BRAS 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 Overview 1

2 Troubleshooting Subscriber Connectivity 3

2.1 Step 1: Navigating to the Correct Context 6

2.2 Step 2: Displaying Information About My Subscribers 6

2.3 Step 3: Checking System Health 11

2.4 Step 4: Checking for Configuration Errors 12

2.5 Step 5: Checking for Available IP Addresses 13

2.6 Step 6: Checking Interface Connectivity 13

2.7 Step 7: Checking Bindings 20

2.8 Step 8: Checking Licenses 22

2.9 Step 9: Checking Authentication 23

3 Troubleshooting PPP 27

3.1 PPP Troubleshooting Tasks 28

3.2 Step 1: Navigating to the Correct Context 30

3.3 Step 2: Checking Port Counters 30

3.4 Step 3: Verifying that PPP is Receiving Packets 31

3.5 Step 4: Checking PPP Circuit Counters 33

3.6 Step 5: Checking the PPP State on the Circuit 34

3.7 Step 6: Displaying PPP Summary Information 35

3.8 Step 7: Checking Interfaces 36

3.9 Step 8: Checking PPP Bindings 36

3.10 Step 9: Checking Subscribers 36

3.11 Step 10: Displaying Subscriber Routes 37

3.12 Step 11: Checking PPP Process 37

3.13 Step 12: Checking the RADIUS Server 37

3.14 Step 13: Checking the PPP Configuration 38

3.15 Step 14: Debugging PPP 39

4 Troubleshooting PPPoE 43

4.1 Overview of PPPoE 43

4.2 Before You Begin 44

4.3 PPPoE Sample Configuration 45

4.4 PPPoE Troubleshooting Tasks 46
4.5 Step 1: Navigating to the Correct Context 48
4.6 Step 2: Checking Port Counters 48
4.7 Step 3: Checking PPPoE Counters 49
4.8 Step 4: Verifying PPPoE Circuit Counters 52
4.9 Step 5: Checking the PPPoE State on the Circuit 54
4.10 Step 6: Checking Interfaces 55
4.11 Step 7: Checking Bindings 55
4.12 Step 8: Checking Subscribers 55
4.13 Step 9: Displaying PPPoE Summary Information 56
4.14 Step 10: Checking the PPPoE Configuration 58
4.15 Step 11: Checking PPPoE Process 58
4.16 Step 12: Displaying Subscriber Routes 58
4.17 Step 13: Checking the RADIUS Server 59
4.18 Step 14: Debugging PPPoE 59

5 L2TP 63
5.1 Terminology 63
5.2 Overview 64
5.3 L2TP Tunnels and Peers 65
5.4 Tunnel Switching 65
5.5 L2TP Packet Exchange 66
5.6 Understanding Tunnel Information on the LAC 67

6 Troubleshooting Specific L2TP Issues 69
6.1 No Replies to SCCRQ 71
6.2 Basic L2TP Tunnel Setup Problems 72
6.3 Tunnel Authorization Problems 73
6.4 LAC 1-Pass RADIUS Problems 74
6.5 L2TP Session Setup 76
6.6 CDN for an Unknown Session ID or Duplicate Remote Session ID 77
6.7 Stuck Sessions or Tunnels 77
6.8 Scaling Issues 78
6.9 Fragmentation 79
6.10 LNS PPP Session Setup 80

7 Troubleshooting General LAC L2TP Issues 83

7.1 Tasks to Troubleshoot General LAC L2TP Issues 84
7.2 Step 1: Checking Specific LAC Issues 86
7.3 Step 2: Navigating to the Correct Context 86
7.4 Step 3: Checking LAC Port Counters 86
7.5 Step 4: Displaying LAC Tunnel-Level Counters 87
7.6 Step 5: Displaying LAC IPC Counters 88
7.7 Step 6: Checking LAC Interfaces 89
7.8 Step 7: Verifying LAC L2TP Establishment 89
7.9 Step 8: Checking the LAC Status of L2TP Peers 89
7.10 Step 9: Performing LAC L2TP Tunnel and Session Testing 90
7.11 Step 10: Displaying L2TP Group Information on the LAC 92
7.12 Step 11: Displaying LAC Summary Peer Information 92
7.13 Step 12: Checking LAC Bindings 92
7.14 Step 13: Checking the LAC IP Route Summary Information 93
7.15 Step 14: Verifying the LAC Routes 93
7.16 Step 15: Displaying LAC PPP Summary Information 93
7.17 Step 16: Checking LAC L2TP Process 93
7.18 Step 17: Checking the LAC L2TP Configuration 93
7.19 Step 18: Checking the RADIUS Server 94
7.20 Step 19: Debugging the LAC 94

8 Troubleshooting LNS General L2TP Issues 95

8.1 Tasks to Troubleshoot General LNS Issues 96
8.2 Step 1: Checking Specific LNS Issues 98
8.3 Step 2: Navigating to the Correct Context on the LNS 98
8.4 Step 3: Checking LNS Port Counters 98
8.5 Step 4: Checking LNS Circuit Counters 99
8.6 Step 5: Displaying LNS Tunnel-Level Counters 99
8.7 Step 6: Displaying LNS IPC Counters 100
8.8 Step 7: Verifying LNS L2TP Establishment 102
8.9 Step 8: Checking L2TP Peers on LNS 103
8.10 Step 9: Displaying LNS L2TP Summary Information 105
8.11 Step 10: Checking LNS Bindings 105
8.12 Step 11: Checking LNS Interfaces 105
8.13 Step 12: Displaying LNS PPP Summary Information 105
8.14 Step 13: Checking LNS IP Routes 105
8.15 Step 14: Displaying LNS Subscriber Routes 106

8.16 Step 15: Verifying LNS Routes 106
8.17 Step 16: Checking the LNS L2TP Process 106
8.18 Step 17: Checking the LNS Configuration 107
8.19 Step 17: Checking the RADIUS Server 107
8.20 Step 18: Debugging the LNS 107

9 L2TP Debug Commands 109

10 Overview of DHCP 111
10.1 About DHCP 111

11 Troubleshooting Subscriber Connectivity on the Proxy or Relay 113
11.1 Troubleshooting Specific CLIPS Issues 114
11.2 DHCP Relay Is Not Receiving Offers 115
11.3 SmartEdge Router Is Not Sending Offers to Subscribers 115
11.4 Subscribers Are Not Receiving Offers 116
11.5 Subscriber Request Is Not Receiving An Acknowledgement 116
11.6 Subscribers Coming Through the Relay or Proxy Lose Connectivity 117
11.7 Subscribers Cannot Access the Network 117

12 Troubleshooting General DHCP Relay or Proxy Issues 119
12.1 Tasks to Troubleshoot the DHCP Relay or Proxy 120
12.2 Step 1: Checking Specific Troubleshooting DHCP Proxy or Relay Issues 122
12.3 Step 2: Navigating to the Correct Context 122
12.4 Step 3: Checking DHCP Relay or Proxy Statistics 122
12.5 Step 4: Checking Relay or Proxy Port Counters 126
12.6 Step 5: Verifying the Status of Existing Sessions on the Relay or Proxy 126
12.7 Step 6: Testing the DHCP Client and External DHCP Server 127
12.8 Step 7: Checking Relay or Proxy Interfaces 127
12.9 Step 8: Checking Bindings on the Relay or Proxy 127
12.10 Step 9: Checking Subscribers on the Relay or Proxy 128
12.11 Step 10: Checking the External DHCP Server IP Address on the SmartEdge Router 128
12.12 Step 11: Displaying Subscriber Routes and the Route to the External DHCP Server 128
12.13 Step 12: Checking All IP Routes on the Relay or Proxy 129

