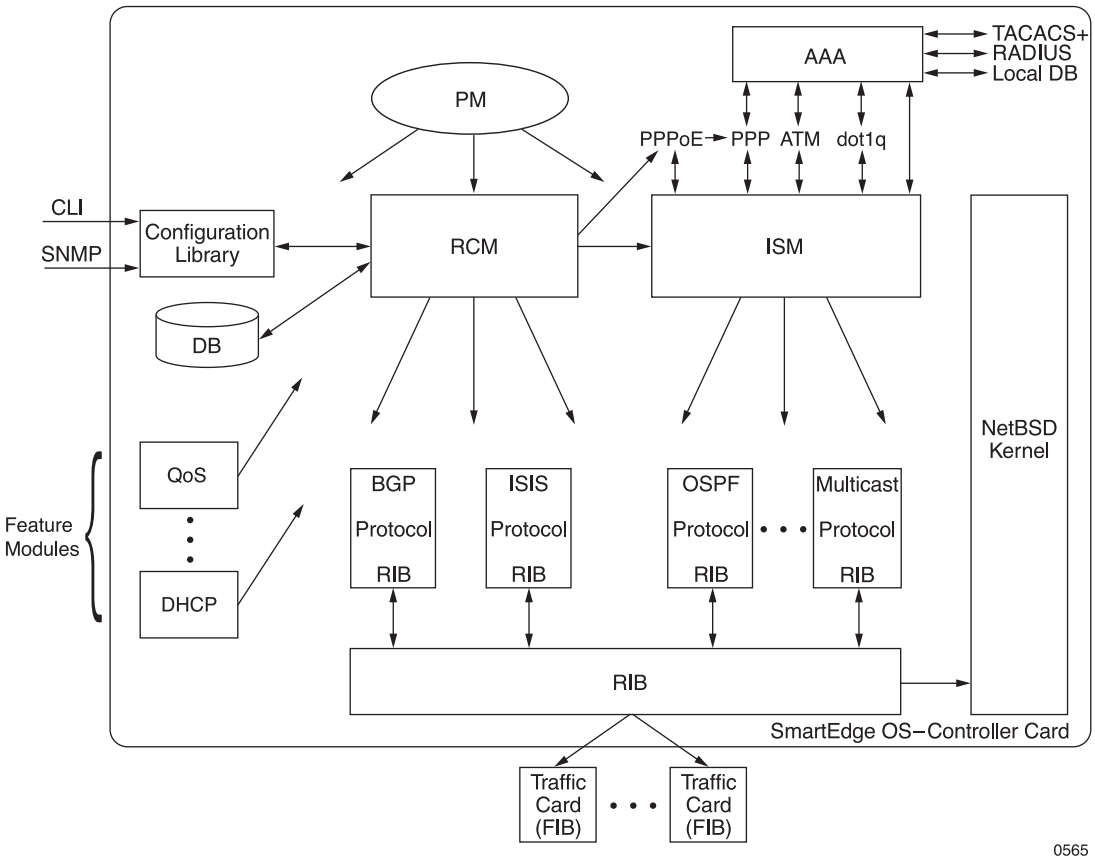
The SmartEdge OS is the advanced software system that works in conjunction with the ASIC-based SmartEdge hardware products to provide a scalable and robust multiservice platform. The features described in the following sections are especially important for operations tasks:

- System Architecture
- Independent System Processes
- System Redundancy and Synchronization
- Contexts
- User Interface

System Architecture

The SmartEdge OS performs the route processing and other control functions and runs on the controller card. The packet forwarding function is performed by Packet Processing ASICs (PPAs) on the individual traffic cards. Figure 1-1 illustrates the SmartEdge OS architecture.

Figure 1-1 SmartEdge OS Architecture



Independent System Processes

The SmartEdge OS is based on a general-purpose operating system; each major system component (see Table 1-1) runs as a separate process in the system.

Table 1-1 SmartEdge OS Components

System Component	Function
Authentication, authorization, and accounting (AAA)	Forces all authentication requests and accounting updates to a single set of Remote Authentication Dial-In User Service (RADIUS) servers.
NetBSD kernel	Provides a lean and stable base for the SmartEdge OS.
Process Manager (PM)	Monitors and controls the operation of the other processes in the system.
Router Configuration Manager (RCM)	Controls all system configurations using a transaction-oriented database.
Interface and Circuit State Manager (ISM)	Monitors and disseminates the state of all interfaces, ports, and circuits in the system.
Routing protocols	Run as an independent processes, maintaining independent Routing Information Bases (RIBs). The routing processes send the routing information to the central RIB.
RIB	Downloads forwarding tables to the traffic cards.
Feature modules	Run as independent processes, each in its own protected address space.
Traffic card	Includes the PPA ASICs, which contain the Forwarding Information Base (FIB) and forwarding code.

The implementation of the major software components as independent processes provides several benefits:

- Processes in the system can be independently stopped, restarted, and upgraded without reloading the entire system or individual traffic cards.
- The system continues to operate in the event of a failure or disruption to any single component.

The separation of the route processing and control functions (performed by the SmartEdge OS software running on the controller card) from the forwarding function (performed on the individual traffic cards) also provides several benefits:

- Dedicated route processing functions are not affected by heavy traffic; dedicated packet forwarding is not affected by routing instability in the network.
- The architecture enables line-rate forwarding on all traffic cards. New features can be added to the control software on the controller without affecting the forwarding performance.
- The architecture provides nonstop forwarding during system upgrades or reloads; the traffic cards continue to forward packets.

System Redundancy and Synchronization

Note In the following descriptions, the term, controller card, applies to the Cross-Connect Route Processor (XCRP) or the XCRP Version 3 (XCRP3) Controller card, unless otherwise noted.

Among other redundancy features, the SmartEdge routers and the operating system support dual controller cards; one card acts as the active controller and the other acts as its hot standby.

Both controller cards contain compact-flash cards that store the operating system image, its associated files, and the configuration database. A synchronization process ensures that the standby controller is always ready to become the active controller:

- When either the software release or the firmware on the active controller is upgraded, the standby controller automatically synchronizes its software or firmware version to that of the active controller.
- When a user modifies the contents of the compact-flash card (for example, by saving a configuration to a file, copying a file, or deleting a file), the change is propagated to the compact-flash card of the standby controller.
- The configuration databases of the active and standby controllers are always synchronized.

To guard against system inconsistency, the synchronization process is protected. While the synchronization is in progress, switchover from the active to the standby controller is not allowed. If the active controller should fail during such a time, the standby does not become active. If the user attempts to force a switchover during this synchronization period, the system warns the user that the standby is not ready.

The synchronization process is not affected by traffic card installation and removal. The active controller, and hence the system, continues to forward traffic and detect and notify the administrator of any faults that occur while the standby controller card is being synchronized (FAIL LED is blinking).

After the synchronization is complete, the standby controller is ready to become the active controller, if the active controller card should fail.

Contexts

Most networking products are designed so that the entire set of ports, circuits, and protocols operate together as one global instance. The SmartEdge OS supports an advanced feature called multiple contexts. Each context is a virtual SmartEdge router instance running within a single physical device. A context operates as a separate routing and administrative domain, with separate routing protocol instances, addressing, authentication, accounting, and so on, and does not share this information with other contexts. By separating the address and name spaces in this way, service providers can use multiple contexts to provide direct access to customers, or to provide different classes of services for customers. Service providers use a single physical device to implement this, with one or more contexts being assigned to each service provider or service class. Implementing this today with equipment from other vendors requires multiple devices.

The SmartEdge router is always configured with the special context, “local”. This context is always present on the system and cannot be deleted. In a single-context configuration, the local context is the only context present on the system.

User Interface

The primary user interface to the SmartEdge OS is the command-line interface (CLI). The CLI concepts that apply to operations commands are described in the following sections:

- Command Modes and Prompts
- Privilege Levels
- No Form of Commands

For more information about using CLI commands, see Chapter 2, “Using the CLI.”

Command Modes and Prompts

The two major modes are exec and global configuration. When a session is initiated, the CLI is set to the exec mode by default. The exec mode allows you to examine the state of the system and perform most administration, monitoring, and troubleshooting tasks using a subset of the available CLI commands.

Exec mode prompts can be one of the following forms, depending on the user privilege level (see the “Privilege Levels” section):

```
[local]hostname#
[local]hostname>
```

In this example, `local` is the context in which commands are applied and `hostname` is the currently configured hostname of the router. When you exit exec mode, using the **exit** command, you also end the CLI session.

Global configuration mode is the top-level configuration mode; all other configuration modes stem from this mode. To access global configuration mode, enter the **configure** command in exec mode.

Configuration mode prompts are of the following form:

```
[local]hostname(mode-name)#
```

In the example above, `local` is the context in which commands are applied, `hostname` is the currently configured hostname of the router, and `mode-name` is a string indicating the name of the current configuration mode.

The prompt in global configuration mode, assuming the factory default hostname of `Redback` and the `local` context, is as follows:

```
[local]Redback(config)#
```

Each feature supported through the SmartEdge OS can have one or more configuration modes, some of which you must access to enter an operations command for a particular feature. For more information about configuration modes and command mode hierarchy, see the “Command Mode Hierarchy” section in the “Overview” chapter, in the “*Basic System Configuration Guide* for the SmartEdge OS.

Privilege Levels

The SmartEdge OS supports 16 different privilege levels for administrators and for commands. By default, administrators are assigned an initial privilege level of 6; administrators can only issue commands that are assigned at the same level as their own privilege level or lower than their privilege level. At a privilege level of 6 or higher, the prompt in the CLI displays a number sign (#) instead of an angle bracket (>).

There are two types of administrators:

- Local—An administrator authenticated to the "local" context. The local administrator has a structured administrator name of the form *admin-name***@local**.
- Non-local—An administrator authenticated to any context other than the local context. An example of a non-local administrator has an administrator name of the form *admin-name***@***ctx-name* is `joe@vpn1`, where `vpn1` is the name of the context.

Note The separator character between the *admin-name* and the *ctx-name* arguments is configurable and can be any of %, -, @, _, \\, #, and /. For information about configuring the separator character, see the "AAA Configuration" chapter in the *IP Services and Security Configuration Guide* for the SmartEdge OS. The default value is @, which is used throughout this guide.

An administrator authenticated to the "local" context, given appropriate administrator privileges, can configure all functions on the SmartEdge router, including functions for each context, and global entities, such as ports, port profiles, SNMP, and so on. Non-local administrators have no configuration mode privileges, and have restricted exec mode privileges. To configure administrator privilege levels, see the "Context Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

Each command has a default privilege level that determines, given the privilege assigned to the administrator, who can enter the command. The majority of commands (in exec mode) have a default privilege level of 3, while commands in any configuration mode have a default privilege level of 10. Exceptions are noted in parentheses ( ) in the "Command Mode" section in any command description; for example, "exec (15)". To change the privilege level for a command, see the "Basic System Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

No Form of Commands

Some operations commands support the **no** keyword. Entering the **no** keyword in front of a command disables the function or removes the command from the configuration. For example, to enable the generation of debug messages for communications with another administrator during active Telnet or Secure Shell (SSH) sessions on the same SmartEdge router, enter the **debug talk** command (in exec mode). To subsequently disable the generation of the debugging messages for the circuit, enter the **no debug talk** command (in exec mode).

Operations Tasks

Operations tasks fall into three broad categories:

- Monitoring—Provides information about the state and status of one or more feature elements.
- Administration—Performs routine maintenance functions.
- Troubleshooting—Provides additional state and status information to help determine the cause of an operational problem.

Note Troubleshooting scenarios for isolating a particular type of problem are not included in this guide; they are beyond the scope of this guide.

Operations Commands

Operations commands are characterized as follows:

- Many operations commands are nonintrusive; they do not impact traffic flowing into and out of the SmartEdge router; for example, monitoring commands.
- Not all operations commands are applicable for all features; for example, some features support monitoring commands only; administration and troubleshooting commands are not appropriate.
- Most operations commands are run in exec mode; other administration commands, such as those to manage Automatic Protections Switching (APS) groups or place a card in an out-of-service state, must be entered in a configuration mode.
- Some operations commands require that you have configured a related feature to allow that type of function.

Operations commands are described in the following sections:

- Monitoring Commands
- Administration Commands
- Troubleshooting and Problem Recovery Commands

Monitoring Commands

Monitoring commands allow you to view the state of one or more feature elements. Table 1-2 lists the types of monitoring commands and examples of each type. Many of these monitoring commands can be found in this guide, or in the *Ports, Circuits, and Tunnels Operations Guide* for the SmartEdge OS.

Table 1-2 Types of Monitoring Commands

Type of Command	Example	Function
Device monitoring	**show chassis**	Display status of cards installed in the chassis.
	show hardware	Display detailed card hardware information. For more information on the **show chassis** and the **show hardware** commands, see the “Hardware Operations” chapter in the *Ports, Circuits, and Tunnels Operations Guide* for the SmartEdge OS.
	show port perf-monitor	Display configuration and performance statistics for one or more ports. For more information on this command, see the “Card, Port, and Channel Operations” chapter in the *Ports, Circuits, and Tunnels Operations Guide* for the SmartEdge OS.

Table 1-2 Types of Monitoring Commands *(continued)*

Type of Command	Example	Function
Feature monitoring	**show circuit counters**	Display statistics for one or more circuits. For more information on the **show circuit counters** command, see the "Circuit Operations" chapter in the *Ports, Circuits, and Tunnels Operations Guide* for the SmartEdge OS.
	monitor process	Monitor the status of a process and provide continuous updates. Enter this command in exec mode.
File monitoring	**directory**	Display a list of files in the specified directory. Enter this command in exec mode.
	pwd	Display the current working directory. Enter this command in exec mode.
Process monitoring	**show process**	Display current status of a process. Enter this command in all configuration modes.
Release monitoring	**show release**	Display release and installation information. Enter this command in all modes.
	show version	Display the version of the currently running OS. Enter this command in all modes.
Session (administrator) monitoring	**show privilege**	Display the current privilege level for the current session. Enter this command in all modes.
	show public-key	Display the public keys for an administrator. Enter this command in all modes.
System monitoring	**show clock-source**	Display clock source information. Enter this command in all modes.
	show configuration	Display the configuration commands for a feature. Enter this command in all modes.
	show memory	Display memory statistics. Enter this command in all modes.
	show redundancy	Display state of the standby controller card. Enter this command in all modes.
	show system alarm	Display system alarms at one or more levels. Enter this command in all modes. For more information on the **show redundancy** and **show system alarm** commands, see the "Hardware Operations" chapter in the *Ports, Circuits, and Tunnels Operations Guide* for the SmartEdge OS.

Administration Commands

Administration commands allow you to perform routine maintenance. Table 1-3 lists the types of administration commands, run in exec mode, and examples of each type. Many of these administration commands can be found in this guide, or the *Ports, Circuits, and Tunnels Operations Guide* for the SmartEdge OS.

Table 1-3 Types of Administration Commands

Type of Command	Example	Function
Device management	**mount** /md	Mount a mass-storage device.
	shutdown	Disable a port (stop operations on it).
		For more information on the **mount** /md and **shutdown** commands, see the "Hardware Operations" chapter in the *Ports, Circuits, and Tunnels Operations Guide* for the SmartEdge OS.
Feature management	**clear circuit counters**	Clear circuit counters for one or more circuits. Enter this command in exec mode.
		For more information on this command, see the "Circuit Operations" chapter in the *Ports, Circuits, and Tunnels Operations Guide* for the SmartEdge OS.
File management	**delete**	Delete a file. Enter this command in exec mode.
	mkdir	Create a directory. Enter this command in exec mode.
Process management	**process start**	Start a process. Enter this command in exec mode.
	process stop	Stop a process. Enter this command in exec mode.
Release management	**release upgrade**	Install another release. Enter this command in exec mode.
	release erase	Remove a release. Enter this command in exec mode.
Session (administrator) management	**enable**	Modify the privilege level for the current session. Enter this command in exec mode.
	ssh	Establish a SSH session from the SmartEdge router to a host. Enter this command in exec mode.
System management	**bulkstats force transfer**	Immediately transfer the bulkstats data file to the configured receiver. Enter this command in exec mode.
	clock set	Set the system time. Enter this command in exec mode.

Troubleshooting and Problem Recovery Commands

Troubleshooting commands allow you to view information or determine the low-level state of a feature element. Table 1-4 lists the types of troubleshooting and problem recovery commands, which are run in various modes, and examples of each type. Many of these troubleshooting and recovery commands can be found in this guide, or in the *Ports, Circuits, and Tunnels Operations Guide* for the SmartEdge OS.

Table 1-4 Types of Troubleshooting and Problem Recovery Commands

Type of Command	Example	Function
Feature troubleshooting	**debug snmp**	Initiate internal monitoring of a feature and the generation of messages, which can be stored in the system log buffer or displayed in real time.
		Enter this command in exec mode.
System troubleshooting or problem recovery	**reload**	Reload the operating system. Enter this command in exec mode.
	save seos-core	Save a core dump of the operating system to a pair of files on the mass-storage device /md partition. Enter this command in exec mode.

Table 1-4 Types of Troubleshooting and Problem Recovery Commands *(continued)*

Type of Command	Example	Function
Device troubleshooting or problem recovery	**bert**	Test a DS-3 channel or port, DS-1 channel, or E3 port. For information on the **bert** command, see the "Card, Port, and Channel Operations" chapter in the *Ports, Circuits, and Tunnels Operations Guide* for the SmartEdge OS.
	ping	Test IP connectivity to a host. Enter this command in exec mode.
	format microdrive	Reformat the mass-storage device.
	diag on-demand	Initiate on-demand diagnostics for a card.
		Enter **format microdrive** and the **diag on-demand** commands in exec mode. For information on the **format microdrive** and the **diag on-demand** commands, see the "Hardware Operations" chapter in the *Ports, Circuits, and Tunnels Operations Guide* for the SmartEdge OS.
Process troubleshooting or problem recovery	**process set**	Set process management parameters for a specified process. Enter this command in exec mode.
	process coredump	Initiate a core dump of a process and save it in a crash file. Enter this command in exec mode.
	process restart	Restart a process that has stopped. Enter this command in exec mode.

Part 2

Getting Started

This part describes the SmartEdge® OS operations functions, tasks and displays the command history used to access and navigate the SmartEdge OS command-line interface (CLI), and administer file storage and releases.

This part consists of the following chapters:

- Chapter 2, “Using the CLI”
- Chapter 3, “File and Release Operations”

Using the CLI

This chapter describes the tasks and commands you use to navigate the command-line interface (CLI) to the SmartEdge® OS. The CLI only requires you to enter enough of any command or keyword to uniquely identify it.

Note In the following descriptions, the term, controller card, applies to the Cross-Connect Route Processor (XCRP) or the XCRP Version 3 (XCRP3) Controller card, unless otherwise noted.

The primary administrator interface to the SmartEdge OS is the CLI. You access the CLI from the console port or through a remote session (for example, Telnet or Secure Shell [SSH]) to monitor, administer, and troubleshoot the SmartEdge OS. To access the SmartEdge OS software and its CLI, use either of the following methods:

- Connect to the console port—Located on the controller card and labeled “Craft 2”; you can connect a terminal to this port, either directly or through a terminal server.

  If the console port has been secured, you are prompted to log on; if the console port has not been secured, you initiate your session by simply pressing **Enter**.

- Connect to the Ethernet management port—Located on the controller card and labeled “ENET”; you can use this port to connect a terminal to the system over a LAN if remote access using Telnet or SSH has been enabled.

  If the Ethernet management port has been configured, you are prompted to log on.

To log on to the system, you must enter a valid administrator name and password at the appropriate prompts to gain access. The administrator name is of the form *admin-name***@***ctx-name*. The *ctx-name* specifies the name of the context the system uses for authentication. You can include a context for a logon, but the context name is optional—if a context name is not supplied, the local context is assumed.

Note The separator character between the *admin-name* and the *ctx-name* arguments is configurable and can be any of %, -, @, _, \\, #, and /. For information about configuring the separator character, see the “AAA Configuration” chapter in the *IP Services and Security Configuration Guide* for the SmartEdge OS. The default value is @, which is used throughout this guide.

When you connect to the system either directly to the console or remotely to the management port, the password you enter is not echoed.

If the management port has been configured, you can establish a Telnet or SSH session to the system. There are many tools that provide Telnet and SSH access to remote systems. These tools are beyond the scope of this document. In general, you must provide the system name (the hostname configured for the system) or IP address (the IP address configured for the system management port), as well as an administrator name and password.

If you forget a password, you must delete the administrator account and create a new one; there is no way to modify the password for an administrator account.

If you forget all passwords on the system, you must perform the password discovery procedure described in the "Recover a Lost Password" section in Appendix A, "Boot Loader Operations."

The SmartEdge OS provides default settings for local console sessions. You can customize these settings for the duration of the current session. To change the settings, see Chapter 4, "Session Operations." After you are logged on to the system, you have access to the CLI, based on the context to which you are logged on and the privilege level of your account.

This chapter includes the following sections:

- Operations Tasks
- Command Descriptions

Operations Tasks

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 Descriptions" section.

This section includes the following topics:

- Display Help for a Command
- Navigate the CLI
- Recall Previous Command Entries
- Edit Command Entries
- Filter Show Command Output

Display Help for a Command

You can access the online help for the CLI in the following ways:

- Use the **?** command when entering a command to display the options available at the current state of the command syntax.
- Use the **help** command to display how to use the ? character to obtain help.

Table 2-1 lists these commands; enter either command in any mode.

Table 2-1 Access Online Help

Task	Root Command	Notes
Obtain help for the current command.	**?**	
Obtain help for using the ? command.	**help**	

Note To enter the ? character as part of a command, when it is not a request for online Help, enter the **Esc** character followed by the **?** character.

Navigate the CLI

To navigate the CLI, perform the tasks described in Table 2-2.

Table 2-2 Navigate the CLI

Task	Command
Return the privilege level for the current exec session to the initial privilege level configured for the current administrator account. Enter this command in exec mode.	**disable**
Change the current privilege level for an exec session while in exec mode. Enter this command in exec mode.	**enable**
Return to exec mode while in any configuration mode. Enter this command in all modes.	**exit**
End the exec session. Enter this command in all configuration modes.	**end**
Displays the current configuration of the SmartEdge router, or the contents of a previously saved configuration file on the local file system. Enter this command in all modes.	**show configuration**
Display the command history for the current session. Enter this command in all modes.	**show history**
Display outstanding transactions for other administrators or for internal processes. Enter this command in all modes.	**show transaction**

Recall Previous Command Entries

Table 2-3 lists two Emacs-style command keyboard sequences that allow you to step through previously entered commands.

Table 2-3 Recall Previously Entered Commands

Keyboard	Description
Ctrl+**p** or up arrow	Recalls previous command in the command history
Ctrl+**n** or down arrow	Recalls next command in the command history

Edit Command Entries

Table 2-4 lists additional Emacs-style command keyboard sequences.

Table 2-4 Additional Emacs-Style Keyboard Sequences

Keyboard	Description
Ctrl+**f** or right arrow	Moves cursor forward one character
Ctrl+**b** or left arrow	Moves cursor backward one character
Esc+**f**	Moves cursor forward one word
Esc+**b**	Moves cursor backward one word
Ctrl+**a**	Moves cursor to beginning of line
Ctrl+**e**	Moves cursor to end of line
Ctrl+**k**	Deletes to end of line
Ctrl+**u**	Deletes to beginning of line
Ctrl+**d**	Deletes character
Esc+**d**	Deletes word
Ctrl+**c**	Quits editing the current line
Ctrl+**l**	Refreshes (redraws) the current line
Ctrl+**t**	Transposes current character with previous

For more information on Emacs key bindings, see the GNU Emacs documentation available at http://www.gnu.org.

Filter Show Command Output

The following example displays all lines from the output for the **show configuration** command (in any mode) beginning with the line before the first line that contains the word (pattern), `ospf`, and including the `6` lines after the first occurrence of the pattern:

```
[local]Redback#show configuration | begin before 1 after 6 ospf

router ospf 64001
  spf-timers 1 1
  area 0.0.0.0
   interface 10.100.11.10
  area 0.0.0.11
   interface 10.100.11.27
   interface 10.100.11.49
```

The following example displays all lines in the current configuration file that contain the word (pattern), `port`:

```
[local]Redback#show configuration | include port

card ether-12-port 1
```

```
card oc12-4-port 2
card gigaether-4-port 3
port ethernet 1/1
port ethernet 1/2
port ethernet 1/3
port ethernet 1/4
port pos 2/1
port pos 2/2
port pos 2/3
port pos 2/4
```

Show Command Output with Modifiers

All **show** commands accept a common set of keywords and arguments called modifiers, which you can use to refine the output displayed by the SmartEdge OS. You can apply multiple modifiers to a **show** command.

The syntax for the output modifiers is as follows:

[| {**begin** [**before** *lines*] [**after** *lines*] [*pattern*] | **count** | **exclude** *pattern* | **include** *pattern* | {**grep** [**options** *options*] *pattern}* | **save** *filename*}]

Table 2-5 describes how each modifier affects the **show** command output.

Table 2-5 Modifier Syntax Descriptions

Modifier	Description
|	Modifies the output displayed with the keywords that follow.
begin	Displays output beginning at the first occurrence of text matching the specified pattern.
before *lines*	Optional. Number of lines before the first line containing the matching pattern to display.
after *lines*	Optional. Number of lines after the first line containing the matching pattern to display.
pattern	Regular expression for a pattern to be searched for in the display output. For more information on regular expressions, see the GNU documentation available at http://www.gnu.org.
count	Displays only the number of lines of output for the command.
exclude	Excludes all lines that contain text that matches the specified pattern from the display.
include	Includes only the lines that contain text that matches the specified pattern in the display.
grep	Includes only the lines that contain text that matches the specified pattern in the display.
options *options*	Optional. UNIX **grep** command options. For more information on grep options, see the GNU grep documentation available at http://www.gnu.org.
save *filename*	Output saved to the specified filename.

Command Descriptions

This section describes the syntax and usage guidelines for the commands used to navigate the CLI and display command history. The commands are presented in alphabetical order.

?
disable
enable
end
exit
help
show configuration
show history
show transaction

?

?

Purpose

Displays brief system help on the available commands or command options.

Command Mode

all modes

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **?** command to display brief system help on the available commands or command options.

To list all valid commands available in the current mode, enter a question mark (**?**) at the system prompt.

To list the associated keywords or arguments for a command, enter the **?** command in place of a keyword or argument on the command line. This form of help is called full help, because it lists the keywords or arguments that apply to the command based on the full command, keywords, and arguments you have already entered.

To obtain a list of commands or keywords that begin with a particular character string, enter the abbreviated command or keyword immediately followed by the **?** command. This form of help is called partial help, because it lists only the commands or keywords that begin with the abbreviation you entered.

Examples

The following example displays exec commands available for a user with a privilege level of 6 (> prompt):

```
[local]Redback>?

  atm         ATM Operations
  debug       Modify debugging parameters
  disable     Drop into disable user mode
  edit        Edit a file with vi
  enable      Modify command mode privilege
  exit        Exit exec mode
  help        Description of the interactive help system
  monitor     Monitor information
  more        Display the contents of a file
  mrinfo      Request multicast router information
  mtrace      Trace reverse multicast path from source to receiver
  no          Disable an interactive option
```

```
  ping        Packet Internet Groper Command
  show        Show running system information
  ssh         Execute SSH/SSHD commands
  talk        talk to user
  telnet      Telnet to a host
  terminal    Modify terminal settings
  traceroute  Trace route to destination
```

The following example displays how to use partial help to display all commands (in global configuration mode) that begin with the character sequence `sy`:

```
[local]Redback(config)#sy?

  system    system clock-source
```

The following example displays how to use full help to display the next argument of a partially complete **system clock** command (in global configuration mode):

```
[local]Redback(config)#system clock ?

  summer-time   Configure summer (daylight savings) time
  timezone      Configure time zone

[local]Redback(config-ctx)#system clock
```

Related Commands

help

disable

disable

Purpose

Returns the privilege level for the current exec session to the initial privilege level configured for the current administrator account.

Command Mode

exec

Syntax Description

This command has no arguments or keywords.

Default

None

Usage Guidelines

Use the **disable** command to return the privilege level for the current exec session to the initial privilege level configured for the current administrator account. The **no enable** command (in exec mode) performs the same function. This command is available for any privilege level.

Examples

The following example displays the enable privilege level for the current exec session:

```
[local]Redback#show privilege

Current privilege level is 15
```

The following example returns the current exec session to the initial privilege level for the administrator:

```
[local]Redback#disable
[local]Redback>show privilege level

The current privilege level is 6
```

Related Commands

exit
show privilege

enable

enable [*level*]

no enable

Purpose

Modifies the privilege level for the current exec session.

Command Mode

exec

Syntax Description

level	Optional. Requested privilege level. The range of values is 0 to 15; if you do not enter a value, the system defaults to 15.

Default

When you enter this command without the *level* argument, the current exec session is held at level 15. For whatever value is set, the administrator's privilege level must be the same or higher.

Usage Guidelines

Use the **enable** command to modify the privilege level for the current exec session. Use the *level* argument to select the desired privilege level, up to the maximum privilege level configured for this administrator account. If this argument is omitted, the maximum privilege level (15) is enabled. This command is available for any privilege level.

If enable password authentication is enabled on the system (by default, local authentication is enabled; see the **enable authentication** command (in context configuration mode)), but no passwords are configured (using the **enable password** command (in context configuration mode)), you can only enter the **enable** command on the console port; the system does not prompt for a password. After you have configured at least one password, you can enter the **enable** command from the console or a remote session. If an enable password is configured for the requested privilege level, the system prompts for the password; otherwise, the system displays an error message and does not change the privilege level for the exec session. For more information on the **enable authentication** and **enable password** command (in context configuration mode), see the "Context Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

If enable password authentication is disabled on the system, the system does not prompt for a password when you modify the exec session privilege level.

Use the **no** form of this command to return to the initial privilege level configured for the administrator account. The **disable** command (in exec mode) performs the same function.

Examples

The following example displays an administrator attempting to set the privilege level for the exec session to a privilege level for which no password is configured:

```
[local]Redback>enable 10

%No enable password configured for this level
```

The following example sets the current exec session privilege level to 15. The system prompts for the password, which is not displayed on the screen. After the administrator enters the correct password, the system enters privileged mode as indicated by the pound sign (#) in the prompt.

```
[local]Redback>enable 15

Password:
[local]Redback#
```

Related Commands

exit
show privilege

end

end

Purpose

Exits the current configuration mode and returns to exec mode.

Command Mode

all configuration modes

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **end** command to exit the current configuration mode and return to exec mode. When you enter this command, all commands that you have entered since the beginning of the configuration session, or since the last **abort** or **commit** command (in configuration mode), are committed to the database.

Examples

The following example displays an administrator exiting interface configuration mode and returning to exec mode:

```
[local]Redback(config-if)#end
[local]Redback#
```

Related Commands

exit

exit

exit

Purpose

Exits the current configuration mode and returns to the next highest-level configuration mode. At the exec prompt, closes an active terminal or console session, and terminates the session.

Command Mode

all modes

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **exit** command to exit the current configuration mode, return to exec mode, or close an active terminal or console session.

Entering this command in any configuration mode exits the current configuration mode and returns to the next highest level configuration mode. When you enter this command in global configuration mode and return to exec mode, all commands that you have entered since the beginning of the configuration session, or since the last **abort** or **commit** command (in any configuration mode), are committed to the database.

Examples

The following example displays an administrator exiting global configuration mode and returning to exec mode:

```
[local]Redback(config)#exit
[local]Redback#
```

The following example displays how to exit an active Telnet session:

```
[local]Redback>exit
```

Related Commands

None

help

help

Purpose

Describes how to use the question mark (**?**) command to display help about available commands or command options.

Command Mode

all modes

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **help** command to display a brief description of the **?** command. You can enter this command in any mode. The output describes full help, which you use to identify all possible arguments to a command or command keyword; and partial help, which you use to identify how to complete a command keyword.

Examples

The following example displays the output from the **help** command:

```
[local]Redback>help

Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)
```

Related Commands

?

show configuration

show configuration [*url*] [*feature*]

Purpose

Displays the current configuration of the SmartEdge router, or the contents of a previously saved configuration file on the local file system.

Command Mode

all modes

Syntax Description

url Optional. URL of a configuration file to be displayed.

feature Optional. Feature or function for which the configuration is to be displayed, according to one of the keywords or constructs listed in Table 2-6.

Default

The entire running configuration displays and includes only those commands that are required to modify the default configuration of the SmartEdge router.

Usage Guidelines

Use the **show configuration** command to display the current configuration of the SmartEdge router, or the contents of a previously saved configuration file on the local file system.

. Table 2-6 lists the optional keywords and constructs for the **show configuration** *feature* argument.

Table 2-6 Optional Keywords and Constructs for the *feature* Argument

Keyword or Construct	Description
acl	Displays only configuration information related to access control lists (ACLs).
aps	Displays only configuration information related to Automatic Protection Switching (APS).
arp	Displays only configuration information related to the Address Resolution Protocol (ARP).
atm	Displays only configuration information related to Asynchronous Transfer Mode (ATM).
bgp	Displays only configuration information related to the Border Gateway Protocol (BGP).
bridge	Displays only configuration information related to bridges.
bypass	Displays only configuration information related to cross-connected, or multiprotocol, circuit configuration.
card [*slot*]	Traffic cards, or optionally, a traffic card in a specific slot number. Displays only configuration information related to traffic cards, or if the *slot* argument is used, only information related to the card in the specified slot.
context *ctx-name*	Context for which configuration information displays.
dhcp	Displays only configuration information related to the Dynamic Host Configuration Protocol (DHCP) Relay/proxy.

