General Troubleshooting Guide

SmartEdge OS Software

FAULT TRACING DIRECT.

Copyright

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

SmartEdge	is a registered trademark of Telefonaktiebolaget LM Ericsson.

Contents

1 Introduction

This document provides general troubleshooting techniques for the SmartEdge® router. It describes how to deal with hardware and software problems, as well as data link layer, subscriber, and RADIUS server issues. For troubleshooting techniques used in dealing with all issues, see *Basic Troubleshooting Techniques*.

2 Troubleshooting Hardware Problems

This section describes how to troubleshoot hardware problems. For more information about troubleshooting hardware problems and how to interpret alarms, see the SmartEdge router hardware guides.

Use Table 1 as a guide to troubleshoot hardware problems.

Table 1 Software Diagnostics Tasks

Task	Command	Notes	Checked?

Step 1: Checking Hardware	`show hardware`
	`show hardware detail`
	`show chassis`
	`show hardware detail`
	`| grep option '- E' 'Alarm Slot'`
		• Display hardware status.
		• Display detailed hardware status.
		• Check FGPA versions on line cards.
		• Display hardware alarms.
		• Check which generation card you are using.	

Step 2: Displaying Chassis Information	`show chassis`	Display chassis information and the cards that are installed and configured.	
Step 3: Displaying Results from Power-on Diagnostics	`show diag pod`	Verify operation status of the controller cards and line cards after a system is powered on or cards are hot-swapped.	
Step 4: Checking Fan Tray Power	`show diag pod fantray detail`	Display detailed test results of the POD for the fan tray or the fan and alarm unit in the chassis.	

Step 5: Displaying Information About the Backplane	`show hardware backplane`
	`show hardware backplane detail`
		Display summary or detailed information about the backplane.	

Step 6: Checking System Alarms	`show system alarm`
	`show system alarm all`
		Display system, card, port, channel or subchannel alarms.
		Use the detailed keyword to display all alarms at all levels.	

Step 7: Checking On-Demand Diagnostics	`diag on-demand standby`
	`show diag on-demand standby`
	`show diag on-demand card`
		• Test the chassis, standby controller card and line cards.
		• Display results on the ODD session.	

Step 8: Checking CF Card and External Storage Device	`show disk`	Display status for the internal (NetBSD compact-flash) card, or the external mass-storage device.	

2.1 Step 1: Checking Hardware

To check the hardware status of your router, use the **show hardware** command.

2.1.1 Displaying Hardware Status

The following example shows you how to display hardware status using the **show hardware** command. The chassis power, fantray power-on-diagnostics, and fantray have a status of failed. Slot 1 and 5 do not have cards configured and are not considered active and, as result, are not managed. A Temp (temperature) status of “Hot” or “Extreme”, indicates an environment or chassis issue.

```
[local]Redback# show hardware
Fan Tray Status        Present
Fan (s) Status         Normal
Power Supply A Status  Normal
Power Supply A Status  Normal
Active Alarms          Fan tray failure detected
                       Fantray power-on diagnostic failed
                       Chassis power failure - side A1
                       Chassis power failure - side A2
Slot Type          Serial No      Rev Ver Mfg Date     Voltage  Temp
---- ---------     -------------- --- --- -----------  ------- ---
N/A  backplane     B2024080600966 2   4   30-AUG-2006  N/A      N/A
N/A  fan tray      9W044080603171 4   4   30-AUG-2006  N/A      N/A
1    ge-5-port     0G615110600869 61  4   01-NOV-2008  N/A      N/A
3    ge-10-port    7U055090601012 5   4   15-SEP-2006  OK       NORMAL
5    ge3-4-port    A6045110602085 4   4   07-DEC-2006  N/A      N/A
7    xcrp4         6Y51B130704671 51  4   04-APR-2008  OK       NORMAL
8    xcrp4         6Y095110401610 9   4   28-DEC-2007  OK       NORMAL
```

Recommended Action: Issue the **show system alarm all** command to get more detailed information about the fan tray and chassis failures. For sample output related to this example, see Section 2.6.2 on page 22. To see the configure status of the slots, issue the **show chassis** command. For information about the **show chassis** command, see Section 2.2 on page 10.

2.1.2 Checking FPGA Versions on a Line Card

Each line card has one or more FPGAs; each SEOS release has a supported FPGA version. After you install a new software release image, an FPGA image mismatch between the FPGA version supported by the new software and the FPGA version on the line card might occur. Upgrading the FPGA image is optional but strongly recommended.

Note: Upgrading a line card FPGA interrupts traffic forwarding on the affected card for up to 5 minutes. We recommend that you upgrade your FPGA mismatches during a maintenance window.

If you upgrade a FPGA that does not need to be upgraded, the system indicates that upgrading the card is not required.

The following example indicates a FPGA mismatch. When you examine the output of the **`show hardware card 1 detail`** command, you see that the Fpga file rev `0x42` is greater than the value of the current image on the line card rev `0x41`. This indicates that a newer FPGA image is available for the line card.

```
[local]Redback# show hardware card 1 detail
...
Slot :         1                Type               : 10ge-1-port
Serial No      : A821G240840410   Hardware Rev       : 21
EEPROM id/ver  : 0x5a/4           Mfg Date           : 20-JUN-2008
HubFpga rev    : 0x41             HubFpga file rev   : 0x42
```

Recommended Action: Reload line card `1` with the newer FPGA image by using the **`reload fpga 1`** command.

Use Table 2 as a guide to troubleshooting FPGA mismatch issues.

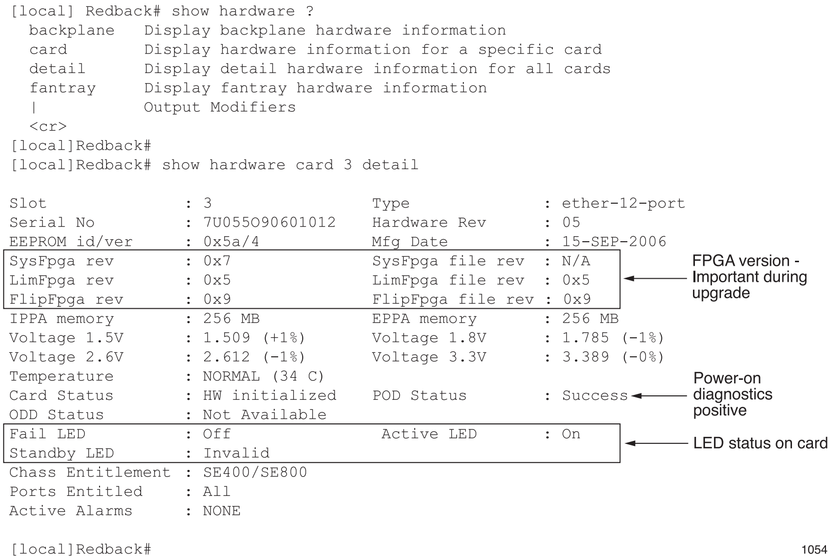
Table 2 FPGA Tasks

#	Task	Root Command	Notes	Checked?
1	Determine which FPGA cards require an upgrade.	**`show chassis`**	Issue this command in any mode. If the line card has an “M” flag (a FPGA mismatch), the line card requires an FPGA upgrade. (This flag appears only for mandatory FPGA upgrades; it does not appear for optional FPGA upgrades.) If a line card has an M flag, the card will not be initialized.	
2	Upgrade each line card that has a ‘M’ flag.	**`reload fpga card`***`slot`*	Enter this command in exec mode.	
3	Verify whether each line card requires an optional FPGA upgrade.	**`show hardware card`** *`slot`* **`detail`**	For each line card, issue the **`show hardware card detail`** command in exec mode. If the output shows that the value of the name Fpga file rev is greater than the value of the name Fpga rev, a newer FPGA image is available for the line card.	
4	Install the optional upgrades on each line card.	**`reload fpga`** *`slot`*	Enter this command in exec mode. When a newer image is available for the line card, upgrade the line card to the newer FPGA image.	
5	Verify that the upgraded FPGA versions are correct.	**`show hardware card`** *`slot`* **`detail`**	After you upgrade the FPGA image on the line card, verify that the FPGA versions are correct.	

2.1.3 Displaying Detailed Hardware Status

The following example shows how to display detailed hardware status, such as the FPGA version, the power-on diagnostics, LED status on the card, and active alarms. For Gigabit Ethernet cards, details of the installed SFPs are also be displayed.

If your card status is `Card Status :  HW failure POD Status : Fail Card State :  PPA download failure`, insert the card into a free slot to and check to see if the POD status is successful. If the POD status fails, contact you local technical representative.



```
[local] Redback# show hardware ?
  backplane   Display backplane hardware information
  card        Display hardware information for a specific card
  detail      Display detail hardware information for all cards
  fantray     Display fantray hardware information
  |           Output Modifiers
  <cr>
[local]Redback#
[local]Redback# show hardware card 3 detail

Slot               : 3                  Type               : ether-12-port
Serial No          : 7U055O90601012     Hardware Rev       : 05
EEPROM id/ver      : 0x5a/4             Mfg Date           : 15-SEP-2006
SysFpga rev        : 0x7                SysFpga file rev   : N/A
LimFpga rev        : 0x5                LimFpga file rev   : 0x5
FlipFpga rev       : 0x9                FlipFpga file rev  : 0x9
IPPA memory        : 256 MB             EPPA memory        : 256 MB
Voltage 1.5V       : 1.509 (+1%)        Voltage 1.8V       : 1.785 (-1%)
Voltage 2.6V       : 2.612 (-1%)        Voltage 3.3V       : 3.389 (-0%)
Temperature        : NORMAL (34 C)
Card Status        : HW initialized     POD Status         : Success
ODD Status         : Not Available
Fail LED           : Off                 Active LED        : On
Standby LED        : Invalid
Chass Entitlement  : SE400/SE800
Ports Entitled     : All
Active Alarms      : NONE

[local]Redback#
```

FPGA version - Important during upgrade
Power-on diagnostics positive
LED status on card
1054

Figure 1 Displaying Detailed Hardware Status

2.1.4 Displaying Hardware Alarms Using GREP

Use the **`show hardware detail`** command to display detailed information about all hardware in the system.

The following example shows you how to display the status chassis alarms by using the **`grep options '-E' 'Alarm | Slot'`**. This **`grep`** command looks for the keywords “Alarm” and “Slot”.

```
[local]Redback# show hardware detail | grep options '-E' 'Alarm|Slot'

Active Alarms    Chassis power failure - side B
Slot            : N/A               Type       : backplane
Slot            : N/A               Type       : fan tray
Slot            : 1                 Type       : oc3e-8-port
Active Alarms   : NONE
Slot            : 4                 Type       : atm-oc3-2-port
Active Alarms   : NONE
Slot            : 5                 Type       : ge-10-port
Active Alarms   : N/A
Slot            : 8                 Type       : xcrp4 - T1/E1
Active Alarms   : Backup fail: peer dead
Slot            : 12                Type       : fege-60-2-port
Active Alarms   : N/A
Slot            : 14                Type       : ge-10-port
```

2.1.5 Checking PPA Versions

Use the following table to determine whether a card version is PPA2 or PPA3. Run the **show chassis** command to view the card types installed on your system.

Table 3 PPA Support

CARD	PPA Version
8-port ATM OC-3c/STM-1c	PPA2
2-port ATM OC-12c/STM-4c	PPA2
8-port POS OC-3c/STM-1c	PPA2
4-port POS OC-12c/STM-4c	PPA2
4-port POS OC-48c/STM-16c	PPA2
1-port OC-192c/STM-64c	PPA2
Channelized 8-port OC-3/STM-1 or 2-port OC-12/STM-4	PPA2
60-port Fast Ethernet Card	PPA2
10-port Gigabit Ethernet 1020	PPA2
20-port Gigabit Ethernet 1020	PPA2
4-port Gigabit Ethernet 3	PPA2
5-port Gigabit Ethernet Card	PPA2
20-port Gigabit Ethernet	PPA3
10-port Gigabit Ethernet DDR	PPA3
20-port Gigabit Ethernet DDR	PPA3
1-port 10 Gigabit Ethernet Card	PPA2
4-port 10 Gigabit Ethernet DDR	PPA3
1-port 10 Gigabit Ethernet/OC-192c DDR	PPA2

2.2 Step 2: Displaying Chassis Information

Table 4 describes the output fields for the **`show chassis`** command, which you use to display information about installed and configured cards. For detailed information about each field displayed, see the *Command List*.

Table 4 Field Descriptions for the show chassis Command

Field	Description
Current platform is	Chassis type: • SE100—SmartEdge 100 router. • SE400—SmartEdge 400 router. • SE600— The SmartEdge 600 router is a carrier-class product with an architecture that supports packetized traffic. It can be used as an edge aggregation router and simultaneously as a broadband remote access server (BRAS) to directly connect customers to the network. It supports a variety of interfaces and vital services, such as routing protocols, quality of service (QoS), and inbound and outbound access control lists (ACLs). • SE800e—SmartEdge 800 router: equipped with BNC connectors. • SE800s—SmartEdge 800 router: equipped without BNC connectors. • SE1200—Standard SmartEdge router. • SE1200h— The SmartEdge 1200H router is a carrier-class product with an architecture that supports packetized traffic. It has a higher power rating than the SmartEdge 1200 router allowing it to support a greater number of PPA3-based line cards. The SmartEdge 1200H router can be used as an edge aggregation router and simultaneously as a broadband remote access server (BRAS) to directly connect customers to the network. It supports a variety of interfaces and vital services, such as routing protocols, quality of service (QoS), and inbound and outbound access control lists (ACLs). New services can easily be added with software upgrades. Because of the optimized packet-forwarding capabilities and support of high-bandwidth uplink interfaces, the SmartEdge 1200H router can also be used in the metropolitan core to aggregate traffic from other routers into the long-haul transit core. • SE1200 NEBS—NEBS-compliant SmartEdge 1200 router.
Slot	*`slot`*—Slot number for this unit.

Table 4 Field Descriptions for the show chassis Command

Field	Description
Configured-type	Slot is configured for one of the following card types: • ***`traffic-card-type`***—Line card needs to be configured after installing the card in the slots. • xcrp—Controller card of any type or controller carrier card needs to be installed; it does not have to be configured. • none—Nonpreconfigured slot.
Installed type	Slot has card installed: • carrier—I/O carrier card; always reported for slot 2 for the SE100 chassis. • ***`traffic-card-type`***—Line card. • xcrp—Controller card of any type. • none—Empty slot. • unknown—Installed but not initialized Controller card.