12.14 Step 13: Verifying DHCP Clients on the Relay or Proxy 129

12.15 Step 14: Examining ARP Entries on the Relay or Proxy 130

12.16 Step 15: Checking Relay or Proxy Configuration Issues 130

12.17 Step 16: Checking the DHCP Process on the Relay or Proxy 130

12.18 Step 17: Checking the RADIUS Server 130

12.19 Step 18: Debugging the DHCP Proxy or Relay 131

13 Troubleshooting the Internal DHCP Server 135

13.1 Tasks to Troubleshoot Internal DHCP Issues 136

13.2 Step 1: Navigating to the Correct Context 138

13.3 Step 2: Verifying Internal DHCP Server Statistics 138

13.4 Step 3: Checking Port Counters 139

13.5 Step 4: Checking Interfaces on the Internal DHCP Server 139

13.6 Step 5: Checking Bindings 140

13.7 Step 6: Verifying that the Circuit is Present on the Internal DHCP Server 140

13.8 Step 7: Verifying Leases on the Internal DHCP Server 140

13.9 Step 8: Checking Subscribers 141

13.10 Step 9: Displaying Summary IP Route Information on the Internal DHCP Server 141

13.11 Step 10: Displaying Subscriber Routes and the Route to the Internal DHCP Server 141

13.12 Step 11: Verifying ARP Entries 142

13.13 Step 12: Checking the DHCP Process on the Internal DHCP Server 142

13.14 Step 13: Checking the Internal DHCP Server Configuration 143

13.15 Step 14: Checking the RADIUS Server 143

13.16 Step 15: Debugging the Internal DHCP Server 144

13.17 Claiming Back a DHCP IP Address 146

14 Troubleshooting General CLIPS Issues 149

14.1 Tasks to Troubleshoot CLIPS Issues 150

14.2 Step 1: Navigating to the Correct Context 152

14.3 Step 2: Checking Port Counters 152

14.4 Step 3: Displaying CLIPS Counters 153

14.5 Step 4: Checking CLIPS Circuit Counters 153

14.6 Step 5: Checking Interfaces 153

14.7 Step 6: Checking Bindings 154

14.8 Step 7 Displaying Summary of CLIPS Sessions 154

14.9 Step 8: Displaying All Dynamic CLIPS Sessions 154

14.10 Step 9: Displaying CLIPS Sessions that are Down 154

14.11 Step 10: Checking Why CLIPS Sessions Are Not Up 154

14.12 Step 11: Checking Subscribers 155

14.13 Step 12: Displaying IP Route Summary Information 155

14.14 Step 13: Displaying CLIPS Groups 156

14.15 Step 14: Checking ARP Entries 156

14.16 Step 15: Checking the CLIPS Process 156

14.17 Step 16: Checking the CLIPS Configuration 156

14.18 Step 17: Checking the RADIUS Server 157

14.19 Step 18: Debugging CLIPS 157

15 Troubleshooting the RADIUS Server 159

15.1 Checking RADIUS Server Configuration and Status Information 159

15.2 Checking RADIUS Statistics 160

15.3 Checking RADIUS Counters 162

15.4 Debugging RADIUS Attributes 163

15.5 Checking RADIUS Connections 163

15.6 Checking Incoming Requests on the Port 164

1 Overview

This document provides troubleshooting techniques for BRAS problems on the SmartEdge® router, including subscriber connectivity, Point-to-Point Protocol (PPP), PPP over Ethernet (PPPoE), Layer 2 Tunneling Protocol (L2TP), Dynamic Host Configuration Protocol (DHCP), clientless IP service selection (CLIPS), and Remote Authentication Dial-In User Service (RADIUS) problems.

For information about how to get help with a command, the role of contexts in troubleshooting, how to perform basic debugging tasks, and use basic troubleshooting commands, how to access the SmartEdge router components, perform backups, collect troubleshooting data, and enable logging, see *Basic Troubleshooting Techniques*.

For information about troubleshooting general issues, including hardware, see the *General Troubleshooting Guide*.

2 Troubleshooting Subscriber Connectivity

This section shows you to troubleshoot subscriber connectivity problems.

Note: Some commands in this guide are not supported on versions prior to Release 6.2.1.

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

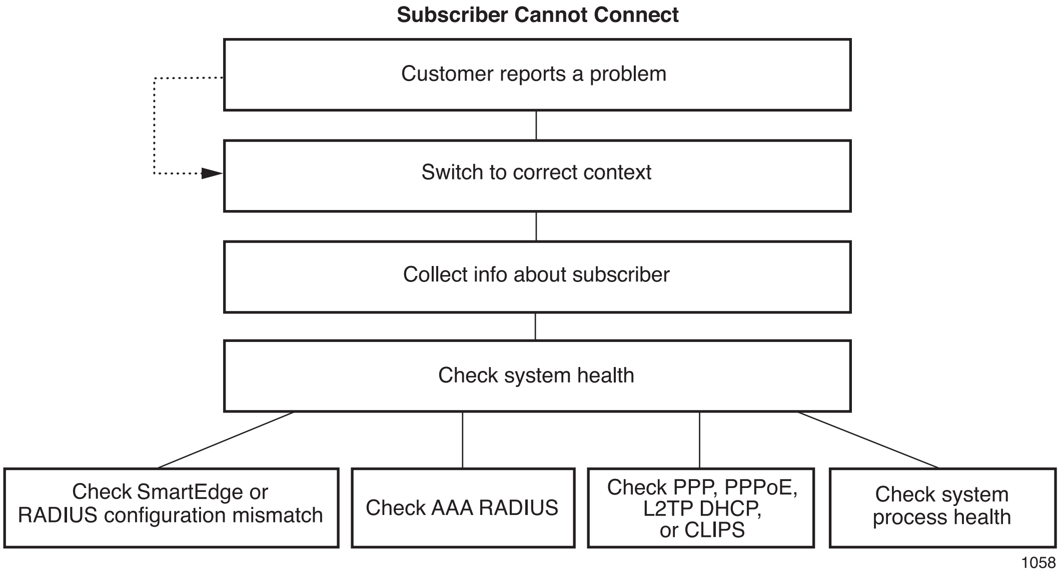

Subscriber Cannot Connect
Customer reports a problem
Switch to correct context
Collect info about subscriber
Check system health
Check SmartEdge or RADIUS configuration mismatch
Check AAA RADIUS
Check PPP, PPPoE, L2TP DHCP, or CLIPS
Check system process health
1058

Figure 1 Troubleshooting Subscriber Software Connectivity

Use Table 1 as a guide to troubleshooting BRAS 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 1 Tasks to Troubleshoot Subscriber Connectivity Issues

Task	Command	Notes	Checked?

Navigating to the Correct Context	`show context all`
	`context` *`context-name`*
		Display all the contexts on your router and then navigate to the context you that want to troubleshoot.	

Displaying Subscribers Information	`show subscriber active`
	`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 AAA logs of subscribers.	

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

Checking for Configuration Errors	`show configuration context`
	`context-name`
		• 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?	

Checking Available IP Addresses	`show ip pool`	Display addresses available in an IP pool.	

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, and debug PPPoE discovery.
		• Display general counters and counters specific to the circuit type for one or more circuits in the system.
		• Display port counters.	

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

Table 1 Tasks to Troubleshoot Subscriber Connectivity Issues

Task	Command	Notes	Checked?

Checking Authentication	`show subscriber log`
	`debug aaa exception`
	`show circuit` *`slot/port`*
	`vpi-vci`
		• 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.	

Troubleshooting PPP			
Troubleshooting PPPoE			
Troubleshooting Specific L2TP Issues			
Troubleshooting General LAC Issues			
Troubleshooting General LNS Issues			
Troubleshooting Subscriber Connectivity on the Proxy or Relay			
Troubleshooting General DHCP Relay or Proxy Issues			
Troubleshooting the Internal DHCP Server			
Troubleshooting CLIPS			
Troubleshooting the RADIUS Server			

2.1 Step 1: Navigating to the Correct Context

Use the **show context all** command to view all your contexts and then navigate to the context that you want to troubleshoot. For information about contexts, see *Understanding How the Active Context Affects Debug Output*.

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#
```

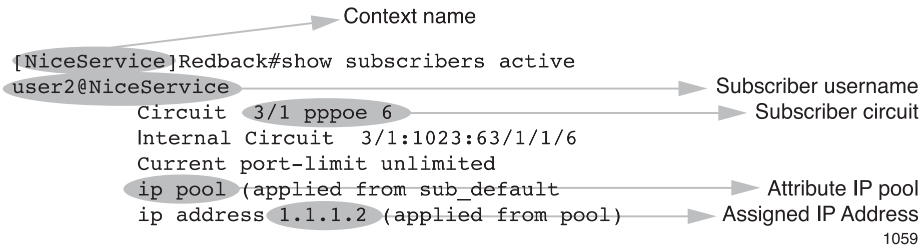
2.2 Step 2: Displaying Information About My Subscribers

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

2.2.1 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.



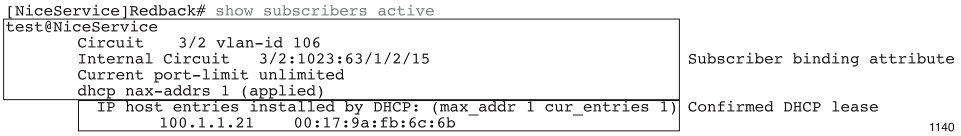
```
[NiceService]Redback#show subscribers active
user2@NiceService
          Circuit  3/1 pppoe 6
          Internal Circuit  3/1:1023:63/1/1/6
          Current port-limit unlimited
          ip pool (applied from sub_default
          ip address 1.1.1.2 (applied from pool)
```

Figure 2 Show Subscribers Active Command Output Fields

Table 2 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 illustration identifies the **`show subscribers active`** command output fields for a DHCP lease.