Table 2-6 Optional Keywords and Constructs for the *feature* Argument *(continued)*

Keyword or Construct	Description
dns	Displays only configuration information related to the Domain Name System (DNS).
dot1q	Displays only configuration information related to the 802.1Q protocol.
forward	Displays only configuration information related to forward policy configuration.
fr	Displays only configuration information related to the Frame Relay.
gre	Displays only configuration information related to Generic Routing Encapsulation (GRE) tunnels.
hr	Displays only configuration information related to HTTP redirect.
igmp	Displays only configuration information related to the Internet Group Management Protocol (IGMP).
interface	Displays only configuration information related to interfaces.
isis	Displays only configuration information related to the Intermediate System-to-Intermediate System (IS-IS) protocol.
l2tp	Displays only configuration information related to Layer 2 Tunneling Protocol (L2TP) peers and groups.
l2vpn	Displays only configuration information related to Layer 2 Virtual Private Networks (L2VPNs).
ldp	Displays only configuration information related to the Label Distribution Protocol (LDP).
link-group	Displays only configuration information related to link groups.
log	Displays only configuration information related to the system logging facility.
mpls	Displays only configuration information related to multiprotocol label switching (MPLS).
mpls-static	Optional. Displays only configuration information related to MPLS static.
msdp	Displays only configuration information related to Multicast Source Discovery Protocol (MSDP).
nat	Displays only configuration information related to Network Address Translation (NAT).
nd	Displays only configuration information related to Neighbor Discovery (ND) protocol.
ntp	Displays only configuration information related to Network Time Protocol (NTP).
ospf	Displays only configuration information related to the Open Shortest Path First (OSPF) protocol.
ospf3	Displays only configuration information related to the Open Shortest Path First (OSPF) version 3 protocol.
pim	Displays only configuration information related to Protocol Independent Multicast (PIM).
policy	Displays only configuration information related to routing policies.
port [*slot*[**/***port*]]	All ports on all traffic cards, or all ports on a particular traffic card, or a specific port on a particular traffic card. Displays only port configuration information for traffic cards. If the *slot* argument is specified, displays only port information for the traffic card in the specified slot. If the *port* argument is also used, displays only information for the specified port number on that traffic card.
ppp	Displays only configuration information related to the Point-to-Point Protocol (PPP).
pppoe	Displays only configuration information related to the PPP over Ethernet (PPPoE).
qos	Displays only configuration information related to quality of service (QoS).
rip	Displays only configuration information related to the Routing Information Protocol (RIP).
rsvp	Displays only configuration information related to the Resource Reservation Protocol (RSVP).
snmp	Displays only configuration information related to the Simple Network Management Protocol (SNMP).

Table 2-6 Optional Keywords and Constructs for the *feature* Argument *(continued)*

Keyword or Construct	Description
software license	Displays only configuration information related to software licenses.
static	Displays only configuration information related to static routes.
tunnel	Displays only configuration information related to Generic Routing Encapsulation (GRE) tunnels.

You can use **show configuration** command in any mode. However, the optional keywords and constructs that are available and the information that they display depend on the mode in which you enter the command. For example, when you enter the **show configuration** command in context configuration mode, the system displays only the commands that apply to that context.

Use the **show configuration** command with the *url* argument to display the current system configuration or a previously saved configuration. When referring to a file on the local file system, the URL takes the following form:

[*/device*][*/directory*]*/filename.ext*

The *device* argument can be **flash**, or if a mass-storage device is installed, **md**. If the *device* argument is not specified, the default value is the device in the current working directory. If the *directory* argument is not specified, the default value is the current directory. Directories can be nested. The *filename* argument can be up to 256 characters in length.

Note You can also use this command to display the contents of a previously saved configuration file; see Chapter 3, “File and Release Operations.”

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, “Context, Interface, and Subscriber Operations.”

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see the “Filter Show Command Output” section.

Examples

The following example displays the active configuration of the system (in exec mode) running in the router:

```
[local]Redback#show configuration

Building configuration...

Current configuration:
!
!  Configuration last changed by user 'pm' at Mon Jan 28 06:18:22 2005
!
context local
---(more)---
```

The following example displays a previously saved configuration file, `full.cfg`, (in exec mode):

```
[local]Redback#show configuration /flash/full.cfg bgp

!
!  Configuration last changed by user 'pm' at Fri Mar 21 06:18:22 2003
!
context local
!
 ip localhost localhost 127.0.0.1
---(more)---
```

Related Commands

context
save configuration

show history

show history [**configuration**]

Purpose

Displays the command history for the current session.

Command Mode

all modes

Syntax Description

configuration	Optional. Displays a list of configuration commands entered during the current session. This keyword is available only in exec mode.

Default

Displays a list of commands entered during the current session within the current mode group (exec or configuration).

Usage Guidelines

Use the **show history** command to display the command history for the current session. The history log contains up to 40 commands. To restrict the history to only the configuration commands entered during the session, use the optional **configuration** keyword, which is only available in exec mode.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Examples

The following example displays output from the **show history** command (in global configuration mode):

```
[local]Redback(config)#show history

config
show clock
```

Related Commands

None

show transaction

show transaction

Purpose

Displays information about outstanding configuration database transactions made by other administrators in all configuration modes, or created by internal processes.

Command Mode

all modes

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show transaction** command to display information about outstanding configuration database transactions made by other administrators (in all configuration modes), or created by internal processes. Outstanding transactions are those that have been configured by other administrators or started by an internal process, but have not yet been committed to the configuration database. Table 2-7 lists the possible states that might be displayed for a transaction.

Table 2-7 Transaction States

State	Description
Active	Transaction is active for configuration changes.
Ready	Transaction just got the lock it was waiting for and is ready to proceed.
Blocked	Transaction is blocked waiting for a lock. The information field displays the transaction ID that holds the lock.
Blocked on User	Transaction is blocked by administrator input on whether to continue waiting for the lock to clear. The information field displays the transaction ID that holds the lock.
Pending Rollback	Administrator has requested to stop waiting for the lock and the system is preparing to rollback the current command.
Abort	Transaction is being erased.
Committing	Transaction is marked for commit.
Commit - Duplicated	Transaction is duplicated to the standby controller card.
Commit - Synched	Transaction is committed on the standby controller card.
Committed	Transaction has completed the committing on the active controller card.
Commit - Blocked	Commit is held up because of a global database lock. Waiting to commit after the lock is clear.

Table 2-7 Transaction States *(continued)*

State	Description
Waiting to Commit	Transaction has been time committed. It will be committed at a certain time. The information field displays the time until the commit.
Invalid	The transaction is invalid.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example shows the outstanding database transactions created, but not committed, by the `admin`, `admin1`, and `admin2` administrators:

```
[local]Redback>show transaction

TID       State                Sequence       State Information
          User                 Comment
------------------------------------------------------------------------------
1037      Blocked              73544          Waiting on TID 1035
          admin1               adding circuit under port 1
1035      Active               3634           None
          admin1               changing port 1
1032      Commit - Duplicated  564654         None
          admin1
1026      Waiting to Commit    2343564        Committing in 25 min
          admin                adding admin2 at midnight
1022      Active               565            None
          admin
1011      Abort                84454          None
          admin                deleting admin2
```

Related Commands

context

File and Release Operations

This chapter describes the tasks and commands used to administer file storage and release operations in the SmartEdge® OS.

For information about the commands used to configure these features, see the "Configuration File Management" chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

Note In the following descriptions, the term, controller card, applies to the Cross-Connect Route Processor (XCRP) or the XCRP Version 3 (XCRP3) Controller card, unless otherwise noted.

The term, chassis, refers to any SmartEdge chassis; the term, SmartEdge 800, refers to any version of the SmartEdge 800 chassis.

This chapter includes the following sections:

- Operations Tasks
- Command Descriptions

Operations Tasks

Note In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the full description for the command in the "Command Descriptions" section.

This section includes the following topics:

- Software Storage Organization
- Directory and File Operations
- Release Operations

Software Storage Organization

Each SmartEdge chassis can contain one or two controller cards. If there are two controller cards, one is active and the other is standby. Each controller card has two internal compact-flash cards: one to store the SmartEdge OS, configuration, and other system files, and one to store the low-level software. The compact-flash card for the low-level software is not accessible from the command-line interface (CLI).

The internal compact-flash card that stores the operating system files is also referred to as the NetBSD compact-flash card. Storage on the NetBSD compact-flash card is divided into three independent partitions: p01, p02, and /flash:

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

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

  The controller cards in the SmartEdge router ship with the current SmartEdge OS 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 and is used to store configuration files.

- The size of the NetBSD compact flash cards in the active and standby controllers cards need not match, but both cards must have at least 192 MB capacity.

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.

Directory and File Operations

The SmartEdge OS 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 3-1; enter all commands in exec mode. In addition to the tasks listed in Table 3-1, this section also includes a procedure to recover file space: “Recover File Space.”

Table 3-1 Directory and File Operations Tasks

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

Table 3-1 Directory and File Operations Tasks *(continued)*

Task	Command
Display the contents of a file on the local file system, one page at a time.	**more**
Display the current working directory.	**pwd**
Force a synchronization of the files on the standby controller card with those on the active controller card.	**release sync**
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.[1]	**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.[2]	**show configuration**

1. For information about configuration files, see the "Configuration File Management" chapter in the *Basic System Configuration Guide* for the SmartEdge OS.
2. For more information abut this command, see "Chapter 2, "Using the CLI."

Note The following guidelines apply to copy operations:

- For copy operations that require the use of 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.

Recover File Space

Synchronization of the active and standby controller cards occurs after a **reload** or **release sync** command (in exec mode), or after a 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.

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

   release sync

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

Release Operations

In addition to the SmartEdge OS system image stored on the local file system, each controller card contains a boot loader image and a minikernel image in its EEPROM. To monitor and administer the releases on the system, perform one or more of the tasks described Table 3-2; enter all commands in exec mode. To upgrade the system image on the controller cards, see the “Upgrade the System Image” section.

Table 3-2 Release Operations Tasks

Task	Command
Install an alternate release on the system.	**release download**
Manually erase an alternate system image.	**release erase**
Upgrade the system to use the alternate installed release when reloading.	**release upgrade**
Display release and installation information for the software images currently installed on the system.	**show release**
Display the current version of the software running on the system.	**show version**

Table 3-2 Release Operations Tasks *(continued)*

Task	Command
Upgrade the boot loader image in the EEPROM on the active controller card in a working system and reloads it.	**upgrade bootrom**
Upgrade the minikernel image in the EEPROM on the active controller card in a working system and reloads it.	**upgrade minikernel**

Upgrade the System Image

The SmartEdge router ships with the current SmartEdge OS release installed in the active partition, either p01 or p02. The system is configured to automatically load the installed release when the system is powered up. To upgrade the system image, you install the new image in the alternate partition and then make the alternate partition the active partition; the previously active partition then becomes the alternate partition.

Note For commands that request the use of a transfer protocol, such as FTP, SCP, or TFTP, it is assumed that a server is configured with a user account and password and reachable by the SmartEdge router to service these requests. If you are accessing a remote server, you must also have configured the management port to enable remote access.

Note Perform this procedure from the console port on the active controller card to view the progress of the upgrade operation. Remote sessions to the system are disconnected during the reload process.

To upgrade the system image, perform the following steps:

1. Verify the current software release (or releases) installed on your system; enter the following command (in any mode):

   show release

2. Install the new software release image in the alternate partition; enter the following command (in exec mode):

   release download *protocol***://***username*[**:***passwd*]**@**{*ip-addr* | *hostname*} [*//directory*]*/filename.ext*

   where the *protocol* argument is **ftp** or **scp**, the *username* and *passwd* arguments specify the user and an optional password on the server, the *ip-addr* argument is the IP address of the server, the *hostname* argument is the hostname of the server, the optional *directory* argument specifies a directory, and the *filename* argument is the name of the new software release image file.

Note Use double slashes (//) if the pathname to the directory on the remote server is an absolute pathname; use a single slash (/) if it is a relative pathname (under the hierarchy of *username* account home directory).

The following example uses FTP to download the release image file, `SEOS-5.0.3.tar.gz`, from the `images/REL_5_0_3` folder on the server at IP address, `10.13.49.100`, to the alternate boot system partition on the SmartEdge router:

```
[local]Redback#release download ftp://guest@10.13.49l.100//images/REL_5_0_3/
SEOS-5.0.3.tar.gz
```

Note If the system currently has an existing alternate software release image installed, you are prompted to confirm that you want to erase the existing alternate image. Enter **y** for yes.

3. Configure the system to reload using the newly installed image in the alternate partition after the download procedure is completed:

   a. Enter the following command (in exec mode):

      release upgrade

   b. Enter **y** for yes when the system prompts you to confirm that you want to reboot the system and make the alternate partition with the newly installed image become the active partition.

   c. The system might prompt you to save the current configuration.

   d. Enter **y** for yes and, optionally, provide a filename for the configuration, or enter **n** for no.

   Note If you enter **y**, but do not specify a filename for the configuration, the system saves the current configuration in the redback.cfg file. It is this configuration that is loaded when the system reloads.

   e. The system reloads with the new software release image.

4. Verify that the system is running the new SmartEdge OS release; enter the **show release** command (in any mode).

   In the following example, the newly installed software release, `SEOS-5.0.3`, is running on the system and stored in the active system boot partition:

   show release

```
Installed releases:

p02: active (will be booted after next reload)
-----------------------------------------------
Version SEOS-5.0.3-Release
Built on Mon Jan 03 10:00:01 PST 2005
Copyright (C) 1998-2005, Redback Networks Inc. All rights reserved.
p01: alternate
--------------
Version SEOS-2.5.5-Release
Built on Mon Aug 18 10:00:01 PDT 2003
Copyright (C) 1998-2003, Redback Networks Inc. All rights reserved.
```

Command Descriptions

This section describes the syntax and usage guidelines for the commands used to monitor, troubleshoot, and administer file storage and release operations. The commands are presented in alphabetical order.

cd
copy
delete
directory
edit
mkdir
more
pwd
release download
release erase
release sync
release upgrade
rename
rmdir
save configuration
show release
show version
upgrade bootrom
upgrade minikernel

cd

cd *url*

Purpose

Changes the current working directory.

Command Mode

exec (10)

Syntax Description

url	Name of the preferred working directory. Enter **..** to change to the parent of the current directory.

Default

None

Usage Guidelines

Use the **cd** command to change the current working directory. By default, the current working directory when you log on to the system is /flash.

You must specify a directory on the local file system, with a URL in the following form:

[/*device*][/*directory*]...[/*directory*]

The value for the *device* argument can be **flash**, or if a mass-storage device is installed, **md**. If you do not specify the *device* argument, the default value is the device in the current working directory. Directories can be nested to any level.

Examples

The following example changes the current working directory to `/flash/config/old`:

```
[local]Redback>cd /flash/config/old

Current directory is now /flash/config/old
```

The following example changes the current working directory to the parent directory:

```
[local]Redback>cd ..

Current directory is now /flash/config
```

The following example changes the current working directory to the mass-storage device:

```
[local]Redback>cd /md

Current directory is now /md
```

Related Commands

directory
mkdir
pwd

copy

copy [**mate**] *src-url dest-url* [**passive**] [**-noconfirm**]

Purpose

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.

Command Mode

exec (10)

Syntax Description

mate	Optional. Specifies that the source file is on the other controller card.
src-url	URL of the file that is to be copied.
dest-url	URL of the destination of the copy operation.
passive	Optional. Specifies passive mode for the File Transfer Protocol (FTP).
-noconfirm	Optional. Avoids a confirmation prompt when overwriting an existing file on the local file system.

Default

None

Usage Guidelines

Use the **copy** command to copy files to or from the system. At least one of the files, either the source or destination file, must be on a local file system.

Use the **mate** keyword to specify that the source file is on the other controller card (the controller card to which you are not connected).

Note You can only copy files from the other controller card; you cannot copy files to it.

When referring to a file on the local file system, the URL takes the following form:

[*/device*][*/directory*]*/filename.ext*

The value for the *device* argument can be **flash**, or if a mass-storage device is installed, **md**. If you do not specify the *device* argument, the default value is the device in the current working directory. If you do not specify the *directory* argument, the default value is the current directory. Directories can be nested. The value for the *filename* argument can be up to 256 characters in length.

You can also copy files using Remote Copy Protocol (RCP), Secured File Transfer Protocol (SFTP), or Trivial File Transfer Protocol (TFTP).

Note It is assumed that there is a system configured and reachable by the SmartEdge Router to service these requests.

Table 3-3 describes the syntax for the *url* argument when copying the file to a remote server.

Table 3-3 Syntax for the *url* Argument in the copy Command

Server Protocol	URL Format
FTP, SCP, or SFTP	**ftp:**//*username*[**:***passwd*]@{*ip-addr* | *hostname*}[//*directory*]/*filename***.***ext* **scp:**//*username*[**:***passwd*]@{*ip-addr* | *hostname*}[//*directory*]/*filename***.***ext* **sftp:**//*username*[**:***passwd*]@{*ip-addr* | *hostname*}[//*directory*]/*filename***.***ext*
RCP	**rcp:**//*username*@{*ip-addr* | *hostname*}[//*directory*]/*filename***.***ext*
TFTP	**ftp:**//{*ip-addr* | *hostname*}[//*directory*]/*filename***.***ext*

Note Use double slashes (//) if the pathname to the directory on the remote server is an absolute pathname; use a single slash (/) if it is a relative pathname (under the hierarchy of *username* account home directory).

The *filename* argument can be up to 256 characters in length. You can only use the *hostname* argument if Domain Name System (DNS) is enabled with the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands (in context configuration mode); see the "DNS Configuration" chapter in the *IP Services and Security Configuration Guide* for the SmartEdge OS.

Examples

The following example copies a file using TFTP from a remote server to the local file system. If the file already exists, the system prompts you to overwrite the existing file.

```
[local]Redback#copy tftp://192.168.3.141//configs/current.cfg /flash/current.cfg
```

The following example copies a file from one location to another of the local file system:

```
[local]Redback#copy /flash/redback.cfg /flash/backup/redback.cfg
```

The following example uses FTP to copy a file from a remote server with an IP address of `192.168.145.99` to the **/flash** directory:

```
[local]Redback#copy ftp://john:test@192.168.145.99//configs/redback.cfg /flash/
```

The following example performs the same operation described in the preceding example, except that the FTP operation is passive:

```
[local]Redback#copy ftp://john:test@192.168.145.99//configs/redback.cfg /flash/ passive
```

The following example copies a file from the mass-storage device of the standby controller card to the flash file system:

```
[local]Redback#copy mate /md/backup/redback1031.cfg /flash/backup/redback1031.cfg
```

Related Commands

delete
directory
rename

delete

delete [**mate**] [**crashfile**] *url* [**-noconfirm**]

Purpose

Deletes a file from the local file system on either the active or standby controller card.

Command Mode

exec (10)

Syntax Description

mate	Optional. Specifies that the file to be deleted is on the controller card to which you are not connected.
crashfile	Optional. Specifies that the file to be deleted is a crash file.
url	URL of the file to be deleted.
-noconfirm	Optional. Deletes files without asking for confirmation.

Default

None

Usage Guidelines

Use the **delete** command to delete a file from the local file system on either the active or standby controller card.

Use the **mate** keyword to specify the controller card to which you are not connected.

When referring to a file, the URL takes the following form:

[/*device*][/*directory*]/*filename***.***ext*

The value for the *device* argument can be **flash**, or if a mass-storage device is installed, **md**. If you do not specify the *device* argument, the default value is the device in the current working directory. If you do not specify the *directory* argument, the default value is the current directory. Directories can be nested. The value for the *filename* argument can be up to 256 characters in length.

Use the command-line interface (CLI) online Help for this command or the **show crashfiles** command (in any mode) to list the crash files currently located on the system.

If you do not specify the **-noconfirm** keyword, the system prompts you to confirm the deletion. Enter **y** to confirm the operation; if you enter any other character, the system does not delete the file.

Examples

The following example deletes a file in a nested subdirectory:

```
[local]Redback#delete /flash/backup/old/current.cfg
```

The following example deletes a crash file using the online Help to determine the URL; a confirmation message is accepted:

```
[local]Redback#delete crashfile ?

  /md/dlmd_50.core
  /md/dlmd_50.mini.core
  WORD                  URL of file to delete in local filesystem

[local]Redback#delete crashfile /md/dlmd_50.core
Are you sure you want to delete /md/dlmd_50.core ?y
```

Related Commands

copy
directory
rename
show crashfiles

directory

directory [**mate**] [*url*] [**-size** | **-time**] [**-reverse**]

Purpose

Displays a list of files in the specified directory on the local file system on either the active or standby controller card.

Command Mode

exec (10)

Syntax Description

mate	Optional. Specifies that the directory is on the controller card to which you are not connected.
url	Optional. URL of the directory with the filenames to be listed; if omitted, uses the current working directory.
-size	Optional. Specifies that the files are displayed in order of size, starting with the smallest.
-time	Optional. Specifies that the files are displayed in order of time, starting with the oldest.
-reverse	Optional. Specifies that files are displayed in reverse order.

Default

Files in the current working directory are displayed in alphabetical order.

Usage Guidelines

Use the **directory** command to display a list of files in the specified directory on the local file system on either the active or standby controller card. The output displays in the same format as the UNIX **ls(1) -l** command.

Use the **mate** keyword to specify the controller card to which you are not connected.

When referring to a directory on the local file system, the URL takes the following form:

[/*device*][/*directory*]...[/*directory*]

The value for the *device* argument can be **flash**, or if a mass-storage device is installed, **md**. If you do not specify the *device* argument, the default value is the device in the current working directory. If you do not specify the *directory* argument, the default value is the current directory. Directories can be nested. The value for the *filename* argument can be up to 256 characters in length.

Examples

The following example displays a list of files in the root directory of the flash file system:

```
[local]Redback#directory /flash

Contents of /flash
total 44
-rw-r--r--  1 root  0   595 Mar 11 05:24 basic.cfg
drwxr-xr-x  4 root  0   512 Jan 22 07:19 foo
-rw-r--r--  1 root  0  7252 Mar 11 05:24 redback.bin
-rw-r--r--  1 root  0  5454 Mar 11 05:24 redback.cfg
-rw-r--r--  1 root  0  5017 Mar 11 05:24 redback.cfg.bak
drwxr-xr-x  3 root  0   512 Mar 11 05:24 saved
```

Related Commands

copy **rename**
mkdir **rmdir**

edit

edit *url*

Purpose

Using the vi editor, creates or opens an existing file on the local file system for editing.

Command Mode

exec (10)

Syntax Description

url	URL of the file to be created or edited.

Default

None

Usage Guidelines

Use the **edit** command to create or open an existing file on the local file system for editing.

Use the **:q!** command to discard any edits and exit the editor; use the **:wq!** command to save any edits and exit the editor.

Examples

The following example opens the `redback.cfg` file using the vi editor:

```
[local]Redback#edit redback.cfg
!
!  Configuration last changed by user 'pm' at Mon Jan  3 08:04:25 2005
!
service multiple-contexts
!
context local
!
  ip domain-lookup
!
 interface mgmt
  ip address 10.1.1.3/21
!
 enable encrypted 1 $1$........$kvQfdsjs0ACFMeDHQ7n/o.
!
 user test encrypted 1 $1$........$kvQfdsjs0ACFMeDHQ7n/o.
!
 ip route 10.1.0.0/16 10.12.208.1 cost 1 permanent
 ip route 155.53.0.0/16 10.12.208.1 cost 1 permanent
!
```

```
port ethernet 7/1
! XCRP management ports on slot 7 and 8 are configured through 7/1
 no shutdown
 bind interface mgmt local
!
system hostname supercomm7
!
service console-break
!
end
```

Related Commands

directory
pwd

mkdir

mkdir *url*

Purpose

Creates a new directory on a local file system.

Command Mode

exec (10)

Syntax Description

url	URL of the directory to be created.

Default

None

Usage Guidelines

Use the **mkdir** command to create a new directory on the local file system.

When specifying a directory on the local file system, the URL takes the following form:

[/*device*][/*directory*].../*directory*

The value for the *device* argument can be **flash**, or if a mass-storage device is installed, **md**. If you do not specify the *device* argument, the default value is the device in the current working directory. If you do not specify the *directory* argument, the default value is the current directory. Directories can be nested. The value for the *filename* argument can be up to 256 characters in length.

Examples

The following example creates a new top-level directory, `backups`, on the flash file system:

```
[local]Redback#mkdir /flash/backups
```

Related Commands

directory
rename
rmdir

more

more *url*

Purpose

Displays the contents of a file on the local file system, one page at a time.

Command Mode

exec

Syntax Description

url	URL of the file to be displayed.

Default

None

Usage Guidelines

Use the **more** command to display the contents of a file on the local file system, one page at a time.

At the end of each page, SmartEdge OS prints "--More--" to indicate the presence of more output. You can use a subset of the commands available in the UNIX **more(1)** command, such as pressing **Space** to show the next page of output, pressing **Enter** to show one additional line of output, or typing **q**, to end the display.

When referring to a file on the local file system, the URL takes the following form:

[/*device*][/*directory*]/*filename.ext*

The value for the *device* argument can be **flash**, or if a mass-storage device is installed, **md**. If you do not specify the *device* argument, the default value is the device in the current working directory. If you do not specify the *directory* argument, the default value is the current directory. Directories can be nested. The value for the *filename* argument can be up to 256 characters in length.

Examples

The following example displays the contents of the file, `/flash/redback.cfg`. At the prompt, the user ends the display by entering **q**:

```
[local]Redback>more /flash/redback.cfg

context local
!
 interface 1/1
  ip address 10.5.1.2/16
  ip router isis tag
!
```

```
 interface 2/1
  ip address 10.7.1.1/16
  ip router isis tag
--More--q
[local]Redback#
```

Related Commands

directory

pwd

pwd

Purpose

Displays the current working directory.

Command Mode

exec (10)

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **pwd** command to display the current working directory.

Examples

The following example displays the current working directory:

```
[local]Redback#pwd

/flash/config
```

Related Commands

cd
directory
mkdir

release download

release download [**modular**] *url*

Purpose

Installs an alternate release on the system.

Command Mode

exec (10)

Syntax Description

modular	Optional. Places the downloaded patch file on the active partition rather than the alternate boot system partition. Subscriber sessions will remain active while the line card Packet Processing ASIC (PPA) software is upgraded with the new patch release.
url	URL of a pre-existing configuration file. See the "Usage Guidelines" section for the format of this argument.

Default

None

Usage Guidelines

Use the **release download** command to install an alternate release on the system. Use the **modular** keyword to place the downloaded patch file on the active partition, rather than the alternate boot system partition. If there is not room on the active partition for the patch file, an informational log message is generated.

When a release is installed in the alternate boot system partition, use the **release upgrade** command (in exec mode) to reboot the system, and install the new release in the active boot system partition.

If an alternate release already exists, you are prompted for confirmation for the system to automatically erase the existing alternate image.

When referring to a file on the local file system, the *url* argument takes the following form:

[/*device*][/*directory*]/*filename***.***ext*]

The value for the *device* argument can be **flash**, or if a mass-storage device is installed, **md**. If you do not specify the *device* argument, the default value is the device in the current working directory. If you do not specify the *directory* argument, the default value is the current directory. Directories can be nested. The value for the *filename* argument can be up to 256 characters in length.

When using File Transfer Protocol (FTP) or Secured Copy Protocol (SCP) to install a configuration file from a remote server, the *url* argument takes the following form, where the *protocol* argument is **ftp** or **scp**, the *username*[**:***passwd*] construct specifies the user and an optional password, the *ip-addr* argument is the IP address of the server, and the *hostname* argument is the hostname of the server:

*protocol***://***username*[**:***passwd*]**@**{*ip-addr* | *hostname*}[//*directory*]/*filename***.***ext*

If a username is not specified, the SmartEdge router sends the username for the SmartEdge administrator account for the current logon session.

Note Use double slashes (*//directory*) if the pathname to the directory on the remote server is an absolute pathname; use a single slash (*/directory*) if it is a relative pathname (under the hierarchy of *username* account home directory).

The value for the *filename* argument can be up to 256 characters in length. You can only use the *hostname* argument if Domain Name System (DNS) is enabled with the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands (in context configuration mode); see the "DNS Configuration" chapter in the *IP Services and Security Configuration Guide* for the SmartEdge OS.

Examples

The following example installs a new release:

```
[local]Redback#release download

ftp://guest@10.13.49.100//images/REL_5_0_3/SEOS-5.0.3.tar.gz

The following "alternate" release will be erased:

Version SE800-2.4.3
Built on Mon Jan 13 10:00:05 PST 2002
Copyright (C) 1998-2002, Redback Networks Inc. All rights reserved.

Are you sure you wish to erase this release? (y/n) y

Erasing the "alternate" release...

Installing from guest@10.13.49.100//images/REL_5_0_3/SEOS-5.0.3.tar.gz
Connected to 10.13.49.100.
.
.
.
################################################################################
226 Binary Transfer complete.
36562688 bytes received in 05:30 (108.14 KB/s)
221 Goodbye.
Installation completed successfully.
```

Related Commands

release erase
release upgrade
show release

release erase

release erase

Purpose

Manually erases the alternate image on the system.

Command Mode

exec (10)

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **release erase** command to manually erase the alternate image on the system. You cannot use this command if the system is configured to use the alternate image upon reload.

Examples

The following example erases the alternate system image:

```
[local]Redback#release erase

The following "alternate" release will be erased:

Version SE800-2.4.4.0.158-Release
Built on Wed Mar  5 10:00:02 PST 2003
Copyright (C) 1998-2003, Redback Networks Inc. All rights reserved.

Are you sure you wish to erase this release? (y/n) y

Erasing the "alternate" release...
```

Related Commands

release download
release upgrade
show release

release sync

release sync

Purpose

Forces a synchronization of the files on the standby controller card with those on the active controller card.

Command Mode

exec (10)

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **release sync** command to force a synchronization of the files on the standby controller card with those on the active controller card.

Use this command when you want to ensure that a file loaded on the active controller card is duplicated on the standby controller card.

Note The synchronization process is not affected by traffic card installation and removal; the active controller, and hence the system, continues to forward traffic and detect and notify the administrator of any faults that occur while the standby controller is being synchronized (FAIL LED is blinking).

Examples

The following example forces a synchronization of the files on the standby controller card with those on the active controller card:

```
[local]Redback#release sync
```

Related Commands

None

release upgrade

release upgrade [**at** *at-time* | **in** *in-time* | **modular**]

Purpose

Upgrades the system to use the alternate installed release when reloading.

Command Mode

exec (10)

Syntax Description

at *at-time* Optional. Specified time at which to perform the release upgrade. The value for the **at** *at-time* construct is in a *yyyy***:***mm***:***dd***:***hh***:***mm*[**:***ss*] format, where *yyyy* = year, *mm* = month, *dd* = day, *hh* = hour, *mm* = minute, and [**:***ss*] is optional seconds.

in *in-time* Optional. Number of minutes to wait before performing the release upgrade. The value for the **in** *in-time* construct is in a *dd***:***hh***:***mm* format, where *dd* = day, *hh* = hour, and *mm* = minute.

modular Optional. Performs an upgrade using the patch file previously downloaded to the box. The patch file version displays during the upgrade, and the system loads and prompts for confirmation before proceeding. At the end of the installation, an informational log message is sent, indicating the success or failure of the operation.

Default

None

Usage Guidelines

Use the **release upgrade** command to upgrade the system to use the alternate installed release when reloading. The system prompts you to save the configuration file and then reloads the system.

Note Perform this procedure from the console port on the active controller card, to view the progress of the upgrade operation. Remote sessions to the system are disconnected during the reload process.

If there is a standby controller card installed, it is automatically synchronized with the active controller card.

After the upgrade is complete, press **Enter** to display the `login` prompt.

Note This command does not cause a switchover to the standby controller card in a redundant controller card configuration.

Note Subscriber sessions will remain active while the line card Packet Processing ASICs (PPA) software is upgraded with the new patch release.

Note If, at the time the upgrade is performed, the application finds that the upgrade does not succeed (for example there is not a valid release image in the alternate partition), the upgrade is aborted and a message is logged. Use the **show log** command (in exec mode) to display the stored messages.

Use the optional **at** *at-time* construct to specify the time at which to perform the release upgrade, or the **in** *in-time* construct to specify the number of minutes to wait before performing the release upgrade.

Note If the box is reloaded before the time that is specified, the **at** *at-time* or **in** *in-time* construct is not issued.

Examples

The following example configures the system to reload using the alternate installed image:

```
[local]Redback#release upgrade

The system will reboot and the following release will become active:

Version SEOS-5.0.3-Release
Built on Mon Jan  10 01:30:02 PST 2005
Copyright (C) 1998-2005, Redback Networks Inc. All rights reserved.

Are you sure you wish to continue? (y/n) y

Setting boot partition to "alternate"...

The "reload" command will reboot all cards on this system
Do you want to save the current configuration? (y/n) y
.
.
.
Configuration complete
% Startup configuration processing took: 33 seconds
```

Related Commands

release download
release erase
show log
show release

rename

rename *current-url new-url* [**-noconfirm**]

Purpose

Renames a file or directory on the local file system.

Command Mode

exec (10)

Syntax Description

current-url	Current URL of the file (or directory) that is to be renamed.
new-url	URL of the file (or directory) after renaming.
-noconfirm	Optional. Replaces an existing file (or directory) without asking for confirmation.

Default

None

Usage Guidelines

Use the **rename** command to rename a file or directory on the local file system. The *current-url* and *new-url* arguments use the following form:

[/*device*][/*directory*]/*filename*.*ext*

The value for the *device* argument can be **flash**, or if a mass-storage device is installed, **md**. If you do not specify the *device* argument, the default value is the device in the current working directory. If you do not specify the *directory* argument, the default value is the current directory. Directories can be nested. The value for the *filename* argument can be up to 256 characters in length.

This command works only for renaming files and directories on a single local file system device; that is, the URLs must be identical, except for the *filename*.*ext* argument. The command fails if the values of the *current-url* and *new-url* arguments are identical; this is the URLs are identical.

A file with the new name must not already exist; that is, the SmartEdge OS does not overwrite an existing file on the local file system without first seeking confirmation. Use the **-noconfirm** optional keyword to avoid the confirmation prompt.

Examples

The following example renames the file, `redback.bin`, to `old.bin`:

```
[local]Redback#rename /flash/redback.bin /flash/old.bin
```

Related Commands

copy
delete
directory

rmdir

rmdir *url*

Purpose

Removes a directory from the local file system.

Command Mode

exec (10)

Syntax Description

url	URL of the directory to be removed.

Default

None

Usage Guidelines

Use the **rmdir** command to remove a directory on the local file system.