Table 4 Field Descriptions for the show chassis Command

Field	Description
Initialized	State of card: • No—PPAs have not been initialized for this card. • Yes—PPAs have been initialized for this card.
Flags	Flags status of card: • A—Active Crossconnect. • B—Standby Crossconnect; not displayed for the SE 100 chassis. • C—All segmentation and reassembly controllers (SARCs) ready. • D—Card has been assigned as the default line card; displayed for slot 2 in the SmartEdge 100 chassis. • E—Egress Packet Processing ASIC (PPA) is ready; displayed for slot 2 in the SmartEdge 100 chassis. • G—FPGA is upgrading; displayed for slot 2 in the SmartEdge 100 chassis. • H—Card is administratively shut down; displayed for slot 2 in the SmartEdge 100 chassis. • I—Ingress PPA is ready; displayed for slot 2 in the SmartEdge 100 chassis. • M—FPGA is mismatch; displayed for slot 2 in the SmartEdge 100 chassis.(1) • N—SONET EU is enabled; not displayed for the SmartEdge 100 chassis. • O—Card is in the ODD state; displayed for slot 2 in the SmartEdge 100 chassis. • R—Line card is ready; displayed for slot 2 in the SmartEdge 100 chassis. • S—Segmented PPA is ready; not displayed for the SmartEdge 100 chassis. • U—Line card PPAs are up; not displayed for the SmartEdge 100 chassis. • W—Warm reboot; card has not been reloaded since the last switchover; not displayed for the SmartEdge 100 chassis. • X—XCRP cards are mismatched. The standby and active controller cards are not identical; not displayed for the SmartEdge 100 chassis.

Table 4 Field Descriptions for the show chassis Command

(1) The version of the FPGA that is installed on this line card and the version that is shipped with this release of the SmartEdge OS do not match; you must update the FPGA on this line card for it to initialize. To upgrade the FPGAs on this line card, see the Release Notes for the SmartEdge OS for the release that is installed on this SmartEdge router.

The following example displays output from the **`show chassis`** command for a SmartEdge 800e router. In slot `13`, e-3-6-port displays a normal status of `Yes IEUDRC`. Use the Flags legend in the output to interpret the results of the output and check for the correct flag status:

```
[local]Redback# show chassis

Current platform is SE800e
(Flags: A-Active Crossconnect    B-StandBy Crossconnect  C-SARC Ready
D-Default Traffic Card   E-EPPA Ready            G-Upgrading FPGA
H-Card Admin State SHUT  I-IPPA Ready            M-FPGA Mismatch
N-SONET EU Enabled       O-Card Admin State ODD  R-Traffic Card Ready
S-SPPA Ready             U-Card PPAs UP          W-Warm Reboot
X-XCRP mismatch)
Slot: Configured-type           Slot: Installed-type    Initialized Flags
-------------------------------------------------------------------------
1 : atm-oc3e-8-port             1 : atm-oc3e-8-port           Yes IEUDRC
2 : atm-oc3e-8-port             2 : atm-oc3e-8-port           Yes IEURC
3 : atm-oc3e-8-port             3 : atm-oc3e-8-port           Yes IEURC
4 : atm-oc3e-8-port             4 : atm-oc3e-8-port           Yes IEURC
5 : ge-10-port                  5 : ge-10-port                Yes IEUR
6 : ge-10-port                  6 : ge-10-port                Yes IEUR
7 : xcrp                        7 : xcrp                      Yes A
8 : xcrp                        8 : xcrp                      Yes B
9 : ge-10-port                  9 : ge-10-port                Yes IEUR
10 : ge-10-port                 10 : ge-10-port               Yes IEUR
11 : atm-oc3e-8-port            11 : atm-oc3e-8-port          Yes IEURC
12 : atm-oc3e-8-port            12 : atm-oc3e-8-port          Yes IEURC
13 : atm-oc3e-8-port            13 : atm-oc3e-8-port          Yes IEURC
14 : atm-oc3e-8-port            14 : atm-oc3e-8-port          Yes IEURC
```

The following example displays output from the **`show chassis`** command for a SmartEdge 400 router. In this example, the standby cross connect, identified by the `B` flag, is not initialized because it and the active cross connect, identified by the `A` flag, are not identical. The `X` flag indicates that the standby and active cross connect have an XCRP mismatch.

```
[local]Redback#show chassis
Current platform is SE400
 (Flags: A-Active Crossconnect    B-StandBy Crossconnect  C-SARC Ready
         D-Default Traffic Card   E-EPPA Ready            G-Upgrading FPGA
         H-Card Admin State SHUT  I-IPPA Ready            M-FPGA Mismatch
         N-SONET EU Enabled       O-Card Admin State ODD  R-Traffic Card Ready
         S-SPPA Ready             U-Card PPAs UP          W-Warm Reboot
         X-XCRP mismatch)
Slot: Configured-type           Slot: Installed-type    Initialized Flags
-------------------------------------------------------------------------
  1 : none                        1 : oc48e-4-port              No
  2 : none                        2 : oc48e-4-port              No
  3 : none                        3 : oc48e-4-port              No
  4 : none                        4 : oc12e-2-port              No
  5 : none                        5 : xcrp4                     No  BX
  6 : xcrp4                       6 : xcrp                      Yes A
```

Recommended Action: Make sure the active XCRP matches the standby XCRP.

2.3 Step 3: Displaying Results from Power-on Diagnostics

This section shows how to configure and use the SmartEdge power-on diagnostics (POD) and system alarm and provides instructions on troubleshooting line cards by using CLI commands.

2.3.1 Terminology

Controller card—The Cross-Connect Route Processor (XCRP4) Controller card, including the controller carrier card, unless otherwise noted.

Controller carrier card—The controller functions on the circuit board within the SmartEdge 100 chassis.

I/O carrier card—The line card functions on the circuit board; these functions are compatible with the similar functions that are implemented on all SmartEdge 400 and SmartEdge 800 line cards.

Chassis—Any SmartEdge chassis; SmartEdge 800 refers to any version of the SmartEdge 800 chassis; the SmartEdge 800s refers only to the SmartEdge 800s chassis.

Traffic card—SmartEdge 100 media interface card (MIC) or a line card installed in any other SmartEdge chassis, unless otherwise noted.

2.3.2 Overview of Power-on Diagnostics

The configuration tasks and commands described in this section allow you to perform general system-wide monitoring and testing tasks, such as enabling power-on diagnostics and alarms.

Note: Unless explicitly stated in the command descriptions, the SmartEdge 100 router supports all tasks described in this section.

Power-on diagnostics (POD) verify the correct operation of the controller cards, backplane, fan tray, and each installed line card during a power-on or reload sequence. These tests also run whenever a controller card or line card is installed in a running system. The POD for each component consist of a series of tests, each of which can indicate a component failure.

During each test, the POD display results and status; if an error occurs, the test lights the FAIL LED on the failing card but does not stop the loading of the SmartEdge OS. A backplane or fan tray that fails lights the FAN LED on the fan tray.

The maximum test time is 130 seconds: 60 seconds for a controller card, 10 seconds for the backplane and fan tray, and 5 seconds for each installed line card. If the system has two controller cards, the controller tests run in parallel.

To display results from POD, enter one of the following commands in any mode:

```
show diag pod component
```

```
show diag pod component detail
```

Table 5 lists the values for the *component* argument.

Table 5 Components Tested by POD

Component	Component Argument Values
Backplane	`backplane`
Controller card	`card 7` and `card 8` for the SE 800 and SE 1200 `card 5` and `card 6` for the SE 400
Fan tray	`fan tray`
Line card	`card` *n* (slot number from 1 to 6 or 9 to 14)

The **detail** keyword displays which test the component failed.

In general, if a component fails to pass its POD tests, you might need to replace it. Contact your local technical support representative for more information about the results of a failed test.

POD are enabled by default in the SmartEdge OS; if they have been disabled, you can enable them with the **diag pod** command in global configuration mode.

2.3.3 Power-on Diagnostics and System Alarm Configuration Tasks

To enable power-on diagnostics (POD) and the system alarm, perform the tasks described in Table 6; enter all commands in global configuration mode.

Table 6 Enable Power-on Diagnostics and System Alarm

Task	Root Command	Notes
Enable power-on diagnostics.	**`diag pod`**	This is the default condition.

Enable the alarm for the air filter in a SmartEdge chassis, or enable the redundancy alarm for SmartEdge systems with two controllers, or enable the transceiver alarm.	**`system alarm air-filter`**
	`system alarm redundancy`
	`system alarm transceiver`	

2.3.4 Hardware Monitoring Tasks

To monitor or administer devices, perform the relevant tasks described in Table 7. Enter the **`service air-filter`** command in exec mode; enter the **`show`** commands in any mode.

Table 7 Hardware Monitoring Tasks

Task	Root Command
Display chassis installed and configured cards and their status.	**`show chassis`**
Display chassis power data for the installed cards.	**`show chassis power`**
Display information about the system hardware.	**`show redundancy`**
Display the state of the standby controller card and verify whether it is ready to become active.	**`show redundancy`**
Display system-, card-, port-, channel-, or subchannel-level alarms.	**`show system alarm`**
Display information about the system hardware.	**`show hardware`**

Note: To enable the alarm for the air filter in a SmartEdge 400 chassis, enter the **`service alarm`** command (in global configuration mode).

2.3.5 Port, Channel, and Line Card Troubleshooting Commands

To troubleshoot a port or channel or restore a card to normal operations, perform the relevant tasks described in Table 8.

Table 8 Port, Channel, and Line Card Troubleshooting

Task	Root Command
Reload traffic and services cards in the chassis.	**`reload card`** *`slot`*
Reload the code in the FPGAs on a particular line card.	**`reload fpga card`** *`slot`*
Reload the specified MIC and all associated components and reformat the compact-flash (CF) card installed in the external slot of the SmartEdge 100 chassis.	**`reload mic`**

Note: If you plug an external loopback plug into a copper GE port that is not shut down, the port becomes stuck in the autonegotiating, link-down state.

2.3.6 Enabling Power-on Diagnostics

The following example shows how to enable power-on diagnostics in configuration mode. You do not need to reload the system to apply the changes. However, you will need to reload any cards already in use to have POD run on them.

```
[local]Redback#
[local]Redback#configure
[local]Redback#(config)#diag
[local]Redback#exit
[local]Redback#reload
```

2.3.7 Displaying Results of the Power-on Diagnostics

By default, POD is enabled on all cards. If it is disabled, you can enable POD with the following `diag pod` command. The POD sequence includes a configured card when the card is seated into a configured slot. If the slot does not have a POD status, the card is not configured.

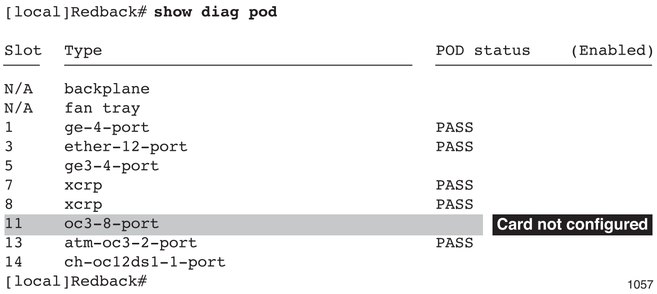
```
[local]Redback# (config)#diag pod
[local]Redback# (config)# end
[local]Redback# show diag pod card slot detail
[local]Redback# show diag pod


Slot Type                           POD status(Enabled)
 --------------------------------------------------------
N/A backplane
N/A fan tray
1 ge3-4-port                        PASS
3 ge-10-port                        PASS
5 ge3-4-port
7 xcrp                              PASS
8 xcrp                              PASS
11 oc3e-8-port
13 atm-oc3-2-port                   PASS

[local]Redback# show diag pod card 3 detail
Slot Type                           POD status(Enabled)
----------------------------------------------------------
 3    ge-10-port                    PASS
      Start at 22:49:30 02/13/2007
      Card Type Valid               PASS
      JAM 1 SCL                     PASS
      JAM 0 SCL                     PASS
      EPPA SCL                      PASS
      IPPA SCL                      PASS
      SCL Hub                       PASS
      Octal Phy                     PASS
      Voltage Check                 PASS
      Temperature Check             PASS
      Verify Card Type              PASS
      Verify EEPROM Check Sum       PASS
      System FPGA PASS
      IPPA file load (PPA binary)   PASS
      IPPA Memory PASS
      EPPA file load (PPA binary)   PASS
      EPPA Memory                   PASS
      Lim Bus                       PASS
      fpga Config Check             PASS
      Flip 0 Bus                    PASS
      Flip 1 Bus                    PASS
      ie21440 Emac 0                PASS
      ie21440 Emac 1                PASS
```

2.3.8 Displaying a Card that Is Not Configured

Only configured cards are listed in the POD status in the power on diagnostics sequence when seated into a configured slot. Each time a card is reseated, it undergoes the POD again. The following example shows a card that is not configured.



```
[local]Redback# show diag pod

Slot   Type                                      POD status    (Enabled)
----   ---------------------------------------   ------------------------

N/A    backplane
N/A    fan tray
1      ge-4-port                                 PASS
3      ether-12-port                             PASS
5      ge3-4-port
7      xcrp                                      PASS
8      xcrp                                      PASS
11     oc3-8-port
13     atm-oc3-2-port                            PASS
14     ch-oc12ds1-1-port
[local]Redback#
```

2.4 Step 4: Checking Fan Tray Power

Use the **show diag pod fantray detail** command to display test results of the POD for the fan tray, or the fan and alarm unit. Use the **clear diag on-demand** command to clear the log entries for on-demand diagnostic (ODD) sessions for one or more cards. For more information about POD, see the SmartEdge router hardware guides.

The following example shows that fantray power A has POD status of FAIL:

```
[local]Redback#show diag pod fantray detail
Slot Type                                        POD status (Enabled)
--------------------------------------------------------------------
N/A fan tray
Fantray Present                                  PASS
Fantray Primary CheckSum                         PASS
Fantray Secondary CheckSum                       PASS
Fantray ID Check                                 PASS
Fantray Power A                                  FAIL
Fantray Power B                                  PASS


Test Failure Details:POD test. Time: 00:00:13  12/11/2008
TestName: Fantray Power A, slot 16
Error: 0x1d02 -> FANTRAY_POWER_FAIL
Fantray Power A fail
```

Recommended Action: The fan tray power POD status alarm has a POD status of FAIL probably because only one of power supplies is connected to the fan tray; this configuration is supported. Check to see if you are using redundant fan tray power supplies. If so, use a multimeter to verify the current on the failed power source.

2.5 Step 5: Displaying Information About the Backplane

2.5.1 Displaying Hardware Backplane Information

Use the **`show hardware backplane`** command to display information about the backplane. For more information about this command, see *Command List*.

The following example shows how to display information about the backplane.

```
[local]Redback# show hardware backplane
Slot  Type      Serial No      Rev  Ver Mfg  Date    Voltage Temp
----  --------  -------------- ---  --- -----------  ------- ----
N/A   backplane 0A014090501402  1    4  21-DEC-2005  N/A     N/A
```

2.5.2 Displaying Detailed Backplane Information

The following example displays detailed information about the backplane on a SmartEdge 800e router.

```
[local]Redback# show hardware backplane detail
Slot             :N/A                 Type           : backplane
Serial No        :8Y034090502265      Hardware Rev   : 03
EEPROM id/ver    :0x5a/4              Mfg Date       : 12-OCT-2005
MAC Address      :00:30:88:01:45:FA
ODD Status       :Not Available
Chassis Type     :SE800e
```

2.6 Step 6: Checking System Alarms

The **show system alarm** command displays system, card, port, channel or subchannel-level alarms. When you use the **all** option, the system displays alarms at all levels. For more information about alarms and how to interpret them, see the SmartEdge router hardware guides.