```
[NiceService]Redback# show subscribers active
test@NiceService
       Circuit   3/2 vlan-id 106
       Internal Circuit   3/2:1023:63/1/2/15
       Current port-limit unlimited
       dhcp nax-addrs 1 (applied)
         IP host entries installed by DHCP: (max_addr 1 cur_entries 1)
               100.1.1.21    00:17:9a:fb:6c:6b
```

Figure 3 Show Subscribers Active Command Output Fields

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, use the **`debug circuit`** command and specify the circuit that you obtained from the **`show subscribers active`** ***`username`*** command to obtain more information about the issue.

The following example displays information about the DHCP hosts after they have been established on the active subscriber circuits:

```
[atm_subs]Redback#show subscribers active
sub1@atm_subs
        Circuit   1/4:1 vpi-vci 0 101
        Internal Circuit   1/4:1:63/1/2/24579
        Current port-limit unlimited
        profile gold (applied)
        dhcp max-addrs 10 (applied)
        ip interface gold (applied)
        IP host entries installed by DHCP: (max_addr 10 cur_enties 10)
                120.1.1.199    00:dd:00:00:00:0a
                120.1.1.191    00:dd:00:00:00:09
                120.1.1.192    00:dd:00:00:00:08
                120.1.1.200    00:dd:00:00:00:07
                120.1.1.194    00:dd:00:00:00:05
                120.1.1.193    00:dd:00:00:00:06
                120.1.1.196    00:dd:00:00:00:03
                120.1.1.195    00:dd:00:00:00:04
                120.1.1.197    00:dd:00:00:00:02
                120.1.1.198    00:dd:00:00:00:01
sub2@atm_subs
        Circuit   1/4:1 vpi-vci 0 102
        Internal Circuit   1/4:1:63/1/2/24580
        Current port-limit unlimited
        profile silver (applied)
        dhcp max-addrs 10 (applied)
        ip interface silver (applied)
          IP host entries installed by DHCP: (max_addr 10 cur_enties 10)
                120.1.2.191    00:dd:00:00:00:14
                120.1.2.192    00:dd:00:00:00:13
                120.1.2.193    00:dd:00:00:00:12
                120.1.2.194    00:dd:00:00:00:11
                120.1.2.195    00:dd:00:00:00:10
                120.1.2.196    00:dd:00:00:00:0f
                120.1.2.197    00:dd:00:00:00:0e
                120.1.2.198    00:dd:00:00:00:0d
                120.1.2.199    00:dd:00:00:00:0c
                120.1.2.200    00:dd:00:00:00:0b
sub3@atm_subs
        Circuit   1/4:1 vpi-vci 0 103
        Internal Circuit   1/4:1:63/1/2/24581
        Current port-limit unlimited
        profile bronze (applied)
        dhcp max-addrs 10 (applied)
        ip interface bronze (applied)
        IP host entries installed by DHCP: (max_addr 10 cur_enties 10)
                120.1.3.191    00:dd:00:00:00:1e
                120.1.3.192    00:dd:00:00:00:1d
                120.1.3.193    00:dd:00:00:00:1c
                120.1.3.194    00:dd:00:00:00:1b
                120.1.3.195    00:dd:00:00:00:1a
                120.1.3.196    00:dd:00:00:00:19
                120.1.3.197    00:dd:00:00:00:18
                120.1.3.198    00:dd:00:00:00:17
                120.1.3.199    00:dd:00:00:00:16
                120.1.3.200    00:dd:00:00:00:15
```

Use the **`show subscribers active handle`** command to find the circuit information (for example, useful for the (Slot/Port/PVC), when you only have the internal handle:

```
[local]Redback#show subscribers active handle 3/1:1023:63/1/2/12375

Circuit 3/1 vpi-vci 0 380 =============>VPI-VCI Info.*
Internal Circuit 3/1:1023:63/1/2/12375*
Current port-limit unlimited
ip address 10.1.1.1 (applied)
dns primary 10.10.10.10 (not applied)
dns secondary 10.10.10.11 (not applied)
```

2.2.2 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, use the **clear subscriber** ***username*** command.

2.2.2.1 Displaying Information About All Subscribers in All Contexts

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

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

2.2.2.2 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
```

2.2.2.3 Displaying Summary Subscriber Information

The following example shows how to display summary information about subscribers:

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

2.2.3 Displaying Subscriber Logs

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

2.2.3.1 Wrong Username or Password on Subscriber Binding

The following shows a subscriber log with a `term_ec = 24` error, indicating an authentication error: the subscriber has the wrong user name or password on the subscriber binding:

```
[local]Redback#show subscribers log
32 IN Tue Mar 4 15:31:59.401541
IPC_ENDPOINT = DOT1Qd, MSG_TYPE = SESSION_DOWN, term_ec = 24
CCT_HANDLE = 3/2 vlan-id 105
Internal Circuit = 3/2:103:63/1/2/48
aaa-idx = 300000e, extern-handle = 0, pvd_idx=4008002,
Event Code =0
```

2.2.3.2 Incorrect Context or Domain Name

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

The following example shows a subscriber log with a `term_ec = 26` error code, indicating that the subscriber has an incorrect context or domain name or the context or the domain does not exist:

```
209 IN Mon Jan 2 17:52:17.837
IPC_ENDPOINT = PPPd, MSG_TYPE = SESSION_DOWN, term_ec = 26
Username = user@WRONG,
CCT_HANDLE = 13/1:1 vpi-vci 0 100
Internal Circuit = 13/1:1:63/1/2/11
aaa_idx = 1000005f, extern_handle = 0, pvd_idx = 40080002,
Event code = 0
```

2.2.3.3 Display Information About a Specific Subscriber

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 subscribers 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,
-----------------------------------------------------
```

2.3 Step 3: Checking System Health

Use the **show system alarm**, command to check system health. For information about the **show subscribers summary all** command, see Displaying Summary Information About all Subscribers. For information about the **show system alarm** command, see the *General Troubleshooting Guide*.

2.3.1 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 this command, see the *Command List*. 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.

2.3.2 Displaying System Alarm

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

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

2.3.3 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 alarms 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
```

2.3.4 Displaying Summary Information About all Subscribers

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
```

2.4 Step 4: Checking for Configuration Errors

Use the **show configuration context** command and check for configuration errors listed in Table 3. Use this table as guide to troubleshoot common misconfiguration issues.

Table 3 Configuration Mismatch Checklist

#	Task	Checked?
1	Is the subscriber using an incorrect domain suffix in the username?	
2	Is the user's password, or context configured correctly?	
3	Do the subscriber and server have a VPI/VCI pair that does not match?	
4	Do the subscriber and server VCs have an encapsulation type that does not match?	
5	Do the subscriber and server have an authentication method that does not match?	
6	Is the binding missing or incorrect?	
7	Are the provisioning attributes, for example, ACLs or QoS, missing or incorrect?	
8	Is the interface that the subscriber is binding to not a multibind interface?	
9	Are the maximum number of sessions correctly specified?	
10	Did you forget to commit the configuration?	
11	Is the subscriber's VLAN correctly configured?	

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

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

2.5 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.

2.6 Step 6: Checking Interface Connectivity

Use the **`ping`**, **`show port counters`**, and **`show circuit counters`** commands to check for interface connectivity.

2.6.1 Pinging the Interface

The following example shows you how to ping an interface.

```
[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
```

2.6.2 Verifying Interfaces

Use the **`show ip interface brief`** to verify that the interfaces are up. This command displays the name, IP address, and other information (in brief) for all configured interfaces in the current context. Check the interface state to see if it is operational and binding to determine which physical circuit this interface uses to forward traffic. The binding has to be defined between a physical circuit (as port and PVC) and a logic interface in a context. For information about what to check on a port, see Checking Port Performance.

An interface can be in any of the following states:

- Unbound—The interface is not currently bound to any port or circuit. If the interface is unbound, for example, interface `12/1`, it is a configuration error. The binding has to be configured between some physical circuit (like port or VLAN and interface `12/1`. An interface can be unbound also if a subscriber with dynamic binding is not up, in which case you would troubleshoot the corresponding circuit.

- Bound—The interface is bound to at least one port or circuit; however, none of the bound circuits are up; therefore, the interface is not up. A bound state indicates that interface is correctly configured and that a problem exists on the L1/L2 level.

- 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 following example displays output from the **`show ip interface`** command with the **`brief`** keyword:

```
[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)
```

2.6.3 Checking Port Performance

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 (using the **`no shutdown`** command) or is down (using the **`shutdown`** command). If the Admin state is *shut down*, the port is down.

  Recommended Action: Use 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 following checklist:

Table 4 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 (like multimode or single mode)?	
7	Is the other end port shut down?	
8	Is there an autonegotiation mismatch?	
9	If there is a flow control mismatch as in the case of LAG group, is the line state down?	
10	Is the SmartEdge router Gigabit Ethernet traffic GE port connected to an FE port? SmartEdge router Gigabit Ethernet traffic cards do not support FE speeds. **Note**: This is a 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 **`detail`** or **`live`** keyword 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 5 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
```

Use the **`show port counters live`** 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 increasing, packets are probably being dropped; use the **`show port counters detail`** command for detailed output. 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.

For an ATM port:

- Verify that the ATM port is up using the **show port *slot/port* detail** command. When the port has a MAC address or linkgroup MAC address, verify that it is correct. For more information about this command, see the *Command List*.
- Verify the ATM PVC is up using the **show atm pvc summary** command. For "ppp llc", "ppp nlpid" or "ppp serial" encapsulations, confirm that the PPP daemon has the knowledge of this circuit. If there is a PVC down, use the **show atm pvc all** command to see a specific PVC. For more information about this command, see the *Command List*.
- Verify that ATM PVC is receiving packets using the **show atm counter *slot/port* vpi *vpi* vci *vci***. If the PVC is not receiving packets, check the client settings and connection with the server.

```
[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
```

2.6.4 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
```

2.6.5 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 for, see the *Command List*.

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, 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 3/3 vlan-id 102 detail

[local]Redback#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
 ...
```

Use the **`show circuit counters handle`** ***`handle`*** **`detail`** command to see detailed information about whether the packets are received and sent to the circuit (only in case of unicast messages received from the client).