When referring to a directory on the local file system, the URL takes the following form:

[/*device*][/*directory*]...[/*directory*]

The value for the *device* argument can be **flash**, or if a mass-storage device is installed, **md**. If you do not specify the *device* argument, the default value is the device in the current working directory. If you do not specify the *directory* argument, the default value is the current directory. Directories can be nested. The value for the *filename* argument can be up to 256 characters in length.

Before you remove a directory, you must remove all files from the directory using the **delete** command.

Examples

The following example removes the top-level directory, `backups`, from the flash file system:

```
[local]Redback#rmdir /flash/backups
```

Related Commands

delete
directory
mkdir

save configuration

save configuration [*url*] [**-noconfirm**]

Purpose

Saves the running configuration to a file on a remote server or the local file system.

Command Mode

exec (10)

Syntax Description

url	Optional. URL of the file to which the configuration is saved; if not specified the configuration is saved to redback.cfg file.
-noconfirm	Optional. Replaces an existing file without prompting for confirmation.

Default

Commands are saved to the default configuration file.

Usage Guidelines

Use the **save configuration** command to save the running configuration to a file on a remote server or the local file system.

Only those commands that modify the default configuration of the SmartEdge router are saved.

When saving the configuration to the local file system, the URL takes the following form:

[/*device*][/*directory*]/*filename***.***ext*

The value for the *device* argument can be **flash**, or if a mass-storage device is installed, **md**. If you do not specify the *device* argument, the default value is the device in the current working directory. If you do not specify the *directory* argument, the default value is the current directory. Directories can be nested. The value for the *filename* argument can be up to 256 characters in length.

The value for the *filename* argument can be up to 256 characters in length. If you do not specify the *filename***.***ext* argument, the configuration is saved to the redback.cfg file.

To ensure that the binary database file (/flash/redback.bin) is created correctly when saving to the redback.cfg file, enter this command without a filename, or specify redback.cfg as the filename without a device or directory. For information about these files, see the “Configuration File Management” chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

When saving the configuration to a remote server, you can use the File Transfer Protocol (FTP), Remote Copy Protocol (RCP), Secured Copy Protocol (SCP), Secured File Transfer Protocol (SFTP), or Trivial File Transfer Protocol (TFTP).

Table 3-4 describes the syntax for the *url* argument when saving the file to a remote server.

Table 3-4 Syntax for the *url* Argument in the save configuration Command

Server Protocol	URL Format
FTP, SCP, or SFTP	**ftp:**//*username*[**:***passwd*]@{*ip-addr* | *hostname*}[//*directory*]/*filename***.***ext* **scp:**//*username*[**:***passwd*]@{*ip-addr* | *hostname*}[//*directory*]/*filename***.***ext* **sftp:**//*username*[**:***passwd*]@{*ip-addr* | *hostname*}[//*directory*]/*filename***.***ext*
RCP	**rcp:**//*username*@{*ip-addr* | *hostname*}[//*directory*]/*filename***.***ext*
TFTP	**ftp:**//{*ip-addr* | *hostname*}[//*directory*]/*filename***.***ext*

You can specify the *hostname* argument only if Domain Name System (DNS) is enabled with the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands (in context configuration mode); see the "DNS Configuration" chapter in the *IP Services and Security Configuration Guide* for the SmartEdge OS.

Note Use double slashes (//) if the pathname to the directory on the remote server is an absolute pathname; use a single slash (/) if it is a relative pathname (under the hierarchy of *username* account home directory).

If you attempt to overwrite an existing file on the local file system, the system prompts you for confirmation. Use the **-noconfirm** optional keyword to replace an existing file without providing confirmation to the system. In either case, the system saves a backup of the existing file with the .bak file extension. Only a single copy of the file is saved as a backup.

Examples

The following example saves the current active system configuration to a file, `current.cfg`, on the local file system. The user is prompted to overwrite an existing file.

```
[local]Redback#save configuration /flash/current.cfg

Save to file: current.cfg
Target file exists, overwrite? y
```

The following example shows that the existing `current.cfg` file has been saved as `current.cfg.bak`:

```
[local]Redback#directory /flash

Contents of /flash
total 2590
-rw-r--r--  1 root  10000     4564 Jan 28 2005  current.cfg
-rw-r--r--  1 root  10000     3654 Jan 28 2005  current.cfg.bak
-rw-r--r--  1 root  10000     1578 Jan 28 2005  redback.cfg
```

Related Commands

show configuration

show release

show release

Purpose

Displays release and installation information for the software images currently installed on the system.

Command Mode

all modes

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show release** command to display the release and installation information for the software images currently installed on the system. The active image shows the software that is currently loaded in the system, and the alternate image shows the alternate image available on the system.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays the release and installation information for the installed software images:

```
[local]Redback>show release

Installed releases:

p02: active (will be booted after next reload)
-----------------------------------------------
Version SEOS-5.0.3-Release
Built on Mon Jan 03 10:00:01 PST 2005
Copyright (C) 1998-2005, Redback Networks Inc. All rights reserved.
```

```
p01: alternate
--------------
Version SEOS-5.0.3-Release
Built on Mon Jan 18 10:00:01 PDT 2005
Copyright (C) 1998-2005, Redback Networks Inc. All rights reserved.
```

Related Commands

context
release download
release erase
release upgrade

show version

show version

Purpose

Displays the current version of the software running on the system.

Command Mode

all modes

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show version** command to display the current version of the software running on the system.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context.For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays output from the **show version** command:

```
[local]Redback>show version

Redback Networks SmartEdge OS Version SEOS-5.0.3-Release
Built by sysbuild@@lx-lsf159Fri Jan 28 01:30:02 PST 2005
Copyright (C) 1998-2005, Redback Networks Inc. All rights reserved.
System Bootstrap version is PowerPC,1.0b1267
Installed minikernel version is 20
Router Up Time -   22 hours 1 minute 18 secs
```

Related Commands

context

upgrade bootrom

upgrade bootrom {**ftp:** | **scp:** | **/md**} *url* [**no-reload**]

Purpose

Upgrades the boot loader image in the EEPROM on the active controller card in a working system and reloads it.

Command Mode

exec

Syntax Description

ftp:	Specifies the File Transfer Protocol (FTP) as the protocol to use when transferring the file from a remote server.
scp:	Specifies the Secured Copy Protocol (SCP) as the protocol to use when transferring the file from a remote server.
/md	Specifies the /md directory on the mass-storage device on the active controller card as the location for the file.
url	URL for the file that contains the boot loader image.
no-reload	Optional. Cancels the reload when upgrading the system. The upgrade does not take place until the reload occurs at a later time.

Default

None

Usage Guidelines

Use the **upgrade bootrom** command to upgrade the boot loader image in the EEPROM on the active controller card in a working system and reload it.

Use this command on a working system; if the system is not working, you must use the boot loader interface to upgrade the boot loader image. The procedure is described in the "Upgrade Operations" section in Appendix A, "Boot Loader Operations."

Use the **show version** command (in exec mode) to display the version of the boot loader that is currently installed. In the display, the boot loader is referred to as the system bootstrap. Contact your local technical support representative to determine if the boot loader that is currently installed needs to be upgraded. Your representative can also help you access the URL to use to download the boot loader image file.

Note The boot loader image is also referred to as the bootrom.

When referring to a file on a remote server, the syntax for the *url* argument is:

//username[**:***passwd*]**@**{*ip-addr* | *hostname*}[*//directory*]*/filename***.***ext*

Note Use double slashes (*//directory*) if the pathname to the directory on the remote server is an absolute pathname; use a single slash (*/directory*) if it is a relative pathname (under the hierarchy of *username* account home directory).

When referring to a file on the /md directory, the URL takes the following form:

[*/directory*]*/filename.ext*

Directories can be nested. The value for the *filename* argument can be up to 256 characters in length.

Note If you find a file in the /flash directory that appears to be a boot loader image file, it might be the result of upgrading boot loader using the procedure that is described in Appendix A "Boot Loader Operations." Do not use this file to upgrade the boot loader using the **upgrade bootrom** command.

When you specify the **ftp:** or **scp:** keywords, this command downloads the requested file to the /flash directory, upgrades the bootrom, and then deletes the file.

When you specify the /md keyword, this command copies the file to the /flash directory from the /md directory, upgrades the bootrom, and then deletes the file on the /flash directory; the file on the /md directory is not altered. You must have first downloaded the file to the /md directory using the **copy** command (in exec mode).

Note If you inadvertently copied the file to the /flash directory, you can move it to the /md directory, using the **copy** and **delete** commands (in exec mode).

If there is a standby controller card installed in the system, this command either synchronizes it with the active controller card automatically or, if you are upgrading a boot loader with version 1205 or earlier, asks you to perform the synchronization manually. If manual synchronization is needed, the following message is printed:

```
% It appears that this is an upgrade from an old bootrom,
% in order to complete the upgrade it will be needed to run
% the command "reload standby" after this card finishes
% the upgrade and returns to the CLI
```

In this case, enter the **reload standby** command (in exec mode) after the upgrade of the boot loader is complete, and the command-line interface (CLI) prompt displays.

To temporarily defer the automatic reload of the system to process the upgrade, use the optional **no-reload** keyword. The optional **no-reload** keyword can perform more than one upgrade during one reload operation to minimize impact on network traffic. For example, you can issue the **upgrade bootrom** and **upgrade minikernel** command (in exec mode), with the optional **no-reload** keyword, followed by a **release upgrade** command (in exec mode), to upgrade to an image in the alternate partition. Thus, with one reload of the system, three components are upgraded.

Note When using the upgrade command with the optional **no-reload** keyword, the actual upgrade of the bootrom or minikernel does not happen until the system reloads at a later time.

Note If after issuing the **upgrade bootrom** command, there is a synchronizing operation between Cross-Connect Route Processor (XCRP) Controller cards in the system, the temporary upgrade files may be overwritten and the upgrade operation may not have the intended effects when the system reloads. To minimize this risk, use the optional **no-reload** keyword on a synchronized system, then reload the system after issuing the **upgrade bootrom** command (in exec mode), as soon as possible.

You can also use the **show redundancy** command (in any mode), to view the status of the synchronization state before you use the **upgrade bootrom** command. For more information on the **show redundancy** command (in any mode), see the "Hardware Operations" chapter in the *Ports, Circuits, and Tunnels Operations Guide* for the SmartEdge OS.

Examples

The following example displays the current version of the boot loader and then upgrades the boot loader image in the EEPROM on the active controller card. In this example, the current version is `0b1267`. The FTP is used to download the file from a remote server; the controller card is then reloaded. Interactive responses are shown in bold.

```
[local]Redback#show version

Redback Networks SmartEdge OS Version SE800-5.0.3-Release
Built by sysbuild@@lx-lsf27 Mon Jan 03 10:00:01 PDT 2005
Copyright (C) 1998-2005, Redback Networks Inc. All rights reserved.
System Bootstrap version is PowerPC,1.0b1187

[local]Redback#upgrade bootrom ftp://admin@10.10.1.2//bootroms/of1267.bin

This operation will cause the box to reload, do you want to continue?y
copying from ftp://admin@10.10.1.2//bootroms/1.0b1267.bin to local:/flash/of.bin...
Connected to 10.10.1.2.
.
.
.
**********************************
684 KB  724.97 KB/s    00:00 ETA
Nov 9 12:52:16: %DLM-6-INFO: Standby xcrp's /flash may not be in sync
226 File send OK.
700437 bytes received in 00:01 (682.20 KB/s)
221 Goodbye.
.
.

Nov 15 11:49:34: %ALAPI-6-INFO: XCRP in slot 7, will now reload

.
.
.
rebooting
.
.
.
```

.

The following example displays the output of the **upgrade bootrom** command (in exec mode), using the optional **no-reload** keyword:

```
[local]Redback#upgrade bootrom /md/of1267.bin no-reload

copying from md:/md/of1267.bin to local:/flash/of.bin...
```

Files are copied over, but the boot loader image is not reloaded.

Related Commands

copy
show version
upgrade minikernel

upgrade minikernel

upgrade minikernel {**ftp:** | **scp:** | **/md**} *url* [**no-reload**]

Purpose

Upgrades the minikernel image in the EEPROM on the active controller card in a working system and reloads it.

Command Mode

exec

Syntax Description

ftp:	Specifies the File Transfer Protocol (FTP) as the protocol to use when transferring the file from a remote server.
scp:	Specifies the Secured Copy Protocol (SCP) as the protocol to use when transferring the file from a remote server.
/md	Specifies the /md directory on the mass-storage device on the active controller card as the location for the file.
url	URL for the file that contains the minikernel image.
no-reload	Optional. Cancels the reload when upgrading the minikernel image. The upgrade does not take place until the reload occurs at a later time.

Default

None

Usage Guidelines

Use the **upgrade minikernel** command to upgrade the minikernel image in the EEPROM on the active controller card in a working system and reload it.

Use this command on a working system; if the system is not working, you must use the boot loader interface to upgrade the minikernel image as described in the "Upgrade Operations" section in Appendix A, "Boot Loader Operations."

When upgrading the minikernel image on a system that has a boot loader image file installed with version of 1205 or earlier, you must first upgrade the boot loader image, using the **upgrade bootrom** command (in exec mode), before you can upgrade the minikernel image.

Contact your local technical support representative to determine if the minikernel image that is currently installed needs to be upgraded. Your representative can also help you access the URL to use to download the minikernel image file.

When referring to a file on a remote server, the syntax for the *url* argument is:

//username[**:***passwd*]**@**{*ip-addr* | *hostname*}[*//directory*]*/filename***.***ext*

Note Use double slashes (//) if the pathname to the directory on the remote server is an absolute pathname; use a single slash (/) if it is a relative pathname (under the hierarchy of *username* account home directory).

When referring to a file on the /md directory, the syntax for the *url* argument is:

[/*directory*]/*filename.ext*

Directories can be nested. The value for the *filename* argument can be up to 256 characters in length.

Note If you find a file in the /flash directory that appears to be a minikernel image file, it might be the result of upgrading the minikernel image using the procedure that is described in Appendix A, "Boot Loader Operations." Do not use this file to upgrade the minikernel image using the **upgrade minikernel** command.

When you specify the **ftp:** or **scp:** keyword, this command downloads the requested file to the /flash directory, upgrades the minikernel image, and then deletes the file.

When you specify the /md keyword, this command copies the file to the /flash directory from the /md directory, upgrades the minikernel image, and then deletes the file on the /flash directory; the file on the /md directory is not altered. You must have first downloaded the file to the /md directory using the **copy** command (in exec mode).

Note If you inadvertently copied the file to the /flash directory, you can move it to the /md directory, using the **copy** and **delete** commands (in exec mode).

If a standby controller card is installed on the system, it is synchronized automatically with the active controller card with this command, unless you are running a boot loader version 1205 or earlier. In that case, you must synchronize the standby controller manually, using the **reload standby** command (in exec mode), after the upgrade of the minikernel image is completed and the command-line interface (CLI) prompt displays.

To temporarily defer the automatic reload of the system to process the upgrade, use the optional **no-reload** keyword. The optional **no-reload** keyword can perform more than one upgrade during one reload operation to minimize impact on network traffic. For example, you can issue the **upgrade bootrom** and **upgrade minikernel** command (in exec mode), with the optional **no-reload** keyword, followed by a **release upgrade** command (in exec mode), to upgrade to an image in the alternate partition. Thus, with one reload of the system, three components are upgraded.

Note When using the upgrade command with the optional **no-reload** keyword, the actual upgrade of the bootrom or minikernel image does not happen until the system reloads at a later time.

Note If after issuing the **upgrade minikernel** command, there is a synchronizing operation between Cross-Connect Route Processor (XCRP) Controller cards in the system, the temporary upgrade files may be overwritten and the upgrade operation may not have the intended effects when the system reloads. To minimize this risk, use the optional **no-reload** keyword on a synchronized system, then reload the system after issuing the **upgrade minikernel** command (in exec mode), as soon as possible.

You can also use the **show redundancy** command (in any mode), to view the status of the synchronization state before you use the **upgrade minikernel** command. For more information on the **show redundancy** command (in any mode), see the "Hardware Operations" chapter in the *Ports, Circuits, and Tunnels Operations Guide* for the SmartEdge OS.

Examples

The following example upgrades the minikernel image in the EEPROM on the active controller card using the FTP to download the file from a remote server; the controller card is then reloaded. Interactive responses are shown in bold; the `save the current configuration` message displays only if the current configuration appears to have been modified and not saved.

```
[local]Redback#upgrade minikernel

ftp://smartedge@10.10.2.1//minikernels/netbsd.min.v20.bz2.bin

This operation will cause the box to reload, do you want to continue?y
Do you want to save the current configuration? (y/n) y
copying from ftp://smartedge@10.0.2.1//minikernels/netbsd.min.v20.bz2.bin to
local:/flash/netbsd.min.bz2...
Connected to 10.0.2.1.
.
.
.
**********************************| 951 KB 1.10 MB/s
00:00 ETA
226 Transfer complete.
974310 bytes received in 00:00 (1.10 MB/s)
221 Goodbye.
Nov 15 15:37:07: %DLM-6-INFO: Standby xcrp's /flash may not be in sync
[local]Redback#Sep 25 15:37:10: %ALAPI-6-INFO: XCRP in slot 7, will now reload
.
.
.
Updating minikernel...
Erasing flash...done
Writing minikernel [974310 bytes]...done
Verifying minikernel...done
Õ
[0]Booting(2)....
Enabling L1/L2 Caches...
Reset Cause:
SCC Watchdog Reset (PPC Subsystem ONLY)
ISA reset (PPC Subsystem ONLY)
.
.
.
Welcome to SmartFirmware(tm) for Redback PowerPC Copyright (c) 1999-2005
by Redback Networks, Inc. version of1267
SmartFirmware(tm) Copyright 1996-2005 by CodeGen, Inc.
All Rights Reserved.
Auto-boot in 0 seconds - press SE* to abort, ENTER to boot:
```

The following example displays the output of the **upgrade minikernel** command using the optional **no-reload** keyword:

```
[local]Redback#upgrade minikernel /md/netbsd.min.v21.bz2 no-reload

copying from md:/md/netbsd.min.v21.bz2 to local:/flash/netbsd.min.bz2...
```

Files are copied over, but the boot loader image is not reloaded.

Related Commands

copy
upgrade bootrom

Part 3

Basic System Operations

This part describes the SmartEdge® OS operations functions, tasks, and commands used to monitor, administer, and troubleshoot sessions; system clock and services; contexts, interfaces, and subscribers, and monitor and test system-wide functions and features, such as software processes, and so on.

This part consists of the following chapters:

- Chapter 4, “Session Operations”
- Chapter 5, “System Operations”
- Chapter 6, “Context, Interface, and Subscriber Operations”
- Chapter 7, “Software Operations”

Session Operations

This chapter describes the tasks and commands used to monitor, administer, and troubleshoot administrator sessions through the SmartEdge® OS.

For information about the commands used to configure these features, see the "System Access Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

Note In the following descriptions, the term, controller card, applies to the Cross-Connect Route Processor (XCRP) or the XCRP Version 3 (XCRP3) Controller card, unless otherwise noted.

This chapter includes the following sections:

- Operations Tasks
- Command Descriptions

Operations Tasks

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 Descriptions" section.

To monitor, administer, and troubleshoot administrator sessions, perform the tasks described in Table 4-1; enter all commands in exec mode.

Table 4-1 Session Operations Tasks

Task	Command
Enables the generation of debug messages for Secure Shell (SSH).	**debug ssh**
Enables the generation of debug messages for communications with another administrator during active Telnet or SSH sessions on the same SmartEdge router.	**debug talk**
Displays the current privilege level for the current exec session.	**show privilege**
Displays information about configured Secure Shell (SSH) attributes and the number of current connections.	**show ssh-attributes**
Establishes a remote session from the SmartEdge system to a host using SSH.	**ssh**
Generates a new Secure Shell (SSH) key on the system.	**ssh server-keygen**

Table 4-1 Session Operations Tasks *(continued)*

Task	Command
Enables you to establish communications with another administrator during active Telnet or Secure Shell (SSH) sessions on the same SmartEdge router.	**talk**
Establishes a remote Telnet session from the SmartEdge router to a host using Telnet.	**telnet**
Sets the terminal length for the current session.	**terminal length**
Displays the event log output.	**terminal monitor**
Sets the terminal width for the current session.	**terminal width**

Command Descriptions

This section describes the syntax and usage guidelines for the commands used to monitor, troubleshoot, administer, and manage sessions. The commands are presented in alphabetical order.

debug ssh
debug talk
show privilege
show ssh-attributes
show terminal
ssh
ssh server-keygen
talk
telnet
terminal length
terminal monitor
terminal width

debug ssh

debug [**boot** {**active** | **standby**} | **switchover**] **ssh** {**all** | **ssh-general** | **sshd-detail** | **sshd-general**}

no debug [**boot** {**active** | **standby**} | **switchover**] **ssh** {**all** | **ssh-general** | **sshd-detail** | **sshd-general**}

Purpose

Enables the generation of debug messages for Secure Shell (SSH).

Command Mode

exec

Syntax Description

boot	Optional. Enables the generation of debug messages during a system reload.
active	Enables the generation of debug messages for the active controller card.
standby	Enables the generation of debug messages for the standby controller card.
switchover	Optional. Enables the generation of debug messages during a switchover from the active to the standby controller.
all	Generates all debug messages related to SSH.
ssh-general	Generates general debug messages related to SSH.
sshd-detail	Generates detailed daemon (server) debug messages related to SSH.
sshd-general	Generates general daemon (server) debug messages related to SSH.

Default

The generation of debug messages for SSH is disabled.

Usage Guidelines

Use the **debug ssh** command to generate debug messages for the SSH.

Caution Risk of performance loss. Enabling the generation of debug messages can severely affect system performance. To reduce the risk, exercise caution when enabling the generation of any debug messages on a production system.

Use the **boot active** or **boot standby** construct to enable debugging messages during a system reload for the active or standby controller card, respectively.

Use the **switchover** keyword to enable debugging messages while the system is switching from the active to the standby controller card.

To store messages in the system log buffer, use the **logging debug** command (in global configuration mode). Use the **show log** command (in exec mode) to display these stored messages.

To display messages in real time, use the **logging console** command (in context configuration mode) if you are connected to the system through the console port. Or, use the **terminal monitor** command (in exec mode) if you are connected to the system through a Telnet or Secure Shell (SSH) session.

Note For more information about the **logging** commands, see the "Logging Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS. For information about the **terminal monitor** command, see the description of the **terminal monitor** command in this guide.

Use the **no** form of this command to disable the generation of debug messages for SSH.

Examples

The following example enables the generation of detailed debug messages for SSH:

```
[local]Redback#debug sshd-detail
```

Related Commands

show log
ssh
terminal monitor

debug talk

debug [**boot** {**active** | **standby**} | **switchover**] **talk**

no debug [**boot** {**active** | **standby**} | **switchover**] **talk**

Purpose

Enables the generation of debug messages for communications with another administrator during active Telnet or Secure Shell (SSH) sessions on the same SmartEdge router.

Command Mode

exec

Syntax Description

boot	Optional. Enables the generation of debug messages during a system reload.
active	Enables the generation of debug messages for the active controller card.
standby	Enables the generation of debug messages for the standby controller card.
switchover	Optional. Enables the generation of debug messages during a switchover from the active to the standby controller.

Default

The generation of debug messages for talk is disabled.

Usage Guidelines

Use the **debug talk** command to enable the generation of debug messages for communications with another administrator during active Telnet or SSH sessions on the same SmartEdge router.

Caution Risk of performance loss. Enabling the generation of debug messages can severely affect system performance. To reduce the risk, exercise caution when enabling the generation of any debug messages on a production system.

Use the **boot active** or **boot standby** construct to enable debugging messages during a system reload for the active or standby controller card, respectively.

Use the **switchover** keyword to enable debugging messages while the system is switching from the active to the standby controller card.

To store messages in the system log buffer, use the **logging debug** command (in global configuration mode). Use the **show log** command (in exec mode) to display these stored messages.

To display messages in real time, use the **logging console** command (in context configuration mode) if you are connected to the system through the console port. Or, use the **terminal monitor** command (in exec mode) if you are connected to the system through a Telnet or SSH session.

Note For more information about the **logging** commands and the **terminal monitor** command, see the "Logging Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS, and in Chapter 4, "Session Operations," respectively.

Use the **no** form of this command to disable the generation of debug messages for SSH.

Examples

The following example enables the generation of detailed debug messages for talk:

```
[local]Redback#debug talk
```

Related Commands

show log
talk

show privilege

show privilege

Purpose

Displays the current privilege level for the current exec session.

Command Mode

all modes

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show privilege** command to display the current (administrator) privilege level for the current exec session.

Note To display the assigned privilege for a command, use the **show configuration** command (in any mode).

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct preceding the **show** command to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays output from the **show privilege** command:

```
[local]Redback>show privilege

Current privilege level is 6
```

Related Commands

context

show ssh-attributes

show ssh-attributes

Purpose

Displays information about configured Secure Shell (SSH) attributes and the number of current connections.

Command Mode

all modes

Syntax Description

This command has no arguments or keywords.

Default

None

Usage Guidelines

Use the **show ssh-attributes** command to display information about configured SSH attributes and the number of current connections.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct preceding the **show** command to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays SSH attributes:

```
[local]Redback>show ssh-attributes

               ssh attributes
               --------------
               start-drop      50      (connections)
               rate-drop       100      (percentage)
               full-drop       50      (connections)
               current         0       (connections)
```

Related Commands

context
talk

show terminal

show terminal

Purpose

Displays terminal settings for the current session.

Command Mode

all modes

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show terminal** command to display terminal settings for the current session.

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering show command output, see Chapter 2, “Using the CLI.”

Examples

The following example displays the terminal settings for the current session:

```
[local]Redback>show terminal

terminal name    = /dev/ttyp0
terminal width   = 98
terminal length  = 50
terminal monitor = disabled
```

Related Commands

terminal length
terminal monitor
terminal width

ssh

ssh {*ip-addr* | *hostname*} [**cipher** *name*] [*admin-name*] [**v2**]

Purpose

Establishes a Secure Shell (SSH) session from the SmartEdge router to a host using SSH.

Command Mode

exec

Syntax Description

ip-addr	IP address of the host with which to establish the Telnet session.
hostname	Hostname of the host with which to establish the Telnet session. The Domain Name System (DNS) must be enabled to use the *hostname* argument.
cipher *name*	Optional. Cipher to use for encrypting the session according to one of the keywords listed in Table 4-2.
admin-name	Optional. Name of administrator to log on to a remote system.
v2	Optional. Forces the use of SSH Version 2.

Default

The session uses SSH Version 1 with Triple Data Encryption Standard (3DES) encryption.

Usage Guidelines

Use the **ssh** command to establish a SSH session from the SmartEdge router to a host using SSH. You can only use the *hostname* argument if DNS is enabled using the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands (in context configuration mode). For more information about these commands, see the "DNS Configuration" chapter in the *IP Services and Security Configuration Guide* for the SmartEdge OS.

Table 4-2 lists the keywords for the optional **cipher** *name* construct.

Table 4-2 Cipher Names

Keyword	Description
3des	Specifies 3DES encryption. Valid for SSH Version 1; this is the default value.
3des-cbc	Specifies 3DES-CBC encryption. Valid for SSH Version 2.
aes128-cbc	Specifies Advanced Encryption Standard (AES) 128-CBS encryption. Valid for SSH Version 2.
aes192-cbc	Specifies AES 192-CBC encryption. Valid for SSH Version 2.
aes256-cbc	Specifies AES 256-CBC encryption. Valid for SSH Version 2.
arcfour	Specifies ArcFour encryption. Valid for SSH Version 2.

Table 4-2 Cipher Names *(continued)*

Keyword	Description
blowfish	Specifies Blowfish encryption. Valid for SSH Version 1.
blowfish-cbc	Specifies Blowfish Cipher Block Chaining (CBC) encryption Valid for SSH Version 2.
cast128-cbc	Specifies CAST128-CBC encryption. Valid for SSH Version 2.
des	Specifies Data Encryption Standard (DES) encryption. Valid for SSH Version 1.
rijndael128-cbc	Specifies Rijndael128-CBC encryption. Valid for SSH Version 2.
rijndael192-cbc	Specifies Rijndael192-CBC encryption. Valid for SSH Version 2.
rijndael256-cbc	Specifies Rijndael256-CBC encryption. Valid for SSH Version 2.
rijndael-cbc@lysator.liu.se	Specifies Rijndael-CBC@lysator.liu.se encryption. Valid for SSH Version 2.

Examples

The following example establishes an SSH session with a host at IP address, `192.168.190.32`:

```
[local]Redback>ssh 192.168.190.32
```

Related Commands

None

ssh server-keygen

ssh server-keygen

Purpose

Generates a new Secure Shell (SSH) key on the system.

Command Mode

exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **ssh server-keygen** command to generate a new SSH key on the system. If a key already exists, the existing key is replaced.

Examples

The following example enables SSH on the system:

```
[local]Redback>ssh server-keygen
```

Related Commands

debug ssh
show ssh-attributes
talk

talk

talk *admin-name*[**@***ctx-name*] [*tty-name*]

Purpose

Enables you to establish communications with another administrator during active Telnet or Secure Shell (SSH) sessions on the same SmartEdge router.

Command Mode

exec

Syntax Description

admin-name	Name of the administrator with whom you want to establish communications.
ctx-name	Optional. Name of the context in which the administrator account is configured. Required only if the administrator you want to talk to is in a context that is different from the one in which your administrator account is configured.
tty-name	Optional. Name of the Teletypewriter (TTY) for a particular administrator session. Use this option to talk to an administrator who is logged on more than once.

Default

Disabled. If the *ctx-name* argument is not entered, the system assumes the “local” context.

Usage Guidelines

Use the **talk** command to establish communications with other active administrators during active Telnet or Secure Shell (SSH) sessions on the same SmartEdge router. This visual communication program copies lines from one administrator’s terminal to that of another administrator.

When communication is established, two administrators can type simultaneously, with their output appearing in separate windows. To exit, press **Ctrl**+**x**+**c**. The system restores the terminal to its previous state.

Examples

The following example displays a sample message that indicates the `admin1` administrator is contacting you through the talk program:

```
Message from Redback Talk Daemon@Redback at 5:50 ...
"admin1" wants to talk to you, respond with: talk admin1@local ttyp0
```

Related Commands

show administrators

telnet

telnet {*ip-addr* | *hostname*} [*port*]

Purpose

Establishes a remote Telnet session from the SmartEdge router to a host.

Command Mode

exec

Syntax Description

ip-addr	IP address of the host with which to establish the Telnet session.
hostname	Name of the host with which to establish the Telnet session. The Domain Name System (DNS) must be enabled to use the *hostname* argument.
port	Optional. Transmission Control Protocol (TCP) port used to communicate with the host. The range of values is 1 to 65,536; the default value is 23.

Default

None

Usage Guidelines

Use the **telnet** command to establish a Telnet session from the SmartEdge router to a host.

Note By default, Telnet service is disabled in all non-local contexts. Use the **service** command (in context configuration mode) to enable it for the context.

You can only use the *hostname* argument if DNS is enabled with the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands (in context configuration mode). For more information about these commands, see the "DNS Configuration" chapter in the *IP Services and Security Configuration Guide* for the SmartEdge OS.

Use the *port* argument to specify a port other than the default TCP port. Ensure that the port on the remote host is activated for Telnet.

Examples

The following example establishes a Telnet session with a host at IP address, `192.168.190.32`:

```
[local]Redback>telnet 192.168.190.32
```

The following example establishes a Telnet session to a host at IP address, `192.168.190.32`, using port `2222`:

```
[local]Redback>telnet 192.168.190.32 2222
```

Related Commands

None

terminal length

terminal length *length*

default terminal length

Purpose

Sets the terminal length to be used for the administrator's terminal for the duration of the current exec session.

Command Mode

exec

Syntax Description

length	Number of lines to be used for the terminal length. The range of values is 0 to 512; the default value is 24.

Default

The default terminal length is 24 lines.

Usage Guidelines

Use the **terminal length** command to set the length in terminal lines for an exec session. Upon exit of the exec session, the value is reset to the default length of 24 lines. Setting the terminal length to 0 disables auto-more processing.

Use the **default** form of this command to return the terminal length to the default value.

Examples

The following command sets the session terminal length to `30` lines:

```
[local]Redback>terminal length 30
```

Related Commands

terminal width

terminal monitor

terminal monitor

no terminal monitor

Purpose

Enables the display of system events on a remote (Telnet or Secure Shell [SSH]) session continuously as they are logged.

Command Mode

exec

Syntax Description

This command has no keywords or arguments.

Default

Events are not logged to administrator terminals.

Usage Guidelines

Use the **terminal monitor** command to enable the display of events on the current terminal. This command can be useful for viewing the Event Log output while connected to a system by Telnet or SSH, rather than working on the console.

Use the **no** form of this command to disable terminal monitoring.

Examples

The following example enables the display of logged events on the current terminal while connected using Telnet:

```
[local]Redback>terminal monitor
```

Related Commands

show log

terminal width

terminal width *width*

default terminal width

Purpose

Sets the terminal width in characters to be used for the administrator's terminal for the duration of the current exec session.

Command Mode

exec

Syntax Description

width	Preferred terminal width setting in characters. The range of values is 5 to 65,536; the default value is 80.

Default

The default terminal width is 80 characters.

Usage Guidelines

Use the **terminal width** command to set the width in characters of the terminal for an exec session. Upon exit from the this session, the value is reset to the default width of 80 characters.

Use the **default** form of this command to change the terminal width to the default value.

Examples

The following command changes the session terminal width to `70` characters:

```
[local]Redback>terminal width 70
```

Related Commands

terminal length

System Operations

This chapter describes the tasks and commands used to set the system clock and monitor clock, command-line interface (CLI), and services in the SmartEdge® OS.

For information about the commands used to configure these features, see the "Basic System Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

Note In the following descriptions, the term, controller card, applies to the Cross-Connect Route Processor (XCRP) or the XCRP Version 3 (XCRP3) Controller card, unless otherwise noted.

This chapter includes the following sections:

- Operations Tasks
- Command Descriptions

Operations Tasks

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 Descriptions" section.