To enable the system alarm, enter the **system alarm command** in global configuration mode. The default state of this alarm is disabled. This command enables the alarm for the air filter in the SmartEdge chassis, the redundancy alarm for SmartEdge systems with two controllers, and the transceiver alarm.

2.6.1 Displaying System Alarm

The following example shows an active alarm using the **show system alarms** command.

```
[local]Redback# show system alarm
Timestamp        Type     Source    Severity   Description
-----------------------------------------------------------------------------
Jan 19 10:37:58  chassis            Minor      Chassis power failure - side B
```

2.6.2 Displaying All System Alarms

The following example show active alarms on the fantray and chassis using the **show system alarm** command with the keyword **all**, which displays alarms at all levels:

```
[local]Redback# show system alarm all
Timestamp         Type    Source  Severity   Description
-----------------------------------------------------------------------------
Jun 12 17:42:56   chassis         Minor      Fan tray failure detected
Jun 12 17:42:56   chassis         Minor      Fantray power-on diagnostic failed
Jun 12 17:42:56   chassis         Minor      Chassis power failure - side A1
Jun 12 17:42:56   chassis         Minor      Chassis power failure - side A2
```

2.7 Step 7: Checking On-Demand Diagnostics

This section shows how to determine if problems are caused by hardware malfunctions using on-demand diagnostics (ODD). For more information about ODD, see the SmartEdge hardware guides.

2.7.1 Overview of On-Demand Diagnostics

You can use on-demand diagnostics ODD to verify hardware status or isolate a fault in a field replaceable unit (FRU).

If a component fails to pass POD or ODD tests, you might need to replace it. Contact your local technical support representative for more information about the results of a failed test.

Four levels of tests are supported; not all cards support all levels of tests. Table 9 lists the levels and types of tests performed, and the components for which the tests are supported on the SmartEdge routers. The packet mesh test verifies the correct operation of each traffic and services card selected for the mesh test (at level 2) and the mesh between them. The slot argument range is different on other platforms.

Table 9 ODD Test Levels

Level	Components	Tests
1	All	Duplicates the tests of the POD; runs in 5 to 10 seconds.
2	Standby controller card, line cards only	Includes level 1 tests—all onboard active components on the line interface module (LIM) of the board, including memory, registers, PPA DIMMs and SRAM, PPA, and other onboard processors; runs in 5 to 10 minutes. The SmartEdge 100 platform does not support a standby controller card.

Table 9 ODD Test Levels

Level	Components	Tests
3	Line cards, I/O carrier card, and MICs and standby XCRP4 controller cards	Includes level 2 tests, and verifies the data paths for the entire card with internal loopbacks; runs in 10 to 15 minutes.
4	Line cards, I/O carrier card, and MICs and standby XCRP4 controller cards.	Includes level 3 tests—Tests the entire card using external loopbacks; must be run on site with external loopback cables installed; runs in 10 to 15 minutes. To run external loopback tests you must install external cabling: • Fast Ethernet/Gigabit Ethernet line cards—install external loopback plugs on the FE and GE ports • GE ports— can be connected back-to-back • BiDirectional SFPs— require explicit cabling between left and right hand ports and requires both left and right hand BiDi SFPs • 5-port GE—This line card is an exception for this ODD test. One way to test this extra port is by having two 5-port GE cards in the system and connecting them. • Copper SFPs—install external loopback cables between neighboring ports.

Note: Any MIC, if it is installed, is tested as part of the testing of the I/O carrier card.

If the level you select is not supported for the unit you want to test, the tests run at the highest level for that unit. For example, if you specify level 3 for an XCRP4 Controller card, the system runs the tests at level 2 instead.

Table 10 lists the available parameters for an ODD session.

Table 10 Parameters for ODD Sessions

Parameter	Description
`card` *`card-type slot`*	Specifies the line card in the slot to be tested; see Table 11.
`standby`	Tests the standby controller card (can only be run from the active XCRP card). The SmartEdge 100 platform does not support a standby controller card.
`level` *`level`*	Specifies the level at which the test is to be initiated.
`loop` *`loop-num`*	Specifies the number of times to repeat the diagnostic test.

For the SmartEdge 100 chassis, the controller carrier card is in slot 1; the I/O carrier card, including native ports and MICs, is in slot 2.

For a SmartEdge 400 chassis, the standby controller is in slot 5 or 6; for a SmartEdge 800 or SmartEdge 1200 chassis, the standby controller is in slot 7 or 8.

For both the SE600 and SE1200H chassis, the standby controller is in 7 or 8.

Table 11 lists the values for the *`slot`* argument for the SmartEdge 400, SmartEdge 800, SmartEdge 600, SmartEdge 1200, SmartEdge 1200H line cards.

Table 11 Tests the Line Card, Services Card, Storage Card, or Standby Controller Card Slots for the diag on-demand Command

	***`slot`* Argument Range**		
Type of Line Card/Description	**SmartEdge 800 router, SmartEdge router 1200 or 1200H.**	**SmartEdge 400 router**	**SmartEdge 600 router**
SONET/SDH			
OC-192c/STM-64c OC-48c/STM-16c OC-12c/STM-4c OC-3c/STM-1c	1 to 6 and 9 to 14	1 to 4	1 to 6
ATM			
ATM OC-12c/STM-4c ATM OC-3c/STM-1c	1 to 6 and 9 to 14	1 to 4	1 to 6
Ethernet			
10/100 Ethernet Fast Ethernet-Gigabit Ethernet (FE-GE) Gigabit Ethernet Advanced Gigabit Ethernet Gigabit Ethernet 1020 (GE 1020) Gigabit Ethernet 3 (GE3) 10 Gigabit Ethernet (10GE)	1 to 6 and 9 to 14	1 to 4	1 to 6
Advanced Services Engine			
ASE (1)	1 to 6 and 9 to 14	1 to 4	1 to 6

Table 11 Tests the Line Card, Services Card, Storage Card, or Standby Controller Card Slots for the diag on-demand Command

	`slot` Argument Range		
Type of Line Card/Description	**SmartEdge 800 router, SmartEdge router 1200 or 1200H.**	**SmartEdge 400 router**	**SmartEdge 600 router**
SmartEdge Storage Engine			
SSE [2]	1 to 6 and 9 to 14	N/A	1 to 6

(1) To test ASPs, they must be provisioned before running ODD. For more information about running ODD on ASE cards see ASE Troubleshooting Guide.

(2) For more information about running ODD on SSE cards, see SSE Configuration and Operation

Note: Low-density versions of the line cards are also supported, but only the enabled ports are tested. Use the **`show hardware`** command (in any mode) with the **`card`** and **`detail`** keywords to determine which ports are enabled.

2.7.1.1 Guidelines for SmartEdge 400, 600, 800, 1200, and 1200H Chassis

The following guidelines apply to the on-demand testing of line cards, services cards, storage cards, or standby controller cards on SmartEdge 400, 600, 800, 1200 and 1200H chassis:

- ODD testing requires version 2.0.2.9 or later of the system boot ROM. To view the currently installed version, enter the **`show version`** command in any mode. To upgrade the boot ROM, see the *Installing the SmartEdge OS*.
- To test a line card, you must put it in the ODD state; see Run ODD for SmartEdge Chassis 400, 800, 1200 for instructions.

  The cards that you can test depend on the release of the software. In the current release, you can test the following cards:

  - XCRP4 controller cards, when they are in the standby state.

    You cannot run ODD tests on the active XCRP controller card. To test the active controller card, perform an XCRP switchover and run the test from the newly active controller card.
  - ATM OC-12c/STM-4c line cards, and second-generation ATM OC line cards.
  - Fast Ethernet-Gigabit Ethernet (FE-GE) line cards.
  - Gigabit Ethernet line cards (all versions).
  - SONET/SDH OC-3c/STM-1c line cards, OC-12c/STM-4c line cards, OC-48c/STM-16c, OC-192c/STM-64c line cards.

  - Advanced Services Engine (ASE) cards.
  - SmartEdge Storage Engine (SSE) cards.

  Note: The SmartEdge 1200 router does not support the mesh test.

- Low-density versions of line cards are also supported, but only the enabled ports are tested.
- Before you can test a traffic or services card, you must take it out of service and put it in the ODD state. The standby controller card does not need this preparation.

2.7.1.2 Guidelines for the SmartEdge 100 Chassis

The following guidelines apply to the on-demand testing of carrier cards and MICs in a SmartEdge 100 chassis:

- The cards that you can test depend on the release of the software. In the current release, you can test:
  - Controller carrier card (controller functions)
  - I/O carrier card (line card functions)
  - Ethernet management ports, native ports, and MIC ports
  - ATM OC-3c/STM-1c MIC ports
- Before you can test the carrier card and any MIC, you must take the system out of service.

Note: The SmartEdge 100 router does not support the mesh test.

2.7.1.3 Viewing and Recording ODD Results

A session log stores the most recent results for each card, in main memory and also on the compact-flash card for low-level software. In addition, a history file on the compact-flash card stores the results for the previous 100 sessions.

You can display partial test results while the tests are in progress; a notification message is displayed when the session is complete. To view test results, enter the **`show diag on-demand`** command (in any mode) at any time. You can display the latest results for a traffic or standby controller card from the log or the results for one or more sessions from the history file.

Note: If you are connected to the system using the Ethernet management port, you must enter the **`terminal monitor`** command (in exec mode) before you start the test session so that the system displays the completion message. For more information about the **`terminal monitor`** command, see *Basic Troubleshooting Techniques*.

To display the results from ODD sessions, perform one of the following tasks; all commands can be entered in any mode.

1. Display results for all components from the last initiated session using the **`show diag on-demand`** command.

2. Display results for a line card using the **`show diag on-demand card`** *`slot`* command.

3. Display results for the standby controller card using the **`show diag on-demand standby`** command.

4. Display results for the last *n* sessions with the **`show diag on-demand history`** *`n`* command.

   The latest session is displayed first. Up to 100 sessions can be listed.

2.7.1.4 ODD Test Result Definitions

For SmartEdge line cards, if the version of the Sys FPGA is not 0x7 or later, the voltage check, temperature check, and bus tests cannot be run; they are skipped, and the session status is reported as “Incomplete”. To identify which version of Sys FPGA you have, enter the **`show hardware`** command with the **`card`** and **`detail`** keywords (in any mode) to display the FPGA version in the SysFpga field.

In general, if a unit fails a test, you should replace it. Contact your local technical support representative for more information about the results of a failed test. For information about how to upgrade a FPGA version on a line card, see Section 2.1 on page 4.

Table 12 lists the states of the LEDs when an ODD session runs on a line card or standby controller card in a SmartEdge 400, 800, 1200 chassis.

Table 12 Card LED States During and After an ODD Session

Traffic or Standby Controller Card State	State of LEDs
Out of service (`shutdown` command)	FAIL, ACTIVE, and STDBY LEDs are off.
ODD (`on-demand-diagnostic` command)	FAIL, ACTIVE, and STDBY LEDs are off.
Session is in progress	FAIL, ACTIVE, and STDBY LEDs blink.
End of session with one or more failures	FAIL LED on; ACTIVE, and STDBY LEDs are turned off until the card is returned to the in-service state.
End of terminated session	FAIL LED off; ACTIVE, and STDBY LEDs are turned off until the card is returned to the in-service state.
End of successful session	FAIL LED, ACTIVE, and STDBY LEDs are turned off until the card is returned to the in-service state.

Table 13 lists the states of the SmartEdge 100 LEDs when an ODD session runs on either the controller carrier card or I/O carrier card.

Table 13 SmartEdge 100 LED States During ODD

ODD Test Configuration[(1)]	STAT LED (Green)	ALRM LED (Red)	SWAP LED (Blue)	Native Port LEDs	MIC Port LEDs
Controller functions only ; no MICs are inserted or configured. No ports are configured.	Flashes during tests	OFF	OFF	OFF	N/A[(2)]
Controller functions with MICs inserted; MIC and native ports are configured and are UP.	Flashes during tests	OFF	OFF	Unaffected by ODD[(3)]	Unaffected by ODD3
Line card functions only ; no MICs are inserted or configured. No ports are configured.	Unaffected by ODD	OFF	Unaffected by ODD	OFF	N/A2
Line card functions with MICs inserted; MIC and native ports are configured and are UP.	Unaffected by ODD	Unaffected by ODD	Unaffected by ODD	OFF	OFF

(1) Configuration is lost if not saved before running ODD.

(2) No MICs are installed in the MIC slots.

(3) LEDs are unaffected except for a brief blink during port initialization if they were on before ODD.

Table 14 lists the possible status for an ODD session.

Table 14 Status Descriptions for an ODD Session

Session Status	Description
Aborted	Session was terminated by the user or when the standby controller card was removed.
Incomplete	At least one of the requested tests could not be run.
In-Progress	Session is currently in progress.
n Failures	Session was completed with a number of test failures.
Passed	All tests passed.

Table 15 lists the displayed descriptions for the test status.

Table 15 Status Descriptions for a Test

Test Status	Description
Aborted	Test was started but terminated when the standby controller card was removed.
Failed	Test ran and failed.
Not Run	Test has not yet run (initial state).
Passed	Test ran successfully.
Running	Test is currently in progress.
Skipped	Test could not be run; for example, the part revision is earlier than the required minimum version, or no file was found.

In the case of a mesh test failure, the test results can mean that one of the cards has failed, one of the slots has failed, or that the mesh itself has failed. Use the **`mesh`** and **`detail`** keywords with the **`show diag`** command to display the results of the mesh test; depending on the results, you can run the mesh test several times with different slot combinations. Mesh test results are cumulative; you can view the results of all slot combinations before notifying your local technical support representative.

Perform the following steps to initiate an ODD session:

1. If you are testing a line card, change its state to ODD; otherwise, proceed to step 2.

2. To test one or more components, enter one of the commands in Table 10.

2.7.1.5 Clearing Results from ODD Sessions

To clear or display the results from on-demand diagnostic sessions, perform the tasks described in Table 16. Enter the **`clear diag`** and **`diag on-demand`**

mesh commands in exec mode. Enter the **show diag** command, which can display results for up to 20 sessions from the history log, in any mode.

Table 16 Administer ODD and POD Results

Task	**Root Command**
Clear the results from the last initiated session.	**clear diag on-demand**
Clear the latest results for all components tested.	**clear diag on-demand all**
Clear the latest results for a line card.	**clear diag on-demand card** *slot*
Clear the latest results for the standby controller card.	**clear diag on-demand standby**
Reset the results from mesh tests.(1) (2)	**diag on-demand mesh**
Display the results of power-on or on-demand diagnostic tests.	**show diag**

(1) The mesh test results are cumulative for each slot combination that you run to allow you to view results from all the slot combinations. Results are not cleared until you explicitly reset them with this command.