If there are no packets entering the circuit or port, investigate the fault at the circuit and port level.

The following example shows detailed information about a circuit that has unknown encapsulations :

```
[local]Redback#show circuit counters handle 255/22:1:26/1/1/10
detail | include Unk

Unknown Encaps  :         44  Unknown Encaps  :        7882
Unknown Encaps  :          0  Unknown Encaps  :           0
Unknown Encaps  :          0  Unknown Encaps  :           0
```

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
```

2.7 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, use 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
```

2.8 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 subscribers summary all`** command. Some licenses have no limits. If the feature is enabled, check that the correct license is 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
```

2.9 Step 9: Checking Authentication

The SmartEdge router uses RADIUS servers to authenticate 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 a 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 subscriber log`** command is also useful for checking authentication requests. We recommend that you use the **`show subscribers log username`** ***`subscriber`*** 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 Displaying Subscriber Logs.

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

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

2.9.1 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: Use the **show circuit** command to obtain more information about the unknown circuit.

2.9.2 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 check list to check for common AAA configuration issues.

Table 6 AAA Troubleshooting Check List

#	AAA Troubleshooting Check List	Checked?
1	Does the subscriber have an incorrect username, password, or context?	
2	Is an incorrect domain configured 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*** **protocol radius** [**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, use the **debug aaa all** command.

2.9.3 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 using the following commands: **debug aaa authen, and debug aaa auth** and **debug aaa exception**.

4. If authentication is through RADIUS, verify that the RADIUS server is functioning using the **show radius server** and **show radius statistics** commands. For information about these commands, see Troubleshooting RADIUS.

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

3 Troubleshooting PPP

This section describes how to troubleshoot PPP. For information about troubleshooting PPPoE, see Troubleshooting PPPoE. For information about operational commands, see the *Command List*.

The following is a sample PPP configuration for the SmartEdge router in context `isp1`:

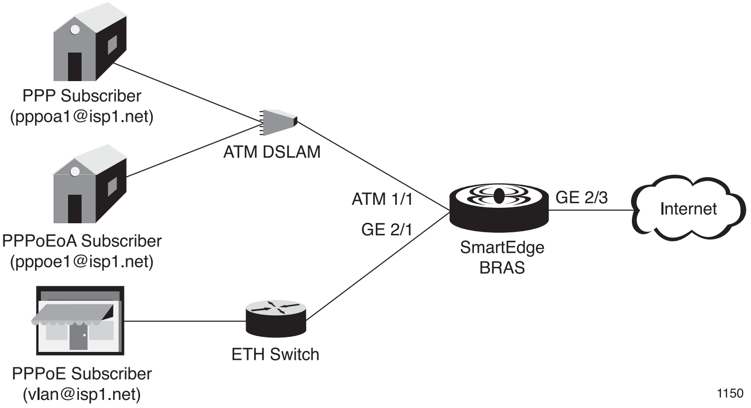


Figure 4 PPP Network Topology

```
context isp1
 interface forPPP-clients multibind
  ip address 1.1.1.1/24
  ip pool 1.1.1.0/24
 interface toInternet
  ip address 2.1.1.1/24
 ip route 0.0.0.0/0 2.1.1.254
 aaa authentication subscriber local
 subscriber default
  ip address pool
 subscriber name pppoa1
  password test1
 subscriber name pppoe1
  password test2
 subscriber name vlan1
  password test3
 atm profile ubr
  shaping ubr
!
port atm 1/1
 no shutdown
 atm pvc 1 32 profile ubr encapsulation ppp
  bind authentication chap pap
 atm pvc 1 33 profile ubr encapsulation pppoe
  bind authentication chap pap
!
port ethernet 2/1
 encapsulation dot1q
 dot1q pvc 32 encapsulation pppoe
  bind authentication chap pap
!
port ethernet 2/4
 no shutdown
 bind interface toInternet isp1.net
```

3.1 PPP Troubleshooting Tasks

Use Table 7 as a guide to troubleshooting PPP issues. Before you begin, get a description of the problem and check if you made any recent changes or upgrades to the network.

Note: When working with technical support representatives, run the **`show tech-support`** command on your router and have it available to assist in troubleshooting.

Table 7 Tasks to Troubleshoot PPP Issues

Task	Command	Notes	Checked?

Step 1: Navigating to the Correct Context	**`show context all`**
	`context` ***`context-name`***
		Display all the contexts on your router and then navigate to the context you want to troubleshoot.	

Step 2: Checking Port Counters	**`show port counters live`**	Check port statistics.	

Step 3: Verifying that PPP is Receiving Packets	**`show ppp counters`**
	`show ppp counters detail`
		Display summary or detailed statistics for PPP packets and session counters on the system.	

Step 4: Checking PPP Circuit Counters	**`show circuit counters ppp`**
	`show circuit counters ppp detail`		

Step 5: Checking the PPP State on the Circuit	**`show circuit detail`**
	`show circuit handle detail`
	`show circuit ppp detail`		

Step 6: Displaying PPP Summary Information	**`show ppp summary`**
	`show circuit ppp detail clear`
	`show circuit ppp down detail`
		• Displays statistics for PPP packets and session counters on the system
		• Specifies that only PPP sessions for which the LCP is in the INITIAL, CLOSED, or STOPPED state are to be displayed.
		• Displays detailed information about circuits that are down.	

Step 7: Checking Interfaces	**`show ip interface brief`**	Make sure the interfaces are up.	
Step 8: Checking PPP Bindings	**`show bindings summary`**	Display the configured bindings for one or more subscribers, ports, channels, or PVCs on the system.	
Step 9: Checking Subscribers	**`show subscribers active`**	Display information about active subscribers.	
Step 10: Displaying Subscriber Routes	**`show ip route subscriber`**	Verify where the subscriber is terminating. Make sure the IP address negotiated during the IPCP stage is correctly installed in the routing table.	

Step 11: Checking PPP Process	**`show process ppp`**
	`show crashfiles`
		• Verify that the PPP process is running.
		• If the PPP process is not running, check for a core dump.	

Step 12: Checking the PPP Configuration	**`show configuration ppp`**	Display PPP configuration.	

Table 7 Tasks to Troubleshoot PPP Issues

Task	Command	Notes	Checked?
Step 13: Checking the RADIUS Server		If you have configured a RADIUS server, make sure the RADIUS attributes are configured correctly for your clients. For information about checking the RADIUS Server, see Troubleshooting the RADIUS Server.	
Step 14: Debugging PPP		**Caution**: Enabling the generation of debug messages can severely affect system performance.	

3.2 Step 1: Navigating to the Correct Context

Use the **show context all** command and display all the contexts on your router and then navigate to the context you want to troubleshoot—in this case, the `isp1` context.

The following example shows how to view all contexts on your router and then navigate to context `isp1`:

```
[local]Redback#show context all
Context Name     Context ID     VPN-RD    Description
----------------------------------------------------
local             0x40080001
isp1              0x40080002

[local]Redback#
[local]Redback#context isp1
[isp1]Redback#
```

3.3 Step 2: Checking Port Counters

Use the **show port counter live** command to check port performance. For information about this command, see Checking Port Performance.

For an ATM port:

- Verify that the ATM port is up using the **show port *slot/port* detail** command. When the port has a MAC address or linkgroup MAC address, verify that it is correct.

- Verify the ATM PVC is up using the **show atm pvc summary** command. For "ppp llc", "ppp nlpid", or "ppp serial" encapsulations, confirm that the PPP daemon recognizes this circuit. If a PVC is down, use the **show atm pvc all** command to see all PVCs.

- Verify that ATM PVC is receiving packets by using the **show atm counter *slot/port* vpi *vpi* vci *vci*** command. If the PVC is not receiving packets, check the client settings and connection with the server.

3.4 Step 3: Verifying that PPP is Receiving Packets

Use the **show ppp counters** to check that the PPP daemon is receiving packets. This command displays statistics for PPP packets and session counters on the system.

The following example shows how to display the context-specific PPP counters for the current context:

```
[local]Redback#show ppp counters context
Last cleared: Never
received: bytes 260, packets 26,
unsupported packets 0
sent: bytes 260, packets 26
LCP echo request : received 26, sent 0, dropped 0
LCP echo response : received 0, sent 26, dropped 0
LCP protocol reject : received 0, sent 0, dropped 0
```

The **clear** option provides more recent PPP counter information. Use the **clear** option after the **show ppp counters** or **show ppp counters detail** commands to clear the counters and recollect them after 30 seconds. After 30 seconds, look at what caused PPP to go down. If you want to keep a record of your show counters for an extended period of time, capture your log information and save it before you use this option. Otherwise, use the **show ppp counters** command.

The following example shows how to display global PPP counters:

```
[isp1]Redback#show ppp counters clear
Current time: Mon Apr 23 07:31:45 2007
 Last cleared: Never Packet
Wed Jun 30 21:56:07 2005
Packet--------------------------------------------------------
In                          285     Out                    287
Session-------------------------------------------------------
LCP Up                       72     LCP Down                68
IPCP Up                      12     IPCP Down                6
Authen Success                0     Authen Failure           0
Session Up                    0     Session Down             0
SessionControl------------------------------------------------
Starting                      0     Authenticating           0
Pended (current)              0     Pended (total)           0
Packet Drop
Session pended                0     At Limit                 0
Timeout-------------------------------------------------------
ConfReq                      85     TermReq                 19
CHAP Challenge                0     UPAP Listen              0
PacketDropIn--------------------------------------------------
Session is Down              17     Bad FSM State           32
```

The following example shows how to display detailed information for global PPP counters:

```
[isp1]Redback#show ppp counters detail clear
Packet--------------------------------------------------------
In                           40 Out                         40
ConfReq                      24  ConfReq                    10
ConfAck                      10  ConfAck                    10
ConfNak                       0  ConfNak                     4
ConfRej                       0  ConfRej                    10
TermReq                       4  TermReq                     2
TermAck                       2  TermAck                     4
Authen Proto                  6  Authen Proto                6
other                         0  other                       0
Session-------------------------------------------------------
LCP Up                        6 LCP Down                     6
 IPCP Up                      4 IPCP Down                    4
 Authen Success               4 Authen Failure               2
 Session Up                   4 Session Down                 6
SessionControl------------------------------------------------
 Starting                     0 Authenticating               0
 Pended (current)             0 Pended (total)               0
 Packet Drop
 Session pended               0 At Limit                     0
Timeout-------------------------------------------------------
 ConfReq                      0 TermReq                      4
 CHAP Challenge               0 UPAP Listen                  0
PacketDropIn--------------------------------------------------
 Session is Down              1 Bad FSM State                0
DownCause-----------------------------------------------------
 Rcvd TermReq                 4 Rcvd PPPoE PADT              0
 No ConfReq Resp              0 No Echo Resp                 0
 Authen Failed                2 Session Down                 0
 LCP Down                     0 Circuit Down                 0
 Port Down                    0 Port Delete                  0
```

3.5 Step 4: Checking PPP Circuit Counters

Use the **`show circuit counters ppp detail`** command to check the status of the PPP protocol.

The following example shows you how to check the PPP state. The PPP Cntrl counters should increase. The remaining counters should be zero (0).

```
[ips1]Redback# show circuit counters ppp detail
Circuit: 1/4 vlan-id 10 pppoe 62, Internal id: 6/2/62, Encap:
ether-dot1q-pppoe-ppp
Packets                                  Bytes
--------------------------------------------------------------------
Receive         :                    50  Receive         :      3950
Receive/Second  :                  0.00  Receive/Second  :      0.00
Transmit        :                    51  Transmit        :      3968
Xmits/Queue                              Xmits/Queue
0             :                    51    0             :       3968
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
Xmit Q Deleted  :                   0  Xmit Q Deleted  :          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
WRED Drops Total:                     0  WRED Drops Total:        0
WRED Drops/Queue                         WRED Drops/Queue
0             :                     0    0             :          0
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
Tail Drops Total:                     0  Tail Drops Total: 0
Tail Drops/Queue                         Tail Drops/Queue
0             :                     0    0             :          0
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
PPP Counters
Cntrl Rcv       :                     4  Cntrl Rcv       : 190
Cntrl Tx        :                     4  Cntrl Tx        : 170
Cntrl Drops Rcv :                     0
Retries Rcv     :                     0
Termreqs Rcv    :                     0
PPPoE Counters
Cntrl           :                     0  Cntrl           : 0
Session Drops   :                     0
PADT Sent       :                     0
PADR Drops      :                     0
PADI Drops      :                     0
PADT Drops      :                     0
Bad Code        :                     0
Rate Refresh Interval : 60 seconds
```

3.6 Step 5: Checking the PPP State on the Circuit

Use the **`show circuit detail`** or **`show circuit handle`** ***`handle`*** **`detail`** commands to check the PPP state on the circuits. Make sure the encapsulation type is correct.

Check the following:

- Verify the circuit is up and the PPP LCP and the PPP ICP states are Opened
- Verify the encapsulation type. It should be ***-pppoe-ppp-combined**
- Verify the MTU size. It should be **1492**.

```
[isp1]dback# show circuit detail
Circuit: 3/1 pppoe 1, internal id: 1/1/7015, state: Up
interface bound : pool@test
subscriber bound : pppoa1@isp.net
bind type : chap pap
admin state : 1 hardware address : 00:30:88:00:77:0c
media type : ethernet encap type : ethernet-pppoe-ppp-combined
mode type : 0x2 port type : etherne
mtu size : 1492 cfg mtu size : 1500
ipv6 mtu size : 1500 ipv6 cfg mtu size : 1500
cct speed : 100000 cct rx speed : 0
cct flags (attr) : 0x1
slot mask : 0x0 ppa cct clear : FALSE
if flags : 0x0
profile id : 0 version : 207874
PPP OSINLCP State : Initial PPP MPLSCP State : Initial
PPPOE State : READY
internal handle : 3/1:1023:63/1/1/7015
```

Note: To find a circuit handle, use the **`show circuit`** ***`circuit-type`*** **`detail | grep [`*`ip-address`*` | `*`username`*` | `*`mac-address`*`]`** command. When you use this command, make sure the encapsulation type is correct.

3.7 Step 6: Displaying PPP Summary Information

Use the **show ppp summary** command to display summary output for PPP sessions in the current context. When you use this command, for "ppp llc", "ppp nlpid", or "ppp serial" encapsulations, make sure that the PPP daemon recognizes this circuit . You can also use the **show ppp down** command to specify that only PPP sessions for which the LCP is in the INITIAL, CLOSED, or STOPPED state are displayed:

```
[isp1]Redback#show ppp summmary
Wed Jun 30 21:54:29 2005
Number    LCP    IPCP   NLCP  MPLSCP
Circuit Type   Circuit   Open   Open   Open  Open
------------   -------   ----   ----   ----  ------
mp circuits   2         2      2      0     0
ppp circuits  2         2      2      0     0
Total circuits: 4  up: 4  down: 0
```

If the circuits are down, use the **show circuit ppp down detail** command to collect more information about the issue.

```
[isp1]Redback#show circuit ppp down detail
Circuit: 4/1:1 vpi-vci 1 100, internal id: 1/2/8388608, state: Down
------------------------------------------------------------------------------
interface bound   :
subscriber bound  :
bind type         : chap pap
admin state       : 1            hardware address  :
00:30:88:00:37:11
media type        : atm          encap type        : atm-ppp-vcmux
mode type         : 0x2          port type         : atm
mtu size          : 4470         cfg mtu size      : 4470
ipv6 mtu size     : 4470         ipv6 cfg mtu size : 4470
cct speed         : 149760       cct rx speed      : 149760
cct flags (attr)  : 0x1
slot mask         : 0x0          parent slot mask  : 0x0 ppa cct clear: FALSE
if flags          : 0x0          aaa index         : 0x0
profile id        : 1342193665   version           : 987
h node id         : 0
lg_id             : 0            spg_id            : 0
PPP LCP State     : Initial      PPP IPCP State    : Initial
PPP OSINLCP State : Initial      PPP MPLSCP State  : Initial
internal handle   : 4/1:1:63/1/2/8388608
```

3.8 Step 7: Checking Interfaces

Use the **`show ip interface brief`** to verify that the interfaces are up. This command displays the name, IP address, and other information (in brief) for all configured interfaces in the current context.

The following example displays output from the **`show ip interface`** command with the **`brief`** keyword:

```
[isp1]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)
```

Recommended Action: If the interfaces are down, see Verifying Interfaces and Checking Port Performance.

3.9 Step 8: Checking PPP Bindings

Use the **`show bindings`** command to verify your bindings. For information about this command, see Section 2.7 on page 20.

3.10 Step 9: Checking Subscribers

Use the **`show subscribers`** commands to check your subscribers. Following are some examples of how to use **`show subscribers`** commands:

Table 8 Show Subscriber Command Examples

Command	Description
`show subcribers all|grep` “***`time`***"	Display all subscribers starting at a certain time.
`show subcribers all |grep` “***`@domain-name`***”**`| count`**	Display how many subscribers are online for a particular domain.
`show subcribers active|begin before 3 after 5` “***`user@domain-name`***”	Display three lines prior and five lines after the match of the "***`user@domain-name`***". Normally, the grep shows a single line of the match.
`show subcribers all|grep` “**`PPP`**”	Display all PPP and PPPoE subscribers.
`show subscribers active` ***`username user2@NiceService`***	Display the information for an active subscriber.
`show subcribers all|grep` ***`user2@NiceService`***	Display information about the binding, context, and subscriber.
`show subcribers active handle` ***`handle`***	Display the circuit information; useful for example, for (slot/port/PVC), when you have the internal handle.

For more information about how to use the **show subscribers** command, Displaying Information About My Subscribers.

3.11 Step 10: Displaying Subscriber Routes

Use the **show ip route subscriber** command to check where the subscriber is terminated. Make sure the IP address negotiated during the IPCP stage is correctly installed in the routing table.