Caution Risk of performance loss. Enabling the generation of debug messages can severely affect system performance. To reduce the risk, exercise caution when enabling the generation of any debug messages on a production system.

To monitor and administer the system clock, CLI, and services, perform the tasks described in Table 5-1; enter all commands in exec mode.

Table 5-1 Clock, CLI, and Services Operations Tasks

Task	Command
Sets the time on the system clock.	**clock set**
Displays a list of command aliases defined on the system.	**show alias**
Displays the current system time-of-day in local time.	**show clock**
Displays the clock-source information on the system.	**show clock-source**

Table 5-1 Clock, CLI, and Services Operations Tasks *(continued)*

Task	Command
Displays a list of software licenses and their configuration status.	**show licenses**
Displays a list of macros defined on the system.	**show macro**
Displays enabled and disabled services.	**show service**

Command Descriptions

This section describes the syntax and usage guidelines for the commands used to monitor clock, command-line interface (CLI), and services in the SmartEdge OS. The commands are presented in alphabetical order.

clock set
show alias
show clock
show clock-source
show licenses
show macro
show service

clock set

clock set *yyyy*:*mm*:*dd*:*hh*:*mm*[:*ss*]

Purpose

Sets the time on the system clock.

Command Mode

exec (10)

Syntax Description

yyyy:*mm*:*dd*:*hh*:*mm*[:*ss*]	Year, month, day, hour, minutes, and optionally, seconds. The hour is expressed in a 24-hour format; for example, 6:00 p.m. is 18:00.

Default

None

Usage Guidelines

Use the **clock set** command to set the time on the system clock. The time is saved in a hardware real-time clock. This clock is used for all system timestamps, such as log messages.

To configure the system clock, enter the **system clock-source**, **system clock-source external**, **system clock-source timing-type**, **system clock summer-time**, and **system clock timezone** commands (in global configuration mode). These commands are described in the "Basic System Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

Note The setting of the system clock is not preserved across system reloads.

Examples

The following example sets the clock to `12:01` p.m. on `Jun 28, 2005`:

```
[local]Redback#clock set 2005:06:28:12:01
```

Related Commands

show clock

show alias

show alias [**inherit** | *mode*]

Purpose

Displays a list of command aliases defined on the system.

Command Mode

all modes

Syntax Description

inherit	Optional. Displays the aliases in all modes.
mode	Optional. Command mode in which the alias applies.

Default

Displays all aliases defined on the system.

Usage Guidelines

Use the **show alias** command to display a list of the command aliases defined on the system.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct preceding the **show** command to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays output from the **show alias** command:

```
[local]Redback>show alias

Alias          Mode             Command
spc            all              show port counters
users          exec             show users show clock
```

Related Commands

context
show macro

show clock

show clock [**universal**]

Purpose

Displays the current system time-of-day in local time.

Command Mode

all modes

Syntax Description

universal	Optional. Displays the time in Greenwich Meridian Time (GMT), which is also known as Universal Coordinated Time (UTC).

Default

Displays time in local time.

Usage Guidelines

Use the **show clock** command to display the current system time-of-day (including time zone) in local time. The time displayed is based on configuration information provided using the **clock set** command (in exec mode) and the **system clock timezone** command (in global configuration mode). If no time zone is configured as the local time zone, the system uses GMT as the default time zone. If a local time zone is configured, you can also display GMT using the optional **universal** keyword.

Note The **system clock timezone** command is described in the "Basic System Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays output from the **show clock** command:

```
[local]Redback>show clock

Wed Jun 29 06:29:22 2005 PST

[local]Redback>show clock universal

Wed Jun 29 14:38:19 2005 GMT
```

Related Commands

clock set
context
show clock-source

show clock-source

show clock-source

Purpose

Displays clock source information on the system.

Command Mode

all modes

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show clock-source** command to display clock source information on the system. Table 5-2 lists the fields that are displayed by this command along with their possible values and descriptions.

Table 5-2 Field Descriptions for the show clock-source Command

Field	Value/Description
Timing Type	• sonet—Configured value for the XCRP3 Controller card or the T1 BITS version of the XCRP Controller card. • sdh—Configured value for the XCRP3 Controller card or the E1 SSU version of the XCRP Controller card.
Current clock source	Configured input timing reference for the clock: • external—Input timing reference is from external equipment. • internal—Input timing reference is the Stratum 3 oscillator. • line—Input timing reference is the receive signal from a port on an installed optical traffic card.
Current PLL State	Current state of the Phase Locked Loop (PLL) clock on the controller card: • Free Run—No input timing reference is supplied to the PLL; its output signal is controlled internally. • Holdover—No input timing reference is supplied to the PLL; its output signal is controlled by data gathered from the last time the PLL was in Locked mode. • Locked—The PLL output signal is phase-locked to its input timing reference. • Unlocked—The PLL is attempting to lock the phase of its output signal to its input timing reference.
External primary, secondary	• YES—External clock source configured as the input timing reference. • NO—No external clock source configured.

Table 5-2 Field Descriptions for the show clock-source Command *(continued)*

Field	Value/Description
Line primary, secondary	• NO—No optical port configured as the input timing reference. • *slot*/*port*—Slot and port of the optical traffic card configured as the input timing reference.
Frame Format Rx Primary, Secondary	Configured framing for the external interface: • crc4—E1 interface. • esf—DS-1 interface. • no-crc4—E1 interface. • sf—DS-1 interface.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays the clock source on a system:

```
[local]Redback>show clock-source

Timing Type               : sonet
Current clock source      : internal
Current PLL State         : Free Run (internal clock)
Configured clock sources:
External                  : primary                  : NO
External                  : secondary                : NO
Line                      : primary (slot/port)      : NO
Line                      : secondary (slot/port)    : NO
Interface Information:
                          Primary                    Secondary
Frame Format Rx           sf                         sf
```

Related Commands

context
show clock

show licenses

show licenses [**all**]

Purpose

Displays a list of software licenses and their configuration status.

Command Mode

all modes

Syntax Description

all Optional. Displays the status of all licenses.

Default

Displays only configured licenses.

Usage Guidelines

Use the **show licenses** command to display a list of software licenses and their configuration status.

Examples

The following example displays configured software licenses:

```
[local]Redback>show licenses

 Software Feature            License Configured
--------------------------    ------------------
l2tp all                             YES
subscriber active 8000               YES

 Total active subscriber license configured 8000
```

The following example displays all software licenses and their configuration status:

```
[local]Redback>show licenses all

 Software Feature            License Configured
--------------------------    ------------------
subscriber dynamic-service           NO
l2tp all                             YES
mpls                                 NO
subscriber high-availibility         NO
subscriber active 8000               YES
subscriber bandwidth                 NO

 Total active subscriber license configured 8000
```

Related Commands

None

show macro

show macro [**command**]

Purpose

Displays a list of command macros defined on the system.

Command Mode

all modes

Syntax Description

command Display the commands in the macros.

Default

Macros are listed without their commands.

Usage Guidelines

Use the **show macro** command to display a list of the command macros defined on the system. Macros are also displayed when you use the online help; in this case, the macro name is indicated by the asterisk (*) character preceding it.

Use the **command** keyword to display the commands in each macro.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays the macros defined on the system:

```
[local]Redback>show macro

Macro           Mode
show-all-port   inherit
show-alot       inherit
```

Related Commands

context
show alias

show service

show service

Purpose

Displays enabled and disabled services.

Command Mode

all modes

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show service** command to display enabled and disabled services.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays the output from the **show service** command:

```
[local]Redback>show service

Context Services:
         multiple-contexts      enabled
         card-auto-reload       enabled
         console-break          disabled
         vxworks-log-to-screen  enabled
         upload-coredump        disabled
         crash-dump-dram        disabled
         auto-system-recovery   disabled
```

Related Commands

context

Context, Interface, and Subscriber Operations

This chapter describes the tasks and commands used to monitor, administer, and troubleshoot contexts, interfaces, and subscribers in the SmartEdge® OS.

For information about the commands used to configure these features, see the "Context Configuration," "Interface Configuration," and "Subscriber Configuration" chapters in the *Basic System Configuration Guide* for the SmartEdge OS.

Note When IP Version 6 (IPv6) addresses are not referenced or explicitly specified, the term, IP address, can refer generally to IP Version 4 (IPv4) addresses, IPv6 addresses, or IP addressing. In instances where IPv6 addresses are referenced or explicitly specified, the term, IP address, refers only to IPv4 addresses. For a description of IPv6 addressing and the types of IPv6 addresses, see RFC 3513, *Internet Protocol Version 6 (IPv6) Addressing Architecture*.

IPv6 is a new version of the Internet Protocol, designed as the successor to IP Version 4 (IPv4). IPv6 is fully described in RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*. The changes from IPv4 to IPv6 include:

- Increase in address size from 32 bits to 128 bits
- Simplified header
- Extensible header with optional extension headers
- Designed to co-exist with IPv4
- Uses multicast addresses instead of broadcast addresses

This chapter includes the following sections:

- Operations Tasks
- Command Descriptions

Operations Tasks

Note In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the full description for the command in the "Command Descriptions" section.

This section describes the following types of tasks:

- Context Operations Tasks
- Interface Operations Tasks
- Subscriber Operations Tasks

Context Operations Tasks

Context operations tasks are listed in Table 6-1. Enter **show** commands in any mode; enter all other commands in exec mode.

Table 6-1 Context Operations Tasks

Task	Command
Terminates one or all of an administrator's remote (Telnet or Secure Shell [SSH]) terminal sessions.	**clear administrator**
When entered from exec mode, this command displays context-specific information without entering context configuration mode. When entered from global configuration mode, this command creates a new context or specifies an existing context, and enters context configuration mode.	**context**
Enables the generation of general debug messages for the current context.	**debug context**
Displays all administrator sessions on a system.	**show administrators**
Displays configuration information for a specified context.	**show configuration context**
Displays a list of configured context names.	**show context**
Displays the status of the IP addresses in the specified IP pool, in all IP pools in the specified interface, or in all IP pools in the current context or range.	**show ip pool**
Display an administrator's public keys.	**show public-key**

Interface Operations Tasks

Interface operations tasks are listed in Table 6-2. Enter **show** commands in any mode; enter all other commands in exec mode.

Table 6-2 Interface Operations Tasks

Task	Command
Enable the generation of debug messages for all configured interfaces in the current context.	**debug if**
Display information about interfaces, including the interface bound to the Ethernet management port on the controller card.	**show ip interface**
Displays the status of the IP addresses in the specified IP pool, in all IP pools in the specified interface, or in all IP pools in the current context or range.	**show ip pool**

Subscriber Operations Tasks

Subscriber operations tasks are listed in Table 6-3. Enter **show** commands in any mode. Enter all other commands in exec mode.

Table 6-3 Subscriber Operations Tasks

Task	Command
Clear one or more subscribers in the current context, thus terminating any PPP or PPPoE session or dropping any RFC 1483 bridged-encapsulated circuit connection.	**clear subscriber**
Terminate a subscriber session to allow changes to a subscriber record for a subscriber that is already bound, to take effect.	**clear subscriber**
Display subscriber information.	**show subscribers**

Command Descriptions

This section describes the syntax and usage guidelines for the commands used to monitor, administer, and troubleshoot contexts, interfaces, and subscribers. The commands are presented in alphabetical order.

clear administrator
clear subscriber
context
debug context
debug if
show administrators
show configuration context
show context
show ip interface
show ip pool
show ipv6 interface
show public-key
show subscribers

clear administrator

clear administrator *admin-name* [*tty-name*]

Purpose

Terminates one or all of an administrator's remote (Telnet or Secure Shell [SSH]) terminal sessions.

Command Mode

exec

Syntax Description

admin-name	Name of the administrator whose sessions are to be terminated.
tty-name	Optional. Name of the Teletypewriter (TTY) for a particular session to be terminated.

Default

If you use this command without the optional *tty-name* argument, all sessions for the specified administrator are cleared.

Usage Guidelines

Use the **clear administrator** command to end one or all of an administrator's remote terminal sessions with the following criteria:

- An administrator in the local context can end any administrator session.
- Administrators in any other context can end sessions only in their own context.
- This command does not end the current session.

Use the optional *tty-name* argument to indicate a specific terminal session to be cleared. If you use the command without this argument, all of the specified administrator's sessions are cleared. The output of the **show administrators** command (in exec mode) displays the TTY names.

Examples

The following example clears a single terminal session for a administrator, `test`:

```
[local]Redback#clear administrator test ttyp2
```

Related Commands

show administrators

clear subscriber

For ports on channelized OC-12 or STM-1 cards, the syntax is:

clear subscriber {**session** *slot*/*port*[**:***chan-num*[**:***sub-chan-num*] [*circuit-id*]] [**pppoe** *sess-id*] [**clips-bounce**] | **username** *subscriber* [**clips-bounce**] | **encapsulation ppp** {**all** | **all-context**}

For channelized ports on DS-3 or E1 cards, the syntax is:

clear subscriber {**session** *slot*/*port*[**:***chan-num* [*circuit-id*]] [**pppoe** *sess-id*] [**clips-bounce**] | **username** *subscriber* [**clips-bounce**] | **encapsulation ppp** {**all** | **all-context**}

For clear-channel ports on DS-3, E3, or E1 cards, or ports on Asynchronous Transfer Mode (ATM) OC, ATM DS-3, or Ethernet cards, the syntax is:

clear subscriber {**session** *slot*/*port* [*circuit-id*] [**pppoe** *sess-id*] [**clips-bounce**] | **username** *subscriber* [**clips-bounce**] | **encapsulation ppp** {**all** | **all-context**}}

Purpose

Clears one or more subscriber sessions, thus terminating any Point-to-Point Protocol (PPP) or Point-to-Point Protocol over Ethernet (PPPoE) session or dropping any RFC 1483 bridged-encapsulated circuit connection.

Command Mode

exec

Syntax Description

session	Clears the subscriber sessions on the specified port, channel, subchannel, or circuit with the specified encapsulation type and session identifier.
slot	Chassis slot number for a particular card.
port	Port number on the specified card.
chan-num	Optional. Channel number for which subscriber sessions are cleared. If omitted, clears subscriber sessions for all channels on the specified port. The range of values depends on the type of port; see Table 6-4 for the range of values.
sub-chan-num	Optional. Subchannel number for which subscriber sessions are cleared. If omitted, clears subscriber sessions on all subchannels in the specified channel. The range of values depends on the type of port; see Table 6-4 for the range of values.
circuit-id	Optional. Circuit identifier for which subscriber sessions are cleared, according to one of the constructs listed in Table 6-5. If omitted, clears subscriber sessions on all circuits on the specified port, channel, or sub-channel.
pppoe *sess-id*	Optional. PPPoE session identifier. The range of values is 1 to 65,534. This construct is available only 802.1Q and ATM permanent virtual circuits (PVCs).
username *subscriber*	Name of the subscriber with sessions to be cleared, in any valid structured subscriber name format.

clips-bounce	Optional. Re-authenticates the clientless IP service selection (CLIPS) circuit.
encapsulation ppp	Specifies the encapsulation type for circuits with subscriber sessions to be cleared.
all	Clears all subscriber sessions on circuits with PPP encapsulation in the current context.
all-context	Clears all subscriber sessions on circuits with PPP encapsulation in all contexts. This option is available only in the local context.

Default

None

Usage Guidelines

Use the **clear subscriber** command to clear one or more subscriber sessions, thus terminating any PPP or PPPoE session or dropping any RFC 1483 bridged-encapsulated circuit connection

Table 6-4 lists the range of values for *chan-num* and *sub-chan-num* arguments for various types of channelized ports.

Table 6-4 Range of Values for the *chan-num* and *sub-chan-num* Arguments

Port	Channel Types	*chan-num* Range	*sub-chan-num* Range
Channelized OC-12	DS-3, DS-1	1 to 12	1 to 28
Channelized STM-1	E1, DS-0 channel group	1 to 63	1 to 31
Channelized DS-3	DS-1	1 to 28	–
Channelized E1	DS-0 channel group	1 to 31	–

Table 6-5 lists the values for the *circuit-id* argument.

Table 6-5 Values for the *circuit-id* Argument

Construct	Description
clips *clips-id*	CLIPS circuit on a port, channel, 802.1Q PVC, or ATM PVC. The range of values is 1 to 65,534. If the CLIPS circuit is on an 802.1Q or ATM PVC, you specify this construct in addition to the circuit identifier for the 802.1Q or ATM PVC.
vlan-id *vlan-id*	Virtual LAN (VLAN) tag value for an 802.1Q tunnel or PVC. The *vlan-id* argument is one of the following constructs: • *pvc-vlan-id*—VLAN tag value of a PVC that is not within an 802.1Q tunnel. • *tunl-vlan-id*—VLAN tag value of a tunnel. • *tunl-vlan-id***:***pvc-vlan-id*—VLAN tag value for the tunnel followed by the VLAN tag value for the PVC within the tunnel. The range of values for any VLAN tag value is 1 to 4,095.
vpi-vci *vpi vci*	Virtual path identifier (VPI) and virtual circuit identifier (VCI) for an ATM PVC. The range of values is 0 to 255 and 1 to 65,535, respectively. By convention, VCI 1 to 31 are reserved for system use.

The SmartEdge OS verifies whether the subscriber is currently active, and if so, clears the circuit on which the subscriber sessions are active. In the case of the PPP, the PPP state machine terminates the session, and logs off the subscriber. It then attempts to renegotiate and reauthenticate a new session with the remote peer on that circuit. In the case of RFC 1483 bridge-encapsulated circuits, the circuit is brought down and then back up, and an attempt is made to reauthenticate the subscriber.

Use the **username** *subscriber* construct to clear the sessions for a single subscriber. The *subscriber* argument can include both the subscriber name and the domain name in any valid format, such as *sub-name***@***ctx-name*. The format is configurable. For information about configuring the format, see the "AAA Configuration" chapter in the *IP Services and Security Configuration Guide* for the SmartEdge OS.

If you specify the VLAN tag value for an 802.1Q tunnel, the commands clears subscriber sessions on all the PVCs within the tunnel.

This command is useful to clear a subscriber, thus terminating any PPP or PPPoE session or dropping any RFC 1483 bridged-encapsulated circuit connections, or to modify a subscriber record for a subscriber. The subscriber session is terminated and restarted with the new parameters.

Examples

The following example clears the subscriber, `dave@isp1`:

```
[local]Redback>clear subscriber username dave@isp1
```

Related Commands

show subscribers

context

context *ctx-name* [**show** *show-param*]

no context *ctx-name*

Purpose

When entered (in exec mode), this command changes from the existing context to a new context or displays the specified information for the specified context. When entered (in global configuration mode), this command creates a new context or specifies an existing context, and enters context configuration mode.

Command Mode

exec
global configuration

Syntax Description

ctx-name	Name of a new or existing context.
show *show-param*	Optional. Type of information to be displayed for the specified context.

Default

The "local" context is defined on the system.

Usage Guidelines

Use the **context** command (in exec mode) to change to a different context or to display the specified information for the specified context without entering that context. The **show** *show-param* construct is any show command.

Use the **context** command (in global configuration mode) to create a new context or specify an existing context, and enter context configuration mode.

Note To change to a different context, you must be an administrator authenticated to the "local" context.

You cannot create new contexts on the system unless you have enabled the multiple context feature using the **service multiple-contexts** command (in global configuration mode). For more information on the **service multiple-contexts** command (in global configuration mode), see the "Context Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

The local context has special meaning and is always present. Only an administrator authenticated in the local context can configure the system. Administrators authenticated in the local context can observe any portion of the system, regardless of context. Administrators authenticated in other contexts are restricted to the portion of the system relevant to that context.

Contexts are completely independent name spaces and data spaces. For example, a routing process in one context can share routing information with a routing process in another context through inter-context interfaces just as physical routers are connected together by physical cables.

Use the **no** form of the command to delete a context and all configuration information associated with it.

For more information about creating VPN contexts, see the **context vpn-rd** command (in global configuration mode) in the "Context Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

Examples

The following example shows how to enter context configuration mode to configure the `local` context:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#
```

The following example displays ip route information for the `local` context:

```
[local]Redback>context local show ip route

Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1
N2 - OSPF NSSA external type 2, E1 - OSPF external type 1
E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2
> - Active Route
Type Network Next Hop Dist Metric UpTime Interface
> C 10.3.0.0/16 0 0 01:01:50 three
> C 10.13.49.0/24 0 0 01:01:50 mgmt
> S 155.0.0.0/8 10.13.49.254 1 0 01:01:39 mgmt
> C 193.4.0.0/16 0 0 01:01:50 one
> C 193.10.25.7/32 0 0 01:01:50 lo1
```

Related Commands

show context

debug context

debug [**boot** {**active** | **standby**} | **switchover**] **context general**

no debug [**boot** {**active** | **standby**} | **switchover**] **context general**

Purpose

Enables the generation of debug messages for the current context.

Command Mode

exec (10)

Syntax Description

boot	Optional. Enables the generation of debug messages during a system reload.
active	Enables the generation of debug messages for the active controller card.
standby	Enables the generation of debug messages for the standby controller card.
switchover	Optional. Enables the generation of debug messages during a switchover from the active to the standby controller.
general	Enables the generation of general context debug messages.

Default

Disabled

Usage Guidelines

Use the **debug context** command to enable the generation of debug messages for the current context.

Caution Risk of performance loss. Enabling the generation of debug messages can severely affect system performance. To reduce the risk, exercise caution when enabling the generation of any debug messages on a production system.

Use the **boot active** or **boot standby** construct to enable debugging messages during a system reload for the active or standby controller card, respectively.

Use the **switchover** keyword to enable debugging messages while the system is switching from the active to the standby controller card.

To store messages in the system log buffer, use the **logging debug** command (in global configuration mode). Use the **show log** command (in exec mode) to display these stored messages.

To display messages in real time, use the **logging console** command (in context configuration mode) if you are connected to the system through the console port. Or, use the **terminal monitor** command (in exec mode) if you are connected to the system through a Telnet or Secure Shell (SSH) session.

Note For more information about the **logging** commands, see the "Logging Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS. For information about the **terminal monitor** command (in exec mode), see Chapter 4, "Session Operations."

Use the **no** form of this command to disable the generation of debug messages.

Examples

The following example enables the generation of context debug messages:

```
[local]Redback#debug context general
```

Related Commands

show context

debug if

debug [**boot** {**active** | **standby**} | **switchover**] **if** {**all** | **error** | **rcm**}

no debug [**boot** {**active** | **standby**} | **switchover**] **if** {**all** | **error** | **rcm**}

Purpose

Enables the generation of debug messages for all configured interfaces in the current context.

Command Mode

exec (10)

Syntax Description

boot	Optional. Enables the generation of debug messages during a system reload.
active	Enables the generation of debug messages for the active controller card.
standby	Enables the generation of debug messages for the standby controller card.
switchover	Optional. Enables the generation of debug messages during a switchover from the active to the standby controller.
all	Enables the generation of all debug messages.
error	Enables the generation of only error debug messages.
rcm	Enables the generation of only Router Configuration Manager (RCM) debug messages.

Default

Disabled

Usage Guidelines

Use the **debug if** command to enable the generation of debug messages for all configured interfaces in the current context.

Use the **boot active** or **boot standby** construct to enable debugging messages during a system reload for the active or standby controller card, respectively.

Use the **switchover** keyword to enable debugging messages while the system is switching from the active to the standby controller card.

To store messages in the system log buffer, use the **logging debug** command (in global configuration mode). Use the **show log** command (in exec mode) to display these stored messages.

To display messages in real time, use the **logging console** command (in context configuration mode) if you are connected to the system through the console port. Or, use the **terminal monitor** command (in exec mode) if you are connected to the system through a Telnet or Secure Shell (SSH) session.

Note For more information about the **logging** commands, see the "Logging Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS. For information about the **terminal monitor** command (in exec mode), see Chapter 4, "Session Operations."

Caution Risk of performance loss. Enabling the generation of debug messages can severely affect system performance. To reduce the risk, exercise caution when enabling the generation of any debug messages on a production system.

Use the **no** form of this command to disable the generation of debug messages.

Examples

The following example enables the generation of only `RCM` debug messages for all configured interfaces:

```
[local]Redback#debug if rcm
```

Related Commands

show ip interface

show administrators

show administrators [**active** [*admin-name*]]

Purpose

Displays all administrator sessions on a system.

Command Mode

all modes

Syntax Description

active	Optional. Restricts the display to currently active sessions.
admin-name	Optional. Name of a particular administrator.

Default

Displays all administrator sessions.

Usage Guidelines

Use the **show administrators** command to display all administrator sessions on a system. Use the **active** keyword to limit the display to active sessions. With the **active** keyword, you can also use the *admin-name* argument to specify the sessions corresponding to a particular administrator.

In the display, the * character denotes the administrator session in which this command was entered.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays output from the **show administrators** command when used without optional constructs:

```
[local]Redback>show administrators

  TTY    START TIME               REMOTE HOST             ADMINISTRATOR
-------------------------------------------------------------------------
  ttyp0  Mon Jun 27 14:42:53 2005 nosuchhost.redback.com  test@local
* ttyp1  Mon Jun 27 09:12:31 2005 dhcp-xx.redback.com     last@local
  ttyp2  Mon Jun 27 11:15:43 2005 dhcp-yy.redback.com     test@local
```

The following example displays output from the **show administrators** command when a specific administrator name is specified:

```
[local]Redback>show administrators active test

  TTY    START TIME               REMOTE HOST             ADMINISTRATOR
-------------------------------------------------------------------------
* ttyp0  Mon Jun 27 05:34:38 2005 155.53.6.209            test@local
  ttyp2  Mon Jun 27 11:15:43 2005 dhcp-yy.redback.com     test@local
```

Related Commands

clear administrator
context

show configuration context

show configuration context *ctx-name*

Purpose

Displays configuration information for a specified context.

Command Mode

all modes

Syntax Description

ctx-name	Name of the context for which information is to be displayed.

Default

None

Usage Guidelines

Use the **show configuration context** command to display configuration information for a specified context.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays configuration information for the `local` context:

```
[local]Redback#show configuration context local

Building configuration...

Current configuration:
!
 no ip domain-lookup
!
 interface mgmt
  ip address 10.12.210.37/21
!
!
```

```
 logging console
!
 enable encrypted 1 $1$........$kvQfdsjs0ACFMeDHQ7n/o.
!
!
 user test encrypted 1 $1$........$kvQfdsjs0ACFMeDHQ7n/o.
!
!
 ip route 10.12.0.0/10.210.12.208.1 cost 1 permanent
 ip route 10.13.0.0/10.210.12.208.1 cost 1 permanent
!!
!
end
```

Related Commands

context

show context

show context [*ctx-name* | **all**]

Purpose

Displays a list of configured context names.

Command Mode

all modes

Syntax Description

ctx-name	Optional. Name of a specific context to be included in the display.
all	Optional. Displays information for all contexts.

Default

Displays the current context name.

Usage Guidelines

Use the **show context** command to see if a context has been configured or to obtain a listing of all the configured contexts. When used without the optional *ctx-name* argument, the command displays only the name of the current context.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, “Using the CLI.”

Examples

The following commands display output from the **show context** command:

```
[local]Redback>show context

local(1)

[local]Redback>show context isp-a

isp a(1)
```

```
[local]Redback>show context all

local(1)
isp-a(2)
gypsy12(3)
```

Related Commands

context

show ip interface

show ip interface [*if-name* | **brief** | **xcrp** [**bytes**]]

Purpose

Displays information about interfaces, including the interface bound to the Ethernet management port on the controller card.

Command Mode

all modes

Syntax Description

if-name	Optional. Name of the interface to be displayed.
brief	Optional. Displays the name, IP address, and other information (in brief) for all configured interfaces in the current context.
xcrp	Optional. Displays incoming and outgoing packets, errors, and collisions for the interface to which the Ethernet management port on the controller cards is bound.
bytes	Optional. Displays incoming and outgoing bytes for the interface to which the Ethernet management port on the controller cards is bound.

Default

Displays detailed information for all configured interfaces.

Usage Guidelines

Use the **show ip interface** command to display information about all interfaces, including those on the controller card. Use this command without any argument or keywords to display detailed information on all configured interfaces. Use the *if-name* argument to display information for a particular interface only.

Use the optional **brief** keyword to display only summary information for all configured interfaces.

Use the optional **xcrp** and **bytes** keywords to display a variety of information for the interface to which the Ethernet management port on the controller card is bound, including incoming and outgoing packets, errors, dropped bytes, and collisions.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, “Using the CLI.”

Examples

The following example displays output from the **show ip interface brief** command. An interface can be in any of the following states:

- Unbound—The interface is not currently bound to any port or circuit.
- Bound—The interface is bound to at least one port or circuit; however, none of the bound circuits are up; therefore, the interface is not up.
- Up—At least one of the bound circuits is in the up state; therefore, the interface is also up and traffic can be sent over the interface.

```
[local]Redback>show ip interface brief

Mon Jun 27 06:38:05 2005
Name              Address                 MTU    State      Bindings
fe13/3            3.2.13.3/16             1500   Up         ethernet 13/3
fe13/4            4.2.13.4/16             1500   Up         ethernet 13/4
5/1               10.13.49.166/24         1500   Up         ethernet 5/1
12/1              10.1.1.1/16             0      UnBound
un1               (Un-numbered)           0      UnBound
lo1               100.1.1.1/16            1500   Up         (Loopback)
```

The following example displays information for the `fe13/4` interface:

```
[local]Redback>show ip interface fe13/4

Intf name:       fe13/4
Intf state:      Up                      MTU:             1500
IP address:      4.2.13.4                Prefix len:      16
ISIS Tag:        1                       Levels:          level-1-2
ISIS Metric:     10                      Authentication:  none
OSPF instance:   1                       OSPF net type:   broadcast
OSPF cost:       1                       OSPF state       BDR
Resoln type:     Arp                     ARP timeout      3600
ARP Proxy:       Enabled

Bindings:
Encapsulation    Circuit
ethernet         13/4
```

The following example displays packet information for the interface to which the Ethernet management port is bound:

```
[local]Redback>show ip interface xcrp

Name  Mtu    Network           Address              Ipkts      Opkts     Colls
                                                    Ierrs      Oerrs     Drops
fxp0  1500   <Link>            00:30:88:00:03:6f    62716      22871         0
                                                        2          0         0
fxp0  1500   10.13.49/24       10.13.49.166         62716      22871         0
                                                        2          0         0
ipc0  8192   <Link>                                 32078      26862         0
                                                        0          0         0
```

```
ipc0  8192   127                127.0.2.5           32078      26862         0
                                                        0          0         0
lo0   33228  <Link>                                     0          0         0
                                                        0          0         0
lo0   33228  127                127.0.0.1               0          0         0
                                                        0          0         0
xcrp  65535  <Link>                                     0          0         0
                                                        0          0         0
lc12  65535  <Link>                                  2461       2452         0
                                                        0          0         0
```

The following example displays byte information for the interface to which the Ethernet management port is bound:

```
[local]Redback>show ip interface xcrp bytes

Name  Mtu    Network            Address                 Ibytes       Obytes
fxp0  1500   <Link>             00:30:88:00:03:6f     55787738       2053859
fxp0  1500   10.13.49/24        10.13.49.166          55787738       2053859
ipc0  8192   <Link>                                 3665494016      77265152
ipc0  8192   127                127.0.2.5           3665494016      77265152
lo0   33228  <Link>                                          0             0
lo0   33228  127                12.0.0.1                    0             0
xcrp  65535  <Link>                                          0             0
lc12  65535  <Link>                                          0             0
```

Related Commands

context
save configuration

show ip pool

show ip pool [*name*] [**context** *summary*][**falling-threshold**]

Purpose

Displays the status of the IP addresses in the specified IP pool, in all IP pools in the specified interface, or in all IP pools in the current context or range.

Command Mode

all modes

Syntax Description

name	Optional. Name of the IP pool or interface for which the status of its IP addresses displays.
context summary	Optional. Displays the summary information for all context level IP pool thresholds for the named context.
falling-threshold	Optional. Displays IP pool threshold data for all interfaces in the current context or for the specified interface only.

Default

None

Usage Guidelines

Use the **show ip pool** command to display the status of the IP addresses in the specified IP pool, in all IP pools in the specified interface, or in all IP pools in the current context. The status of the IP addresses includes the number of addresses in use, available, and reserved. Reserved addresses include those used by an interface or the all ones or all zeros address for the interface.

Use the optional *name* argument to specify an IP pool or an interface.

Use the optional **context summary** argument to display the summary information for all context level IP pool thresholds for the named context.

Use the optional **falling-threshold** keyword to display falling-threshold data for each interface.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, “Using the CLI.”

Examples

The following example displays status for all IP address pools in the `ip-dial` context, including a range of IP addresses for the `isp1.net` interface:

```
[local]Redback>context ip-dial

[ip-dial]Redback>show ip pool

Interface "subscribers-am":
        192.168.1.48     255.255.255.248    0 in use,   5 free, 3 reserved.
Interface "subscribers-mr":
        10.142.119.80    255.255.255.240    0 in use,  13 free, 3 reserved.
Interface "subscribers-sz":
        192.168.2.0      255.255.255.0      0 in use, 253 free, 3 reserved.
Interface "isp1.net":
10.1.1.2        10.1.1.100 0 in use,  99 free,   0 reserved
```

The following example displays the falling threshold data for all IP address pools in the `ip-dial` context:

```
[ip-dial]Redback>show ip pool falling-threshold

Context "ip-dial": falling-threshold 17 trap log
Interface "subscribers-am":
        192.168.1.48     255.255.255.248  falling-threshold   3 trap
Interface "subscribers-mr":
        10.142.119.80    255.255.255.240  falling-threshold   5 trap log
Interface "subscribers-sz":
        192.168.2.0      255.255.255.0    falling-threshold   33 log
```

The following example displays the status of the IP addresses in the `ip-pool` pool for the `isp1.net` context:

```
[local]Redback>context isp1.net

[isp1.net]Redback>show ip pool ip-pool

Interface "isp1.net":
   10.1.1.0        /24  ip-pool 0 in use, 253 free,   3 reserved
```

The following example displays a summary of all contexts in the IP pool for the `isp1.net` context:

```
[local]Redback>show ip pool context summary
falling-threshold absolute     1 759        trap log
falling-threshold percentage   1 98         trap
falling-threshold percentage   2 97         trap log

9         in use, 750       free, 9         reserved
768       total,  97  available percentage
```

Related Commands

context
show ip interface

show ipv6 interface

show ipv6 interface [*if-name* | **brief**]

Purpose

Displays information about Internet Protocol Version 6 (IPv6) interfaces, including the interface bound to the Ethernet management port on the controller card.

Command Mode

all modes

Syntax Description

if-name	Optional. Name of the IPv6 interface to be displayed.
brief	Optional. Displays the name, IPv6 address, and other information (in brief) for all configured IPv6 interfaces in the current context.

Default

Displays detailed information for all configured IPv6 interfaces.

Usage Guidelines

Use the **show ipv6 interface** command to display information about all IPv6 interfaces, including those on the controller card. Use this command without any argument or keyword to display detailed information on all configured IPv6 interfaces. Use the optional *if-name* argument to display information for a specific IPv6 interface only. Use the optional **brief** keyword to display only summary information for all configured IPv6 interfaces.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

An interface can be in any of the following states:

- Unbound—The interface is not currently bound to any port or circuit.
- Bound—The interface is bound to at least one port or circuit; however, none of the bound circuits are up, and therefore, the interface is not up.
- Up—At least one of the bound circuits is in the up state; therefore, the interface is also up and traffic can be sent over the interface.

Examples

The following example displays output from the **show ipv6 interface brief** command:

```
[local]Redback>show ipv6 interface brief

Mon Jun 27 06:38:05 2005
Name              Address                  MTU    State      Bindings
fe13/3            3.2.13.3/16              1500   Up         ethernet 13/3
fe13/4            4.2.13.4/16              1500   Up         ethernet 13/4
5/1               10.13.49.166/24          1500   Up         ethernet 5/1
12/1              10.1.1.1/16              0      UnBound
un1               (Un-numbered)            0      UnBound
lo1               100.1.1.1/16             1500   Up         (Loopback)
```

The following example displays information for the `fe13/4` interface:

```
[local]Redback>show ipv6 interface fe13/4

Intf name:       fe13/4
Intf state:      Up                       MTU:              1500
IP address:      4.2.13.4                 Prefix len:       16
ISIS Tag:        1                        Levels:           level-1-2
ISIS Metric:     10                       Authentication:   none
OSPF instance:   1                        OSPF net type:    broadcast
OSPF cost:       1                        OSPF state        BDR
Resoln type:     Arp                      ARP timeout       3600
ARP Proxy:       Enabled

Bindings:
Encapsulation    Circuit
ethernet         13/4
```

The following example displays packet information for the interface to which the Ethernet management port is bound:

```
[local]Redback>show ipv6 interface xcrp

Name  Mtu    Network           Address              Ipkts      Opkts     Colls
                                                    Ierrs      Oerrs     Drops
fxp0  1500   <Link>            00:30:88:00:03:6f    62716      22871         0
                                                        2          0         0
fxp0  1500   10.13.49/24       10.13.49.166         62716      22871         0
                                                        2          0         0
ipc0  8192   <Link>                                 32078      26862         0
                                                        0          0         0
ipc0  8192   127               127.0.2.5            32078      26862         0
                                                        0          0         0
lo0   33228  <Link>                                     0          0         0
                                                        0          0         0
lo0   33228  127               127.0.0.1                0          0         0
                                                        0          0         0
xcrp  65535  <Link>                                     0          0         0
```

```
                                                          0          0         0
lc12  65535  <Link>                                    2461       2452         0
                                                          0          0         0
```

The following example displays byte information for the IPv6 interface to which the Ethernet management port is bound:

```
[local]Redback>show ipv6 interface xcrp bytes

Name  Mtu    Network           Address                 Ibytes       Obytes
fxp0  1500   <Link>            00:30:88:00:03:6f     55787738       2053859
fxp0  1500   10.13.49/24       10.13.49.166          55787738       2053859
ipc0  8192   <Link>                                3665494016      77265152
ipc0  8192   127               127.0.2.5           3665494016      77265152
lo0   33228  <Link>                                         0             0
lo0   33228  127               12.0.0.1                     0             0
xcrp  65535  <Link>                                         0             0
lc12  65535  <Link>                                         0             0
```

Related Commands

context
save configuration

show public-key

show public-key *admin-name*

Purpose

Displays an administrator's public keys.

Command Mode

all modes

Syntax Description

admin-name Name of the administrator for which public key information is to be displayed.

Default

None

Usage Guidelines

Use the **show public-key** command to display an administrator's public keys.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays the public keys configured for the `jewel` administrator:

```
[local]Redback>show public-key jewel

DSA public key(s) for user jewel
RSA public key(s) for user jewel
1024 35 13877892548755011249626406025749447395347780214577723471190493135601780425356
38422909300110544504853632432802464001997177313198444188310892645934968528091708337893
83989152738587950064526673253249893854977936260102627149373407590302521645739523172785
58414474890514861688652497950829684053136276382193869961246761 jewel@pepper
```

Related Commands

context

show subscribers

For ports on channelized OC-12 or STM-1 traffic cards, the syntax is:

show subscribers [**all** | **active** [**all** | **session** *slot*/*port*[**:***chan-num*[**:***sub-chan-num*] [*circuit-id*]] [**pppoe** *sess-id*] | **username** *subscriber*] | **remote-agent-id** *id* | **address username** *subscriber* | **session** *slot*/*port*[**:***chan-num*[**:***sub-chan-num*] [*circuit-id*]] [**pppoe** *sess-id*] | **summary** [**all**] **| username** *subscriber*]

For channelized ports on DS-3 or E1 traffic cards, the syntax is:

show subscribers [**all** | **active** [**all** | **session** *slot*/*port*[**:***chan-num* [*circuit-id*]] [**pppoe** *sess-id*] | **username** *subscriber*] | **remote-agent-id** *id* | **address username** *subscriber* | **session** *slot*/*port*[**:***chan-num* [*circuit-id*]] [**pppoe** *sess-id*] | **summary** [**all**] **| username** *subscriber*]

For clear-channel ports on DS-3, E3, or E1 traffic cards, or ports on Asynchronous Transfer Mode (ATM) OC, ATM DS-3, or Ethernet traffic cards, the syntax is:

show subscribers [**all** | **active** [**all** | **session** *slot*/*port* [*circuit-id*] [**pppoe** *sess-id*] | **username** *subscriber*] | **remote-agent-id** *id* | **address username** *subscriber* | **session** *slot*/*port* [*circuit-id*] [**pppoe** *sess-id*] | **summary** [**all**] **| username** *subscriber*]

Purpose

Displays subscriber information.

Command Mode

all modes

Syntax Description

all	Optional. Displays information for all subscribers in all contexts. This option is available only to administrators in the local context.
active	Optional. Displays a list of active subscribers.
session	Optional. Displays a list of subscribers on the specified port, channel, or circuit with the specified encapsulation type and session identifier.
slot	Chassis slot number for a particular card.
port	Port number on the specified card.
chan-num	Optional. Channel number for which subscribers are displayed. If omitted, displays subscribers for all channels on the specified port. The range of values depends on the type of port; see Table 6-6 for the range of values.
sub-chan-num	Optional. Subchannel number for which subscribers are displayed. If omitted, displays subscribers on all subchannels in the specified channel. The range of values depends on the type of port; see Table 6-6 for the range of values.

circuit-id	Optional. Subscriber circuit identifier, according to one of the constructs in Table 6-7. If omitted, displays subscribers on all types of circuits.
pppoe *sess-id*	Optional. Point-to-Point Protocol over Ethernet (PPPoE) session identifier. The range of values is 1 to 65,535.
summary	Optional. Displays a summary of subscriber information.
username *subscriber*	Optional. Subscriber name for which information is to be displayed, in any valid structured subscriber name format.
remote-agent-id *id*	Optional. Remote agent identifier name for which information is to be displayed, in any valid structured subscriber name format.
address username *subscriber*	Optional. Subscriber name for which the subscriber's IP address is to be displayed.

Default

Displays information for all active subscribers in the current context.

Usage Guidelines

Use the **show subscribers** command to display subscriber information, including the subscriber name, circuit, and start time.

Table 6-6 lists the range of values for the *chan-num* and *sub-chan-num* arguments for various types of channelized ports.

Table 6-6 Range of Values for the *chan-num* and *sub-chan-num* Arguments

Port	Channel Types	*chan-num* Range	*sub-chan-num* Range
Channelized OC-12	DS-3, DS-1	1 to 12	1 to 28
Channelized STM-1	E1, DS-0 channel group	1 to 63	1 to 31
Channelized DS-3	DS-1	1 to 28	–
Channelized E1	DS-0 channel group	1 to 31	–

Table 6-7 lists the values for the *circuit-id* argument.

Table 6-7 Values for the *circuit-id* Argument

Construct	Description
clips *clips-id*	CLIPS circuit on a port, channel, 802.1Q PVC, or ATM PVC. The range of values is 1 to 65,534. If the CLIPS circuit is on an 802.1Q or ATM PVC, you specify this construct in addition to the circuit-id for the 802.1Q or ATM PVC.
vlan-id *vlan-id*	Virtual LAN (VLAN) tag value for an 802.1Q tunnel or PVC. The *vlan-id* argument is one of the following constructs: • *pvc-vlan-id*—VLAN tag value of a PVC that is not within an 802.1Q tunnel. • *tunl-vlan-id*—VLAN tag value of a tunnel. • *tunl-vlan-id*:*pvc-vlan-id*—VLAN tag value for the tunnel followed by the VLAN tag value for the PVC within the tunnel. The range of values for any VLAN tag value is 1 to 4,095.

Table 6-7 Values for the *circuit-id* Argument *(continued)*

Construct	Description
vpi-vci *vpi vci*	Virtual path identifier (VPI) and virtual circuit identifier (VCI) for an Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC). The range of values is 0 to 255 and 1 to 65,535, respectively.

Use the **active** keyword to display information about active subscribers.

Use the **session** keyword to display information about one or more subscribers.

Use the **summary** keyword to display the total number of subscribers and their encapsulations.

Use the **username** *subscriber* construct to display information about a single subscriber. The *subscriber* argument can include both the subscriber name and the domain name in any valid format, such as *sub-name***@***ctx-name*. The format is configurable. For information about configuring the format, see the "AAA Configuration" chapter in the *IP Services and Security Configuration Guide* for the SmartEdge OS.

Use the **remote-agent-id** *id* construct to display the subscriber for the specified remote agent ID.

Use the **address username** *subscriber* construct to display the IP address for the specified subscriber.

Use the **show bindings** command (in all modes) to display information on configured bindings for one or more subscribers. For more information on the **show bindings** command (in all modes), see the "Bind Operations" chapter in the *Ports, Circuits, and Tunnels Operations Guide* for the SmartEdge OS.

If you specify the VLAN tag value for an 802.1Q tunnel, the output includes subscriber information for all the PVCs within the tunnel.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays the default information:

```
[local]Redback>show subscribers

Type     CIRCUIT  SUBSCRIBER          CONTEXT     START TIME
------------------------------------------------------------------------------
PPPOE    00001   pppoe@redback.com    company1    JUN 30 17:46:49 2005
VIPSRC   00002   00:dd:00:00:00:01    isp1        JUN 30 00:03:11 2005
VIPSRC   00003   00:dd:00:00:00:02    isp1        JUN 30 00:03:01 2005
VIPSRC   00004   00:dd:00:00:00:03    isp1        JUN 30 00:03:01 2005
VIPSRC   00005   00:dd:00:00:00:04    isp1        JUN 30 00:03:11 2005
VIPSRC   00006   00:dd:00:00:00:05    isp1        JUN 30 00:03:11 2005
------------------------------------------------------------------------------
Total=6
```

```
Type            Authenticating          Active          Disconnecting
PPP                          0               0                      0
PPPoE                        0               1                      0
DOT1Q                        0               0                      0
CLIPs                        0               5                      0
ATM-B1483                    0               0                      0
ATM-R1483                    0               0                      0
```

The following example displays the information for an active subscriber:

```
[local]Redback>show subscribers active

test@local
        Circuit   13/1 vpi-vci 0 32
        Internal Circuit   13/1:1023:63/1/2/6
        Current port-limit unlimited
        session traffic limit in 2000 (applied)
        session traffic limit out 2000 (applied)
        ip address 10.1.1.11 (applied)
```

Related Commands

clear subscriber
context

Software Operations

This chapter describes the commands used to monitor, administer, and troubleshoot system-wide software functions, including memory usage, processes, IP connectivity, bulkstats, logging, and Simple Network Management Protocol (SNMP) through the SmartEdge® OS.

For information about the commands used to configure these features, see the "System-Wide Management Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

Note In the following descriptions, the term, controller card, applies to the Cross-Connect Route Processor (XCRP) or the XCRP Version 3 (XCRP3) Controller card, unless otherwise noted.

This chapter includes the following sections:

- Operations Tasks
- Command Descriptions

Operations Tasks

Note In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the full description for the command in the "Command Descriptions" section.

This section describes the following types of system operations tasks:

- System-Wide Operations Tasks
- Restart Operations Tasks
- Bulkstats Operations Tasks
- Logging Operations Tasks
- SNMP Operations Tasks

System-Wide Operations Tasks

This section describes general system-wide operations tasks, such as displaying system memory and processes, testing IP connectivity, and enabling debugging messages for all IP packets. System-wide monitoring, administering, and testing operations include:

- System-Wide Software Monitoring Tasks
- System Process Operations Tasks
- Core Dump and Crash File Management Tasks
- Connectivity Testing Tasks

System-Wide Software Monitoring Tasks

You can display system-wide information, such as results of diagnostics tests, hardware types and slot locations, system memory, and so on. To do so, perform the appropriate task listed in Table 7-1; enter all **show** commands in any mode.

Table 7-1 System-Wide Software Monitoring Tasks

Task	Command
Displays Internet Control Message Protocol (ICMP) statistics.	**show icmp statistics**
Displays IP traffic statistics on the active controller card.	**show ip statistics xcrp**
Displays system memory statistics.	**show memory**
Displays configuration information for the advertisement packets or the version of the SNMP traps that are sent to the NetOp™ Element Manager System (EMS) server.	**show netop**
Displays current status of one or all processes running on the system.	**show process**
Displays Router Configuration Manager (RCM) information.	**show rcm**
Displays Transmission Control Protocol (TCP) Internet connections and statistics.	**show tcp**
Displays system information that assists your technical support representative in resolving any problem you may encounter.	**show tech-support**
Display User Datagram Protocol (UDP) socket and statistical information.	**show udp**

System Process Operations Tasks

Process operations commands provide instruction to the process manager (PM). To monitor, administer, or troubleshoot general system processes, perform the appropriate task listed in Table 7-2. Enter **show** commands in any mode; enter all other commands in exec mode.

Table 7-2 System Process Operations Tasks

Task	Command
Enables the generation of debug messages for IP read-write lock events.	**debug iprwlock**
Enables the generation of debug messages for process execution descriptor graph (PEDGR) manager events.	**debug pedgr**
Enables the generation of debug messages for the Process Manager (PM).	**debug pm**
Enables the generation of debug messages for the Router Configuration Manager (RCM).	**debug rcm**
Enables the generation of debug messages for the shared memory library.	**debug shmlib**

Table 7-2 System Process Operations Tasks *(continued)*

Task	Command
Enables the generation of debug messages related to transferring crash files out of the SmartEdge router using the File Transfer Protocol (FTP).	**debug sysmon ftp**
Monitors the current status of IP processes and provide continuous updates to the status.	**monitor ip**
Monitors the current status of a specified category of processes and provide continuous updates to the status.	**monitor process**
Disables the generation of debug message types supported by the SmartEdge OS.	**no debug all**
Restarts a process that has been stopped.	**process restart**
Sets process management parameters.	**process set**
Instructs the Process Manager (PM) to start the specified process.	**process start**
Stops a specified process.	**process stop**
Displays the debug options that are currently enabled.	**show debugging**

Caution Risk of data loss. Stopping a process causes the specified process to terminate and the services provided by the process to become unavailable until the process is restarted using the **process start** command. To reduce the risk, do not stop a process unless you intend to restart the process immediately.

Core Dump and Crash File Management Tasks

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

- Application (process) core dump

  This core dump is usually generated by the operating system as the result of a process internal error, but you can initiate the dump using the **process coredump** command (in exec mode). 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.

Caution Risk of data loss. The generation of a core dump of a process causes the specified process to be interrupted 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.

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 filename is *proc-name*_[*proc-id*].mini.cor**e**.

Note Some process names include the underscore character (_).

If you are monitoring a process and ask for a core dump, the crash filename includes the process name and ID of the process monitoring process in addition to the name and ID of the process it was monitoring.

- 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 filename 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.

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. Filenames are netbsd.0.core.gz and netbsd.0.gz.

Crash files can be automatically uploaded to a remote server that is accessed by the File Transfer Protocol (FTP) if the system has been configured using the **service upload-coredump** command (in global configuration mode). For information about the **service upload-coredump** command (in global configuration mode, see the "System-Wide Management Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

Note Redback® strongly recommends 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 troubleshooting information to the Redback support group; they are useful only to Redback personnel.

Table 7-3 lists the tasks to manage core dumps and crash files; Enter **show** commands in any mode; enter all other commands in exec mode.

Table 7-3 Core Dump Management Tasks

Task	Command
Deletes a file from the local file system on either the active or standby controller card.	**delete**
Initiates a core dump for the specified process and saves it in a crash file.	**process coredump**
Display the size, location, and name of any crash files stored on the system. Enter this command in all modes.	**show crashfiles**
Save a previously written core dump of the operating system to two crash files in the mass-storage device /md directory.	**save seos-core**

Connectivity Testing Tasks

Connectivity is tested by verifying IP reachability of hosts and tracing IP route routes. To perform hardware testing tasks, see the "Hardware Operations" chapter in the *Port, Circuits, and Tunnels Operations Guide* for the SmartEdge OS. To test IP connectivity, perform the appropriate task listed in Table 7-4; enter all commands in exec mode.

Table 7-4 Connectivity Testing Tasks

Task	Command
Tests whether the host is reachable.	**ping**
Traces the IP routes that packets take when traveling to the specified destination.	**traceroute**

Restart Operations Tasks

Restart operations tasks include:

- Enable Automatic Reload
- Manual Reload Tasks

Enable Automatic Reload

The SmartEdge OS supports two controller cards in a SmartEdge router: one that is the active controller card and one that is the standby controller card. The operating system ensures that the standby controller card is always synchronized with the active controller card, so that, in the event of a failure of the active controller card, the standby controller card can become active. To maintain synchronization between the two controller cards, the operating system occasionally performs an automatic reload of the standby controller card. To facilitate the automatic reload of an controller card, boot loader variable, `auto-boot?` variable must be set to true.

For further information about the boot loader interface, see Appendix A, “Boot Loader Operations.”

To verify the setting of the `auto-boot?` variable on both controller cards, perform the tasks described in the following sections:

- Connect a Console to the Console Port on Each Controller Card
- Set the Auto-Boot Variable on the Active Controller Card
- Set the Auto-Boot Variable on the Standby Controller Card

Connect a Console to the Console Port on Each Controller Card

The console port is labeled “Craft 2” on the front panel of the controller card. (Two cables are shipped with the system for connecting consoles to the console ports.)

Note Bootrom variables (including `auto-boot?`) can be accessed when connecting to the SmartEdge router through the console port.

Set the Auto-Boot Variable on the Active Controller Card

After you are connected to the SmartEdge router through the console that is connected to the active controller card, perform the following steps:

1. Enter the **reload** command (in exec mode).
2. Determine the state of the `auto-boot?` variable:
   - If you see the following message on the console connected to the active controller card,

     ```
     Auto-boot in 5 seconds - press SE* to abort, ENTER to boot:
     ```

     the `auto-boot?` variable has already been set to true. Enter **SE*** to cancel the reload process and access the boot loader interface. Proceed to the "Set the Auto-Boot Variable on the Standby Controller Card" section.
   - If the message does not appear, the `auto-boot?` variable is set to false and the `ok` prompt appears. Continue with step 3.
3. Set the `auto-boot?` variable to `true`; enter the following command:

   ```
   ok setenv auto-boot? true
   auto-boot? = true
   ```

4. Because you have modified the boot loader, enter the following command:

   ```
   ok reset
   ```

   The **reset** command resets the hardware and initiates a system reload.
5. Proceed to the "Set the Auto-Boot Variable on the Standby Controller Card" section.

Set the Auto-Boot Variable on the Standby Controller Card

After you are connected to the SmartEdge router through the console that is connected to the standby controller card, perform the following steps:

1. Determine the state of the `auto-boot?` variable:
   - If you see the `standby#` prompt on the console, the `auto-boot?` variable is set to true. No further action is needed.
   - If you see the ok prompt on the console connected to the standby controller card, the `auto-boot?` variable is set to false.
2. Set the `auto-boot?` variable to `true`; enter the following command:

   ```
   ok setenv auto-boot? true
   auto-boot? = true
   ```

3. Because you have modified the boot loader, enter the following command:

   ```
   ok reset
   ```

You are now assured that in the event of an active controller card failure, the system will continue to operate with the standby controller card.

Manual Reload Tasks

If it ever becomes necessary to restart the SmartEdge OS, you can do so without having to power down the system. To restart the operating system manually, you reload the main memory of the active controller card. You can also reload the standby controller card and you can switch over to the standby controller card.

Note Reload the system from the console port on the active controller card, so that you can view the progress of the reload operation. Remote sessions to the system are disconnected during the reload process.

To restart the operating system, perform one of the tasks described in Table 7-5; enter all commands in exec mode.

Table 7-5 Manual Reload Tasks

Task	Command
Reloads the system software on the active controller card first, and then reload the standby controller card.	**reload**
Reloads the system software on the standby controller card only.	**reload standby**
Reloads the system software on the active controller card and, if the standby controller card is ready, cause the standby card to become the active controller card.	**reload switch-over**

Note If any of the **reload** commands cause the error message, "`Release sync unsuccessful - not enough space in file system`", you might need to delete unused configuration and other data files from the /flash or /md file systems on the standby controller card; see the "Recover File Space" section in Chapter 3, "File and Release Operations."

Bulkstats Operations Tasks

Table 7-6 shows the operations tasks for bulk statistics (bulkstats). Enter the **show** commands in any mode; enter all other commands in exec mode.

Table 7-6 Bulkstats Operations Task

Task	Command
Immediately transfers bulkstats data for a specific bulkstats policy to one of the configured receivers, rather than waiting for the next transfer interval.	**bulkstats force transfer**
Displays the bulk statistics (bulkstats) configuration information and data transfer statistics, or the contents of the current collection file that have not yet been successfully transferred to the receiver, for the specified bulkstats policy.	**show bulkstats**

Logging Operations Tasks

Table 7-7 lists the logging operations tasks. Enter the **show** commands in any mode; enter all other commands in exec mode.

Table 7-7 Logging Operations Tasks

Task	Command
Clears the system event log buffer.	**clear log**
Clears the contents of the nonvolatile memory (NVRAM) on the active controller card to which you are connected.	**clear system nvlog**
Enables the generation of debugging messages for the logging facility (logger).	**debug logger**
Enables the generation of debugging messages for the logging facility (logger) Router Configuration Manager (RCM).	**debug logger-rcm**
Saves one of the internal event log buffers to the flash file system.	**save log**
Displays information about system event logs or a previously saved log file.	**show log**
Displays statistics about the system logger, including logger uptime, number of logged messages, number of logged filter messages, and number of logged rate-limited messages.	**show logging**
Displays the contents of the NVRAM on the active controller card to which you are connected.	**show system nvlog**

SNMP Operations Tasks

Table 7-8 lists the operations tasks for Simple Network Management Protocol (SNMP) and Remote Monitoring (RMON). Enter the **show** commands in any mode; enter all other commands in exec mode.

Table 7-8 SNMP Operations Tasks

Task	Command
Enables the generation of SNMP debug messages.	**debug snmp**
Displays commands for the SNMP.	**show configuration snmp**
Displays RMON information.	**show rmon**
Display SNMP statistics, including usage, configured contexts, communities, notifications, SNMP daemon status, targets, and views.	**show snmp**

Command Descriptions

This section describes the syntax and usage guidelines for the commands used to monitor, administer, and troubleshoot system-wide software functions. The commands are presented in alphabetical order.

bulkstats force transfer

bulkstats force transfer policy *bulk-pol-name*

Purpose

Immediately transfers the bulk statistics (bulkstats) data file for the specified policy to the configured receiver, rather than waiting for the next transfer interval.

Command Mode

exec

Syntax Description

policy *bulk-pol-name* Name of the bulkstats policy for which a transfer is to be forced.

Default

Bulkstats data is transferred at scheduled intervals.

Usage Guidelines

Use the **bulkstats force transfer** command to immediately transfer the bulkstats file for the specified policy to a configured receiver, rather than waiting for the next transfer interval. Data is transferred to the primary receiver; if this transfer should fail, an Simple Network Management Protocol (SNMP) trap is generated and data is transferred to the secondary receiver.

Use the **transfer-interval** command (in bulkstats configuration mode) in the current context to modify the interval at which the SmartEdge OS transfers data files to the configured receiver for the specified policy. For more information on the **transfer-interval** command (in bulkstats configuration mode), see the "Bulkstats Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

Examples

The following example forces the bulkstats data file for the `bulk` policy to be transferred immediately to the configured receiver:

```
[local]Redback>bulkstats force transfer policy bulk
```

Related Commands

None

clear log

clear log

Purpose

Clears the system event log buffer.

Command Mode

exec (10)

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **clear log** command to clear the system event log buffer. Use the **save log** command (in exec mode) to keep the current log buffer before you clear it.

Examples

The following example clears the system event log buffer:

```
[local]Redback#clear log
```

Related Commands

save log
show log
show logging
terminal monitor

clear logger statistics drop-counter

clear logger statistics drop-counter {**all** | **debug** | **log**}

Purpose

Clears one or more statistics drop counters for the logging facility (logger).

Command Mode

exec (10)

Syntax Description

all	Clears all drop counters for the logger.
debug	Clears the debug message drop counter for the logger.
log	Clears the log message drop counter for the logger.

Default

None

Usage Guidelines

Use the **clear logger statistics drop-counter** command to clear one or more statistics drop counters for the logger.

Examples

The following example clears the debug message drop counter for the logger:

```
[local]Redback#clear logger statistics drop-counter debug
```

Related Commands

None

clear system nvlog

clear system nvlog

Purpose

Clears the contents of nonvolatile memory (NVRAM) on the controller card to which you are connected.

Command Mode

exec (10)

Syntax Description

This command has no keywords or arguments.

Default

None.

Usage Guidelines

Use the **clear system nvlog** to clear the contents of NVRAM on the controller card to which you are connected. The NVRAM stores logs of trap- and panic-related messages from the operating system and can be used to help debug system crashes in the absence of a local console (connected to the Craft 2 port).

Examples

The following example clears the contents of the NVRAM on the active controller card:

```
[local]Redback#clear system nvlog
```

The following example clears the contents of the NVRAM on the standby controller card; in this example, the administrator is connected to the Craft 2 port on the standby controller card:

```
[local]standby>clear system nvlog
```

Related Commands

show system nvlog

debug iprwlock

debug [**boot** {**active** | **standby**} | **switchover**] **iprwlock**

no debug [**boot** {**active** | **standby**} | **switchover**] **iprwlock**

Purpose

Enables the generation of debug messages for IP read-write lock events.

Command Mode

exec (10)

Syntax Description

boot	Optional. Enables the generation of debug messages during a system reload.
active	Enables the generation of debug messages for the active controller card.
standby	Enables the generation of debug messages for the standby controller card.
switchover	Optional. Enables the generation of debug messages during a switchover from the active to the standby controller.

Default

The generation of debug messages for IP read-write lock events is disabled.

Usage Guidelines

Use the **debug iprwlock** command to enable the generation of debug messages for IP read-write lock events.

Caution Risk of performance loss. Enabling the generation of debug messages can severely affect system performance. To reduce the risk, exercise caution when enabling the generation of any debug messages on a production system.

Use the **boot active** or **boot standby** construct to enable debugging messages during a system reload for the active or standby controller card, respectively.

Use the **switchover** keyword to enable debugging messages while the system is switching from the active to the standby controller card.

To store debug messages in the system log buffer, use the **logging debug** command (in global configuration mode). Use the **show log** command (in exec mode) to display these stored debug messages.

To display messages in real time, use the **logging console** command (in context configuration mode) if you are connected to the system through the console port. Or, use the **terminal monitor** command (in exec mode) if you are connected to the system through a Telnet or Secure Shell (SSH) session.

Note For more information about the **logging** commands, see the "Logging Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS. For information about the **terminal monitor** command, see Chapter 4, "Session Operations."

Use the **no** form of this command to disable the generation of debug messages.

Examples

The following example enables the generation of debug messages for IP read-write lock events:

```
[local]Redback#debug iprwlock
```

Related Commands

show log

debug logger

debug logger

no debug logger

Purpose

Enables the generation of debug messages for the logging facility (logger).

Command Mode

exec (10)

Syntax Description

This command has no keywords or arguments.

Default

The generation of debug messages for the logger is disabled.

Usage Guidelines

Use the **debug logger** command to enable the generation of debug messages for the logger.

Caution Risk of performance loss. Enabling the generation of debug messages can severely affect system performance. To reduce the risk, exercise caution before enabling the generation of any debug messages on a production system.

To store debug messages in the system log buffer, use the **logging debug** command (in global configuration mode). Use the **show log** command (in exec mode) to display these stored debug messages.

To display messages in real time, use the **logging console** command (in context configuration mode) if you are connected to the system through the console port. Or, use the **terminal monitor** command (in exec mode) if you are connected to the system through a Telnet or Secured Shell (SSH) session.

Note For more information about the **logging** commands, see the "Logging Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS. For information about the **terminal monitor** command, see Chapter 4, "Session Operations."

Use the **no** form of this command to disable the generation of debug messages for the logger.

Examples

The following example enables the generation of debug messages for the logger:

```
[local]RedBack#debug logger
```

Related Commands

clear logger statistics drop-counter

debug logger-rcm

debug logger-rcm

no debug logger-rcm

Purpose

Enables the generation of debug messages for the logging facility (logger) Router Configuration Manager (RCM).

Command Mode

exec (10)

Syntax Description

This command has no keywords or arguments.

Default

The generation of debug messages for the logger RCM is disabled.

Usage Guidelines

Use the **debug logger-rcm** command to enable the generation of debug messages for the logger RCM.

Caution Risk of performance loss. Enabling the generation of debug messages can severely affect system performance. To reduce the risk, exercise caution before enabling the generation of any debug messages on a production system.

To store debug messages in the system log buffer, use the **logging debug** command (in global configuration mode). Use the **show log** command (in exec mode) to display these stored debug messages.

To display messages in real time, use the **logging console** command (in context configuration mode) if you are connected to the system through the console port. Or, use the **terminal monitor** command (in exec mode) if you are connected to the system through a Telnet or Secured Shell (SSH) session.

Note For more information about the **logging** commands, see the "Logging Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS. For information about the **terminal monitor** command, see Chapter 4, "Session Operations."

Use the **no** form of this command to disable the generation of debug messages for the logger RCM.

Examples

The following example enables the generation of debug messages for the logger RCM:

```
[local]RedBack#debug logger-rcm
```

Related Commands

debug logger
show log

debug pedgr

debug [**boot** {**active** | **standby**} | **switchover**] **pedgr**

no debug [**boot** {**active** | **standby**} | **switchover**] **pedgr**

Purpose

Enables the generation of debug messages for process execution descriptor graph (PEDGR) events.

Command Mode

exec (10)

Syntax Description

boot	Optional. Enables the generation of debug messages during a system reload.
active	Enables the generation of debug messages for the active controller card.
standby	Enables the generation of debug messages for the standby controller card.
switchover	Optional. Enables the generation of debug messages during a switchover from the active to the standby controller.

Default

The generation of debug messages for PEDGR events is disabled.

Usage Guidelines

Use the **debug pedgr** command to enable the generation of debug messages for PEDGR events.

Caution Risk of performance loss. Enabling the generation of debug messages can severely affect system performance. To reduce the risk, exercise caution when enabling the generation of any debug messages on a production system.

Use the **boot active** or **boot standby** construct to enable debugging messages during a system reload for the active or standby controller card, respectively.

Use the **switchover** keyword to enable debugging messages while the system is switching from the active to the standby controller card.

To store debug messages in the system log buffer, use the **logging debug** command (in global configuration mode). Use the **show log** command (in exec mode) to display these stored debug messages.

To display messages in real time, use the **logging console** command (in context configuration mode) if you are connected to the system through the console port. Or, use the **terminal monitor** command (in exec mode) if you are connected to the system through a Telnet or Secure Shell (SSH) session.

Note For more information about the **logging** commands, see the "Logging Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS. For information about the **terminal monitor** command, see Chapter 4, "Session Operations."

Use the **no** form of this command to disable the generation of debug messages.

Examples

The following example enables the generation of debug messages for PEDGR events:

```
[local]Redback#debug pedgr
```

Related Commands

show log

debug pm

debug [**boot** {**active** | **standby**} | **switchover**] **pm** [**all** | **config** | **general** | **ipc** | **memory-error** | **process**]

no debug [**boot** {**active** | **standby**} | **switchover**] **pm** [**all** | **config** | **general** | **ipc** | **memory-error** | **process**]

Purpose

Enables the generation of debug messages for the Process Manager (PM).

Command Mode

exec (10)

Syntax Description

boot	Optional. Enables the generation of debug messages during a system reload.
active	Enables the generation of debug messages for the active controller card.
standby	Enables the generation of debug messages for the standby controller card.
switchover	Optional. Enables the generation of debug messages during a switchover from the active to the standby controller.
all	Optional. Enables debug messages for all PM events.
config	Optional. Enables debug messages for PM configuration events.
general	Optional. Enables debug messages for general PM events.
ipc	Optional. Enables debug messages for interprocess communication (IPC) PM events.
memory-error	Optional. Enables debug messages for PM memory-error events.
process	Optional. Enables debug messages for PM process events.

Default

The generation of debug messages for the PM is disabled.

Usage Guidelines

Use the **debug pm** command to enable the generation of debug messages for the PM.

Caution Risk of performance loss. Enabling the generation of debug messages can severely affect system performance. To reduce the risk, exercise caution when enabling the generation of any debug messages on a production system.

Use the **boot active** or **boot standby** construct to enable debugging messages during a system reload for the active or standby controller card, respectively.

Use the **switchover** keyword to enable debugging messages while the system is switching from the active to the standby controller card.

To store debug messages in the system log buffer, use the **logging debug** command (in global configuration mode). Use the **show log** command (in exec mode) to display these stored debug messages.

To display messages in real time, use the **logging console** command (in context configuration mode) if you are connected to the system through the console port. Or, use the **terminal monitor** command (in exec mode) if you are connected to the system through a Telnet or Secure Shell (SSH) session.

Note For more information about the **logging** commands, see the "Logging Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS. For information about the **terminal monitor** command, see Chapter 4, "Session Operations."

Use the **no** form of this command to disable the generation of debug messages.

Examples

The following example enables PM memory-error events:

```
[local]Redback#debug pm memory-error
```

Related Commands

show log
show process

debug rcm

debug [**boot** {**active** | **standby**} | **switchover**] **rcm** [**event**]

no debug [**boot** {**active** | **standby**} | **switchover**] **rcm** [**event**]

Purpose

Enables the generation of debug messages for the Router Configuration Manager (RCM).

Command Mode

exec (10)

Syntax Description

boot	Optional. Enables the generation of debug messages during a system reload.
active	Enables the generation of debug messages for the active controller card.
standby	Enables the generation of debug messages for the standby controller card.
switchover	Optional. Enables the generation of debug messages during a switchover from the active to the standby controller.
event	Optional. Enables debugging messages for only RCM events.

Default

The generation of debug messages for the RCM is disabled.

Usage Guidelines

Use the **debug rcm** command to enable the generation of debug messages for the RCM.

Caution Risk of performance loss. Enabling the generation of debug messages can severely affect system performance. To reduce the risk, exercise caution when enabling the generation of any debug messages on a production system.

Use the **boot active** or **boot standby** construct to enable debugging messages during a system reload for the active or standby controller card, respectively.

Use the **switchover** keyword to enable debugging messages while the system is switching from the active to the standby controller card.

Use the optional **event** keyword to enable the debug messages for only RCM events.

To store debug messages in the system log buffer, use the **logging debug** command (in global configuration mode). Use the **show log** command (in exec mode) to display these stored debug messages.

To display messages in real time, use the **logging console** command (in context configuration mode) if you are connected to the system through the console port. Or, use the **terminal monitor** command (in exec mode) if you are connected to the system through a Telnet or Secure Shell (SSH) session.

Note For more information about the **logging** commands, see the "Logging Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS. For information about the **terminal monitor** command, see Chapter 4, "Session Operations."

Use the **no** form of this command to disable the generation of debug messages.

Examples

The following example enables debugging messages for only RCM events:

```
[local]Redback#debug rcm event
```

Related Commands

show log

debug shmlib

debug [**boot** {**active** | **standby**} | **switchover**] **shmlib**

no debug [**boot** {**active** | **standby**} | **switchover**] **shmlib**

Purpose

Enables the generation of debug messages for the shared memory library.

Command Mode

exec (10)

Syntax Description

boot	Optional. Enables the generation of debug messages during a system reload.
active	Enables the generation of debug messages for the active controller card.
standby	Enables the generation of debug messages for the standby controller card.
switchover	Optional. Enables the generation of debug messages during a switchover from the active to the standby controller.

Default

The generation of debug messages for the shared memory library is disabled.

Usage Guidelines

Use the **debug shmlib** command to enable the generation of debug messages for the shared memory library.

Caution Risk of performance loss. Enabling the generation of debug messages can severely affect system performance. To reduce the risk, exercise caution when enabling the generation of any debug messages on a production system.

Use the **boot active** or **boot standby** construct to enable debugging messages during a system reload for the active or standby controller card, respectively.

Use the **switchover** keyword to enable debugging messages while the system is switching from the active to the standby controller card.

To store debug messages in the system log buffer, use the **logging debug** command (in global configuration mode). Use the **show log** command (in exec mode) to display these stored debug messages.

To display messages in real time, use the **logging console** command (in context configuration mode) if you are connected to the system through the console port. Or, use the **terminal monitor** command (in exec mode) if you are connected to the system through a Telnet or Secure Shell (SSH) session.

Note For more information about the **logging** commands, see the "Logging Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS. For information about the **terminal monitor** command, see Chapter 4, "Session Operations."

Use the **no** form of this command to disable the generation of debug messages.

Examples

The following example enables the generation of debug messages for shared memory library events:

```
[local]Redback#debug shmlib
```

Related Commands

show log

debug snmp

debug [**boot** {**active** | **standby**} | **switchover**] **snmp** {**all** | **general** | **packet** | **pdu**}

no debug [**boot** {**active** | **standby**} | **switchover**] **snmp** {**all** | **general** | **packet** | **pdu**}

Purpose

Enables the generation of Simple Network Management Protocol (SNMP) debug messages.

Command Mode

exec (10)

Syntax Description

boot	Optional. Enables the generation of debug messages during a system reload.
active	Enables the generation of debug messages for the active controller card.
standby	Enables the generation of debug messages for the standby controller card.
switchover	Optional. Enables the generation of debug messages during a switchover from the active to the standby controller.
all	Enables the generation of debug messages for all SNMP events.
general	Enables the generation of debug messages for general SNMP events.
packet	Enables the generation of debug messages for SNMP packets.
pdu	Enables the generation of debug messages for the protocol data unit (PDU) field in SNMP packets.

Default

The generation of debug messages for SNMP is disabled.

Usage Guidelines

Use the **debug snmp** command to enable the generation of SNMP debug messages.

Caution Risk of performance loss. Enabling the generation of debug messages can severely affect system performance. To reduce the risk, exercise caution when enabling the generation of any debug messages on a production system.

Use the **boot active** or **boot standby** construct to enable debugging messages during a system reload for the active or standby controller card, respectively.

Use the **switchover** keyword to enable debugging messages while the system is switching from the active to the standby controller card.

To store messages in the system log buffer, use the **logging debug** command (in global configuration mode). Use the **show log** command (in exec mode) to display these stored messages.

To display messages in real time, use the **logging console** command (in context configuration mode) if you are connected to the system through the console port. Or, use the **terminal monitor** command (in exec mode) if you are connected to the system through a Telnet or Secure Shell (SSH) session.

Note For more information about the **logging** commands, see the "Logging Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS. For information about the **terminal monitor** command, see Chapter 4, "Session Operations."

Use the **no** form of this command to disable the generation of SNMP debug messages.

Examples

The following example displays all categories of debug information for SNMP and enables the SNMP server:

```
[local]Redback#debug snmp all
[local]Redback#config
[local]Redback(config)#snmp server
[local]Redback(config)#exit
[local]Redback#

Jun 26 11:06:29: %SNMP-7-GEN: snmp process is ALIVE
Jun 26 11:06:29: %SNMP-7-GEN: snmp ready to receive packets
```

Related Commands

show log

debug sysmon ftp

debug [**boot** {**active** | **standby**} | **switchover**] **sysmon ftp**

no debug [**boot** {**active** | **standby**} | **switchover**] **sysmon ftp**

Purpose

Enables the generation of debug messages related to transferring crash files out of the SmartEdge router using File Transfer Protocol (FTP).

Command Mode

exec (10)

Syntax Description

boot	Optional. Enables the generation of debug messages during a system reload.
active	Enables the generation of debug messages for the active controller card.
standby	Enables the generation of debug messages for the standby controller card.
switchover	Optional. Enables the generation of debug messages during a switchover from the active to the standby controller.

Default

The generation of debug messages related to transferring crash files out of the SmartEdge router using FTP is disabled.

Usage Guidelines

Use the **debug sysmon ftp** command to enable the generation of debug messages related to transferring crash files out of the SmartEdge router using FTP.

Caution Risk of performance loss. Enabling the generation of debug messages can severely affect system performance. To reduce the risk, exercise caution when enabling the generation of any debug messages on a production system.

Use the **boot active** or **boot standby** construct to enable debugging messages during a system reload for the active or standby controller card, respectively.

Use the **switchover** keyword to enable debugging messages while the system is switching from the active to the standby controller card.

To store debug messages in the system log buffer, use the **logging debug** command (in global configuration mode). Use the **show log** command (in exec mode) to display these stored debug messages.

To display messages in real time, use the **logging console** command (in context configuration mode) if you are connected to the system through the console port. Or, use the **terminal monitor** command (in exec mode) if you are connected to the system through a Telnet or Secure Shell (SSH) session.

Note For more information about the **logging** commands, see the "Logging Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS. For information about the **terminal monitor** command, see Chapter 4, "Session Operations."

Use the **no** form of this command to disable the generation of debug messages.

Examples

The following example enables all system monitoring debugging messages:

```
[local]Redback#debug sysmon ftp
```

Related Commands

show debugging
show log

monitor ip

monitor ip route summary

Purpose

Monitors the current status of IP processes and provides continuous updates to the status.

Command Mode

exec

Syntax Description

route	Specifies that Routing Information Base (RIB) information is to be monitored.
summary	Specifies that summaries of all routes are to be provided.

Default

None

Usage Guidelines

Use the **monitor ip** command to monitor the current status of IP processes and to provide periodic updates on status changes.

Press **Ctrl**+**C** to exit monitoring mode.

Examples

The following example enables monitoring of the RIB process and provides status for the process:

```
[local]Redback>monitor ip route summary

Rt Tbl Version:      765133, Nh Tbl Version: 19580
FIB Rt Tbl Version:  765133
Route Source                Tot-Routes     Act-Routes  Max Ever Reached

Connected                            5              5               5
Static                               3              3               3
Isis-Level 1                        34             30              76
Isis-Level 2                        17             17              59
Ospf-IntraArea                       7              3               7
IBGP                             19122          19122           20293
EBGP                             82165          82165          101511

% enter ctrl-C to exit monitor mode, monitor duration(sec): 600    (00:00:10)
```

Related Commands

monitor process

monitor process

monitor process [*proc-name*] [**crash-info** | **detail**]

Purpose

Monitors the current status of a specified category of processes, and provides continuous updates to the status.

Command Mode

exec

Syntax Description

proc-name	Optional. Process that you want to monitor. The *proc-name* argument can be any one of the keywords listed in Table 7-9.
crash-info	Optional. Specifies that process crash information is to be monitored.
detail	Optional. Specifies that detailed process information is to be displayed.

Default

Monitors all processes and displays summary information if no optional keywords are specified.

Usage Guidelines

Use the **monitor process** command to monitor the current status of system processes and to provide periodic updates on status changes. Table 7-9 lists the keywords for the processes supported by this command.

Table 7-9 Keywords for Processes

Keyword	Process
aaad	Authentication, authorization, and accounting (AAA) process
arp	Address Resolution Protocol (ARP) process
atm	Asynchronous Transfer Mode (ATM) process
bgp	Border Gateway Protocol (BGP) process
bridge	Bridge process
clips	Clientless IP service selection process
cls	Classifier Manager process
csm	Controller State Manager (CSM) process
dhcp	DHCP relay/proxy process
dhelperd	DHCP Helper daemon
dlm	Download Manager (DLM) process

Table 7-9 Keywords for Processes *(continued)*

Keyword	Process
dns	Domain Name System (DNS) process
dot1q	8021Q encapsulation process
fr	Frame Relay process
hr	HTTP redirect process
igmp	Internet Group Management Protocol (IGMP) process
isis	Intermediate System-to-Intermediate System (IS-IS) process
ism	Interface and Circuit State Manager (ISM) process
l2tp	Layer 2 Tunneling Protocol (L2TP) process
ldp	Label Distribution Protocol process
lg	Link group (LG) process
lm	Label Manager (LM) process
mpls_static	Multiprotocol label switching (MPLS) static process
msdp	Multicast Source Discovery Protocol (MSDP) process
nat	IP Network Address Translation process
netopd	NetOp process daemon
ntp	Network Time Protocol (NTP) process
odd	On-demand diagnostics (ODD) process
ospf	Open Shortest Path First (OSPF) protocol process
ospf3	Open Shortest Path First Version 3 (OSPF3) protocol process
ped_parse	Process execution descriptor (PED) parse process
pem	Privacy-enhanced mail (PEM) process
pim	Protocol Independent Multicast (PIM) process
ppaslog	Packet Processing ASIC (PPA) syslog (SLOG) process
ppp	Point-to-Point Protocol (PPP) process
pppoe	PPP over Ethernet (PPPoE) process
qos	Quality of service (QoS) process
rcm	Router Configuration Manager (RCM) process
rib	Routing Information Base (RIB) process
rip	Routing Information Protocol (RIP) process
rpm	Routing Policy Manager (RPM) process
rsvp	Resource Reservation Protocol Traffic Engineering (RSVP-TE) process
snmp	Simple Network Management Protocol (SNMP) process
static	Static routing process
stats	Statistics process

Table 7-9 Keywords for Processes *(continued)*

Keyword	Process
sysmon	System monitor process
tunnel	Tunnel management process
vrrp	Virtual Router Redundancy Protocol (VRRP) process
xcd	Cross-connect process daemon

Updates occur every two seconds. Monitoring continues for the number of seconds specified by the **monitor duration** command (in global configuration mode). The default duration is 600 seconds.

Use the **monitor process** command without any keywords to monitor all system processes, or use the appropriate keyword to monitor a specific category of processes.

Press **Ctrl**+**C** to exit monitoring mode.

Examples

The following example enables monitoring of the RIP process and provides status for the process:

```
[local]Redback>monitor process rip

% enter ctrl-C to exit monitor mode, monitor duration(sec): 5600 (00:00:08)

NAME          PID    SPAWN      MEMORY  TIME         %CPU   STATE
rip           12652      1      576K    00:00:00.02  0.00%  run
```

Related Commands

show process

no debug all

no debug all

Purpose

Disables the generation of all debug message types supported by the SmartEdge OS.

Command Mode

exec (10)

Syntax Description

This command has no keywords or arguments.

Default

Debugging is disabled.

Usage Guidelines

Use the **no debug all** command to disable the generation of all debug messages. The functions of the **debug** commands, listed in Table 7-10, are disabled by the **no debug all** command.

Table 7-10 Related Debug Commands

Feature	Command
General system processes	**debug rcm**, **debug snmp**, **debug ssh**
IP routing	**debug ip routing**, **debug isis all**, **debug ospf**, **debug policy general**, **debug rip**, **debug vrrp**
BGP routing	**debug bgp event**, **debug bgp listen**, **debug bgp message**, **debug bgp policy**, **debug bgp rib**, **debug bgp session-state**, **debug bgp update**
IP services	**debug arp**, **debug dhcp-relay**, **debug ip dns**, **debug nat**, **debug ntp**
Quality of service	**debug qos**
Access control lists	**debug cls**, **debug ip-access-list**
Authentication	**debug aaa**

Examples

The following example disables the generation of all debugging messages:

```
[local]Redback#no debug all
```

Related Commands

show log

ping

ping {*ip-addr*} [*number-of-packets*] [**df**] [**flood**] [**numeric**] [**pattern** *hex-pattern*] [**preload**] [**quiet**] [**record**] [**silent**] [**size** *bytes*] [**src** *ip-addr*] [**timeout** *seconds*] [**tos**] [**ttl**] [**verbose**]

Purpose

Tests whether the host is reachable.

Command Mode

exec

Syntax Description

ip-addr	IP address of the host.
number-of-packets	Optional. Number of ping packets to send. The range of values is 1 to 214,748,364; the default value is 5.
df	Optional. Indicates that the packet should not be fragmented in the IP header.
flood	Optional. Floods ping packets.
numeric	Optional. Specifies numeric output only.
pattern *hex-pattern*	Optional. Hex pattern to fill in Internet Control Message Protocol (ICMP) packets. The range of values is 0x0 to 0xffffffff.
preload	Optional. Sends packets as quickly as possible.
quiet	Optional. Suppresses ICMP error messages.
record	Optional. Specifies that the RECORD_ROUTE option is to be included in the ECHO_REQUEST packet.
silent	Optional. Displays only summary lines at start up.
size *bytes*	Optional. Size, in bytes, of the IP datagram. The range of values is 10 to 2,000; the default value is 56.
src *ip-addr*	Optional. Source IP address.
timeout *seconds*	Optional. Amount of time, in seconds, that the system waits for a response for each ping packet. The range of values is 1 to 120; the default value is 120.
tos	Optional. Specifies the type of service (ToS) in hex. The range of values is 0x0 to 0xff; the default value is 0.
ttl	Optional. Specifies the time-to-live (TTL) value. The range of values is 1 to 255; the default value is 255.
verbose	Optional. Enables all possible output.

Default

Sends 56-byte packets to the specified host, using a timeout value of one second.

Usage Guidelines

Use the **ping** command (in exec mode) to test whether the host is reachable.

Press **Ctrl+C** to stop a ping test.

The **ping** and **traceroute** commands (in exec mode) can have vastly different output, depending on the context in which the commands are issued. In particular, an IP address that can be reached by the **ping** or **traceroute** command in one context might not be reachable from another context. Use the **context** command (in exec mode) to switch between contexts.

Use the **ping atm** command (in exec mode) to test Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs) by sending operations, administration, and maintenance (OAM) loopback cells. This command tests the reachability of a neighboring ATM switch or the end of an ATM connection. For more information on **ping atm** command (in exec mode) command, see the "Circuit Operations" chapter in the *Ports, Circuits, and Tunnels Operations Guide* for the SmartEdge OS.

Note To test an ATM PVC by sending OAM loopback cells, use the **ping atm** command (in exec mode).

Table 7-11 lists the characters for the ICMP errors that can be displayed in the output and the error descriptions.

Table 7-11 ICMP Error and Message Code Descriptions

Character	ICMP Error and Message Code Description
!	No error
?	Unknown error code
a	Host access prohibited
A	Network access prohibited
c	Precedence cutoff
C	Communication prohibited
d	Router solicitation
D	Router Advertisement
F	Unreachable because packet requires fragmentation, but "Don't Fragment" bit is set
F	Time-to-live exceeded in reassembly
h	Host isolated
H	Host unknown
i	Information reply
I	Information request
L	Time-to-live exceeded in transmission
m	Timestamp reply
M	Timestamp

Table 7-11 ICMP Error and Message Code Descriptions *(continued)*

Character	ICMP Error and Message Code Description
n	Network unknown
N	Network unreachable
p	Port unreachable
P	Protocol unreachable
Q	Packet lost due to traffic congestion
r	Redirected by host
R	Redirected by network
S	Unreachable because source route failed
t	Bad ToS for host
t	Redirected by host because of ToS
T	Bad ToS for network
T	Redirected by network because of ToS
U	Host unreachable
V	Host precedence violation
x	Address mask reply
X	Address mask request
Z	ICMP parameter problem

Examples

The following example sends five ping packets to host `10.1.1.1` from `10.1.1.2`:

```
[local]Redback>ping 10.1.1.1

PING 10.1.1.1 (10.1.1.1): source 10.1.1.2, 56 data bytes,
timeout is 1 second
.!!!!
----10.1.1.1 PING Statistics----
5 packets transmitted, 4 packets received, 20.0% packet loss
round-trip min/avg/max/stddev = 0.000/0.000/0.000/0.000 ms
```

Related Commands

context
show icmp statistics
traceroute

process coredump

process coredump *proc-name* [*proc-id*]

Purpose

Initiates a core dump for the specified process and saves it in a crash file.

Command Mode

exec (10)

Syntax Description

proc-name	Process name for which a core dump is to be generated. Can be any one of the keywords listed in Table 7-12.
proc-id	Optional. Identification number for the process. The range of values is 1 to 65,535.

Default

None

Usage Guidelines

Use the **process coredump** command to initiate a core dump for the specified process and save it in a crash file.

Caution Risk of data loss. This command causes the specified process to be interrupted for a brief period, 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 enter this command for a process unless the loss of data will not impact current traffic.

Table 7-12 lists the keywords for the processes supported by this command.

Table 7-12 Keywords for Processes

Keyword	Process
aaad	Authentication, authorization, and accounting (AAA) process
arp	Address Resolution Protocol (ARP) process
atm	Asynchronous Transfer Mode (ATM) process
bgp	Border Gateway Protocol (BGP) process
bridge	Bridge process
clips	Clientless IP service selection process
cls	Classifier Manager process
csm	Controller State Manager (CSM) process
dhcp	DHCP relay/proxy process

Table 7-12 Keywords for Processes *(continued)*

Keyword	Process
dhelperd	DHCP Helper daemon
dlm	Download Manager (DLM) process
dns	Domain Name System (DNS) process
dot1q	8021Q encapsulation process
fr	Frame Relay process
hr	HTTP redirect process
igmp	Internet Group Management Protocol (IGMP) process
isis	Intermediate System-to-Intermediate System (IS-IS) process
ism	Interface and Circuit State Manager (ISM) process
l2tp	Layer 2 Tunneling Protocol (L2TP) process
ldp	Label Distribution Protocol process
lg	Link group (LG) process
lm	Label Manager (LM) process
mpls_static	Multiprotocol label switching (MPLS) static process
msdp	Multicast Source Discovery Protocol (MSDP) process
nat	IP Network Address Translation process
netopd	NetOp process daemon
ntp	Network Time Protocol (NTP) process
odd	On-demand diagnostics (ODD) process
ospf	Open Shortest Path First (OSPF) protocol process
ospf3	Open Shortest Path First Version 3 (OSPF3) protocol process
ped_parse	Process execution descriptor (PED) parse process
pem	Privacy-enhanced mail (PEM) process
pim	Protocol Independent Multicast (PIM) process
ppaslog	Packet Processing ASIC (PPA) syslog (SLOG) process
ppp	Point-to-Point Protocol (PPP) process
pppoe	PPP over Ethernet (PPPoE) process
qos	Quality of service (QoS) process
rcm	Router Configuration Manager (RCM) process
rib	Routing Information Base (RIB) process
rip	Routing Information Protocol (RIP) process
rpm	Routing Policy Manager (RPM) process
rsvp	Resource Reservation Protocol Traffic Engineering (RSVP-TE) process
snmp	Simple Network Management Protocol (SNMP) process

Table 7-12 Keywords for Processes *(continued)*

Keyword	Process
static	Static routing process
stats	Statistics process
sysmon	System monitor process
tunnel	Tunnel management process
vrrp	Virtual Router Redundancy Protocol (VRRP) process

The crash file (*proc-name*[*proc-id*].core) is placed in the /md directory in the /flash partition, or when a mass-storage device is included in the system, in the mass-storage device /md directory.

Note We strongly recommend that you configure the system to upload crash files automatically to a remote File Transfer Protocol (FTP) server, using the **service upload-coredump** command (in global configuration mode). By configuring this service, you maximize the use of available disk space and improve system stability and performance. For more information about the **service upload-coredump** command (in global configuration mode), see the "System-Wide Management Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

Note This command is used to provide troubleshooting information to the Redback technical support group.

Examples

The following example initiates a core dump and creates a crash file for the BGP process:

```
[local]Redback#process coredump bgp
```

Related Commands

show crashfiles
show process

process restart

process restart *proc-name* [*delay*]

Purpose

Restarts a process that has been stopped.

Command Mode

exec (10)

Syntax Description

proc-name	Process to be restarted. Can be any one of the keywords listed in Table 7-13.
delay	Optional. Delay, in seconds, before a process is restarted. The range of values is 0 to 4,294,967,295; the default value is 2.

Default

The default for the optional delay is two seconds.

Usage Guidelines

Use the **process restart** command to restart a process that has been stopped. Table 7-13 lists the keywords for the processes supported by this command.

Table 7-13 Keywords for Processes

Keyword	Process
aaad	Authentication, authorization, and accounting (AAA) process
arp	Address Resolution Protocol (ARP) process
atm	Asynchronous Transfer Mode (ATM) process
bgp	Border Gateway Protocol (BGP) process
bridge	Bridge process
clips	Clientless IP service selection process
cls	Classifier Manager process
csm	Controller State Manager (CSM) process
dhcp	DHCP relay/proxy process
dhelperd	DHCP Helper daemon
dlm	Download Manager (DLM) process
dns	Domain Name System (DNS) process
dot1q	8021Q encapsulation process
fr	Frame Relay process

Table 7-13 Keywords for Processes *(continued)*

Keyword	Process
hr	HTTP redirect process
igmp	Internet Group Management Protocol (IGMP) process
isis	Intermediate System-to-Intermediate System (IS-IS) process
ism	Interface and Circuit State Manager (ISM) process
l2tp	Layer 2 Tunneling Protocol (L2TP) process
ldp	Label Distribution Protocol process
lg	Link group (LG) process
lm	Label Manager (LM) process
mpls_static	Multiprotocol label switching (MPLS) static process
msdp	Multicast Source Discovery Protocol (MSDP) process
nat	IP Network Address Translation process
netopd	NetOp process daemon
ntp	Network Time Protocol (NTP) process
odd	On-demand diagnostics (ODD) process
ospf	Open Shortest Path First (OSPF) protocol process
ospf3	Open Shortest Path First Version 3 (OSPF3) protocol process
ped_parse	Process execution descriptor (PED) parse process
pem	Privacy-enhanced mail (PEM) process
pim	Protocol Independent Multicast (PIM) process
ppaslog	Packet Processing ASIC (PPA) syslog (SLOG) process
ppp	Point-to-Point Protocol (PPP) process
pppoe	PPP over Ethernet (PPPoE) process
qos	Quality of service (QoS) process
rcm	Router Configuration Manager (RCM) process
rib	Routing Information Base (RIB) process
rip	Routing Information Protocol (RIP) process
rpm	Routing Policy Manager (RPM) process
rsvp	Resource Reservation Protocol Traffic Engineering (RSVP-TE) process
snmp	Simple Network Management Protocol (SNMP) process
static	Static routing process
stats	Statistics process
sysmon	System monitor process
tunnel	Tunnel management process
vrrp	Virtual Router Redundancy Protocol (VRRP) process

Table 7-13 Keywords for Processes *(continued)*

Keyword	Process
xcd	Cross-connect process daemon

Examples

The following example restarts the BGP process after a five-minute (**300** seconds) delay:

```
[local]Redback#process restart bgp 300
```

Related Commands

process set
show process

process set

process set *proc-name* {**heart-beat** {**on** | **off**} | **kill-time** *seconds* | **max-crashes** *num-crashes* [**within** *seconds*] | **spawn-time** [*seconds*]}

Purpose

Sets process management parameters.

Command Mode

exec (10)

Syntax Description

proc-name	Process for which you are setting management parameters. Can be any one of the keywords listed in Table 7-14.
heart-beat	Specifies that a heartbeat setting follows.
on	Turns the process heartbeat on.
off	Turns the process heartbeat off.
kill-time *seconds*	Number of seconds from issuing the **process set** command after which the Process Manager (PM) kills the specified process. The range of values is 1 to 429,496,729.
max-crashes *num-crashes*	Maximum number of crashes allowed within the time interval specified by the **within** *seconds* construct. The range of values is 0 to 10; the default value is 5.
within *seconds*	Optional. Number of seconds within which the maximum number of crashes is allowed. If not specified, the system uses the default value of 86,400 (24 hours).
spawn-time	Specifies that a spawn time setting follows. If used without the optional *seconds* argument, sets the spawn time to the default value of two seconds.
seconds	Optional with the **spawn-time** keyword. Number of seconds delay between the crash of a process and the subsequent spawn by the Process Manager (PM). The range of values is 1 to 300; the default value is 2.

Default

The heartbeat is on; the maximum number of crashes allowed is five per process within a 24 hour period; the spawn time is two seconds.

Usage Guidelines

Use the **process set** command to set process management parameters including whether the heartbeat is turned on or off, the kill time, the maximum number of crashes allowed within a configurable period of time, and the amount of time between the crash of a process and the subsequent spawn by the PM (spawn time).

Table 7-14 lists the keywords for the processes supported by this command.

Table 7-14 Keywords for Processes

Keyword	Process
aaad	Authentication, authorization, and accounting (AAA) process
arp	Address Resolution Protocol (ARP) process
atm	Asynchronous Transfer Mode (ATM) process
bgp	Border Gateway Protocol (BGP) process
bridge	Bridge process
clips	Clientless IP service selection process
cls	Classifier Manager process
csm	Controller State Manager (CSM) process
dhcp	DHCP relay/proxy process
dhelperd	DHCP Helper daemon
dlm	Download Manager (DLM) process
dns	Domain Name System (DNS) process
dot1q	8021Q encapsulation process
fr	Frame Relay process
hr	HTTP redirect process
igmp	Internet Group Management Protocol (IGMP) process
isis	Intermediate System-to-Intermediate System (IS-IS) process
ism	Interface and Circuit State Manager (ISM) process
l2tp	Layer 2 Tunneling Protocol (L2TP) process
ldp	Label Distribution Protocol process
lg	Link group (LG) process
lm	Label Manager (LM) process
mpls_static	Multiprotocol label switching (MPLS) static process
msdp	Multicast Source Discovery Protocol (MSDP) process
nat	IP Network Address Translation process
netopd	NetOp process daemon
ntp	Network Time Protocol (NTP) process
odd	On-demand diagnostics (ODD) process
ospf	Open Shortest Path First (OSPF) protocol process
ospf3	Open Shortest Path First Version 3 (OSPF3) protocol process
ped_parse	Process execution descriptor (PED) parse process
pem	Privacy-enhanced mail (PEM) process

Table 7-14 Keywords for Processes *(continued)*

Keyword	Process
pim	Protocol Independent Multicast (PIM) process
ppaslog	Packet Processing ASIC (PPA) syslog (SLOG) process
ppp	Point-to-Point Protocol (PPP) process
pppoe	PPP over Ethernet (PPPoE) process
qos	Quality of service (QoS) process
rcm	Router Configuration Manager (RCM) process
rib	Routing Information Base (RIB) process
rip	Routing Information Protocol (RIP) process
rpm	Routing Policy Manager (RPM) process
rsvp	Resource Reservation Protocol Traffic Engineering (RSVP-TE) process
snmp	Simple Network Management Protocol (SNMP) process
static	Static routing process
stats	Statistics process
sysmon	System monitor process
tunnel	Tunnel management process
vrrp	Virtual Router Redundancy Protocol (VRRP) process
xcd	Cross-connect process daemon

The heartbeat is a message that each process sends to the PM to identify itself as an active process. If the heartbeat ceases, the PM considers the process a candidate for automatic restart. It can be useful for debugging processes to turn the heartbeat off so that a hung process is not restarted automatically by the PM.

Examples

The following example sets process management parameters for the BGP process:

```
[local]Redback#process set bgp kill-time 100
[local]Redback#process set bgp max-crashes 3 within 43200
[local]Redback#process set bgp spawn-time 10
```

Related Commands

process restart
show process

process start

process start *proc-name*

Purpose

Instructs the Process Manager (PM) to start the specified process.

Command Mode

exec (10)

Syntax Description

proc-name Process to be started. The *proc-name* argument can be any one of the keywords listed in Table 7-15.

Default

None

Usage Guidelines

Use the **process start** command to instruct the PM to start the specified process. Table 7-15 lists the keywords for the processes supported by this command.

Table 7-15 Keywords for Processes

Keyword	Process
aaad	Authentication, authorization, and accounting (AAA) process
arp	Address Resolution Protocol (ARP) process
atm	Asynchronous Transfer Mode (ATM) process
bgp	Border Gateway Protocol (BGP) process
bridge	Bridge process
clips	Clientless IP service selection process
cls	Classifier Manager process
csm	Controller State Manager (CSM) process
dhcp	DHCP relay/proxy process
dhelperd	DHCP Helper daemon
dlm	Download Manager (DLM) process
dns	Domain Name System (DNS) process
dot1q	8021Q encapsulation process
fr	Frame Relay process
hr	HTTP redirect process

Table 7-15 Keywords for Processes *(continued)*

Keyword	Process
igmp	Internet Group Management Protocol (IGMP) process
isis	Intermediate System-to-Intermediate System (IS-IS) process
ism	Interface and Circuit State Manager (ISM) process
l2tp	Layer 2 Tunneling Protocol (L2TP) process
ldp	Label Distribution Protocol process
lg	Link group (LG) process
lm	Label Manager (LM) process
mpls_static	Multiprotocol label switching (MPLS) static process
msdp	Multicast Source Discovery Protocol (MSDP) process
nat	IP Network Address Translation process
netopd	NetOp process daemon
ntp	Network Time Protocol (NTP) process
odd	On-demand diagnostics (ODD) process
ospf	Open Shortest Path First (OSPF) protocol process
ospf3	Open Shortest Path First Version 3 (OSPF3) protocol process
ped_parse	Process execution descriptor (PED) parse process
pem	Privacy-enhanced mail (PEM) process
pim	Protocol Independent Multicast (PIM) process
ppaslog	Packet Processing ASIC (PPA) syslog (SLOG) process
ppp	Point-to-Point Protocol (PPP) process
pppoe	PPP over Ethernet (PPPoE) process
qos	Quality of service (QoS) process
rcm	Router Configuration Manager (RCM) process
rib	Routing Information Base (RIB) process
rip	Routing Information Protocol (RIP) process
rpm	Routing Policy Manager (RPM) process
rsvp	Resource Reservation Protocol Traffic Engineering (RSVP-TE) process
snmp	Simple Network Management Protocol (SNMP) process
static	Static routing process
stats	Statistics process
sysmon	System monitor process
tunnel	Tunnel management process
vrrp	Virtual Router Redundancy Protocol (VRRP) process
xcd	Cross-connect process daemon

Examples

The following example starts the BGP process:

```
[local]Redback#process start bgp
```

Related Commands

process stop
show process

process stop

process stop *proc-name*

Purpose

Stops the specified process.

Command Mode

exec (10)

Syntax Description

proc-name	Process to be stopped. The *proc-name* argument can be any one of the keywords listed in Table 7-16.

Default

None

Usage Guidelines

Use the **process stop** command to the specified process. Table 7-16 lists the keywords for the processes supported by this command.

Table 7-16 Keywords for Processes

Keyword	Process
aaad	Authentication, authorization, and accounting (AAA) process
arp	Address Resolution Protocol (ARP) process
atm	Asynchronous Transfer Mode (ATM) process
bgp	Border Gateway Protocol (BGP) process
bridge	Bridge process
clips	Clientless IP service selection process
cls	Classifier Manager process
csm	Controller State Manager (CSM) process
dhcp	DHCP relay/proxy process
dhelperd	DHCP Helper daemon
dlm	Download Manager (DLM) process
dns	Domain Name System (DNS) process
dot1q	8021Q encapsulation process
fr	Frame Relay process
hr	HTTP redirect process

Table 7-16 Keywords for Processes *(continued)*

Keyword	Process
igmp	Internet Group Management Protocol (IGMP) process
isis	Intermediate System-to-Intermediate System (IS-IS) process
ism	Interface and Circuit State Manager (ISM) process
l2tp	Layer 2 Tunneling Protocol (L2TP) process
ldp	Label Distribution Protocol process
lg	Link group (LG) process
lm	Label Manager (LM) process
mpls_static	Multiprotocol label switching (MPLS) static process
msdp	Multicast Source Discovery Protocol (MSDP) process
nat	IP Network Address Translation process
netopd	NetOp process daemon
ntp	Network Time Protocol (NTP) process
odd	On-demand diagnostics (ODD) process
ospf	Open Shortest Path First (OSPF) protocol process
ospf3	Open Shortest Path First Version 3 (OSPF3) protocol process
ped_parse	Process execution descriptor (PED) parse process
pem	Privacy-enhanced mail (PEM) process
pim	Protocol Independent Multicast (PIM) process
ppaslog	Packet Processing ASIC (PPA) syslog (SLOG) process
ppp	Point-to-Point Protocol (PPP) process
pppoe	PPP over Ethernet (PPPoE) process
qos	Quality of service (QoS) process
rcm	Router Configuration Manager (RCM) process
rib	Routing Information Base (RIB) process
rip	Routing Information Protocol (RIP) process
rpm	Routing Policy Manager (RPM) process
rsvp	Resource Reservation Protocol Traffic Engineering (RSVP-TE) process
snmp	Simple Network Management Protocol (SNMP) process
static	Static routing process
stats	Statistics process
sysmon	System monitor process
tunnel	Tunnel management process
vrrp	Virtual Router Redundancy Protocol (VRRP) process
xcd	Cross-connect process daemon

Caution Risk of data loss. This command causes the specified process to terminate and the services provided by the process to become unavailable until the process is restarted using the **process start** command. To reduce the risk, do not issue this command unless you intend to restart the process immediately.

Examples

The following example stops the BGP process:

```
[local]Redback#process stop bgp
```

Related Commands

process start
show process

reload

reload

Purpose

Reloads the system software on the active controller card first, and then reloads the standby controller card.

Command Mode

exec (15)

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **reload** command to reload the system software on the active controller card first, and then to reload the standby controller card. When you enter this command, the system performs minimal housekeeping, then reloads as if powered off and then powered on again. The system prompts you to confirm the reload. Type **y** to proceed with the reload, or **n** to cancel the reload.

Examples

The following example reloads the system software on the active controller card first, and then reloads the standby controller card:

```
[local]Redback#reload
```

Related Commands

reload standby
reload switch-over

reload standby

reload standby

Purpose

Reloads the system software on the standby controller card only.

Command Mode

exec (15)

Syntax Description

This command has no keywords or arguments.

Usage Guidelines

Use the **reload** standby command to reload the system software on the standby controller card only.

Examples

The following example reloads the system software on the standby controller card:

```
[local]Redback#reload standby
```

Related Commands

reload
reload switch-over

reload switch-over

reload switch-over

Purpose

Reloads the system software on the active controller card and, if the standby controller card is ready, causes the standby to become the active controller card.

Command Mode

exec (15)

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **reload switch-over** command to reload the system software on the active controller card, and if the standby controller card is ready, causes the standby to become the active controller card.

If the standby is not ready, this command performs the same function as the **reload** command. Both controller cards are reloaded and the current active controller card remains active.

Examples

The following example reloads the system software on the active controller card, and if the standby controller card is ready, causes the standby to become the active controller card:

```
[local]Redback#reload switch-over
```

Related Commands

reload
reload standby

save log

save log [*text*] *filename* [**-noconfirm**]

Purpose

Saves one of the internal event log buffers to the flash file system.

Command Mode

exec (10)

Syntax Description

text	Optional. Event log is saved in plain text. Default form is in binary if this argument is not specified.
filename	Name of the file to which log entries are to be saved. Local filename is specified. If the full path is not specified, the default directory is /flash.
-noconfirm	Optional. Overwrites the specified filename if it already exits without user confirmation.

Default

None

Usage Guidelines

Use the **save log** command to save one of the internal event log buffers to the flash file system for later examination.

To examine the debugging messages, use the **logging debug** command (in global configuration mode); to save the messages prior to examining them, use the **save log** command. You can use the **logging filter** command (in context configuration mode) to specify different levels of logging filters.

For more information about the **logging debug** and **logging filter** commands, see the "Logging Configuration" chapter in the *Basic System Configuration Guide* for the SmartEdge OS.

Examples

The following example saves a copy of the log to the file, `log.sav`, in the /flash directory:

```
[local]Redback>save log log.sav
```

Related Commands

None

save seos-core

save seos-core

Purpose

Saves a previously written core dump of the operating system to the mass-storage device in the /md partition.

Command Mode

exec (10)

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **save seos-core** command to save a core dump, which the operating system kernel has previously written to the swap partition on the mass-storage device, to the /md partition on the same device; the SmartEdge router must have a mass-storage device installed to use this command.

Either controller card can detect a problem and cause its kernel to dump an image of the running operating system on its mass-storage device. When you enter this command, you must be using a command-line interface (CLI) running on that same controller card to allow the command to access the core dump in the swap partition. For example, if the controller card that wrote the core dump has become the standby controller after reloading the operating system, you must connect to the local console for the standby controller card; if it was the active controller card, you can access the CLI from either the local console or the management port. Logging messages identify the controller card that wrote the core dump to the swap partition.

This command saves the core dump in two crash files. The filenames for these files, netbsd.0.core.gz and netbsd.0.gz, are fixed; however, you can rename the files after the save operation is complete. If you rename the files, we recommend that you add only the date to the filenames to ensure that “core” remains in the filename for the netbsd.0.core.gz file.

Note The files created by this command are useful only for the Redback Technical Assistance Center (TAC) when troubleshooting the problem that caused the core dump.

Examples

The following example saves a core dump of the operating system to two crash files in the /md partition on the mass-storage device of the active controller card and renames them to include the date of the core dump:

```
[local]Redback#save seos-core

dumplo = 89128960 (174080 * 512)
savecore:  number read 512 value of magic on disk is 76910538
savecore: newdumpmag: 4958fca
savecore: dumpsize is 91003972
savecore: /md/bounds: No such file or directory
savecore: writing compressed core to /md/netbsd.0.core.gz
savecore: total output bytes(uncompressed):442499072
savecore: writing compressed kernel to /md/netbsd.0.gz

[local]Redback#rename /md/netbsd.0.core.gz /md/netbsd031002.0.core.gz
[local]Redback#rename /md/netbsd.0.gz /md/netbsd031002.0.gz
```

Related Commands

show crashfiles

show bulkstats

show bulkstats policy *bulk-pol-name* [**collection**]

Purpose

Displays the bulk statistics (bulkstats) configuration information and data transfer statistics, or the contents of the current collection file that have not yet been successfully transferred to the receiver, for the specified bulkstats policy.

Command Mode

all modes

Syntax Description

policy *bulk-pol-name*	Name of the bulkstats policy for which bulkstats configuration information and statistics are to be displayed.
collection	Optional. Specifies that the contents of the collection file for the specified policy in its current state is to be shown, rather than the configuration.

Default

Displays bulkstats configuration information for the specified policy.

Usage Guidelines

Use the **show bulkstats** command to display the current bulkstats configuration information and statistics about the data transfer for the specified policy, including:

- IP address of primary receiver
- IP address of secondary receiver
- Transfer mechanism to primary receiver
- Transfer mechanism to secondary receiver
- Time of last successful transfer
- Size (in bytes) of last transferred bulkstats collection file
- IP address of receiver for last successful transfer
- Time of last attempted transfer
- Time of next transfer

Use the optional **collection** keyword to display the contents of the current bulkstats collection file. This can be useful in debugging schema definitions.

Note The contents of a collection file for a policy can be viewed only when bulkstats collection for that policy is disabled.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays bulk statistics information:

```
[local]Redback>show bulkstats policy bulk

Primary receiver: 198.168.145.99 via ftp
Secondary receiver: 198.168.147.31 via ftp
Last successful transfer to 198.168.145.99 on WED JUN 29 14:55:03 2005
Transferred 1019 bytes into
"//snmp:30A8E9F5A5BD154@198.168.145.99/Bulkstats/whitney_161953"
Last transfer attempt: WED JUN 29 14:58:47 2005
Next transfer attempt: FRI JUL 01 09:06:58 2005
```

The following example displays the current collection file:

```
[local]Redback>show bulkstats policy bulk collection

enet0: (454) 0/0 (null) 4632 2a 36 1
atm50: (454) 5/0 (null) 0 0 0 0
atm51: (454) 5/1 (null) 0 0 0 0
```

Related Commands

bulkstats force transfer
context

show configuration snmp

show configuration snmp

Purpose

Displays configuration commands for the Simple Network Management Protocol (SNMP).

Command Mode

all modes

Syntax Description

This command has no keywords or argument.

Default

None

Usage Guidelines

Use the **show configuration** command to display configuration commands for the SNMP (in exec mode).

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays configuration commands for SNMP (in exec mode):

```
[local]Redback#show configuration snmp

Building configuration...

Current configuration:
!
snmp server
snmp engine-id local 80:00:09:30:80:00:0a:0d:31:41:00:a1
snmp engine-id remote victory 00:00:00:63:00:01:3b:39:9b:35:be:6e
snmp view all internet included
snmp community public view all read-write
snmp group group1 read all
snmp group group4 security-model usm auth read all write all notify all
```

```
snmp user user4 engine victory group group4 security-model usm md5 key encoded base64
GFGDL/oidcHnbg7feQxOUQ==
snmp user user4 group group4 security-model usm md5 key encoded base64 GFGDL/oidcHnbg7
feQxOUQ==
snmp target viewport 155.51.31.81 port 15162 security-name user4 version 3 security-
level auth group group4 view all
rmon alarm 10 ipForwDatagrams.0 60 delta rising-threshold 3000000 1 falling-threshold
600000 2
rmon alarm 20 rbnCpuMeterOneMinuteAvg.0 5 absolute rising-threshold 50 3 falling-
threshold 10 4 owner alarmDel6
rmon event 1  log notify owner gold.isp.net description "packets per second too
high in context gold.isp.net"
rmon event 2  log notify owner gold.isp.net description "packets per second is
below 10000 in context gold.isp.net"
rmon event 3  log notify owner gold.isp.net description "One minute average CPU
usage on the device is above 50%"
rmon event 4  log notify owner gold.isp.net description "One minute average CPU
usage on the device is now below 10%"
!
end
```

Related Commands

context

show crashfiles

show crashfiles

Purpose

Displays the size, location, and name of any crash files located on the system.

Command Mode

all modes (10)

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show crashfiles** command to display the size, location, and name of any crash files located in the system. Files are placed in the /md directory in the /flash partition, or when a mass-storage device is included in the system, the mass-storage device /md directory. Crash files are used by Redback personnel to determine the cause of the failure.

This command does not display information about the crash files that have been transferred to a remote File Transfer Protocol (FTP) server.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example lists the size, time, and name of a process crash file and its mini core dump crash file:

```
[local]Redback#show crashfiles

       11277 Mar 31 12:25 /md/exec_cli_274.mini.core
     4507048 Mar 31 12:25 /md/exec_cli_274.core
```

Related Commands

context
delete
process coredump

show debugging

show debugging

Purpose

Displays the debugging options that are currently enabled.

Command Mode

all modes

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show debugging** command to display the debugging options that are currently enabled.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays output from the **show debugging** command:

```
[local]Redback>show debugging

ARP:
   ARP packet debugging is on
General IP:
   IP packet debugging is on
   IP host debugging is on
   IP route debugging is on
   IP interface debugging is on
   ICMP debugging is on
   IP inter-engine communication debugging is on
```

```
   TFTP debugging is on
   TELNET debugging is on
IP Routing:
   RIP protocol debugging is on
```

Related Commands

context
no debug all

show icmp statistics

show icmp statistics

Purpose

Displays Internet Control Message Protocol (ICMP) statistics.

Command Mode

all modes

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show icmp statistics** command to display ICMP statistics.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays output from the **show icmp statistics** command:

```
[local]Redback>show icmp statistics

icmp:
        857 calls to icmp_error
        0 errors not generated because old message was icmp
        Output histogram:
                echo reply: 82
                destination unreachable: 857
                routing redirect: 5
        0 messages with bad code fields
        0 messages < minimum length
        0 bad checksums
        0 messages with bad length
```

```
Input histogram:
        destination unreachable: 872
        echo: 82
        time exceeded: 6
82 message responses generated
```

Related Commands

context
ping

show ip statistics xcrp

show ip statistics xcrp

Purpose

Displays IP traffic statistics on the active controller card.

Command Mode

all modes

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show ip statistics xcrp** command to display IP traffic statistics on the active controller card. The IP traffic statistics are gathered for traffic destined to the system itself and do not include forwarded traffic.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays all IP traffic destined to, or sourced by the system:

```
[local]Redback>show ip statistics xcrp

ip:
        331718 total packets received
        0 bad header checksums
        0 with size smaller than minimum
        0 with data size < data length
        0 with length > max ip packet size
        0 with header length < data size
        0 with data length < header length
        0 with bad options
        0 with incorrect version number
```

```
0 fragments received    0 fragments dropped (dup or out of space)
0 malformed fragments dropped
0 fragments dropped after timeout
0 packets reassembled ok
314961 packets for this host
11722 packets for unknown/unsupported protocol
6 packets forwarded (0 packets fast forwarded)
5129 packets not forwardable
5 redirects sent
88051 packets sent from this host
17 packets sent with fabricated ip header
0 output packets dropped due to no bufs, etc.
0 output packets discarded due to no route
0 output datagrams fragmented
0 fragments created
0 datagrams that can't be fragmented
```

Related Commands

context
show ip interface

show log

show log [**active** | **file** *filename*] [**fac** *log-fac-name* [**level** *level*] [**since** *start-time*] [**until** *end-time*]]

Purpose

Displays information about system event logs or a previously saved log file.

Command Mode

all modes

Syntax Description

active Optional. Displays the system event log.

file *filename* Optional. Log stored in the specified filename.

fac *log-fac-name* Optional. Events for the specified facility. See Table 7-18 for the supported facilities.

level *level* Optional. Only events of the specified level or of higher severity are displayed. See Table 7-17 for the supported levels.

since *start-time* Optional. Only events that happened after the specified time are displayed. This option is useful for viewing the last portion of a log. The *start-time* argument is in a *yyyy***:***mm***:***dd***:***hh***:***mm*[**:***ss*] format, where:

- *yyyy* = year
- *mm* = month
- *dd* = day
- *hh* = hour
- *mm* = minute
- *ss* = optional second

until *end-time* Optional. Only events that happened before the specified time are displayed. This option is useful for viewing the last portion of a log. The *end-time* argument is in a *yyyy***:***mm***:***dd***:***hh***:***mm*[**:***ss*] format, where:

- *yyyy* = year
- *mm* = month
- *dd* = day
- *hh* = hour
- *mm* = minute
- *ss* = optional second

Default

None

Usage Guidelines

Use the **show log** command to display information about system event logs or a previously saved log file.

The **since**, **until**, and **level** keywords are only available after specifying the **active** keyword, or the **file** *filename* construct.

When you enter the **reload** command from the command-line interface (CLI), or a **reboot** command from the boot loader, the system copies its log and debug buffers into these two special files: /md/loggd_dlog.bin and /md/loggd_ddbg.bin. As an aid to debugging, you can display these files using the **show log** command:

show log file /md/loggd_dlog.bin

show log file /md/loggd_ddbg.bin

Table 7-17 lists the *level* argument options.

Table 7-17 Keywords for Event Levels

Level	Description
emergency	Logs only emergency events
alert	Logs alert and more severe events
critical	Logs critical and more severe events
error	Logs error and more severe events
warning	Logs warning and more severe events
notice	Logs notice and more severe events
informational	Logs informational and more severe events
debug	Logs all events, including debug events

Table 7-18 lists the options for the *fac-name* argument.

Table 7-18 Keywords for Facility Names

KeyWord	Facility	Keyword	Facility
aaa	AAA	**pm**	Process Manager
aos	AOS	**ppafwd**	PPA forwarding infrastructure
arp	ARP	**ppainfra**	PPA infrastructure
atm	ATM	**ppaip**	PPA IP
bgp	BGP	**ppal2**	PPA L2
bprelay	Bootp Relay	**ppalg**	PPA Link Group
ccth	Ccth cct handle lib	**ppamedia**	PPA media
chunk	Chunk library	**ppampls**	PPA mpls
cli	CLI	**ppapedgr**	PPA pedgraph
cls	Classifier	**ppaplat**	PPA platform
csm	CSM	**ppaqos**	PPA Qos
cspf	Constrained SPF	**pparedun**	PPA Redundancy

Table 7-18 Keywords for Facility Names *(continued)*

KeyWord	Facility	Keyword	Facility
cxtmgr	Context manager	**ppp**	PPP
dbs	DBS	**pppint**	PPP INTERNAL
dlm	DownLoad Manager	**pppoe**	PPP over Ethernet
dns	DNS	**prp**	Ped Rule Parser
dot1q	dot1q	**qos**	QoS
fr	Frame Relay	**rcm**	Router configuration management
if	Interface configuration	**rdb**	Redundant Database
igmp	IGMP	**rib**	RIB
ipc	Inter-process communication	**rip**	RIP
iprwlock	Inter Process Locks	**rpl**	Router policy library
isis	ISIS debug	**rpm**	Router policy management
ism	ISM	**rsvp**	RSVP
l2vpnmgr	L2VPN Configuration	**serlib**	Stream serializer library
ldp	LDP	**sf**	System function
lg	Link Group	**sftp**	SFTP Client
lm	label manager	**sftpd**	SFTP Server
log	Event Logger	**shmlib**	Shared Memory Library
memmgr	Memory Manager	**snmp**	SNMP
mo	MO	**ssh**	SSH
momi	MOMI	**sshd**	SSHD
mplsmgr	MPLS Configuration	**stat**	Statistics
ms	MPLS Static	**static**	Static route
msdp	MSDP	**sysmgr**	System manager
mtrace	Multicast trace route	**sysmon**	SYSMON
nat	NAT	**talk**	TALK
netopd	netopd	**tasksrv**	Task Services
ntp	NTP	**tunnel**	tunnel
ospf	OSPF	**vlan**	VLAN ID
pem	pem	**vrrp**	VRRP
pim	PIM	**xcd**	XCD

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays a partial listing of the active system event log:

```
[local]Redback>show log

Mar 10 21:25:25: %CSM-6-CARD: card oc3-8-port INSERTED in slot 1 READY
Mar 10 21:25:26: %CSM-6-CARD: card ch-ds3-12-port INSERTED in slot 2 READY
Mar 10 21:25:26: %CSM-6-CARD: card atm-ds3-12-port INSERTED in slot 3 READY
Mar 10 21:25:26: %CSM-6-PORT: pos 1/1 link state UP, admin is UP
Mar 10 21:25:26: %CSM-6-PORT: pos 1/2 link state UP, admin is UP
Mar 10 21:25:26: %CSM-6-PORT: pos 1/3 link state UP, admin is UP
Mar 10 21:25:26: %CSM-6-PORT: pos 1/4 link state UP, admin is UP
Mar 10 21:25:26: %CSM-6-PORT: channelized-ds3 2/1 link state UP, admin is UP
Mar 10 21:25:26: %CSM-6-PORT: ds1 2/1:1 link state UP, admin is UP
Mar 10 21:25:26: %CSM-6-PORT: ds1 2/1:5 link state UP, admin is UP
Mar 10 21:25:26: %CSM-6-PORT: ds1 2/1:6 link state UP, admin is UP
Mar 10 21:25:26: %CSM-6-PORT: ds1 2/1:7 link state UP, admin is UP
Mar 10 21:25:26: %CSM-6-PORT: ds1 2/1:8 link state UP, admin is UP
Mar 10 21:25:26: %CSM-6-PORT: ds1 2/1:15 link state UP, admin is UP
Mar 10 21:25:26: %CSM-6-PORT: ds1 2/1:16 link state UP, admin is UP

.....
```

The following example displays only that portion of the active log that was entered after `00:00 a.m.` on `March 20`:

```
[local]Redback>show log active since 2005:03:20:00:00:00

Mar 20 01:16:15: %SYSLOG-6-INFO: ftpd[79]: connection from 127.0.2.5
Mar 20 01:16:16: %SYSLOG-6-INFO: ftpd[79]: FTP LOGIN FROM 127.0.2.5 as nobody
Mar 20 01:16:37: %SYSLOG-6-INFO: ftpd[79]: put /md/rcm_41.core = 9340060 bytes
```

Related Commands

context
save log
terminal monitor

show logging

show logging [**filter**]

Purpose

Displays system logger statistics, including logger uptime, number of logged messages, number of logged filter messages, and number of logged rate-limited messages.

Command Mode

all modes

Syntax Description

filter	Optional. Displays the filter logging level for each log filter type.

Default

None

Usage Guidelines

Use the **show logging** command to display statistics about the system logger, including logger uptime, number of logged messages, number of logged filter messages, and number of logged rate-limited messages.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays output from the **show logging** command:

```
[local]Redback>show logging

L% Logging Information
% ==================
%         Logger Uptime : 21:23:44 Mon Jun 27 2005
%    Logger Buffer (KB) : Log:        822, Dbg:       1024
%  Logger Buffer Locked : Log:          N, Dbg:          N
%          # Logged msg : Log:       2889, Dbg:          0
```

```
%     # Logged Filtered : Log:          0, Dbg:          0
% # Logged Rate Limited : Log:          0, Dbg:          0
%                ==================
%   Logger Drop Counter : All drop counters are all ZERO
```

The following example displays logging levels for each filter type:

```
[local]Redback>show logging filter

 Console priority critical (2)
 Monitor priority critical (2)
 File priority critical (2)
 Syslog priority critical (2)
```

Related Commands

context

show memory

show memory

Purpose

Displays system memory statistics.

Command Mode

all modes

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show memory** command to display statistics about the available and allocated memory in the system memory partition, which is useful for determining if the system is running low on available memory.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays output from the **show memory** command:

```
[local]Redback>show memory

Memory:total 60556k, Used 22836k, Free 32660k
```

Related Commands

context
show process

show netop

show netop {**advertise** | **snmp version**}

Purpose

Displays configuration information for the advertisement packets or the version of the Simple Network Management Protocol (SNMP) traps that are sent to the NetOp™ Element Manager System (EMS) server.

Command Mode

all modes

Syntax Description

advertise	Displays configuration information for advertisement packets.
snmp version	Displays the version of the SNMP traps that are sent to the NetOp EMS server.

Default

None

Usage Guidelines

Use the **show netop** command to display configuration information for the advertisement packets or the version of the SNMP traps that are sent to the NetOp EMS server.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays the configuration data for the advertisement packets sent to a NetOp EMS server:

```
[local]Redback>show netop advertise

IP Address      Port   Interval   Node Group
192.168.0.1     6581   10         NOCuser1
```

Related Commands

context

show process

show process [*proc-name*] [**crash-info** | **detail**]

Purpose

Displays current status of one or all processes running on the system.

Command Mode

all configuration modes

Syntax Description

proc-name	Optional. Process for which you want to display information. The *proc-name* argument can be any one of the keywords listed in Table 7-19.
crash-info	Optional. Specifies that process crash information is to be monitored.
detail	Optional. Specifies that detailed process information is to be displayed.

Default

When used without any optional constructs, this command displays summary status of all tasks running.

Usage Guidelines

Use the **show process** command to display current information on a specific category of processes, or on all running processes. Table 7-19 lists the keywords for the processes supported by this command.

Table 7-19 Keywords for Processes

Keyword	Process
aaad	Authentication, Authorization, and Accounting (AAA) process
arp	Address Resolution Protocol (ARP) process
atm	Asynchronous Transfer Mode (ATM) process
bgp	Border Gateway Protocol (BGP) process
bridge	Bridge process
clips	Clientless IP Service Selection process
cls	Classifier Manager process
csm	Controller State Manager (CSM) process
dhcp	DHCP Relay/Proxy process
dhelperd	DHCP Helper daemon
dlm	Download Manager (DLM) process
dns	Domain Name System (DNS) process
dot1q	8021Q encapsulation process

Table 7-19 Keywords for Processes *(continued)*

Keyword	Process
fr	Frame Relay process
hr	HTTP Redirect process
igmp	Internet Group Management Protocol (IGMP) process
isis	Intermediate System-to-Intermediate System (IS-IS) process
ism	Interface and Circuit State Manager (ISM) process
l2tp	Layer 2 Tunneling Protocol (L2TP) process
ldp	Label Distribution Protocol process
lg	Link group (LG) process
lm	Label Manager (LM) process
mpls_static	Multiprotocol label switching (MPLS) static process
msdp	Multicast Source Discovery Protocol (MSDP) process
nat	IP Network Address Translator process
netopd	NetOp process
ntp	Network Time Protocol (NTP) process
odd	On-demand diagnostic process
ospf	Open Shortest Path First (OSPF) protocol process
ospf3	Open Shortest Path First Version 3 (OSPF3) protocol process
ped_parse	Process execution descriptor (PED) parse process
pem	Privacy-Enhanced Mail (PEM) process
pim	Protocol Independent Multicast (PIM) process
ppaslog	Packet Processing ASIC (PPA) syslog (SLOG) process
ppp	Point-to-Point Protocol (PPP) process
pppoe	PPP over Ethernet (PPPoE) process
qos	Quality of service (QoS) process
rcm	Router Configuration Manager (RCM) process
rib	Routing Information Base (RIB) process
rip	Routing Information Protocol (RIP) process
rpm	Routing Policy Manager (RPM) process
rsvp	Resource Reservation Protocol Traffic Engineering (RSVP-TE) process
snmp	Simple Network Management Protocol (SNMP) process
static	Static routing process
stats	Statistics process
sysmon	System Monitor process
tunnel	Tunnel management process

Table 7-19 Keywords for Processes *(continued)*

Keyword	Process
vrrp	Virtual Router Redundancy Protocol (VRRP) process
xcd	Cross-connect process

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays output from the **show process** command:

```
[local]Redback>show process

Load Average : 1.37 1.39 1.40

NAME          PID    SPAWN    MEMORY  TIME           %CPU   STATE    UP/DOWN
csm         10989        1      544K  00:02:45.10    0.00%  run      02:54:18
rcm         10990        1     2008K  00:00:56.44    0.00%  run      02:54:16
ism         10991        1      504K  00:01:50.71    0.00%  run      02:54:15
rpm         10992        1      404K  00:00:24.31    0.00%  run      02:54:15
rib         10993        1      992K  00:00:45.41    0.00%  run      02:54:15
ntp         10995        1      496K  00:00:40.43    0.00%  run      02:59:29
static      13035        4      444K  00:00:04.34    0.00%  run      02:59:29
isis            0        0        0K  Not Avail      0.00%  demand   02:54:13
rip         12652        1      576K  00:00:11.01    0.00%  run      02:59:29
bgp             0        0        0K  Not Avail      0.00%  demand   02:54:13
igmp            0        0        0K  Not Avail      0.00%  demand   02:54:13
ospf        11089        1      704K  00:34:31.05    0.00%  run      02:59:29
sysmon      10997        1      396K  00:00:32.27    0.00%  run      02:35:08
dns         10998        1      404K  00:00:24.98    0.00%  run      02:35:08
```

The following example displays output from the **show process crash-info** command:

```
[local]Redback>show process crash-info

ME TIME STATUS
ospf Mon Jan 27 14:05:43 2001 Kill (9)
ism Mon Jan 27 14:28:26 2001 Kill (9)
ism Mon Jan 27 14:28:50 2001 Kill (9)
```

The following example displays output from the **show process ism detail** command:

```
[local]Redback>show process ism detail

Process (PID)       : ism (20536)
Spawn count         : 1
Memory              : 708K
Time                : 00:00:00.16
%CPU                : 0.00%
State               : run
Up time             : 02:37:15
Heart beat          : Enabled
Spawn time          : 2 seconds
Max crashes allowed : 5
Crash thresh time   : 86400 seconds
Total crashes        : 0
Images: (Spawns, Max spawns, Version, Path)
   (*) 1, 3, v1, /usr/redback/bin/ism

Client IPC Endpoints:
   EP 0100007f 060058fe - RIB-IPC-MSG-EP-NAME:00000000
   EP 0100007f 060058fe - NTP-ISM-MSG-EP-NAME:00000000

Server IPC Endpoints:
   EP 0100007f 080058fe - ISM2-CLIENT-NETBYTE-EP-NAME:00000000
   EP 0100007f 070058fe - ISM2-CLIENT-EP-NAME:00000000
   EP 0100007f 060058fe - ISM-CLIENT-EP-NAME:00000000
   EP 0100007f 050058fe - ISM-CONF-EP-NAME:00000000
```

Related Commands

context
process set

show rcm

show rcm {**memory** | **session**}

Purpose

Displays Router Configuration Manager (RCM) information.

Command Mode

all configuration modes

Syntax Description

memory	Displays RCM memory usage.
session	Displays RCM session information.

Default

None

Usage Guidelines

Use the **show rcm** command to display RCM information.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays output from the **show rcm memory** command:

```
[local]Redback>show rcm memory

Displaying memory usage by RCM:
  Internal chunk memory                     : 125200 bytes
  Dynamically memory allocated by all       : 13844 bytes
  Memory allocated for msg by RCM components : 0 bytes
```

The following example displays output from the **show rcm session** command:

```
[local]Redback>show rcm session

CLI pid      State                  Trans ID      Waiting on
-------------------------------------------------------------------
13117        Not in transaction     N/A           None
13059        Not in transaction     N/A           None
12610        In transaction         3062          None
```

Related Commands

context
debug rcm

show rmon

show rmon {**alarms** | **events**}

Purpose

Displays Remote Monitoring (RMON) information.

Command Mode

all modes

Syntax Description

alarms	Displays RMON alarm records.
events	Displays RMON event records.

Default

None

Usage Guidelines

Use the **show rmon** command to display RMON information.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays RMON alarms:

```
[local]Redback>show rmon alarm

rmon alarm 5 ipInReceives.0 50 delta rising-threshold 5000 5 falling-threshold 200 6
owner "gold.isp.net"
rmon alarm 10 ipForwDatagrams.0 60 delta rising-threshold 3000000 1 falling-threshold
600000 2
rmon alarm 20 rbnCpuMeterOneMinuteAvg.0 5 absolute rising-threshold 50 3
falling-threshold 10 4 owner "alarmDel6"
```

The following example displays RMON events:

```
[local]Redback>show rmon events

rmon event 1 log notify owner gold.isp.net description "packets per second too high in
context gold.isp.net"
rmon event 2 log notify owner gold.isp.net description "packets per second is below
10000 in context gold.isp.net"
rmon event 3 log notify owner gold.isp.net description "One minute average CPU usage on
the device is above 50%"
rmon event 4 log notify owner gold.isp.net description "One minute average CPU usage on
the device is now below 10%"
rmon event 5 log notify owner gold.isp.net description "The total number of input IP
datagrams received from interfaces per second is 100 and above"
rmon event 6 log notify owner gold.isp.net description "The total number of input IP
datagrams received from interfaces per second is 4 and below"
```

Related Commands

context

show snmp

show snmp [**accesses** | **communities** | **server** | **targets** | **views**]

Purpose

Displays Simple Network Management Protocol (SNMP) information, including usage, configured contexts, communities, notifications, SNMP daemon status, targets, and views.

Command Mode

all modes

Syntax Description

accesses	Optional. Displays usage.
communities	Optional. Displays the communities.
server	Optional. Displays the current state of the SNMP daemon and the User Datagram Protocol (UDP) port on which it is currently configured to listen.
targets	Optional. Displays configured SNMP targets (notification receivers).
views	Optional. Displays the configured Management Information Base (MIB) views.

Default

None

Usage Guidelines

Use the **show snmp** command to display SNMP statistics, including usage, configured contexts, communities, notifications, SNMP daemon status, targets, and views.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays output from the **show snmp views** command:

```
[local]Redback>show snmp views

restricted system - included non-volatile
restricted snmp - included non-volatile
restricted snmpEngine - included non-volatile
restricted snmpMPDstats - included non-volatile
restricted usmStats - included non-volatile
```

Related Commands

context
debug snmp

show system nvlog

show system nvlog

Purpose

Displays the contents of nonvolatile memory (NVRAM) on the controller card to which you are connected.

Command Mode

all modes

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show system nvlog** to display the contents of NVRAM on the controller card to which you are connected. The NVRAM stores logs of trap- and panic-related messages from the operating system and can be used to help debug system crashes in the absence of a local console (connected to the Craft 2 port).

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays the contents of the NVRAM on the active controller card:

```
[local]Redback>show system nvlog

panic: testing
Redback: dumpsys called

dumping to dev 10,33 offset 8
dump succeeded
!!!vxWorks sent REBOOT intr, will shutdown BSD!!!
!!!vxWorks sent REBOOT intr, will shutdown BSD!!!
!!!vxWorks sent REBOOT intr, will shutdown BSD!!!
```

Related Commands

clear system nvlog
context

show tcp

show tcp [**brief** [**all**] | **statistics** | **tcb** *tcpcb-addr*]

Purpose

Displays Transmission Control Protocol (TCP) Internet connections and statistics.

Command Mode

all modes

Syntax Description

brief	Optional. Displays active Internet connections.
all	Optional. Displays active Internet connections, including servers. Used in conjunction with the **brief** keyword.
statistics	Optional. Displays TCP statistics.
tcb *tcpcb-addr*	Optional. Information for the specified TCP connection only.

Default

None

Usage Guidelines

Use the **show tcp** command to display TCP Internet connections and statistics.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct preceding the **show** command to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays output the **statistics** keyword is specified:

```
[local]Redback>show tcp statistics

tcp:
        85778 packets sent
                33921 data packets (934491 bytes)
                323 data packets (91638 bytes) retransmitted
```

```
        26522 ack-only packets (77668 delayed)
        0 URG only packets
        0 window probe packets
        24871 window update packets
        141 control packets
123389 packets received
        33053 acks (for 936341 bytes)
        537 duplicate acks
        0 acks for unsent data
        102667 packets (37396219 bytes) received in-sequence
        132 completely duplicate packets (189 bytes)
        0 old duplicate packets
        167 packets with some dup. data (232 bytes duped)
        39 out-of-order packets (13 bytes)
        0 packets (0 bytes) of data after window
        0 window probes
        7 window update packets
        1 packet received after close
        0 discarded for bad checksums
        0 discarded for bad header offset fields
        0 discarded because packet too short
26 connection requests
75 connection accepts
82 connections established (including accepts)
98 connections closed (including 24 drops)
18 embryonic connections dropped
32255 segments updated rtt (of 32538 attempts)
333 retransmit timeouts
        1 connection dropped by rexmit timeout
0 persist timeouts (resulting in 0 dropped connections)
110 keepalive timeouts
        86 keepalive probes sent
        24 connections dropped by keepalive
6023 correct ACK header predictions
89333 correct data packet header predictions
224 PCB hash misses
64 dropped due to no socket
0 connections drained due to memory shortage
1 bad connection attempt
79 SYN cache entries added
        0 hash collisions
        75 completed
        0 aborted (no space to build PCB)
        0 timed out
        0 dropped due to overflow
        0 dropped due to bucket overflow
        4 dropped due to RST
        0 dropped due to ICMP unreachable
1 SYN,ACK retransmitted
1 duplicate SYN received for entries already in the cache
0 SYNs dropped (no route or no space)
```

The following example displays output when a TCP connection address is specified:

```
[local]Redback>show tcp tcb 0xe091a630

TCP Protocol Control Block at 0xe091a630:

Timers:         REXMT: 1430     PERSIST: 0      KEEP: 15827     2MSL: 0

State: ESTABLISHED, flags 0x38a0, inpcb 0xe090ca80

rxtshift 0, rxtcur 3, dupacks 0
peermss 498, ourmss 8152, segsz 498

snd_una 2215311423, snd_nxt 2215311425, snd_up 2215311423
snd_wl1 16681764, snd_wl2 2215311423, iss 2215310590, snd_wnd 8271

rcv_wnd 24456, rcv_nxt 16681766, rcv_up 16681764, irs 16681574
rcv_adv 16706222, snd_max 2215311425, snd_cwnd 51294, snd_ssthresh 1073725440
max_sndwnd 8466

idle 0, rtt 1, rtseq 2215311423, srtt 35, rttvar 3, rttmin 2

oobflags 0, iobc 0, softerror 0

snd_scale 0, rcv_scale 0, req_r_scale 0, req_s_scale 0
ts_recent 0, ts_regent_age 0, last_ack_sent 16681766
```

The following example displays output when no arguments are specified:

```
[local]Redback>show tcp

Active Internet connections
PCB      Recv-Q Send-Q Local Address         Foreign Address       State
e091a630      0      2 10.12.208.61.23       155.53.14.198.1193    ESTABLISHED
e091a4d0      0      0 127.0.2.5.65533       127.0.2.3.6667        ESTABLISHED
e091a420      0      0 127.0.2.5.65534       127.0.2.3.6666        ESTABLISHED
```

Related Commands

context
show udp

show tech-support

show tech-support

Purpose

Displays system information that assists your technical support representative in resolving any problem you may encounter.

Command Mode

all modes

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show tech-support** command to display information that assists your technical support representative in resolving any problem you may encounter. The information contains software version information, system uptime, task information, configuration information, and current state of each traffic card.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays output from the **show tech-support** command in the order that they appear (only the headings of the various types of information are listed):

```
[local]Redback#show tech-support

------------------ Current time -------------------
Mon Jun 27 10:00:01 PDT 2005
```

```
------------------ Version Info -------------------

Redback Networks SmartEdge OS Version SE800-5.0.3-Release
Built by sysbuild@@lx-lsf93 Mon Jan 28 10:00:01 PDT 2005
Copyright (C) 1998-2005, Redback Networks Inc. All rights reserved.
System Bootstrap version is PowerPC,1.0b1266
Router Up Time -   21 hours 26 minutes 23 secs

------------------ Release info -------------------

Installed releases:

p01: active (will be booted after next reload)
-----------------------------------------------
Version SE800-2.4.4.0-Release
Built on Mon Jun 27 10:00:01 PDT 2005
Copyright (C) 1998-2003, Redback Networks Inc. All rights reserved.

p02: alternate
--------------
Version SE800-2.3.3.0-Release
Built on Fri Aug  12 01:00:03 PDT 2005
Copyright (C) 1998-2003, Redback Networks Inc. All rights reserved.