(2) These tests are not supported on the SmartEdge 100 chassis.

2.7.2 Running ODD for SmartEdge 400, 800, 600, 1200 and 1200H Chassis

2.7.2.1 Running ODD on a Chassis

To run ODD tests on a SmartEdge 400, 800, 600, 1200, and 1200H chassis, perform the follow tasks.

1. Initiate an ODD session on a chassis with one of the following tasks:

    - Initiate a session for a specific unit with the **`diag on-demand`** command.

    - Initiate a mesh test for two or more line cards with the **`diag on-demand mesh`** command.

    To terminate an ODD session, enter the **`no`** form of the **`diag on-demand`** command.

2.7.2.2 Running ODD on a Line Card, Services Card, or Storage Card

Before running ODD on a line card, services card, or storage card, you must remove it from service. To remove a card from service and run ODD on it, perform the following tasks (all commands are entered in card configuration mode, unless otherwise noted):

1. In global configuration mode, specify the line card or service card and access card configuration mode using the **`card`** *`type slot`* command.

2. Put the ports in the OSS state with the **`shutdown`** command.

    This command saves the state of the native ports and MIC ports and circuits configured on them.

    If there are cross-connected circuits configured on any of the ports, this command disables the cross-connections and saves their state.

3. Put the line card functions on the carrier card in the ODD state with the **`on-demand-diagnostics`** command.

4. Commit the previous commands to the database and return to global configuration mode with the **`end`** command.

5. In global configuration mode, run the ODD session with the **`diag on-demand card`** *`slot`* **`level-num`** *`level`* **`loop-num`** command.

    Do not interrupt the system during the ODD process. When the process is complete, the router displays a message in the CLI.

Note: If ASE card memory errors occur during ODD, perform the following actions:

- If there were multibit errors during the memory testing, RMA the card immediately.
- If there were only single bit errors during the memory testing, RMA the card at the next scheduled service period, if a replacement is not available.

2.7.2.3 Return a Card to In-Service State

After testing a line card, you must return it to the in-service state. To return the line card to the in-service state from the ODD state, perform the following tasks; enter the commands in card configuration mode unless otherwise noted:

1. In global configuration mode, specify the card that was tested and access card configuration mode using the **`card`** ***`type slot`*** command.
2. Remove the card from the ODD state and put it in the OSS state using the **`no on-demand-diagnostic`** command.
3. Return the card to the in-service state; restore any cross-connections using the **`no shut down`** command.

   This command restores any cross-connections to their state at the time of the shutdown.
4. Commit the previous commands to the database and return to exec mode with the **`end`**.

Note: To reload the card by using the **`reload card`** in exec mode, you must first remove the card from the ODD state.

2.7.2.4 Preparing and Running ODD on XCRP Controller Cards

You can execute ODD only on the standby XCRP card (and you must enter the command from the CLI on the active XCRP card).. To test the active XCRP card, you must perform a manual switchover. Because the standby XCRP is already out of service, the configuration commands to put a card in the out-of-service state (OSS) or ODD state are not applicable.

To run ODD on the XCRP controller cards, perform the following steps logged on through the console:

1. In exec mode on the active XCRP card CLI, enter the **`diag on-demand standby`** [**`level`** ***`level-num`***] [**`loops`** ***`loop-num`***] command.
2. Perform an XCRP switchover with the **`reload switchover`** command.
3. When the switchover is complete (redundancy is fully restored), run ODD on the new standby XCRP card.

To view the results of an ODD test, see Section 2.7.1.4 on page 29.

2.7.2.5 Indications of SmartEdge 400, 600, 800, 1200, and 1200H ODD Test Failures

Table 17 lists the alarms, FAIL LED, ODD history, log, and ODD status for a card after an ODD session during which the card failed one or more tests. It also lists the effects of various actions on these indicators.

The following guidelines apply to the data and operations listed in Table 17:

- You can display alarm, LED, and ODD status using the **`show hardware`** command (in any mode).
- You can clear the ODD log or history using the **`clear diag on-demand`** command (in exec mode).
- If you replace a line card or standby controller card or reload the system, this could cause the power-on diagnostics (POD) to run; after that, the LED status reflects the results of the POD tests. You cannot reload a line card or standby controller card when it is in the ODD state.

Table 17 ODD and LED Conditions for Any SmartEdge XCRP Controller or Line Card

State(1) of Indicator After	Clear Log(2)	Clear History	Replace Card(3)	Reload System	Reload Card or Change State—ODD to OSS	Successful ODD Session
Alarm conditions	On	On	Cleared	Cleared	On	Cleared
Alarm status	On	On	Cleared	Cleared	On	Cleared
FAIL LED	On	On	Cleared	Cleared	On	Cleared
LED status	Unchanged	Unchange d	See Note 3	See Note 3	See Note 3	See Table 12.
ODD history	Unchanged	Cleared	Unchanged	Unchanged	Unchanged	History file is updated
ODD log	Cleared	Unchange d	Unchanged	Unchanged	Unchanged	Log is updated
ODD status	Failed	Failed	Not available	Not available	Failed	No failures were detected

(1) You can display alarm, LED, and ODD states by using the ***show hardware*** *command with the* ***detail*** *keyword (in any mode).*

*(2) You can clear the ODD log or history using the****clear diag*** *command (in exec mode).*

(3) Replacing a card or reloading the system causes the POD to run; the LED status reflects the results of the POD tests. You cannot reload a card if it is in the ODD state.

2.7.3 Running ODD for the SmartEdge 100 Components

2.7.3.1 Running ODD for the SmartEdge 100 Chassis

To run ODD tests on the controller carrier card in a SmartEdge 100 chassis, enter the **diag on-demand** command in exec mode.

Specify slot 1 for the **card** ***slot*** construct.

2.7.3.2 Preparing I/O Carrier Cards and MIC Ports and Running ODD on Them

To run ODD tests on the I/O carrier card (line card functions) for all native and MIC ports in a SmartEdge 100 chassis, perform the following tasks; enter all commands in exec mode.

Any MIC, if it is installed, is tested as part of the testing of the line card functions on the carrier card.

1. In global configuration mode, specify the carrier card to be tested and access card configuration mode with the **card** ***type slot*** command.

2. Save the state of the native ports and MIC ports and circuits configured on them and put the ports in the OSS state with the **shutdown** command.

   If there are cross-connected circuits configured on any of the ports, this command disables the cross-connections and saves their state.

3. Put the line card functions on the carrier card in the ODD state with the **on-demand-diagnostic** command.

4. Run the ODD session with the **diag on-demand card** ***slot*** **level*****level-num*** **loop** ***loop-num*** command.

5. Commit the previous commands to the database and return to exec mode with the **end** command.

6. Initiate an ODD session with the **diag on-demand** command.

   Specify slot `2` for the **card** ***slot*** construct.

   To terminate a running ODD session, enter the **no** form of the **diag on-demand** command. Otherwise, do not interrupt the system during the ODD process. When the process is complete, the router displays a message in the CLI.

7. Return the I/O carrier card to the in-service state; see Section 2.7.2.3 on page 34.

2.7.3.3 Indications of SmartEdge 100 ODD Test Failures

Table 18 lists the condition of the alarms, LED status, ODD history, log, and ODD status for a card after an ODD session during which the card failed one or more tests. It also lists the effect of various actions on these indicators.

Note:

The following guidelines apply:

- You can display alarm, LED, and ODD status by using the **`show hardware`** command (in any mode).
- You can clear the ODD log or history using the **`clear diag`** command (in exec mode).
- Replacing a MIC or reloading the system causes the power-on diagnostics (POD) to run; the LED status reflects the results of the POD tests. You cannot reload a MIC if it is in the ODD state.

Table 18 ODD and LED Conditions for a SmartEdge 100 I/O Carrier Card

Status of/After	Clear Log	Clear History	Replace Card	Reload System	Reload Card or Change State—ODD to OSS	Successful ODD Session
LED status	Unchanged	Unchanged	See previous Note	See previous Note	See previous Note	See Table 13
ODD history	Unchanged	Cleared	Unchanged	Unchanged	Unchanged	History file updated
ODD log	Cleared	Unchanged	Unchanged	Unchanged	Unchanged	Log updated
ODD status	Failed	Failed	Not Available	Not Available	Failed	Passed

2.8 ODD Examples

From the CLI on the active XCRP card, run ODD on the standby controller card and display results:

```
[local]Redback#diag on-demand standby level 2 loop 4
[local]Redback#show diag on-demand standby
```

Initiate a session on the Ethernet card in slot **3**, display results, and return the card to the in-service state:

```
!Place the card in ODD state
[local]Redback#configure
[local]Redback(config)#card ge-10-port 3
[local]Redback(config-card)#shutdown
[local]Redback(config-card)#on-demand-diagnostic
[local]Redback(config-card)#end

!Run an ODD session
[local]Redback#diag on-demand card 3 level 3 loop 5

!Display results
[local]Redback#show diag on-demand card 3

!Return the card to the in-service state
[local]Redback(config)#card ge-10-port 3
[local]Redback(config-card)#no on-demand-diagnostic
[local]Redback(config-card)#no shutdown
[local]Redback(config-card)#end
```

Display the output from the `show diag on-demand card 2 detail` command. The output shows a failed LIM loopback and an FPGA revision that is lower than the minimum required. The voltage, temperature, and bus tests are skipped because the FPGA rev on the line card is lower than the minimum required.

```
[local]Redback#show diag on-demand card 2 detail
Slot Number                   : 2
Card Type                     : SE_ETH100_12_PKT_CARD
Detected Card Type            : SE_ETH100_12_PKT_CARD
Serial Number                 : 7U123456789012
Detected Serial Number        : 7U123456789012
Test Level                    : 4
Loop Count                    : 1
Time                          : 0:22:11 AM 11/9/2002
Test Summary                  : 1 Failure
Test Results Loop 1:
   Card Type Valid             : Passed
   JAM 1 SCL                   : Passed
   JAM 0 SCL                   : Passed
   EPPA SCL                    : Passed
   IPPA SCL                    : Passed
   SCL Hub                     : Passed
   Octal Phy                   : Passed
   Voltage Check               : Skipped
   Temperature Check           : Skipped
   Verify Card Type            : Passed
   Verify Check Sum            : Passed
   Tioga Bus                   : Skipped
   IPPA file load              : Passed
   IPPA Memory                 : Passed
   EPPA file load              : Passed
   EPPA Memory                 : Passed
   Lim Bus                     : Passed
   fpga Config Check           : Passed
   Flip 0 Bus                  : Passed
   Flip 1 Bus                  : Passed
   ie21440 Emac 0              : Passed
   ie21440 Emac 1              : Passed
   IPPA SRAM Mem Test          : Passed
   EPPA SRAM Mem Test          : Passed
   SCL Stress                  : Passed
   lxt9763 Reg Phy 0           : Passed
   lxt9763 Reg Phy 1           : Passed
   Backplane internal loopback: Passed
   PPA loopback                : Passed
   LIM internal loopback       : Passed
   LIM external loopback       : Failed


Test Failure Details:
- LIM external loopback, slot 2, port 12
PORT_LINK_FAIL
Port link is down.
- Voltage Check, slot 2
  TEST_NOT_RUN
  Test skipped, FPGA revision is lower than the minimum required   revision
- Temperature Check, slot 2
  TEST_NOT_RUN
  Test skipped, FPGA revision is lower than the minimum required
 revision
```

2.9 Step 8: Checking CF Card and External Storage Device

2.9.1 Checking Fixed Internal CF Card

Use Table 19 as a guide to troubleshooting a fixed NetBSD internal CF card.

Table 19 Troubleshooting a Fixed Internal Flash Card

#	Task	Command	Notes
1	Check the fixed internal CF card status for soft and hard errors. If the internal CF card is mounted and the number of soft errors is increasing, there might be a problem with the CF card.	`show disk internal`	Enter this command in any mode.
2	If software errors persist, back up all the internal CF card files on to the local PC, or use FTP to send the files to a local PC or server.		
3	Reinstall the SEOS software.	installsys	**Important** • The `installsys` command requires console access. • Make sure that you have the SEOS software available so that you can reinstall it on to the internal CF card. • If you need to reformat your fixed CF card, contact your local technical support representative before doing so.
4	Check the internal CF card status for soft and hard errors.	`show disk internal`	

2.9.2 Checking External Mass Storage Device

Use Table 20 as a guide to troubleshooting an external mass storage device card.

Table 20 Troubleshooting a Card

#	Task	Command	Notes
1	Check the external mass-storage device card for soft and hard errors.	`show disk external`	Issue this command in any mode.
2	If there are soft errors, make sure that the external mass storage device is mounted.	`show disk external`	
3	If the disk is mounted and the number of soft errors is increasing, replace the external mass-storage device.		**Important**: If you remove the external mass storage device without issuing the `unmount /md` command, you will cause a system reload. The system automatically mounts the mass storage device when it is inserted.
4	If there are no soft and hard errors on the external mass-storage device card, unmount the device.	`unmount/md`	
5	Reseat the mass-storage device card.		
6	Mount the mass-storage device card.	`mount/md`	
7	Back up all the mass-storage device card files on to the local PC, or use FTP to send the files to a local PC or server.		
8	Format the mass-storage device card.	`format media-device`	
9	Check the mass-storage device card status.	`show disk external`	
10	If the format and status are OK, copy the files back to the device.		If the format or status fails on the removable mass-storage device card, replace it.

3 Troubleshooting Software Problems

Use Table 21 as a guide to troubleshooting software problems. Check each task that you have completed and document your results.

Table 21 Software Diagnostics Tasks

Task	Command	Notes	Complete?
Step 1: Checking Software and Firmware Compatibility			
Step 2: Checking Software Version	**`show version`**	Display the current version of the software running on the system.	
Step 3: Checking Release and Installation Information	**`show release`**	Display the release and installation information for the software images on the system and the partitions in which they are installed.	

Step 4: Checking Processes	**`show process`**
	`show process cpustats`
	`show process detail`
	`show process crash-info`
	`show log | grep` “*`time`*”
	`show process | grep options`
	`'-E'` `'[1-9][0-9]{0,2}\...%'`
		• Display current information on a specific category of processes, or on all running processes.
		• Display CPU statistics.
		• Display detailed information about specific processes.
		• Display crash information.
		• Display events near the time of the problem.
		• Display the time of the crash.
		• Display any process that is using CPU resources.	

Step 5: Collecting Crash File Data	**`show crashfiles`**
	`show log active all | include core | include dump`
		• Display the size, location, and name of any crash files located on the system.
		• Display core dump timestamp.	

Step 6: Checking RMON Alarms and Events	**`show rmon events`**
	`show rmon alarms`
		• Display RMON alarms.
		• Display RMON events.	