```
[ips1]Redback# show ip route subscriber
Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B
 - IBGP
    A,H - derived hidden
    O   - OSPF, IA - OSPF inter area, N1  - OSPF NSSA external type 1
    N2  - OSPF NSSA external type 2,  E1  - OSPF external type 1
    E2  - OSPF external type 2
    I   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2
    IPH - IP Host, SUB A - Subscriber address, SUB S - Subscriber
 static
       A - Derived Default
       >   - Active Route
Type    Network       Next Hop   Dist  Metric  UpTime       Interface
> SUB A 20.1.1.1/32                15      0   00:01:08     LNS1
> SUB A 20.1.1.2/32                15      0   00:01:08     LNS1
> SUB A 30.1.1.0/32                15      0   00:01:08     LNS1
```

3.12 Step 11: Checking PPP Process

Use the **show process ppp** command to verify that the PPP process is running. For detailed information, use the **detail** keyword. If the PPP process is not running, use the **show crashfiles** command to check if there is a core dump. If there are crash files, contact technical support.

```
[isp1]Redback#show process ppp
NAME PID  SPAWN MEMORY TIME         %CPU  STATE UP/DOWN
ppp  166  3     3436K  00:00:00.59  0.00% run   00:02:20

[local]Redback#show crashfiles
4844 Jul  4 16:02 /md/pppd_43.mini.core
5944456 Jul  4 16:02 /md/pppd_43.core
4812 Jul  4 16:03 /md/pppd_526.mini.core
5923992 Jul  4 16:03 /md/pppd_526.core
```

3.13 Step 12: Checking the RADIUS Server

If you have configured a RADIUS server, make sure the RADIUS attributes are configured correctly for your clients. For information about checking the RADIUS Server, see Section 15 on page 159, Troubleshooting the RADIUS Server.

3.14 Step 13: Checking the PPP Configuration

Use the **`show configuration ppp`** command and check for configuration issues listed in Table 9. Use this table as guide to troubleshoot common misconfiguration issues.

Table 9 PPP Configuration Mismatch Checklist

#	Task	Checked?
1	Does the user have the wrong username or password? This is a very common issue with PPP. To test authentication, use the **`test aaa authentication username`** ***`ppp-login`*** **`password`** ***`password`*** command in the correct context and verify that the PPP account is correct. For information about authentication, see Checking Authentication.	
2	Is the multibind option configured correctly on the SmartEdge router?	
3	Is the IP pool configuration missing?	
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	Do the client and server have a VPI/VCI pair that does not match?	
7	Do the client and server VCs have an encapsulation type that does not match?	
8	Do the client and server have an authentication method that does not match?	
9	Is the configuration matching what is expected to be running on the system?	

Note: Verify that the PPA circuit is receiving packets by using the **`show circuit counter`** ***`slot/port`*** **`vpi`** ***`vpi`*** **`vci`** ***`vci`*** **`detail`** command. For an ATM card, if the packets are not received, investigate the packet and cell drop between Segmentation and Reassembly (SAR) and the PPA.

3.15 Step 14: Debugging PPP

Use the **`debug ppp`** command to enable the generation of debug messages for various types of PPP events on the system.

`debug` [**`boot`** {**`active`** | **`standby`**} | **`switchover`**] **`ppp`** {**`all`** | *`event-type`*}

`no debug` [**`boot`** {**`active`** | **`standby`**} | **`switchover`**] **`ppp`** {**`all`** | *`event-type`*}

`boot`	Optional. Enables the generation of debug messages during a system reload. Use the **`boot active`** or **`boot standby`** construct to enable debug messages during a system reload for the active or standby controller card, respectively.
`active`	Enables the generation of debug messages for the active controller card.
`standby`	Enables the generation of debug messages for the standby controller card and enable debug messages while the system is switching from the active to the standby controller card.[1]
`switchover`	Optional. Enables the generation of debug messages during a switchover from the active to the standby controller.[2]
`all`	Enables the generation of debug messages for all PPP event types.
`event-type`	Type of event, according to one of the keywords listed in Table 10.

(1) The SmartEdge 100 router does not support the ***standby*** *keyword.*
(2) The SmartEdge100 router does not support the ***switchover*** *keyword.*

Table 10 PPP Events

Keyword	**Description**
`all`	All PPP related events.
`authentication`	PAP/CHAP authentication events
`circuit`	Circuit-related events
`config`	Configuration-related events
down	PPP session down-related events
`exception`	Exception events, such as when a timer expires
`fsm`	State-change events for the Finite State Machine (FSM)
`ipc`	Interprocess communication (IPC) events
`ipcp`	Internet Protocol Control Protocol (IPCP) events
`ism`	Interface and Circuit State Manager (ISM) events
`lcp`	Link Control Protocol (LCP) events
`multilink`	PPP multilink events
`negotiation`	Negotiation events
`nlcp`	Network Link Control Protocol (NLCP) events
`packet`	PPP packet events
`phase`	PPP phase events
`ppa`	Packet Processing ASIC (PPA) events

Keyword	Description
`rcm`	Router Configuration Manager (RCM) events
`session`	PPP session-related events
`timer`	PPP timer-related events

Caution!

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

To store debug messages in the system log buffer, use the **`logging debug`** command (in global configuration mode). Use the **`show log`** command (in exec mode) to display these stored debug messages. For information about the **`show log`** command, see the *Command List*.

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

Use the **`no`** form of this command to disable the generation of debug messages for PPP events.

3.15.1 Debugging PPP Packets

Use the **`debug ppp packet`** command to determine why a PPP session is not coming up. It shows all the negotiation while keeping debugging to a minimum. Check for any increasing exception counters, such as At Limit, No Circuit, and No Unit. These may indicate that the PPP daemon does not recognize the circuit where packets were received, or another software problem.

Monitoring the following:

- LCP messages
  - in <<, or out >> LCP packets for information
  - LCP negotiation methods: PAP, CHAP or none
  - LCP MRU size
  - ConfReq and ConfAck ID matching messages
  - PPP-ERR

Recommended Action: Enable the **`debug ppp all`** command to obtain detailed information about the issue.

- Authentication messages
  - PAP or CHAP AuthReq and AuthAck
  - Authentication ID number matching
  - Username and password.

    `Recommended Action`: If any of these messages fail, debug AAA. For information about troubleshooting RADIUS, see Troubleshooting RADIUS.

- IPCP negotiation messages
  - IPCP negotiation options (IP Address)
  - IPCP ConfReq and ConfAck
  - Subscriber IP Address is within subnet

The following example shows you how to use the **`debug ppp packet`** command.

```
[isp1]Redback# debug ppp packet
[isp1]Redback#terminal monitor
[isp1]Redback##show debug // Display enabled debug commands.
```

3.15.2 PPP Circuit-Level Debug Commands

The following example show how to enable the generation of all PPP debug messages for all circuits on `port 1` on the traffic card in slot 14:

```
[isp1]Redback#debug circuit handle 14/1:1023:63/2/2/1
[local]Redback#debug circuit ppp packet
```

The following example show how to enable the generation of all PPP debug messages circuit handle `14/1:1023:63/2/2/1`:

```
[isp1]Redback#debug circuit handle 14/1:1023:63/2/2/1
[local]Redback#debug circuit ppp all
[isp1]Redback#show debug circuit //Shows circuits that are being debugged.
Circuit debugging:
  14/1:1023:63/2/2/1
```

Note: To find a circuit handle, use the **`show circuit`** ***`circuit-type`*** **`detail | grep [`*`ip-address`*` | `*`username`*` | `*`mac-address`*`]`** command.

4 Troubleshooting PPPoE

This section describes how to troubleshoot PPPoE. For information about troubleshooting PPP, see Troubleshooting PPP. For information about operational commands, see the *Command List*.

4.1 Overview of PPPoE

There are four steps to PPPoE session setup based on RFC 2516, *A Method for Transmitting PPP Over Ethernet (PPPoE)*:

1. The host broadcasts a PPPoE Active Discovery Initiation (PADI) packet.

2. When the access concentrator receives a PADI that it can serve, it replies by sending a PPPoE Active Discovery Offer (PADO) packet to the host.

3. Because the PADI was broadcast, the host may receive more than one PADO packet. The host chooses a PADO packet based on the AC name or the services offered. The host then sends a single PPPoE Active Discovery Request (PADR) packet to the access concentrator that it has chosen.

4. When the access concentrator receives a PADR packet, it prepares to begin a PPP session. It generates a unique session ID for the PPPoE session and replies to the host with a PPPoE Active Discovery Session-confirmation (PADS) packet.

When a host initiates a PPPoE session, it must first perform discovery to identify the Ethernet MAC address of the peer and establish a PPPoE session ID. Although PPP defines a peer-to-peer relationship, discovery is inherently a client/server relationship. In the discovery process, a host (the client) discovers an access concentrator (the server).

Depending on the network topology, there may be more than one access concentrator with which the host can communicate. The discovery stage allows the host to discover all access concentrators and then select one. When discovery is completed, both the host and the selected access concentrator have the information required to build a PPPoE connection.

4.2 Before You Begin

Before you begin, get a description of the problem and check if you made any recent changes or upgrades to your network, and then check whether the issue is at the PPPoE or PPP level. Then, use the following commands to determine if the issue is at the PPPoE or PPP level. If the issue is at the PPPoE level, troubleshoot PPPoE, if not, troubleshoot PPP.

1. **`show process ppp`**
2. **`show process pppoe`**
3. **`debug pppoe exception`**
4. **`debug ppp exception`**
5. **`show ppp counter clear`**
6. **`show ppp counter detail clear`**
7. **`show pppoe counter clear`**
8. **`show pppoe counter detail clear`**

For information about Troubleshooting PPP, see Troubleshooting PPP.

Note: When working with technical support representatives, use the **`show tech-support`** command on your router and have the output available for your local technical support representative to assist in troubleshooting.

4.3 PPPoE Sample Configuration

The following is a sample configuration on a SmartEdge 800 router in context `isp`. This configuration maps to the PPPoE troubleshooting tasks.

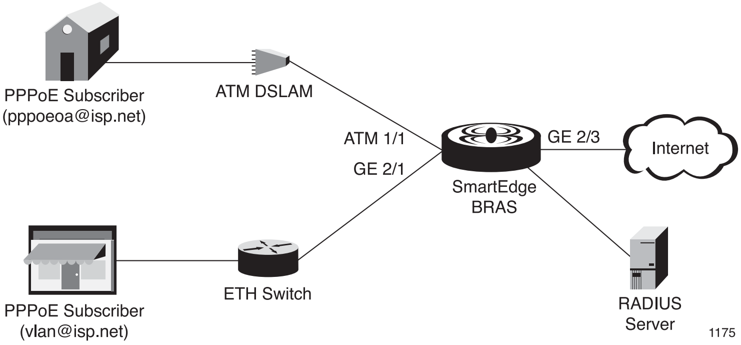


Figure 5 PPPoE Network Topology

```
config
!
context isp
domain isp.net
!
interface pppox multibind
ip address 160.1.1.1/16
ip pool 160.1.0.0/16
!
subscriber pppoeoa
password test1
ip address pool
!
subscriber vlan
password test2
ip address pool
!
subscriber untag1
password test3
ip address pool
!
subscriber untag2
password test4
ip address pool
!
atm profile ubr
shaping ubr
!
port atm 1/1
no shutdown
atm pvc 1 32 profile ubr encapsulation pppoe
bind authentication pap
!
port ethernet 2/1
no shutdown
encapsulation dot1q
dot1q pvc 32
bind auth pap
!
port ethernet 2/2
no shutdown
encapsulation pppoe
bind auth pap max 10
!
```

4.4 PPPoE Troubleshooting Tasks

Use the following table as a guide to troubleshooting general PPPoE issues. Before you begin, get a description of the problem and check if you made any recent changes or upgrades to the network.

Note: When working with technical support representatives, issue the **`show tech-support`** command on your router and have the output available for your technical support representatives to assist in troubleshooting.

Table 11 Tasks to Troubleshoot General PPPoE 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: Checking Port Counters	**`show port counters live`**
	`show port counters detail`
		Check port performance. For information about this command, see Checking Port Performance.	

Step 3: Checking PPPoE Counters	**`show pppoe counters clear`**
	`show pppoe counters detail clear`
		Displays summary or detailed statistics for all PPPoE-encapsulated circuits. Issue these commands to determine if your problem is PPPoE.
		If so, continuing troubleshooting PPPoE; If not, troubleshoot PPP. For information about troubleshooting PPP, see Troubleshooting PPP.	

Step 4: Verifying PPPoE Circuit Counters	**`show circuit counters pppoe`**
	`show circuit counters pppoe detail`
		• Displays summary information or detailed information about PPPoE circuits.
		• When you use the **`show circuit counters detail`** command, check for unknown encapsulation packets. When the PPPoE session is up, the encapsulation type should be **`*-pppoe-ppp-combined`**	

Step 5: Checking PPPoE State on the Circuit	**`show circuit detail`**
	`show circuit` ***`handle`*** **`detail`**
		• Display detailed circuit information.
		• Display detailed circuit handle information.
		• Make sure that PPP LCP State and the PPP ICP State counter have a status of Open.
		• Verify that The encapsulation type is *-pppoe-ppp-combined.
		• The MTU size should be 1492.	

Table 11   Tasks to Troubleshoot General PPPoE Issues

Task	Command	Notes	Checked?
Step 6: Checking Interfaces	`show ip interface brief`	Make sure the interfaces are up.	
Step 7: Checking Bindings	`show bindings summary`	Display the configured bindings for one or more subscribers, ports, channels, or PVCs on the system. For information about this command, see Checking Bindings.	
Step 8: Checking Subscribers	`show active subscribers`		

Step 9: Displaying PPPoE Summary Information	`show pppoe summary`
	`show circuit pppoe down detail`
		• Displays statistics for PPP packets and session counters on the system
		• Displays detail information about circuits that are down.	

Step 10: Displaying Subscriber Routes	`show ip route subscriber`	Verify where the subscriber is terminating. Make sure the IP address negotiated during IPCP stage is correctly installed in the routing table.	

Step 11: Checking PPPoE Process	`show process pppoe`
	`show crashfiles`
		• Verify that the PPPoE process is running.
		• Displays the size, location, and name of any crash files located on the system. Check for a core dump.	

Step 12: Checking the PPPoE Configuration	`show configuration pppoe`		
Step 13: Checking the RADIUS Server		If you have configured a RADIUS server, make sure the RADIUS attributes are configured correctly for your clients. For information about checking the RADIUS Server see, Troubleshooting the RADIUS Server.	
Step 14: Debugging PPPoE		**Caution**: Enabling the generation of debug messages can severely affect system performance.	

4.5 Step 1: Navigating to the Correct Context

Use the **`show context all`** command and display all the contexts on your router and then navigate to the context you want to troubleshoot, in this case, the `isp` context.

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

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

4.6 Step 2: Checking Port Counters

Use the **`show port counters live`** command to check the port counters in real time. Use the **`detail`** keyword to display detailed port counter information. For more information about this command, see Checking Port Status.

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

please wait...
Port Type
1/1 ATM
packets sent : 15000 bytes sent : 20000
packets recvd : 10000 bytes recvd : 50000
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
2/1 ethernet
packets sent : 25000 bytes sent : 40000
packets recvd : 60000 bytes recvd : 80000
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
2/2 ethernet
packets sent : 29000 bytes sent : 20000
packets recvd : 70000 bytes recvd : 30000
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
```

4.7 Step 3: Checking PPPoE Counters

Use the **show pppoe counters** command to display summary or detailed statistics for all PPPoE-encapsulated circuits. For example:

- Packet counts for all PPPoE events, including RX and TX PPPoE PAD counters
- PPPoE invalid discovery packet counters
- PPPoE virtual circuit counters
- PPPoE discovery processing counters
- PPPoE PADM error counters

Make sure that you are receiving traffic; check for dropped packets. The sent and receive packets should closely match.

The **clear** option provides more recent PPPoE counter information. Use the **clear** option after the **show pppoe counters** or **show pppoe counters detail** commands to clear the counters and recollect them after 30 seconds. After 30 seconds, look at what caused PPPoE to go down. If you want to keep a record of the show pppoe counters for an extended period of time, capture your log information and save it before you use this option. Otherwise, use the **show pppoe counters** command.

When you use the **show pppoe counters** command, make sure you use the following checklist:

Table 12 Show PPPoE Counter Checklist

#	Task	Checked?
1	Is the SmartEdge router receiving PADI?	
2	Is the SmartEdge router sending PADO?	
3	Is the SmartEdge router receiving PADR?	
4	Does the SmartEdge router sending PADS?	

If the PPPoE subscribers cannot connect, issue the **`show pppoe counters detail`** command and use the following checklist.

Table 13 Show PPPoE Counter Checklist

#	Task	Checked?
1	dropped packets—Check for an increase in "drop in packets".	
2	PADR, max sess reached—The maximum sessions on a circuit has been reached.	
3	PADR, same MAC starting—This counter mostly applies to settings of max-session > 1. The PPPoE daemon has started bringing up a session with the same MAC address, and unless that session is up, no new session with the same MAC address is accepted. This counter also applies when a PPPoE session is bouncing; the subscriber may have restarted the session attempt before the SmartEdge router finished the PPPoE teardown sequence.	
4	nonsubscriber circuit—The circuit configuration is incomplete. For example, the “bind auth” line or the line card does not have a MAC address configured. **Recommended Action**: Check the circuit configuration and the show port detail output to verify the circuit misconfiguration.	
5	Invalid tag name—The PPPoE subscriber does not use the invalid service tag provided with the PADO packet.	