------------------ show chassis ---------------
.
------------------ Redundancy info ---------------
.
------------------ show configuration---------------
.
------------------ Command history---------------
.
------------------ Hardware details ---------------
.
------------------ Memory Info -------------------
.
------------------ Crashfile information ----------
.
------------------ Process Crash Info ------------
.
------------------ show task info------------------
.
----------------- Interface Details ---------------
.
----------------- Route Table Summary --------------
.
----------------- Multicast Route -----------------
.
----------------- Linecard FIB Info ---------------
.
----------------- Linecard Info -------------------
.
```

```
----------------- Port Details --------------------
.
----------------- Port Counters -------------------
.
----------------- Database Info ----------------------
.
```

Related Commands

context
show configuration
show version

show udp

show udp {**sockets** | **statistics**}

Purpose

Displays User Datagram Protocol (UDP) socket and statistical information.

Command Mode

all modes

Syntax Description

sockets	Displays UDP socket information.
statistics	Displays UDP statistics.

Default

None

Usage Guidelines

Use the **show udp** command to display UDP socket and statistical information.

Note By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description in Chapter 6, "Context, Interface, and Subscriber Operations."

Note By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information about filtering **show** command output, see Chapter 2, "Using the CLI."

Examples

The following example displays output when the **statistics** keyword is specified:

```
[local]Redback>show udp statistics

udp:
        95808 datagrams received
        0 with incomplete header
        0 with bad data length field
        0 with bad checksum
        875 dropped due to no socket
        94931 broadcast/multicast datagrams dropped due to no socket
        0 dropped due to full socket buffers
        2 delivered
```

```
        875 PCB hash misses
        875 datagrams output
```

The following example displays output from the **show udp** when the **sockets** keyword is specified:

```
[local]Redback>show udp sockets

Active Internet connections (including servers)
PCB      Recv-Q Send-Q Local Address         Foreign Address
f07cbb80      0      0 127.0.0.1.64721       *.* vc
f07cb958      0      0 127.0.0.1.64741       *.*
f07cb8a0      0      0 127.0.0.1.64746       *.*
f07cbcf0      0      0 127.0.0.1.64773       *.*
f07cb730      0      0 127.0.0.1.64790       *.*
f07cbc38      0      0 127.0.0.1.64876       *.*
f07cba6c      0      0 127.0.0.1.123         *.*
f07cb7e8      0      0 127.0.0.1.64914       *.*
f07cb78c      0      0 127.0.0.1.64915       *.*
f07cb6d4      0      0 127.0.0.1.64917       *.*
f07cb678      0      0 127.0.0.1.64918       *.*
f07cbbdc      0      0 127.0.0.1.64919       *.*
f07cbe60      0      0 127.0.0.1.64920       *.*
f07cbf18      0      0 127.0.0.1.64921       *.*
f07cbf74      0      0 127.0.0.1.64922       *.*
f07cbebc      0      0 127.0.0.1.6000        *.*
```

Related Commands

context
show tcp

traceroute

traceroute {*ip-addr* | *hostname*} [**count** *number*] [**df**] [**dispTTL** *ttl*] [**icmp**] [**initialttl** *ttl*] [**maxttl** *ttl*] [**nh**] [**nr**] [**port** *port*] [**size** *bytes*] [**source** *ip-addr*] [**timeout** *seconds*] [**tos**] [**verbose**]

Purpose

Traces the IP route that packets take when traveling to the specified destination.

Command Mode

exec

Syntax Description

ip-addr	IP address to be traced.
hostname	Hostname to be traced. Domain Name System (DNS) must be enabled.
count *number*	Optional. Number of probes to send. The range of values is 1 to 1,000; the default value is 3.
df	Optional. Sets the Don't Fragment bit on outbound traceroute packets. With this bit set, the traceroute packet is dropped whenever it would normally be fragmented. An Internet Control Message Protocol (ICMP) Unreachable, Needs Fragmentation packet is sent to the sender.
dispTTL *ttl*	Optional. Display time-to-live (TTL) bit is set.
icmp	Optional. Uses Internet Control Message Protocol (ICMP) echo instead of a User Datagram Protocol (UDP) datagram.
initialttl *ttl*	Optional. Initial time to live. The range of values is 1 to 255.
maxttl *ttl*	Optional. Maximum time to live. The range of values is 1 to 255.
nh	Optional. Uses the next-hop maximum transmission unit (MTU) if there is a need fragmentation error.
nr	Optional. Prints hop addresses numerically rather than symbolically.
port *port*	Optional. Destination UDP port number. The range of values is 1 to 65,535; the default value is 33,434.
size *bytes*	Optional. Datagram size in octets. The range of values is 0 to 32,768.
source *ip-addr*	Optional. IP source address of the ping packets. An interface with this IP address must exist.
timeout *seconds*	Optional. Amount of time, in seconds, for each probe sent. The range of values is 2 to 86,400; the default value is 2.
tos	Optional. Specifies the type of service (ToS) in probe packets. The range of values, in hex, is 0x0 to 0xff.
verbose	Optional. Provides verbose output.

Default

The **traceroute** command sends three 140-byte packets on UDP port 33434, using a timeout of 2 seconds and a time to live value of 30.

Usage Guidelines

Use the **traceroute** command to trace the routes that packets take when traveling to the specified destination. Each line in the display shows the next hop in the path between the system and the destination address.

You can only use the *hostname* argument if DNS is enabled via the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands (in context configuration mode). For more information about these commands, see the "DNS Configuration" chapter in the *IP Services and Security Configuration Guide* for the SmartEdge OS.

If the destination IP address of the traced route results in the packet going through a multiprotocol label switching (MPLS) label-switched path (LSP), the output displays the label stack along each hop of the LSP.

The **ping** and **traceroute** commands (in exec mode) can have vastly different outcomes, depending on the context in which the commands are issued. In particular, a destination (as denoted by an IP address) that can be reached by the **ping** or **traceroute** command in one context might not be reachable from another context.

Press **Ctrl**+**C** to stop a traceroute.

Examples

The following command discovers the route from the local context to the IP address `206.124.29.1`, using `100`-byte packets, UDP port `73`, ttl `20`, timeout `3`, and count `3`:

```
[local]Redback>traceroute 206.124.29.1 timeout 3 count 3 maxttl 20 port 73 size 100

traceroute to (206.124.29.1), 20 hops max, 140 byte packets
 1  155.53.145.254 (155.53.145.254)     0 ms  0 ms  0 ms
 2  155.53.200.254 (155.53.200.254)     0 ms  0 ms 16 ms
 3  206.83.66.193 (206.83.66.193)      16 ms 16 ms 16 ms
 4  206.83.90.66 (206.83.90.66)        16 ms 16 ms 16 ms
 5  157.130.193.197 (157.130.193.197)  16 ms 33 ms 16 ms
 6  157.130.194.18 (157.130.194.18)    16 ms 33 ms 16 ms
 7  209.104.192.49 (209.104.192.49)    50 ms 66 ms 50 ms
 8  209.104.198.38 (209.104.198.38)    50 ms 66 ms 66 ms
 9  206.124.1.22 (206.124.1.22)        66 ms 66 ms 66 ms
10  206.124.29.1 (206.124.29.1)        83 ms 66 ms 83 ms
```

The following example displays a destination IP address of a traced route resulting in the packet going through an MPLS LSP, and includes the label stack along each hop of the LSP:

```
[local]Redback>traceroute 5.5.5.5

se_traceroute to 5.5.5.5 (5.5.5.5), 30 hops max, 40 byte packets
 1  100.1.1.1 (100.1.1.1)   4.749 ms  4.111 ms  3.986 ms
 2  40.1.1.2 (40.1.1.2)   6.321 ms  6.457 ms  5.289 ms
        MplsLabel: 19 MplsExpBits: 0 TTL: 1
        MplsLabel: 786434 MplsExpBits: 0 TTL: 1
 3  60.1.1.1 (60.1.1.1)   3.815 ms  4.159 ms  4.120 ms
        MplsLabel: 786434 MplsExpBits: 0 TTL: 1
 4  5.5.5.5 (5.5.5.5)   5.870 ms  9.108 ms  6.639 ms
```

Related Commands

ping

Part 4

Appendixes

This part describes the SmartEdge® OS boot loader functions, tasks, and commands used to perform system recovery and system upgrade operations, including the alarm conditions and their probable causes.

This part includes Appendix A, “Boot Loader Operations.”

Boot Loader Operations

Most of the tasks associated with configuring and maintaining the SmartEdge® router involve using commands supported by the SmartEdge OS. However, some tasks require that you use the boot loader software installed on the controller cards in the SmartEdge router. This appendix describes all the necessary tasks in the following sections:

- Before You Begin
- System Recovery Operations
- Upgrade Operations
- Boot Loader Commands

Note In the following descriptions, the term, controller card, applies to the Cross-Connect Route Processor (XCRP) or the XCRP Version 3 (XCRP3) Controller card, unless otherwise noted.

Before You Begin

The boot loader image contains system firmware that provides access low-level functions used to manipulate system devices, view and modify boot parameter values, and control boot procedures. The SmartEdge router implements SmartFirmware, an ANSI C implementation of OpenFirmware (IEEE 1275-1994, *Standard for Boot Firmware Initialization Configuration Firmware: Core Requirements and Practices*) plus errata, recommend practices, and accepted proposals to configure system boot parameters and to boot the SmartEdge OS software.

It is assumed that there is a Trivial File Transfer Protocol (TFTP) server that has the needed software image files on it, and that the server is configured and reachable by the SmartEdge router.

Note For the IP address of the TFTP server and for the exact filenames, contact the Redback® Technical Assistance Center (TAC) or your technical support representative.

Software image filenames have the following formats:

- SmartEdge OS image—SEOS-*release*.tar.gz

  The *release* field has three single-digit subfields with the format *n.n.n*

- Boot loader image—of*version*.bin
- Minikernel image—netbsd.min.*version*.bz2.bin

Table A-1 lists examples of the software image filenames.

Table A-1 Software Image Filename Examples

File	Example Filename
SmartEdge OS software release	SEOS-5.0.3.tar.gz
Boot loader image file	of1267.bin
Minikernel image file	netbsd.min.v20.bz2.bin

System Recovery Operations

This section describes the following boot loader interface tasks:

- Recover a Lost Password
- Format Internal Devices, Install a New System Image, or Both

Recover a Lost Password

If you have forgotten the system password, you can use the boot loader interface to disable logon authentication on the console port to log on and configure a new password. This process disables the administrator authentication only for a single console port logon.

Note To perform this procedure, you must access the SmartEdge router through the console port (Craft 2) on the active controller card.

To recover a lost password, perform the following steps:

1. Access the boot loader interface:
   a. Enter the following command (in exec mode) in the SmartEdge OS command-line interface (CLI):

      ```
      reload
      ```

   b. Enter **SE*** to cancel the reload process and access the boot loader interface and prompt (ok) after you see the following message:

      ```
      Auto-boot in 5 seconds - press SE* to abort, ENTER to boot:
      ```

      The reload process is canceled and the boot loader prompt displays.
2. Disable administrator authentication at the console port for a single console logon; enter the following boot loader command:

   ok **setenv user-auth? false**
3. Reset the hardware and boot the system; enter the following boot loader command:

   ok **reset**

4. Modify the enable and administrator account passwords:
   a. After the system has booted, press **Enter** at the console port.

      The system does not prompt for a username and password.

   b. Access global configuration mode; enter the following command (in exec mode) in the SmartEdge OS CLI:

      configure

   c. Create an enable password for privileged access to the system, or modify the enable password; enter the following command (in global configuration mode):

      enable password [**level** *level*] *password*

   d. Access context configuration mode; enter the following command (in global configuration mode):

      context *ctx-name*

   e. Create a new administrator account to access the system, or modify the password for an existing administrator account; enter the following command (in context configuration mode):

      administrator *admin-name* **password** *password*

5. Use the new administrator account and the enable password for subsequent access to the system.

Format Internal Devices, Install a New System Image, or Both

This procedure provides the following two options:

- Individually reformat each compact-flash card and, if installed, the mass-storage device. If the option to format the mass-storage device is selected, the procedure formats the mass-storage device with two partitions, one of which is essential for obtaining operating system core dumps more quickly.
- Download the software image from a server that you specify and installs the system image in one of the system boot partitions on the compact-flash cards.

Caution Risk of data loss. If the mass-storage device (the /md partition) has any useful information (operating system or Packet Processing ASIC ([PPA]) crash files, and so on), that information is destroyed during the reformat operation. To reduce the risk, archive useful information before beginning the procedure.

Note Before attempting this procedure, consult the TAC or your technical support representative. You also need to have at hand the information listed in Table A-2.

Table A-2 lists the information required to reformat internal devices and also to install a new system image.

Table A-2 Optional and Required Data

Prompt	Description	Example Data
IP address	IP address of the Ethernet management port on the controller card to which you will be connected; same value as in the ip-addr parameter.	155.53.53.254
netmask	Network mask for the associated IP network for the SmartEdge router; same value as in the *ip-addr* argument.	255.255.252.0

Table A-2 Optional and Required Data *(continued)*

Prompt	Description	Example Data
gateway IP address	IP address of the gateway router to the IP network of the TFTP server. This address is not used if the TFTP server is on the same subnet as the SmartEdge router.	155.53.39.254
IP address of server	IP address of the TFTP server on which the system image file is located.	155.53.32.126
username and password	Account name and password to access the system image.	test
path to release	URL for the system image to be downloaded.	/images/REL_5_0_3/ SEOS-5.0.3.tar.gz
install directory (p01/p02)	Partition in which to install the system image; usually p01.	p01

Perform the following steps to format internal devices, install a new system image, or both:

1. Connect to the console port of the controller card with a 9,600 baud serial connection.
2. If you see the `ok` prompt, skip to step 3. If you see the # prompt (for example, `[local]Redback#`), enter the following command:

   reload
3. Enter **SE*** to cancel the reload process and access the boot loader interface and prompt (`ok`) after you see the following message:

   ```
   Auto-boot in 5 seconds - press SE* to abort, ENTER to boot:
   ```

   The reload process is canceled and the boot loader prompt displays.
4. Display and verify boot parameters; enter the following boot loader command:

   ok **printenv**

   This command prints all boot parameters.
5. Verify that the parameters listed in Table A-3 are set to the required values.

Table A-3 Boot Parameter Values

Parameter	Value
boot-device	flash
boot-command	bootsys

6. If these values are not correctly set, enter the following boot loader command to set the required values:

   ok **setenv** *parameter value*
7. Reformat the devices and download a new software image:
   a. Invoke the minikernel image; enter the following boot loader command:

      ok **installsys**

   Note If the system returns an error, or does not return a prompt after you enter the **installsys** command, the minikernel image is not installed on the system bootrom. In this case, you must install the minikernel image in the bootrom; perform the procedure described in "Upgrade to a New Minikernel File."

b. Enter the data as requested by the system when it prompts you for the following information: local IP address, the network mask, and the gateway IP address for a server on which the software release is located.

c. Enter **y** at the prompt to format a device; enter **n** to not format the device when the system prompts you to format each compact-flash card, and the mass-storage device (referred to as the hard disk).

d. Enter **y** to install a new release; enter **n** to not install a new release when the system prompts you to install a new software release.

e. If you enter **y**, enter the data as requested by the system when it prompts you for the remote server data: IP address of the server, the username and password, and the URL of the release package.

After the download is complete, the minikernel image exits and the prompt changes to #.

8. Reload the system with the downloaded image:

a. Enter the following boot loader command:

reboot

b. If a standby controller card is present, the system synchronizes it to the updated active controller card:

```
syncing disks... done
rebooting
Program terminated!
[0]Booting(2)....
Enabling L1/L2 Caches...
.
.
```

The following example displays output and responses for step 7; responses are shown in **bold**:

```
Starting System Install Script...


Enter IP address : 10.12.209.197
Enter netmask : 255.255.248.0

Enter gateway IP address : 10.12.208.1
Configuring ethernet interface...
add net default:gateway 10.12.208.1

Checking for presence of first compact flash disk...compact flash disk
detected
Checking for presence of second compact flash disk...compact flash disk
detected

Two compact flash disks detected on XCRP....

Checking for presence of hard disk...hard disk detected
Would you like to erase the vxWorks compact flash disk(Y/N) : y

formatting compact flash disk...done
```

```
Would you like to erase the BSD compact flash disk(Y/N) : y
formatting compact flash disk...10+0 records in
10+0 records out
655360 bytes transferred in 1 secs (655360 bytes/sec)
/dev/rwd1a: 377856 sectors in 1476 cylinders of 8 tracks, 32 sectors
184.5MB in 93 cyl groups (16 c/g, 2.00MB/g, 512 i/g)
super-block backups (for fsck -b #) at:
32, 4160, 8288, 12416, 16544, 20672, 24800, 28928,
32800, 36928, 41056, 45184, 49312, 53440, 57568, 61696,
65568, 69696, 73824, 77952, 82080, 86208, 90336, 94464,
98336, 102464, 106592, 110720, 114848, 118976, 123104, 127232,
131104, 135232, 139360, 143488, 147616, 151744, 155872, 160000,
163872, 168000, 172128, 176256, 180384, 184512, 188640, 192768,
196640, 200768, 204896, 209024, 213152, 217280, 221408, 225536,
229408, 233536, 237664, 241792, 245920, 250048, 254176, 258304,
262176, 266304, 270432, 274560, 278688, 282816, 286944, 291072,
294944, 299072, 303200, 307328, 311456, 315584, 319712, 323840,
327712, 331840, 335968, 340096, 344224, 348352, 352480, 356608,
360480, 364608, 368736, 372864, 376992,
done
Would you like to erase the hard disk(Y/N) : y

Would you like to download a new release(Y/N) : y
Enter IP address of server : 10.12.215.10
Enter username : test
Enter password :
Enter path to release :/images/REL_5_0_3/SEOS-5.0.3.tar.gz
Enter install directory (p01/p02) : p01
ftping release...

ftp://test:test@10.12.215.10//images/REL_5_0_3/SEOS-5.0.3.tar.gz
(13890K)
- [########################] 13890K | 117.69K/s
14223725 bytes transferred in 118.03 sec (117.69k/sec)

copying releases to appropriate compact flash disk....
.
.
.
done

Exiting System Install Script...
#
```

Upgrade Operations

Upgrade operations are described in the following sections:

- Upgrade to a New Boot Loader Image
- Upgrade to a New Minikernel File

Upgrade to a New Boot Loader Image

The boot loader image is stored in the EEPROM on a controller card.

Note Before attempting this procedure, consult the TAC or your technical support representative.

Table A-4 lists the data needed to download the new boot loader file; arguments described are configured through the **setenv** boot loader command.

Table A-4 Data Required to Download the Boot Loader File

Argument	Description	Example
ip-addr	IP address and network mask of the Ethernet management port on the controller card to which you will be connected; format is *A.B.C.D*:*E.F.G.H*.	155.53.53.254:255.255.252.0
gateway-ip-addr	IP address of the gateway router to the IP network on which the server is located. This address is not used if the server is on the same subnet as the SmartEdge router.	155.53.55.254
server-ip-addr	IP address of the server.	10.21.6.200

To upgrade to a new boot loader image in the EEPROM, perform the following steps:

1. Connect to the console port of the controller card with a 9,600 baud serial connection.
2. If you see the `ok` prompt, skip to step 3. If you see the # prompt (for example, `[local]Redback#`), enter the following command:

   reload
3. Enter **SE*** to cancel the reload process and access the boot loader interface and prompt (`ok`) after you see the following message:

   ```
   Auto-boot in 5 seconds - press SE* to abort, ENTER to boot:
   ```

   The reload process is canceled and the boot loader prompt displays.
4. Verify that the arguments listed in Table A-4 are set to the required values; enter the following boot loader commands:

   ok **printenv ip-addr**

   ok **printenv gateway-ip-addr**

   ok **printenv server-ip-addr**

5. If the values for the arguments listed in Table A-4 are not correct, enter the following commands with the correct values:

   ok **setenv ip-addr** *ip-addr*

   ok **setenv gateway-ip-addr** *gateway-ip-addr*

   ok **setenv server-ip-addr** *server-ip-addr*

6. Enter one of the following commands to download the new boot loader image file:

   ok **load net** *filename*

   or

   ok **load hd:a /flash/***filename*

   where the *filename* argument is the filename of the boot loader image file provided by the TAC or your local technical representative; for example, `of1267.bin`.

7. Enter the following command to update the EEPROM:

   ok **update-bootrom**

Upgrade to a New Minikernel File

Note Before attempting this procedure, consult the TAC or your technical support representative.

Table A-5 lists the data needed to download the new minikernel file; arguments described are configured through the **setenv** boot loader command.

Table A-5 Data Required to Download the Minikernel File

Argument	Description	Example
ip-addr	IP address and network mask of the Ethernet management port on the controller card to which you will be connected; format is *A.B.C.D:E.F.G.H*.	155.53.53.254:255.255.252.0
gateway-ip-addr	IP address of the gateway router to the IP network on which the server is located. This address is not used if the server is on the same subnet as the SmartEdge router.	155.53.55.254
server-ip-addr	IP address of the server.	10.21.6.200

To upgrade to a new minikernel file, perform the following steps:

1. Connect to the console port of the controller card with a 9,600 baud serial connection.
2. If you see the `ok` prompt, skip to step 3. If you see the # prompt (for example, `[local]Redback#`), enter the following command:

   reload

3. Enter **SE*** to cancel the reload process and access the boot loader interface and prompt (`ok`) after you see the following message:

   ```
   Auto-boot in 5 seconds - press SE* to abort, ENTER to boot:
   ```

   The reload process is canceled and the boot loader prompt displays.

4. Verify that the arguments listed in Table A-5 are set to the required values; enter the following boot loader commands:

   ok **printenv ip-addr**

   ok **printenv gateway-ip-addr**

   ok **printenv server-ip-addr**

5. If the values for the arguments listed in Table A-5 are not correct, enter the following commands with the correct values:

   ok **setenv ip-addr** *ip-addr*

   ok **setenv gateway-ip-addr** *gateway-ip-addr*

   ok **setenv server-ip-addr** *server-ip-addr*

6. Download the new minikernel image file; enter one of the following boot loader commands:

   ok **load net** *filename*

   or

   ok **load hd:a /flash/***filename*

   where the *filename* argument is the filename of the minikernel image file provided by the TAC or your local technical representative; for example, `netbsd.min.v20.bz2`.

7. Install the new minikernel image; enter the following boot loader command:

   ok **write-kernel**

Boot Loader Commands

Table A-6 describes the boot loader commands supported on the SmartEdge router.

Table A-6 Boot Loader Commands

Syntax	Description	Argument Values
boot net *filename* or **boot hd:a /flash/***filename*	Boots from a TFTP server or from /flash.	Name of the file to be booted.
bootsys	Loads and runs the software image.	None.
cd *path*	Changes the currently open device to the one specified by the *path* argument. The device also parses any optional arguments to configure the device.	*path*—Actual or relative device path. Entering **..** specifies the parent of the current device.
dev *path*	Changes the currently open device to the one specified by the *path* argument. The device also parses any optional arguments to configure the device.	*path*—Actual or relative device path. Entering **..** specifies the parent of the current device.
devalias [*name string*]	Displays all device aliases, if no arguments specified; otherwise, creates a device alias called *name* with the value *string*.	*name*—Optional. Name of the device alias. *string*—Optional. String to which the alias refers.
installsys	Invokes the BSD minikernel.	None.

Table A-6 Boot Loader Commands *(continued)*

Syntax	Description	Argument Values
load net *filename* or **load hd:a /flash/***filename*	Loads an image from a TFTP server or from /flash.	Name of the file to be downloaded.
printenv [*parameter*]	Displays all parameter variables, their current values, and their default values if no argument is specified; otherwise, displays the specified parameter variable.	See Table A-7.
probe-all	Probes the system for all devices and builds the device tree.	None.
reset	Resets the hardware and boots the system.	None.
set-default *var*	Sets the value of a parameter to the default value.	See Table A-7.
set-defaults	Sets all parameter values back to their default values.	None.
setenv *parameter value*	Sets the value of a parameter to a specified value. All characters entered up to the end of the line (including spaces), are stored in NVRAM.	See Table A-7.
show-devs	Displays all the devices in the device tree.	None.
sysinfo	Displays system information including platform, chassis, memory, and environmental information.	None.
update-bootrom	Updates and runs the currently loaded boot loader image.	None.

Table A-7 lists the parameters used with these boot loader commands: **printenv**, **setenv**, and **set-default**.

Table A-7 Parameters Used with printenv, set-default, and setenv Boot Loader Commands

Syntax	Description	Values
auto-boot?	If true, runs the word in **boot-command** after the standard bootup process; otherwise, runs the Forth interpreter on the console and displays an ok prompt.	true or false; the default value is false.
auto-boot-timeout	Time in milliseconds to wait for a key press to abort auto-boot. (This is not a standard OpenFirmware parameter.)	Integer; the default value is 5000.
boot-command	Command to boot the system if the **auto-boot?** value is true.	String; the default value is bootsys.
boot-device	Device to use to load the boot image when the **boot** command is issued. The string is usually an alias to the actual device.	String; the default value is flash.
boot-file-ppc0	NetBSD file to load from the boot device when the **boot** command is issued.	String; the default value is /p01/netbsd.
boot-file-ppc1	vxWorks file to load from the boot device when the **boot** command is issued.	String; the default value is /p01/vxWorks.gz.
diag-device	Device to use to load the diagnostic image if the **diag-switch?** value is true when boot is issued.	String; the default value is net.
diag-file	Diagnostic file to load if the **diag-switch?** value is true when boot is issued.	String; the default value is diag.
diag-switch?	If true, turns on extended tests and displays more verbose output.	true or false; the default value is false.
fcode-debug	Redback® internal use only; do not modify.	true or false; the default value is false.

Table A-7 Parameters Used with printenv, set-default, and setenv Boot Loader Commands *(continued)*

Syntax	Description	Values
gateway-ip-addr	IP address of the gateway router to the IP network on which the TFTP server is located.	String.
ignore-cfgfile	If true, the bootup configuration file is bypassed the first time the system is reloaded, after which the parameter is set to false. This parameter allows you to bypass the loading of a possibly corrupt configuration file. It is set from the ok prompt.	true or false; the default value is false.
input-device	Device path to use for the console input. The **keyboard** value is usually an alias to the actual input device determined in some machine-dependent manner.	String; the default value is keyboard.
inverse-video	If true, displays text on the console as black-on-white; otherwise, displays text on the console as white-on-black. (This is not a standard OpenFirmware parameter).	true or false; the default value is true.
ip-addr	IP address and network mask of the Ethernet management port on the active controller card in the SmartEdge router; format is *A.B.C.D:E.F.G.H*.	String.
little-endian	Redback internal use only; do not modify.	true or false; the default value is false.
load-base	Redback internal use only; do not modify.	0x05600000.
mac_addr	MAC address of the active controller card.	String.
nvramrc	Seven device aliases; Redback internal use only; do not modify.	String.
oem-banner	String to display when the **banner** command is issued, if the **oem-banner?** value is set to true.	String.
oem-banner?	If true, display the contents of the **oem-banner** value when the **banner** command is issued.	true or false; the default value is false.
oem-logo	Bitmap to display if the **oem-logo?** value is true. The contents can be machine-dependent.	Bitmap: 64 x 64 x 1 (512 bytes).
oem-logo?	If true, displays the bitmap in the **oem-logo** value in front of the banner when the **banner** command is issued; otherwise, a default logo (or no logo) displays.	true or false; the default value is false.
output-device	Name of the device to use for console. This is usually an alias to the actual device.	String; the default value is screen.
real-base	Redback internal use only; do not modify.	0x00000000.
real-mode?	Redback internal use only; do not modify.	true.
real-size	Redback internal use only; do not modify.	0x00080000.
screen-#columns	Number of columns desired for console output. If 0 is specified, the largest allowable number is used, depending on the font used.	Integer; the default value is 80.
screen-#rows	Number of rows desired for console output. If 0 is specified, the largest allowable number is used, depending on the font used.	Integer; the default value is 24.
secondary-diag?	If true, run secondary diagnostics at bootup. (This is not a standard OpenFirmware parameter.)	true or false; the default value is true.
server-ip-addr	IP address of the TFTP server.	String.
update-ofw?	Redback internal use only; do not modify.	false.

Table A-7 Parameters Used with printenv, set-default, and setenv Boot Loader Commands *(continued)*

Syntax	Description	Values
use-nvramc?	Redback internal use only; do not modify.	true.
user-auth	If true, prompts users for password authentication. If false, authentication is bypassed. Set this flag to false if password is forgotten or lost. If set to false, it is set to true the next time the device is rebooted.	true or false; the default value is true.
virt-base	Redback internal use only; do not modify.	Integer; the default value is -1.
virt-size	Redback internal use only; do not modify.	Integer; the default value is -1.
vx-config-flags	Redback internal use only; do not modify.	0x0.
vx-other	Redback internal use only; do not modify.	0x7a.
vx-target-name	Redback internal use only; do not modify.	String.
vx-host-name	Redback internal use only; do not modify.	String.

Note Diagnostic syntax, diag-device, diag-file, and diag-switch?, have no affect on the power-on diagnostics (POD) nor are they affected by the POD.

Index

S

T

U

Commands