3.1 Step 1: Are the Software and Firmware Compatible?

Non-matching system components can lead to unexpected problems. The SmartEdge OS, Release 6.1.5.1 to 11.1 requires the following SmartEdge OS, Open Firmware (OFW), and minikernel components to run the specific versions listed in Table 22 (6.1.5.1), Table 23 (6.2.1), and Table 24 (6.3.1 and 6.4.1), and Table 25 (6.5.1).

To determine the versions currently installed, enter the `show version` command. The output includes the versions for:

- SmartEdge OS
- Minikernel
- Boot ROM (OFW)

The output also reports how long the system has been continuously running since the last reboot.

Table 22 Compatible OFW and Minikernel Versions for SmartEdge OS, Release 6.1.5.1

Category	**XCRP4**	**SmartEdge 100**	**ASE Card**
Open Firmware	2.0.2.37	2.0.1.4	2.0.2.33
Minikernel	11.7	2.7	13.5

Table 23 Compatible OFW and Minikernel Versions for SmartEdge OS, Release 6.2.1

Category	**XCRP4**	**SmartEdge 100**	**ASE Card**
Open Firmware	2.0.2.42	2.0.1.4	2.0.2.42
Minikernel	11.7	2.7	13.5

Table 24 Compatible OFW and Minikernel Versions for SmartEdge OS, Release 6.3.1 and 6.4.1

Category	**XCRP4**	**SmartEdge 100**	**ASE Card**
Open Firmware	2.0.2.45	2.0.1.4	2.0.2.45
Minikernel	11.7	2.7	13.5

Table 25 Compatible OFW and Minikernel Versions for SmartEdge OS, Release 6.5.1 and 11.1.1

Category	**XCRP4**	**SmartEdge 100**	**ASE Card**
Open Firmware	2.0.2.45	2.0.1.4	2.0.2.45
Minikernel	11.7	2.7	13.10

Table 26 Compatible OFW and Minikernel Versions for SmartEdge OS, Release 11.1.2

Category	XCRP4	SmartEdge 100	ASE Card
Open Firmware	2.0.2.66	2.0.1.4	2.0.2.66
Minikernel	11.7	2.7	13.10

3.2 Step 2: Checking Software Version

Use the **show version** command to display the version of the software running on the system. Check the bootrom and minikernel images and check the release notes for the recommended versions for your current software.

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

```
[local]Redback#show version
Redback Networks SmartEdge OS Version SEOS-5.0.5-Release
Built by sysbuild@@lx-lsf159Fri Jan 27 01:30:02 PST 2006
Copyright (C) 1998-2006, 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
```

The following example displays output from the **show version** command for a SmartEdge 100 router with one ATM OC3 MIC installed in slot 2. The MIC manufacturing information in the next line gives the Redback© copyright notice.

```
[local]Redback#show version
Redback Networks SmartEdge OS Version SEOS-6.1.5.1-Release
Built by sysbuildd@lx-lsf401 Wed Nov 22 10:05:57 PST 2006
Copyright (C) 1998-2006, Redback Networks Inc. All rights reserved.
System Bootstrap version is PowerPC,rev2.0.1.2 Installed minikernel version is 2.6
...
Linecard 2 MIC _mic_ sarc Version SEOS-7.0.0.0-Release
Built by sysbuildd@lx-lsf401 Wed Nov 22 10:21:45 PST 2006
Copyright(C) 1998-2006, Redback Networks Inc. All rights reserved.
Router Up Time - 3 minutes 42 secs
```

3.3 Step 3: Checking Release and Installation Information

Use the **show release** command to check the release and installation information for the software images on the system and the partitions in which they are installed. The active image shows the software that is currently loaded in the system, and the alternate release shows the alternate image available on the system. This command has no keywords or arguments.

The following example shows you how to check release and installation information for the software images currently installed on the system:

```
[local]Redback#show release


Installed releases:
p02: active (will be booted after next reload)
------------------------------------------------------------------
Version SEOS-6.1.4.0.270-Release
Built on Thu Feb 26 00:00:36 PST 2009
Copyright (C) 1998-2009, Redback Networks Inc. All rights reserved.
p01: alternate
------------------------------------------------------------------
Version SEOS-6.1.4.0.266-Release
Built on Fri Feb 20 00:00:57 PST 2009
Copyright (C) 1998-2009, Redback Networks Inc. All rights reserved.
```

3.4 Step 4: Checking Processes

Use the **show process** command to display current information on a specific category of processes, or on all running processes.

3.4.1 Keywords for the show process Command

Table 27 lists the keywords for the processes supported by this command.

Table 27 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
cfm	Ethernet 802.1ag CFM process
clips	Clientless IP service selection process
cls	Classifier Manager process
crash-info	Process crash information
cspf	Constrained Shortest-Path First process
csm	Controller State Manager (CSM) process
cpustats	Display CPU statistics
d-sbc	Distributed SBC process
detail	Detail process information
dhcp	Dynamic Host Configuration Protocol (DHCP) relay or proxy process
dhelperd	DHCP helper process
dlm	Download Manager (DLM) process
dns	Domain Name System (DNS) process
dot1q	802.1Q encapsulation process
flowd	Flow process(1)
fr	Frame Relay process (2)
gsmp	General Switch Management Protocol (GSMP) process
hr	HTTP redirect process
igmp	Internet Group Management Protocol (IGMP) process

Keyword	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 (LDP) process
lg	Link group (LG) process
lm	Label Manager (LM) process
mip	Mobile IP process
mpls_static	Multiprotocol Label Switching (MPLS) static process
msdp	Multicast Source Discovery Protocol (MSDP) process
nat	IP Network Address Translation (NAT) process
nd	Neighbor discovery (ND) process
netopd	NetOp process, which is only applicable to NetOp EMS.
ntp	Network Time Protocol (NTP) process
odd	On-demand diagnostics (ODD) process
ospf	Open Shortest Path First (OSPF) protocol process
ospf3	OSPF Version 3 (OSPFv3) protocol process
ped_parse	Process execution descriptor (PED) parse process
pem	Port encapsulation module (PEM) process
pim	Protocol Independent Multicast (PIM) process
ppaslog	Packet Processing ASIC (PPA) syslog 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

Keyword	Process
`sysmon`	System monitor process
`tunnel`	Tunnel management process
`vrrp`	Virtual Router Redundancy Protocol (VRRP) process
`xcd`	Cross-connect process

(1) Not all controller cards support flow.

(2) The SmartEdge 100 router does not support Frame Relay.

3.4.2 Displaying Processes

The following example shows how to display output from the **`show process`** command. The PID column shows the process ID. In this example, you have not restarted any static processes and the spawn count for static process is greater than 1. A value greater than 1 indicates that a process has crashed and restarted, which indicates there might be a problem with the static process. In the State column, when the process is in a halt or stop state, restart the process. In the Time column, “Not Avail”, indicates that a process is not configured; for example, BGP.

```
[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
```

Recommended Action: Issue the **`show process crash-info`** command to find the time of the crash. Then issue the **`show log`** command with a **`grep`** option with the timestamp obtained from the **`show process crash-info`** command—for example, **`show log | grep “June 30 15:54`**”—and check for suspicious log events near the time of the problem. The log file prints the time and messages associated with the crash. Use the activity before the crash to help guide your analysis of the root cause of the crash.

3.4.3 Displaying Processes with the Keyword crash-info

The following example shows how to display output from the **`show process`** command with the **`crash-info`** keyword:

```
[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)
```

3.4.4 Displaying Detailed Process ISM Information

The following example shows how to display output from the **`show process`** command with the **`ism detail`** keywords. When you use this command, look for a spawn count greater than 1. The spawn count should be 1 unless you restarted a process. By default, the process stops restarting after 5 crashes (within 86400 seconds). Total crashes should be 0, unless you forced a process to crash.

```
[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
```

Recommended Action: If the total crashes is greater than 0 and the crash is not expected (that is, the administrator did not force the crash), issue the **`show log`** command to determine what activity caused the crash. The log file prints the time and messages associated with the crash. Use the activity before the crash to help guide your analysis of the root cause of the crash.

3.4.5 Displaying CPU Statistics

The following example shows how to display CPU statistics from the **show process cpustats** command:

```
[local]Redback#show process cpustats

Total system CPU % usage (5s, 1m, 5m):  0.00,  0.00,  0.00
Proc/thread name:  5sec  1min  5min    Proc/thread name:  5sec  1min  5min
--------------------------------------------------------------------------
        exec_cli:  0.00  0.00  0.00             staticd:  0.00  0.00  0.00
             ndd:  0.00  0.00  0.00              clipsd:  0.00  0.00  0.00
           l2tpd:  0.00  0.00  0.00              pppoed:  0.00  0.00  0.00
            aaad:  0.00  0.00  0.00                pppd:  0.00  0.00  0.00
           statd:  0.00  0.00  0.00            dhelperd:  0.00  0.00  0.00
            oddd:  0.00  0.00  0.00                  lm:  0.00  0.00  0.00
           dhcpd:  0.00  0.00  0.00                pemd:  0.00  0.00  0.00
            dlmd:  0.00  0.00  0.00                clsd:  0.00  0.00  0.00
        ppaslogd:  0.00  0.00  0.00             sysmond:  0.00  0.00  0.00
            arpd:  0.00  0.00  0.00                ribd:  0.00  0.00  0.00
            rpmd:  0.00  0.00  0.00           ped_parse:  0.00  0.00  0.00
            ism2:  0.00  0.00  0.00                 rcm:  0.00  0.00  0.00
             csm:  0.00  0.00  0.00            exec_cli:  0.00  0.00  0.00
              pm:  0.00  0.00  0.00             syslogd:  0.00  0.00  0.00
           inetd:  0.00  0.00  0.00          mount_udrv:  0.00  0.00  0.00
           loggd:  0.00  0.00  0.00           mount_mfs:  0.00  0.00  0.00
       mount_mfs:  0.00  0.00  0.00      ptdstat_thread:  0.00  0.00  0.00
   reboot_thread:  0.00  0.00  0.00             evnt_th:  0.00  0.00  0.00
  sccmem_cleanup:  0.00  0.00  0.00             ioflush:  0.00  0.00  0.00
          reaper:  0.00  0.00  0.00          pagedaemon:  0.00  0.00  0.00
           nfsio:  0.00  0.00  0.00               nfsio:  0.00  0.00  0.00
           nfsio:  0.00  0.00  0.00               nfsio:  0.00  0.00  0.00
            init:  0.00  0.00  0.00
```

3.4.6 Displaying a Process Using a Grep Pattern

The following example displays processes with 1.00-100.00% CPU usage with the **show process** command that match the **grep** pattern options:

'-E' '[1-9][0-9]{0,2}\...%'

```
[local]Redback# show process | grep options '-E'  '[1-9][0-9]{0,2}\...%'

rcm 254 2 13272K 00:00:00.38 7.53% run 00:00:04
hr  255 1 3400K  00:00:00.09 4.61% run 00:00:02
```

3.5 Step 5: Collecting Crash File Data

When a crash occurs:

1. The automatic core dump is initiated.
2. The process restarts after the core dump is completed.
3. The spawn-count increments.
4. The process restarts and initializes. If the process keeps crashing, the default setting is to stop restarting the process after 5 crashes (within 86400 seconds). You can change the default by using the **`process set max-crashes`** command. The default can be change from 5 to 10 crashes. If you manually restart the process, the process continues to restart and initialize.

If you think that a process has crashed, check for core dumps on the system. The core dump contains crash files. Use the **`show crashfiles`** command to display the size, location, and name of any crash files from the core dump located in the system. Crash files are used by local technical support representatives to determine the cause of the failure.

Note: When you issue the **`show crashfiles`** command, the timestamps of the core files do not reflect the time of the crash because the timestamps are updated after an XCRP switchover. Checking the active log shows the true time of recent crashes. Use the **`show log active all | include core | include dump`** command.

The crash file name is ***`proc-name_proc-id`***.core, and it is stored in the `/md` directory in the root file system on the internal compact-flash card or if a mass-storage device is installed, in the `/md` directory on the device.

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

Note: We strongly recommend that you configure the system to upload crash files automatically to a remote File Transfer Protocol (FTP) server, by 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 this command, see the *Command List*.

Crash files provide useful troubleshooting information to local technical support representatives and are not intended, nor supported, for other use.

The following sections show how to display crash information.

For more information about the **`show process`** command, see Section 3.4 on page 47.

3.5.1 Displaying Crash Files

Display crash files. Here, the PPP process has crashed:

```
[local]Redback# show crashfiles

4812 Feb 13 23:44 /md/pppd_218.mini.core
4912264 Feb 13 23:44 /md/pppd_218.core
```

3.5.2 Displaying PPP Process Crash Information

Display output from the **`show process`** command with the **`ppp crash-info`** keyword. The output tells you when the PPP process failed.

```
[local]Redback#show process ppp crash-info

NAME TIME STATUS
ppp Tue Feb 13 23:44:26 2007 Trap (133)
ppp Wed Feb 14 00:44:31 2007 Software termination (15)
```

3.5.3 Displaying Core Dump Timestamp

Display the core dump timestamp using the **`show log active all | include core | include dump`** command:

```
[local]Redback#show log active all | include core | include dump

Dec 18 08:14:14: %SYSLOG-6-INFO: /netbsd: pid 1627 (pppd), uid 0:
exited on sign  al 5 (core dumped
Dec 19 03:41:10: %SYSLOG-6-INFO: /netbsd: pid 1629 (aaad), uid 0:
exited on sign  al 5 (core dumped)
```

3.6 Step 6: Checking RMON Alarms and Events

The following sections show how to check RMON information.

3.6.1 Displaying 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"
```

3.6.2 Displaying 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"
```

4 Troubleshooting Data Link Layer Problems

Use Table 28 as a guide to troubleshoot data link and networking tasks issues on your SmartEdge router.

Table 28 Datalink Layer and Networking Tasks

Task	Command	Notes	Checked?

Step 1: Checking Ports	`show port`
	`show port counters`
		Display port status or port counters.	

Step 2: Checking Circuits	`show dot1q pvc`	Check the configuration for encapsulation errors about a specific 802.1Q PVC, a set of PVCs, or a summary.	

Step 3: Checking Traffic	`show port counters live`
	`monitor port counters`
	`show circuit counters`
		• Display port performance.
		• Display the current status of ports or channels.
		• Display general counters and counters specific to a circuit type for one or more circuits in the system.	

Step 4: Checking Interfaces	`show ip interface brief`	Check if the interfaces are up.	

4.1 Step 1: Checking Ports

4.1.1 Checking Port Status

Before you check the status of a port, you first need to understand the differences between “Admin state” and the “Line state”:

- Admin state—Refers whether the port has been brought up (by using the **`no shutdown`** command) or is down (by using the **`shutdown`** command). If the Admin state is *shut down*, the port is down.

  Recommended Action: Issue the **`no shutdown`** command on the port to bring up the port.

- Line state—Refers to the physical state of the port.

Recommended Action: When the Line state is *down*, use the checklist in Table 29.

Table 29 Line State Troubleshooting Checklist

#	Line State Troubleshooting Checklist	Checked?
1	Is the cable correctly connecting the two ports or two nodes?	
2	Is there a fault in the cable?	
3	Are you using the right type of cable; for example, with Ethernet, are you using a cross-over cable instead of a straight cable?	
4	When the cable is connected to two nodes, is there a fault in one of the nodes?	
5	Is the card with a fiber port receiving light? Is the LOS LED in the port on?	
6	If you are using fiber optics, are you using the appropriate fiber type (such as multimode or single mode) ?	
7	Is the other end port shut down?	
8	Is there an autonegotiation mismatch?	
9	Is the SmartEdge router Gigabit Ethernet traffic GE port connected to an FE port? The SmartEdge router Gigabit Ethernet line cards do not support FE speeds). **Note**: This is very common issue.	

If the Admin state is *down*, the Line state is always *down*. For the port to be *up*, the Admin state and Line state must both be *up*. To check the status of a port, issue the **`show port detail`** command. You must use the keyword **`detail`** or **`live`** to receive results in real time. For detailed information about each field displayed, see the *Command List*.

Use the following table to determine whether a port is up or down.

Table 30   Port States

Admin State (Configuration)	Line State (Physical)	Result
Up	Down	Down
Up	Up	Up
Down	Up	Down
Down	Down	Down

In the following example, the status of the Ethernet port is down. Although the Ethernet port is in a *no shutdown* state and the Admin state is *up*, the cable has been unplugged from the Ethernet port `2/9` and as a result, the Line state (the physical state) is *down*:

```
[local]Redback#show port 2/9 detail

ethernet 2/9 state is Down
Description                :
Line state                 : Down
Admin state                : Up
Link Dampening             : disabled
Undampened line state      : Down
Dampening Count            : 0
Encapsulation              : ethernet
MTU size                   : 1500 Bytes
NAS Port Type              :
MAC address                : 00:30:88:11:4d:37
Media type                 : 100Base-TX
Speed                      : 10 Mbps
Duplex mode                : half
Loopback                   : off
Active Alarms              : Link down
```

4.1.2 Checking Port Counters

Each line card collects Layer 1, 2, and 3 statistics. To check port counters, generate traffic on the port, issue the **show port counters** command, and then see if traffic is increasing on the port. For detailed information about each field displayed, see the *Command List*.

```
[local]Redback#show port counters

Port                 Type
5/1                  ethernet
packets sent       : 8005965685         bytes sent         : 2192408927283
packets recvd      : 9101523807         bytes recvd        : 8805661380307
send packet rate   : 18310.40           send bit rate      : 33063939.07
recv packet rate   : 21044.35           recv bit rate      : 173686607.12
rate refresh interval : 60 seconds
6/1                  ethernet
packets sent       : 8037296427         bytes sent          : 2268361201464
packets recvd      : 10724872023        bytes recvd         : 10311852048330
send packet rate   : 17996.42           send bit rate       : 35636342.79
recv packet rate   : 25119.94           recv bit rate       : 204946341.89
rate refresh interval : 60 seconds
11/1                 atm
packets sent       : 544505671          bytes sent          : 283005479428
packets recvd      : 549407041          bytes recvd         : 309464283046
send packet rate   : 815.74             send bit rate       : 3056642.82
recv packet rate   : 858.92             recv bit rate       : 4099034.04
rate refresh interval : 60 seconds
```

4.2 Step 2: Checking Circuits

Many circuit issues are caused by configuration errors. To check the configuration for encapsulation errors, use the **show dot1q pvc** command. Make sure that state of the encapsulation for the PVC is up. For detailed information about each field displayed see the *Command List*.

The following example displays information for 802.1Q PVCs in all contexts. The PPPoE PVC is down.

```
[local]Redback# show dot1q pvc all

Port    Vlan    Profile    State Encaps    Binding
3/2     105                Down  pppoe     user@isp1.net
```

Recommended Action: When the PPPoE PVC is down, use the following checklist.

Table 31 Check 802.1Q PVCs

#	Task	Root Command	Checked?
1	Check for errors in your configuration.	**show configuration**	
2	Display detail information about the 802.1Q PVCs.	**show dot1q pvc detail**	
3	Display information for the specified inactive 802.1Q PVCs.	**show dot1q pvc down detail**	
4	Display detailed information about the PPP counters.	**show ppp counters detail**	

4.3 Step 3: Checking Traffic

4.3.1 Checking Port Performance

Use the **show port counters** command to check port performance. By default, this command displays only summary counter information for all ports with their last known values, which have been cached; cached values are updated every 60 seconds. Use the **live** keyword to force the system to read and display live data for all summary counters except rate counters. If the counters are not incrementing, packets are probably being dropped. If the counters are not incrementing, issue the **show port counters detail** command. For detailed information about each field displayed, see the *Command List*.

Note: Depending on your configuration, it may take a few minutes to display information in real time when you use the **live** keyword.

```
[local]Redback#show port counters live

please wait...
Port            Type
5/3             ethernet
packets sent       : 0                   bytes sent         : 0
packets recvd      : 0                   bytes recvd        : 0
send packet rate   : 0.00                send bit rate      : 0.00
recv packet rate   : 0.00                recv bit rate      : 0.00
rate refresh interval : 60 seconds
7/1            ethernet
packets sent       : 13609               bytes sent         : 1292265
packets recvd      : 32791               bytes recvd        : 2035443
14/1           ethernet
packets sent       : 0                   bytes sent         : 0
packets recvd      : 0                   bytes recvd        : 0
send packet rate   : 0.00                send bit rate      : 0.00
recv packet rate   : 0.00                recv bit rate      : 0.00
rate refresh interval : 60 seconds
```

4.3.2 Monitoring Traffic on a Port

You can verify that you are receiving packets on your ports by running the **monitor port counters** command, which checks the current status of ports or channels and provides continuous status updates. This command can adversely impact system performance. Press **Ctrl+C** to exit monitoring mode. For detailed information about each field displayed see the *Command List*.

The following example shows that no packets have been received during the 600 second interval on Ethernet port **5/1**, which indicates there is an issue external to the SmartEdge router:

```
[local]Redback#monitor port counters 5/1


This may adversely impact system performance
% enter ctrl-C to exit monitor mode, monitor duration(sec): 600 (00:00:02)
Port            Type                      Pkts/Bytes Sent    Pkts/Bytes Received
5/1             ethernet                                3                      0
                                                      126                      0
```

4.3.3 Checking Circuit Performance

Use the **`show circuit counters`** command to display general counters and counters specific to a circuit type. Check for dropped packets in the Adj Drops, Down Drops, and Unknown Encaps fields. Use the **`show circuit counters ?`** command to display the various levels that you can check. For detailed information about each field displayed, see the *Command List*.

The following example displays detailed information about circuit counters for a PPPoE PVC. The values in the Adj Drops, Down Drops, and Unknown Encaps fields, which are highlighted in bold, have a value of zero (0), which indicates that the circuit is not dropping packets and is functioning correctly:

```
[local]Redback#show circuit counters pppoe detail

please wait...
Circuit: 13/1:1 vpi-vci 0 100, Internal id: 1/2/6, Encap: atm-ppp-auto
Packets                                  Bytes
------------------------------------------------------------------------
Receive          :         2550   Receive             :           140022
Receive/Second   :         0.50   Receive/Second      :            27.00
Transmit         :           45   Transmit            :             5309
Xmits/Queue                      Xmits/Queue
 0               :           45     0                 :             5309
 1               :            0     1                 :               0
 2               :            0     2                 :               0
 3               :            0     3                 :               0
 4               :            0     4                 :               0
 5               :            0     5                 :               0
 6               :            0     6                 :               0
 7               :            0     7                 :               0
 8               :            0     8                 :               0
Transmit/Second  :         0.00    Transmit/Second    :             0.00
IP Multicast Rcv :            0   IP Multicast Rcv   :                0
IP Multicast Tx  :            0   IP Multicast Tx    :                0
Unknown Encaps   :            0   Unknown Encaps     :                0
Down Drops       :            0   Down Drops         :                0
Unreach Drops    :            0   Unreach Drops      :                0
Adj Drops                     0   Adj Drops          :                0
...
```

The following example displays detailed information about circuit counters for a VLAN circuit. The values in the Adj Drops, Down Drops, and Unknown Encaps fields, have a value of zero (0), which indicates that the circuit is not dropping packets and is functioning correctly:

```
[local]Redback#show circuit counters 3/3 vlan-id 102 detail

Circuit: 3/3 vlan-id 102, Internal id: 1/2/22, Encap: ether-dot1q
Packets                      Bytes
---------------------------------------------------------------------
Receive        : 26599       Receive         :               2297014
Receive/Second : 0.10        Receive/Second  :                  8.60
Transmit       : 26538       Transmit        :               2285512
Xmits/Queue                  Xmits/Queue
0             : 26538         0             :               2285512
1             : 0             1             :                     0
2             : 0             2             :                     0
3             : 0             3             :                     0
4             : 0             4             :                     0
5             : 0             5             :                     0
6             : 0             6             :                     0
7             : 0             7             :                     0
8             : 0             8             :                     0
 Transmit/Second :      0.10  Transmit/Second :                 8.60
IP Multicast Rcv:         0  IP Multicast Rcv:                    0
IP Multicast Tx :         0  IP Multicast Tx :                    0
Unknown Encaps  :         0  Unknown Encaps  :                    0
Down Drops      :         0  Down Drops      :                    0
Unreach Drops   :         0  Unreach Drops   :                    0
Adj Drops       :         0  Adj Drops       :                    0
...
```

4.4 Step 4: Checking Interfaces

Use the **show ip interface brief** command to check if the interfaces are up. This command displays information about all interfaces, associated addresses, states, and bindings, including the interface bound to the Ethernet management port on the controller card.

An interface can be in any of the following states:

- Unbound—The interface is not currently bound to any port or circuit. The binding is not valid.

  Note: In some cases, an interface can have an Unbound state and still be valid; for example, multibind interfaces where no active PPPoE or CLIPS sessions are active.

- 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. The binding is valid. The state *Bound* is expected behavior for multibind interfaces where there are no active subscribers.

- 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. The binding is valid.

For detailed information about each field displayed, see the *Command List*.

The following example displays output from the **show ip interface brief** command. Interfaces **12/1** and **un1**, currently are not bound to any port or circuit:

```
[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)
```

5 Troubleshooting Subscriber Connectivity

This section shows you to troubleshoot subscriber connectivity problems.

The following diagram shows the general procedure for troubleshooting subscriber software connectivity issues:

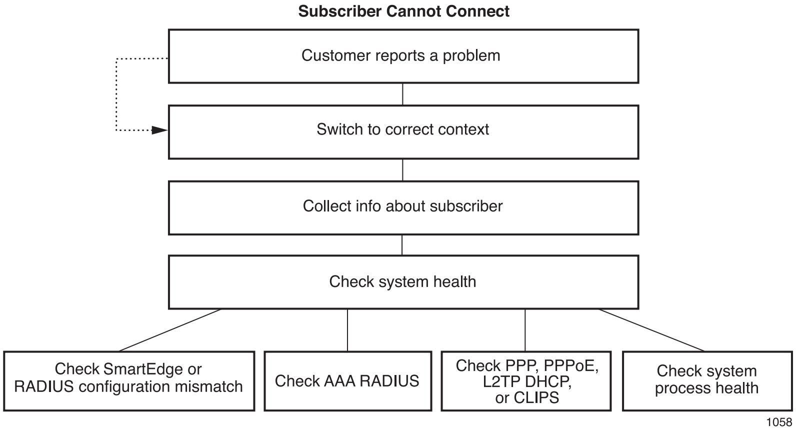

Subscriber Cannot Connect
Customer reports a problem
Switch to correct context
Collect info about subscriber
Check system health
Check SmartEdge or RADIUS configuration mismatch
Check AAA RADIUS
Check PPP, PPPoE, L2TP DHCP, or CLIPS
Check system process health
1058

Figure 2 General Procedure for Troubleshooting Subscriber Connectivity

Use Table 32 as a guide to troubleshooting software subscriber connectivity issues. Check each task that you have completed and document your results. Before you begin, get a description of the problem and check if you made any recent changes or upgrades to their network.

Table 32 Tasks to Troubleshoot Subscriber Connectivity Issues

Task	Command	Notes	Checked?
Step 1: Navigating to the Correct Context	`show context all`	Display all the contexts on your router and then navigate to the context you want to troubleshoot.	

Step 2: Displaying Information About My Subscribers	`show subscribers active username`
	`show subscribers all`
	`show subscribers log`
		• Display slot, port, circuit, IP address, and attributes of active subscriber sessions.
		• Display information about all subscribers in all contexts.
		• Display the authentication, authorization, and accounting (AAA) logs of subscribers.	

Step 3: Checking System Health	`show system alarm`
	`show subscribers summary all`
	`show port`
		• Display system-level, card-level, port-level, channel-level, or subchannel-level alarms.
		• Display information about all subscribers in all contexts.
		• Display port status.
			.

Step 4: Checking for Configuration Errors	`show configuration context`	• On the SmartEdge router, check for a configuration mismatch. • On the RADIUS server, check for a configuration mismatch. • Did you forget to commit your configuration?	
Step 5: Checking for Available IP Addresses	`show ip pool`	Display addresses available in an IP pool.	

Table 32 Tasks to Troubleshoot Subscriber Connectivity Issues

Task	Command	Notes	Checked?

Step 6: Checking Interface Connectivity	`ping`
	`show circuit counters`
	`show port counters`
		• ATM—Ping known IP address and ping ATM.
		• Ethernet—Ping known IP address, check counters, and check if other sessions are successful.
		• Dot1Q VLAN—Ping known IP address, check counters, and check PPP state for the circuit.
		• Circuit—Ping ATM or counters, debug PPPoE discovery.
		• Display general counters and counters specific to the circuit type for one or more circuits in the system.
		• Display port counters. For information about the show port counters command, see Checking Port Counters.	

Step 7: Checking Bindings	`show bindings`	Display the configured bindings for one or more subscribers, ports, channels, or PVCs on the system.	
Step 8: Checking Licenses	`show licenses`	Display a list of software licenses and their configuration status.	

Step 9: Checking Authentication	`show subscribers log`
	`debug aaa exception`
	`show circuit slot/port vpi-vci`
		• Display the AAA log.
		• Display inbound and outbound messages from the AAA server.
		• Display information about VPI and VCI for an ATM PVC.
		• Display an AAA packet or function events that unexpectedly end a task.
		• Check for incorrect subscriber usernames or passwords.	

Step 10: Checking Access Protocol State	`show circuit counters`	Check the state of CLIPS, DHCP, LTP2, or PPP access protocol.	

5.1 Step 1: Navigating to the Correct Context

Use the **`show context all`** to view all your contexts and then navigate to the context that you want to troubleshoot—in this case `NiceService`. For information about the role of contexts in troubleshooting, see *Basic Troubleshooting Techniques*.

The following example shows how to view all contexts on your router and then navigate to context `NiceService:`

```
[local]Redback#show context all

Context Name         Context ID      VPN-RD   Description
------------------------------------------------------
local                0x40080001
NiceService          0x40080002
[local]Redback#
[local]Redback#context NiceService
[NiceService]Redback#
```

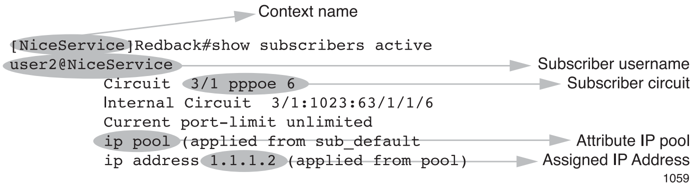
5.2 Step 2: Displaying Information About My Subscribers

Use the **`show subscribers`** command to display subscriber information within the current context. This includes basic subscriber status fields, DSL attributes, attributes of active subscriber sessions, Mobile IP attributes, AAA logs, a summary of subscriber information, and IP addresses associated with subscribers.

5.2.1 Displaying Active Subscribers

The **`show subscribers`** command displays subscriber usernames, circuits that they are associated with, the contexts that they are bound to. The **`active`** keyword provides information on the dynamic policy rules applied to active subscriber sessions.

The following illustration identifies the **`show subscribers active`** command output fields:



```
[NiceService]Redback#show subscribers active
user2@NiceService
          Circuit  3/1 pppoe 6
          Internal Circuit  3/1:1023:63/1/1/6
          Current port-limit unlimited
          ip pool (applied from sub_default
          ip address 1.1.1.2 (applied from pool)
```

Figure 3 Show Subscribers Active Command Output Fields

Table 33   Output Fields for the show subscribers all Command

Field	Description
Type	Displays the port or circuit encapsulation type
Circuit	Displays the slot/port type of encapsulation, and session ID
Subscriber	Displays the subscriber username
Context	Displays the context name bound to the subscriber
Start Time	Displays the session start time

The following example displays the information for an active subscriber; it includes both the absolute time-out action and traffic limit action fields:

```
[local]Redback# show subscribers active username client32@lns.com

client32@lns.com
Circuit   L2TP LNS 8744119
Internal Circuit   255/16:1023:63/5/2/8744119
Current port-limit unlimited
context-name lns (applied)
ip pool   (applied from sub_default)
absolute timeout action 1 (applied from sub_default)
traffic limit action 1 (applied from sub_default)
ip address 192.168.27.2 (applied from pool)
timeout absolute 60 (applied)
timeout idle 60 (applied)
```

Recommended Action: If you find a problem with the subscriber, issue the **`debug circuit`** command and specify the circuit that you obtained from the **`show subscriber active username`** command to obtain more information about the issue.

5.2.2 Displaying Information About All Subscribers

Use the **show subscribers all** command to display information about all subscribers in all contexts. The **all** keyword is available only to administrators in the local context. To clear a subscriber session, issue the **clear subscriber username** command.

The following example shows how to display information about all subscribers in all contexts:

```
[local]Redback#show subscribers all
```

5.2.3 Displaying Information About an Individual Subscriber

The following example shows how to display information about the binding, context, and subscriber:

```
[local]Redback# show sub all | grep user2@NiceService
pppoe 3/1 pppoe 7 user2@NiceService abc Aug 17 03:02:31
```

5.2.4 Logging Subscribers

Use the **show subscribers log** command to display the authentication, authorization, and accounting (AAA) logs of subscribers.

```
[local]Redback#show subscribers log
```

Use the **show subscribers log username** or **show subscribers log session** commands to see only the logs relevant to the problem session. Enter the subscriber argument as a structured subscriber ***username*** in the form ***subscriber@context***. The following example shows how to display log information about subscriber `user2` in the `NiceService` context using the **grep** options to search for a subscriber endpoint that is case insensitive:

```
[local]Redback#show sub log username user2@NiceService |
grep options '-E -i' 'ipc_endpoint|--|\.'

------------------------------------------------------
0 IN Wed Aug 17 03:02:31.35980
IPC_ENDPOINT = PPPd, MSG_TYPE = AUTHEN_REQUEST,
----------------------------------------------------
1 OUT Wed Aug 17 03:02:31.40586 IPC_ENDPOINT = PPPd,
MSG_TYPE= DB_RESPONSE,
----------------------------------------------------
2 IN Wed Aug 17 03:02:31.51376
IPC_ENDPOINT = PPPd, MSG_TYPE = SESSION_UP,
-----------------------------------------------------
3 OUT Wed Aug 17 03:02:31.51680
IPC_ENDPOINT = ISM-IF, MSG_TYPE = IF-BIND,
-----------------------------------------------------
4 OUT Wed Aug 17 03:02:31.51714
IPC_ENDPOINT = ISM-CCT, MSG_TYPE = CCT-GEN-CFG,
-----------------------------------------------------
```

5.3 Step 3: Checking System Health

Use the **show system alarm**, **show subscribers summary all**, and **show port** commands to check system health. For information about the **show system alarm** command, see Section 2.6 on page 22. For information about the **show port** command, see Section 4.1 on page 56.

The following example shows how to display information about all subscribers in all contexts. The administrators must have system-wide privileges.

```
[local]Redback#show subscribers summary all

------------------------------------------------------------------------
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
```

5.4 Step 4: Checking for Configuration Errors

Issue the **`show configuration context`** command and check for configuration errors listed in Table 34. Use this table as guide to troubleshoot common misconfiguration issues.

Table 34 Configuration Mismatch Checklist

#	Task	Checked?
1	Is the **multibind** option configured correctly?	
2	Is the IP pool configuration missing?	
3	Is the configured subscriber IP address outside the IP pool range?	
4	Is the IP pool configuration configured to provide enough addresses for the subscribers?	
5	Is the subscriber using an incorrect domain suffix in the username?	
6	Is the user’s password, or context configured correctly?	
7	Do the client and server have a VPI/VCI pair that does not match?	
8	Do the client and server VCs have an encapsulation type that does not match?	
9	Do the client and server have an authentication method that does not match?	
10	Is the binding missing or incorrect?	
11	Are the provisioning attributes, for example, ACLs or QoS, missing or incorrect?	
12	Is the interface that the subscriber is binding to not a multibind interface?	
13	Does the PPPoE client’s service name (if not blank) not match the domain name of the server?	
14	Are the maximum number of sessions correctly specified?	
15	Did you forget to commit the configuration?	
16	Is the subscriber’s VLAN correctly configured?	

The following example shows how to display the `NiceService` context configuration:

```
[local]Redback#show configuration context NiceService
```

5.5 Step 5: Checking for Available IP Addresses

Use the **`show ip pool`** command to check the status of available 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.

The following example displays the 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.
```

Recommended Action: If you have a problem with the IP pool, check the IP pool configuration to see if there are enough addresses available for the subscribers. You might need to increase the pool range. The default subnet mask for the IP pool is `/16`, which supports a maximum of 65,533 subscribers.

5.6 Step 6: Checking Connectivity on an Interface

Use the **ping**, **show port counters**, and **show circuit counters** commands to check for interface connectivity. For information about the **show port counters** command, see Section 4.1 on page 56.

```
[ISP1]Redback# ping 100.1.1.3

PING 100.1.1.3 (100.1.1.3): source 100.1.1.1, 36 data bytes,
timeout is 1 second
!!!!!  ----100.1.1.3 PING Statistics---- 5 packets transmitted, 5 packets received,
0.0% packet loss round-trip min/avg/max/stddev = 1.814/2.030/2.546/0.315 ms
[local]Redback# ping atm channel end-to-end 13/1 vpi 1 vci 100 count 5
Sending 5, End-to-End F5 (Channel) cells on 13/1 :1 vpi 1 vci 100
Timeout is 2 seconds, Interval between Cells is 100 milliseconds
!!!!! Success rate is 100.0 percent (5/5)
```

In the following example, look for packets being received that correspond to requests from the subscriber. If you do not use the **detail** or the **live** keywords, the counters are cached and are updated every 60 seconds:

```
[ISP2]Redback# show circuit counters 3/1 detail

please wait...
Circuit: 3/1 pppoe 1, Internal id: 1/1/4, Encap:
ethernet-pppoe-ppp-combined
Packets                          Bytes
-------------------------------------------------------------
Receive         :        43      Receive         :      4008
Receive/Second  :        0.05    Receive/Second  :      5.10
Transmit        :        44      Transmit        :      3890
Transmit/Second :        0.05    Transmit/Second :      5.10
IP Multicast Rcv:        0       IP Multicast Rcv:      0
IP Multicast Tx :        0       IP Multicast Tx :      0
Unknown Encaps  :        0       Unknown Encaps  :      0
Down Drops      :        0       Down Drops      :      0
Unreach Drops   :        0       Unreach Drops   :      0
Adj Drops       :        0       Adj Drops       :      0
WRED Drops Total:        0       WRED Drops Total:      0
Tail Drops Total:        0       Tail Drops Total:      0
PPP Counters cntrl:      3       cntrl           :      133
cntrl drops     :        0
retries         :        0
termreqs        :        0
PPPoE Counters
cntrl           :        2
cntrl           :        120
session drops   :        0
PADT sent       :        0
PADR drops      :        0
PADI drops      :        0
PADT drops      :        0
bad code        :        0
Rate Refresh Interval :  60 seconds
```

5.7 Step 7: Checking Bindings

Use the **show bindings** command to display the configured bindings for one or more subscribers, ports, channels, or PVCs on the system. Look at the Summary information to see if the total number bindings is bound. If not, check to see if the bound field increments. (Some of the bindings might be in transitory period.) If the bindings do not increment, issue the **show debug circuit** command to gather more information about the circuit.

The following example displays all bindings in the current context, `local`:

```
[local]Redback#show bindings


Circuit                          State Encaps           Bind Type  Bind Name
1/1                              Up    cisco-hdlc       interface  toTokyo@London
1/2                              Up    cisco-hdlc       interface  toLondon@Tokyo
1/3                              Up    cisco-hdlc       interface  toLA1@NYC1
1/4                              Up    cisco-hdlc       interface  toNYC1@LA1
2/1:5                            Up    cisco-hdlc       interface  toNYC2@London
2/1:6                            Up    cisco-hdlc       interface  toNYC1@London
2/1:7                            Up    cisco-hdlc       interface  toLA1@Tokyo
2/1:8                            Up    cisco-hdlc       interface  toLA2@Tokyo
2/1                              Up    cisco-hdlc
2/2:5                            Up    cisco-hdlc       interface  toLondon@NYC2
2/2:6                            Up    cisco-hdlc       interface  toLondon@NYC1
2/2:7                            Up    cisco-hdlc       interface  toTokyo@LA1
2/2:8                            Up    cisco-hdlc       interface  toTokyo@LA2
2/2:15                           Up    cisco-hdlc
2/2:16                           Up    cisco-hdlc
2/2                              Up    cisco-hdlc
5/1                              Down  ethernet
6/1:1 vpi-vci 1 101              Down  bridge1483       interface  internal@London
6/1:1 vpi-vci 1 102              Down  bridge1483       interface  internal@Tokyo
6/1:1 vpi-vci 4 4                Down  multi1483
6/1:1 vpi-vci 44 45              Down  multi1483
6/1:1 vpi-vci 55 66              Down  multi1483
7/1                              Up    ethernet         interface  adm@local
10/1:1                           Down  frame-relay
10/1:1 dlci 0                    Down  frame-relay
10/1:1 dlci 1023                 Down  frame-relay
10/1:1 dlci 16                   Down  frame-relay
10/1:3                           Down  cisco-hdlc
11/1                             Down  cisco-hdlc
12/1                             Down  ethernet         interface  toNYC1@NYC2
12/1 vlan-id 1                   Down  dot1q multi
12/2                             Down  ethernet         interface  toNYC2@NYC1
12/3                             Down  ethernet         interface  toLA2@LA1
12/4                             Down  ethernet         interface  toLA1@LA2
GRE 1.2.3.4 key 1                Down  gre
Link share ethernet              Down  ethernet
Summary:
   total: 38              up: 19             down: 19
   bound: 19         unbound: 19          no-bind: 19
    auth: 0        interface: 19       subscriber: 0
     atm: 5            chdlc: 20            dot1q: 1            ether: 7
      fr: 4              gre: 1              mpls: 0              ppp: 0
   pppoe: 0            clips: 0
```

The following example displays binding information for all PVCs configured with the **`bind interface`** command for port `1` on the card in slot `2`:

```
[local]Redback(config-ctx)#show bindings 2/1 interface
```

```
Circuit         State Encaps           Bind Type  Bind Name
2/1:5           Up    cisco-hdlc       interface  toNYC2@London
2/1:6           Up    cisco-hdlc       interface  toNYC1@London
2/1:7           Up    cisco-hdlc       interface  toLA1@Tokyo
2/1:8           Up    cisco-hdlc       interface  toLA2@Tokyo
Summary:
   total: 4             up: 4             down: 0
   bound: 4        unbound: 0          no-bind: 0
    auth: 0      interface: 4       subscriber: 0
     atm: 0          chdlc: 4            dot1q: 0       ether: 0
      fr: 0            gre: 0             mpls: 0       ppp: 0
   pppoe: 0          clips: 0
```

The following example displays all bindings for all Frame Relay PVCs for port 1 on the card in slot 10:

```
[local]Redback(config-ctx)#show bindings 10/1 fr
```

```
Circuit                           State Encaps        Bind Type  Bind Name
10/1:1                            Down  frame-relay
10/1:1 dlci 0                     Down  frame-relay
10/1:1 dlci 1023                  Down  frame-relay
10/1:1 dlci 16                    Down  frame-relay
Summary:
   total: 4               up: 0             down: 4
   bound: 0          unbound: 4          no-bind: 4
    auth: 0        interface: 0       subscriber: 0
     atm: 0            chdlc: 0            dot1q: 0         ether: 0
      fr: 4              gre: 0             mpls: 0          ppp: 0
   pppoe: 0            clips: 0
```

5.8 Step 8: Checking Licenses

Use the **show licenses** command to display a list of software licenses and their configuration status. To see if you are operating within the licensed limits (for example, number of subscribers), issue the **show subscriber summary all** command. Some licenses have no limits. If the feature is enabled, then check for the correct license to be installed.

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
```

5.9 Step 9: Checking Authentication

The SmartEdge router uses RADIUS servers for AAA of subscribers. The SmartEdge RADIUS client passes subscriber information to designated RADIUS servers, and then acts on the returned response. RADIUS servers receive user connection requests, authenticate the user, and then return all configuration information required for the client to deliver service to the subscriber.

A number of counters are incremented whenever a RADIUS server encounters errors. For example, if an RADIUS server rejected authentication requests because it is too busy, you can check the `authen fail due to throttling` counter. The output from the **`show subscribers log`** command is also useful for checking authentication requests. We recommend that you use the **`show subscribers log username`** or **`show subscribers log session`** commands to view only the logs relevant to the problem during the session. For an example of the **`show subscribers log username`** command, see Section 5.2.4 on page 70.

Use the following commands to troubleshoot authentication problems, such as an incorrect username, password, or an unstructured username:

- **`show subscribers log`**
- **`show circuit slot/port vpi-vci`**
- **`debug aaa exception`**

5.9.1 Displaying AAA Logs

Use the **`show subscribers log`** command to display the AAA log. The output tracks inbound and outbound messages from the AAAd process.

The following example displays an unknown circuit from the AAA log:

```
[local]Redback#show subscribers log

---------------------------------------------------------
Total log size : 25000
Next log index : 1893
Log wrapped    : 58 time(s)
---------------------------------------------------------
0       OUT     Thu Sep 11 17:33:36.548471
IPC_ENDPOINT = ISM-IF, MSG_TYPE = IF-UNBIND,
Username = user2@NiceService,
CCT_HANDLE = Unknown circuit
Internal Circuit = 2/14:1023:63/6/2/27408
aaa_idx = 10056cc9, extern_handle = 4f, pvd_idx = 4008000d,
Event code = 0
---------------------------------------------------------
1       IN      Thu Sep 11 17:33:36.548486
IPC_ENDPOINT = PPPd, MSG_TYPE = SESSION_DOWN, term_ec = 142
terminate cause = No traffic within idle timeout period
Username = user2@NiceService,
CCT_HANDLE = Unknown circuit
Internal Circuit = 2/14:1023:63/6/2/27409
aaa_idx = 10056cca, extern_handle = 50, pvd_idx = 4008000d,
Event code = 0
```

Recommended Action: Issue the **`show circuit`** command to obtain more information about the unknown circuit.

5.9.2 Debugging AAA

Use the **`debug aaa exception`** command to display a AAA packet or function that unexpectedly ends a task; for example, an invalid password or username during authentication. In the output, all debug messages for successful authentication are filtered out, and only the error-condition debug logs are displayed—particularly useful when many subscribers are authenticating simultaneously.

Use the following AAA troubleshooting checklist to check for common AAA configuration issues.

Table 35 AAA Troubleshooting Check List

#	AAA Troubleshooting Check List	Checked?
1	Does the subscriber have an incorrect username, password, or context?	
2	Do you have incorrect domain on the client?	
3	Is the binding missing?	
4	Are the provisioning attributes; for example, ACLs and QoS, missing or incorrect?	
5	Is the circuit up?	
6	Is the interface subscriber binding not a multibind interface?	
7	Is the RADIUS server client correctly configured?	
8	Is the RADIUS server reachable? • Ping the RADIUS server and verify that the RADIUS server file has the IP address of your SmartEdge router. • Test the communications link to a RADIUS server using the **`test aaa`** {**`authentication`** | **`accounting`**} **`username`** *`name`***`password`** *`pwd`* **`protocolradius`** [**`server-ip`** *`ip-addr`* **`port`** *`port`*] Port 1812 or port 1645 tests authentication and authorization; port 1813 or 1646 tests accounting.	
9	Do the RADIUS ports configured on the SmartEdge router match the ports on the RADIUS server?	

The following example shows how to display the AAA log, which shows a subscriber with incorrect credentials:

```
[local]Redback#debug aaa exception

Feb 6 15:47:15: [13/1:1:63/1/2/11]: %AAA-7-EXCEPT1: aaa_idx 10000029:
Cannot bind subscriber user2@NiceService to valid context
Feb 6 15:47:15: [13/1:1:63/1/2/11]: %AAA-7-EXCEPT1: aaa_idx 10000029:
aaa_remove_session_from_trees: remove session that is not bound to any context yet
```

Recommended Action: Make sure that the subscriber is correctly configured. To determine the cause of the exception, issue the **`debug aaa all`** command.

5.9.3 Displaying Information About a VPI and VCI for an ATM PVC

Use the **`show circuit slot/port vpi-vci`** to display information about VPI and VCI for an ATM PVC. In the following example the circuit is down because it is unbound “`no-bind:1`”:

```
[local]Redback#show circuit 4/2:1 vpi-vci 200 20

Circuit               Internal Id   Encap          State Bound to
4/2:1 vpi-vci 200 20  1/2/27        atm-cell       Down
Summary:
  total: 1
     up: 0             down: 1
  bound: 0          unbound: 1
   auth: 0        interface: 0       subscriber: 0   bypass: 0
   no-bind: 1          atm: 1             chdlc: 0   dot1q: 0
     ether: 0           fr: 0               gre: 0
      mpls: 0          ppp: 0             pppoe: 0
     clips: 0         vpls: 0              ipip: 0
     ipsec:      ipv6v4-man: 0      ipv6v4-auto: 0
```

Recommended Action:

1. Check if the port is down.

2. Check for a configuration mismatch.

3. If the configuration is correct, check to see why the circuit is down. Check for authentication issues by using the following commands:

   - **`debug aaa authen`**

   - **`debug aaa auth`**

   - **`debug aaa exception`**

4. If authentication is through RADIUS, verify that the RADIUS server is alive by using the **`show radius server`** and **`show radius statistics`** commands.

5. Use the **`debug pppoe exception`** command to see if there are any unexpected events with PPPoE.

5.10 Step 10: Checking Access Protocol State

Use the **`show circuit counters`** command to check the status of CLIPS, DHCP, L2TP, and PPP protocols.

The following example shows you how to check the PPP state. The PPPoE Cntrl counters, which are highlighted in bold, should increase. The remaining counters should be zero (0).

```
[local]Redback# show circuit counters pppoe detail

please wait... Circuit: 3/1 pppoe 1, Internal id: 1/1/7015,
Encap: ethernet-pppoe-ppp-combined

Packets                             Bytes
-------------------------------------------------------------------
Receive          :               9  Receive         :           540
Receive/Second   :            0.00  Receive/Second  :          0.00
Transmit         :              10  Transmit        :           425
Transmit/Second  :            0.00  Transmit/Second :          0.00
IP Multicast Rcv :               0  IP Multicast Rcv:             0
IP Multicast Tx  :               0  IP Multicast Tx :             0
Unknown Encaps   :               0  Unknown Encaps  :             0
Down Drops       :               0  Down Drops      :             0
Unreach Drops    :               0  Unreach Drops   :             0
Adj Drops        :               0  Adj Drops       :             0
WRED Drops Total :               0  WRED Drops Total:             0
Tail Drops Total :               0  Tail Drops Total:             0
IP Counters
Soft GRE MPLS    :               0  Soft GRE MPLS   :             0
Not IPv4 drops   :               0  Not IPv4 drops  :             0
Unhandled IP Opt :               0
Bad IP Length    :               0
Bad IP Checksum  :               0
Broadcast Drops  :               0
PPP Counters
Cntrl Rcv        :               7  Cntrl Rcv       :           277
Cntrl Tx         :               0  Cntrl Tx        :             0
Cntrl Drops Rcv  :               0
Retries Rcv      :               0
Termreqs Rcv     :               0
PPPoE Counters
Cntrl            :               2  Cntrl           :          120
Session Drops    :               0
PADT Sent        :               0
PADR Drops       :               0
PADI Drops       :               0
PADT Drops       :               0
Bad Code         :               0
```

6 Troubleshooting the RADIUS Server

This section describes how to troubleshoot the RADIUS server and operations.

6.1 Step 1: Checking RADIUS Server Configuration and Status Information

Use the **`show radius server`** command to display RADIUS server configuration and status information.

```
[local]Redback#show radius server


Accounting Server
==============================================================================
  Address       Port      Key            State       State set time
==============================================================================
10.20.1.1       1813      ********       Alive       Thu May 11 17:26:05 2006
Algorithm:                first
Timeout (in sec.):        10
Max retry:                3
Max outstanding:          256
Server timeout (in sec.): 60
Deadtime (in min.):       5
CoA Server
==============================================================================
  Address       Port      Key            State       State set time
==============================================================================
10.20.1.1       3000      ********        Alive      Thu May 11 17:31:15 2006
```

Recommended Action: If you have RADIUS problem:

1. Issue the **`show configuration port`** command and check the configured interface to make sure that it is bound correctly to the context.

2. Issue the **`show port`** command and check the port status to which the context is bound.

3. Ping the RADIUS server from the associated context.

4. If the device is reachable, verify that the AAA parameters are configured correctly by testing the communications link to a RADIUS server. To do so, test the RADIUS communications link with an Authentication-Request message and Accounting-Request message using the **`test aaa`** {**`authentication`** | **`accounting`**} **`username`** ***`name`*** **`password`** ***`pwd`*** **`protocol radius`** [**`server-ip`** ***`ip-addr`*** **`port`** ***`port`***]. Port 1812 or port 1645 tests authentication and authorization; port 1813 or 1646 tests accounting.

6.2 Step 2: Checking RADIUS Statistics

Use the **show radius statistics** command to display RADIUS server statistics.

```
[local]Redback#show radius statistics

====================================================
Context: local
====================================================
Authentication Servers:
Requests send:                   63740919
Requests re-send:                394614
Request timeout:                 32470
Requests send fail:              142022
Requests accepted:               24446395
Requests rejected:               39213618
Response dropped:                0
Req in process:                  0
Req in waiting:                  0
Req in high wait queue:          0
Req in low wait queue:           0
Server slots                     768
Capacity:                        0%
Server marked dead:              31


Accounting Servers:
Requests send:                   90028597
Requests re-send:                724699
Request timeout:                 151259
Requests send fail:              23067
Requests accepted:               89841804
Requests rejected:               0
Response dropped:                0
Req in process:                  1
Req in waiting:                  0
Req in high wait queue:          0
Req in low waitqueue:            0
Server slots                     768
Capacity: 0%
Server marked dead:              22


CoA Servers:


Requests received:               0
Duplicate requests:              0
Response ACK:                    0
Response NAK:                    0


Send Details:


Subscriber authentication:
```

```
Request send:                    89494578
Request retransmit:              410512
Response received:               89433957
Server busy:                     860
Server not ready:                 0
No server:                        0
Server marked dead:               57
Bad attribute:                    0
Socket error:                     0
Send accept to AAAd:              38653147
Send reject to AAAd:              50780781
Send meth fail to AAAd:           11030
Internal error:                   0
Unknown attribute:                0


Authorization:
Request send:                     0
Request retransmit:               0
Response received:                0
Server busy:                      0
Server not ready:                 0
No server:                        0
Server marked dead:               0
Bad attribute:                    0
Socket error:                     0
Send accept to AAAd:              0
Send reject to AAAd:              0
Send meth fail to AAAd:           0
Internal error:                   0
Unknown attribute:                0


Subscriber session accounting:
Request send:                     129690977
Request retransmit:               484140
Response received:                129672566
Server busy:                      4621
Server not ready:                 0
No server:                        0
Server marked dead:               41
Bad attribute:                    0
Socket error:                     0
Accounting accepted:              129672566
Accounting timeout:               18969
Internal error:                   0
Unknown attribute:                0


L2tp accounting:


Request send:                     0
Request retransmit:               0
Response received:                0
Server busy:                      0
Server not ready:                 0
No server:                        0
Server marked dead:               0
Bad attribute:                    0
Socket error:                     0
Accounting accepted:              0
Accounting timeout:               0
Internal error:                   0
Unknown attribute:                0


Accounting On/Off:
```

```
Request send:                    9
Request retransmit:              34
Response received:               9
Server busy:                     0
Server not ready:                0
No server:                       0
Server marked dead:              0
Bad attribute:                   0
Socket error:                    0
Accounting accepted:             0
Accounting timeout:              0
Internal error:                  0
Unknown attribute:               0


Event accounting:


Request send:                    0
Request retransmit:              0
Response received:               0
Server busy:                     0
Server not ready:                0
No server:                       0
Server marked dead:              0
Bad attribute:                   0
Socket error:                    0
Accounting accepted:             0
Accounting timeout:              0
Internal error:                  0
Unknown attribute:               0


Receive Details:
No match request:                93406
No match server:                 0
Invalid packet:                  22
Bogus packet:                    16
Dup response packet:             0
```

Recommended: If you find an issue in the RADIUS statistics output, issue the **`debug aaa all`** command from the local context.

6.3 Step 3: Checking RADIUS Counters

Use the **`show radius counters`** command to display counters for RADIUS access, accounting, and Change of Authorization (CoA) messages. If the RADIUS server is configured as a CoA server, this command also displays CoA server counters. For information about RADIUS counters fields, see the *Command List*.

Table 36 RADIUS Counter Checklist

#	RADIUS counter checklist	Checked ?
1	Are the accounting packets being dropped and or retransmitted?	
2	Are there any timeouts?	
3	Are subscribers reporting authenticating problems? If so, did you check for a slow authentication process?	

The following example displays output from the **`show radius counters`** command:

```
[local]Redback#show radius counters

Server: 64.91.105.246 Port: 1645  Counter start time: Oct 31 04:14:10 2007
--------------------------------------------------------------------------
Access Messages:


Requests sent      : 62641
Requests retried   : 123385
Requests retried   : 123385
---------------------------------------------------------------------------
Requests send fail : 71092
Requests timeout   : 27429
Responses dropped  : 0
Accepts received   : 0
Rejects received   : 0
============================================================================
Server: 64.91.105.246    Port: 1646  Counter start time: Oct 31 04:14:10 2007
---------------------------------------------------------------------------
Accounting Messages:
---------------------------------------------------------------------------


Requests sent       : 282692
Requests retried    : 434608
Requests send fail  : 23067
Requests timeout    : 144479
Responses dropped   : 0
Accepts received    : 0
Rejects received    : 0
```

6.4 Step 4: Debugging RADIUS Attributes

Use the **debug aaa rad-attr** command to enable the debug of messages for RADIUS attributes.

```
[local]Redback#debug aaa rad-attr
The debug output provides information on what action to take to resolve
RADIUS issues.
```

6.5 Step 5: Checking RADIUS Connections

Use the **show radius control** command to display RADIUS server control information. You can see how busy the RADIUS server is processing the authentication and accounting packet. For more information about the fields for the **show radius control** command, see the *Command List*.

```
[local]Redback#show radius control

=========================================================
Context Name: local
---------------------------------------------------------
                         Authentication       Accounting
Number of server:        3                    3
Total slots:             256                  256
Total in waiting queue:  1416                 0
Total in process queue:  200                  0
Server status:           OK                   Ok
```

6.6 Step 6: Checking Incoming Requests on the Port

Use the **debug aaa authentication** and **debug aaa ip-pool** commands to check incoming requests on the port. The debug output provides information on what action to take to resolve an issue.

The following example enables the generation of AAA debug messages:

```
[local]Redback#debug aaa authentication
```

The following example enables the generation of AAA IP pool debug messages:

```
[local]Redback#debug aaa ip-pool
```