The following example shows how to display summary statistics:

```
[local]Redback#show pppoe counters clear


Wed Jun 30 01:37:25 2005
PPPoE PAD counters:
-------------------------------------------------------
sent packets        : 4000         recv packets : 4000
dropped packets     : 0
PADI packets        : 2000         PADO packets : 2000
PADR packets        : 2000         PADS packets : 2000
PADT packets        : 0            PADM packets : 0
PADN packets        : 0
```

The following example shows how to display detailed statistics:

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

```
Wed Jun 30 08:30:40 2005
PPPoE PAD counters:
--------------------------------------------------------------
sent packets        : 4000      recv packets            : 4000
dropped packets     : 0
PADI packets        : 2000      PADO packets            : 2000
PADR packets        : 2000      PADS packets            : 2000
PADT packets        : 0         PADM packets            : 0
PADN packets        : 0
PPPoE invalid discovery packet counters:
--------------------------------------------------------------
invalid version/type     : 0   invalid length           : 0
invalid tag length       : 0   unknown code             : 0
PADIs non-zero sess-id   : 0   PADRs non-zero sess-id   : 0
PADT, bad MAC addr       : 0   bad encaps               : 0
PADR, max sess reached   : 0   PADR, same MAC           : 0
tags not added, large pkt: 0   recv on down circuit     : 0
invalid tag name         : 0   invalid tag name accepted: 0
circuit not created      : 0   circuit not init         : 0
packet on virtual circuit: 0   non subscriber circuit   : 0
unknown circuit          : 0   proc restart drops       : 0
PPPoE virtual circuit counters:
---------------------------------------------------------------
created virtual circuits : 0    deleted virtual circuits : 0
combined circuits used   : 4000 combined circuits reset  : 2000
create failed            : 0    delete failed            : 0
create fail, rcct used   : 0    create fail, no cct      : 0
create fail, cct init    : 0    create fail, vcct exists : 0
circuit lookup failures  : 0
PPPoE PADM error counters:
---------------------------------------------------------------
malformed URLs           : 0    too long expanded URLs   : 0
too long MOTMs           : 0    bad expansion char       : 0
PADX on bad circuit      : 0
PPPoE session counters:
---------------------------------------------------------------
session down cplt recv   : 2000 session down cplt proc   : 2000
stale entry cleanup      : 0    bad state entry cleanup  : 0
session down sent        : 0
```

4.8 Step 4: Verifying PPPoE Circuit Counters

Use the **`show circuit counters pppoe`** command to check the status of the PPPoE. If the sent and received packets information is different than expected, use the **`show circuit counter pppoe detail`** command on the circuit you want to examine.

When troubleshooting PPPoE circuits, we recommend that you use the **`live`** keyword to obtain the most current information on the PPPoE circuit counters.

```
[local]Redback# show circuit counters pppoe live
Circuit            Packets/Bytes Sent  Packets/Bytes Received
2/2 vlan-id 100             32765              3034
                            1506597            1820700
2/2 vlan-id 100 pppoe 1     11                 10
                            480                428
2/2 vlan-id 100 pppoe 2     11                 10
                            480                428
2/2 vlan-id 100 pppoe 3     11                 10
                            480                428
...
```

Use the **`show circuit counters pppoe detail`** command to display detailed information about PPPoE circuits. Verify that the expected result is displayed in the Rx, Tx PPPoE PAD counters. Check for unknown encapsulation packets counters.

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
```

4.9 Step 5: Checking the PPPoE State on the Circuit

Use the **`show circuit detail`** or **`show circuit handle`** ***`handle`*** **`detail`** commands to display detailed information on a circuit or circuit handle. Do the following:

- Verify that the circuit is up. Verify that the MTU size is **1492**
- Verify that the PPP LCP and the PPP ICP states are Opened.
- Verify the encapsulation type is ***-ethernet-pppoe-ppp-combined**.

```
[isp]Redback# show circuit detail
Circuit: 2/1 pppoe 1, internal id: 1/1/7015, state: Up
interface bound : pool@test1
subscriber bound : pppoeoa@isp.net
bind type : chap pap
admin state : 1 hardware address : 00:30:88:00:77:0c
media type : ethernet encap type : ethernet-pppoe-ppp-combined
mtu size : 1492 cfg mtu size : 1500
ipv6 mtu size : 1500 ipv6 cfg mtu size : 1500
cct speed : 100000 cct rx speed : 0
cct flags (attr) : 0x1
slot mask : 0x0 ppa cct clear : FALSE
if flags : 0x0
profile id : 0 version : 207874
PPP OSINLCP State : Initial PPP MPLSCP State : Initial
PPPOE State : READY
internal handle : 3/1:1023:63/1/1/7015
```

Recommended Action:

1. Check the configuration on both endpoints and make sure they match.
2. Ping the ports to check for connectivity.
3. If they are up, begin debugging at the circuit level.

For information about PPPoE debug commands, see Debugging PPPoE.

4.10 Step 6: Checking Interfaces

Use the **show ip interface brief** command to check that your interfaces are up. When PPPoE subscriber interface have no active subscribers, the interface is shown as down.

```
[isp]Redback#show ip interface brief
Mon Jun 27 06:38:05 2009
Name       Address           MTU   State    Bindings
1/1        4.2.13.4/16       1500   Up      ATM 1/1
2/1        10.13.49.166/24   1500   Up      ethernet 2/1
2/2        10.13.49.167/24   1500   Up      ethernet 5/1
pool       160.1.1.1/16         0   Up

//pool indicates a multibind interface.
```

Recommended Action: If the interfaces are down, see Verifying Interfaces and Checking Port Performance.

4.11 Step 7: Checking Bindings

Use the **show bindings** command to check the configured bindings for one or more subscribers, ports, channels, or PVCs on the system. For information about this command, see Checking Bindings.

4.12 Step 8: Checking Subscribers

Use the **show subscribers** commands to check your subscribers. The following are some examples on how to use **show subscribers** commands:

Table 14 Show Subscriber Command Examples

Command	Description
show subscribers all | grep “***time***"	Display all subscribers starting at a certain time.
show subscribers all | grep "*@domain-name*" | **count**	Display how many subscribers are online for a particular domain.
show subscribers active | begin before 3 after 5 “*user@domain-name*”	Display three lines prior and five lines after the match of the "*user@ domain-name*". Normally, the grep only shows a single line of the match.
show subscribers all | grep “**PPP**”	Display all PPP and PPPoE subscribers.
show subscribers active *username user2@NiceService*	Display the information for an active subscriber.
show subscribers all | grep *user2@NiceService*	Display information about the binding, context, and subscriber.

For more information about how to use the **show subscribers** command, see Displaying Information About My Subscribers.

4.13 Step 9: Displaying PPPoE Summary Information

Use the **`show pppoe summary`** command to display information that summarizes the PPPoE sessions from the circuits of ATM, dot1q, and Ethernet. You can also use the **`show pppoe down`** command to specify that only PPP sessions for which the LCP is in the **INITIAL**, **CLOSED**, or **STOPPED** state are to be displayed.

```
[local]Redback#show pppoe summary
NUMBER
CIRCUIT TYPE   CIRCUIT   UP    DOWN
------------   ------- ------ ------
ATM            3         3     0
ETHERNET       0         0     0
DOT1Q          0         0     0
Total circuits: 3 up: 3 down: 0
```

Recommended Action: If your circuit is down, use the **`show circuit pppoe down detail`** command to display detailed information about PPPoE circuits that are down.

Use the **`show circuit pppoe detail`** command to display detailed information on all PPPoE circuits.

```
[isp]Redback#show circuit pppoe detail
Circuit: 5/1 vlan-id 108, internal id: 1/2/35, state: Down
---------------------------------------------------------------------
interface bound :
subscriber bound:
bind type       :
admin state     : 1        hardware address : 00:30:88:00:33:65
media type      : ethernet encap type       : ether-dot1q-pppoe
mode type       : 0x2      port type        : ethernet
mtu size        : 1500     cfg mtu size     : 1500
ipv6 mtu size   : 1500     ipv6 cfg mtu size: 1500
cct speed       : 100000   cct rx speed     : 0
cct flags (attr): 0x0
slot mask       : 0x0     parent slot mask  : 0x0 ppa cct clear:FALSE
if flags        : 0x0     aaa index         : 0x0
profile id      : 0       version           : 188
h node id       : 0
lg_id           : 0       spg_id            : 0
PPPOE State     : DOWN
internal handle : 5/1:1023:63/1/2/35
Summary:
   total: 1
      up: 0             down: 1
   bound: 0          unbound: 1
    auth: 0        interface: 0       subscriber: 0         bypass: 0
    no-bind: 1           atm: 0            chdlc: 0         dot1q: 0
      ether: 0            fr: 0              gre: 0
       mpls: 0           ppp: 0            pppoe: 1
      clips: 0          vpls: 0             ipip: 0
      ipsec: 0    ipv6v4-man: 0      ipv6v4-auto: 0
```

```
[local]Redback#show circuit pppoe down detail
Circuit: 5/1 vlan-id 108, internal id: 1/2/35, state: Down
interface bound :
subscriber bound:
bind type       :
admin state     : 1          hardware address   :
00:30:88:00:33:65
media type      : ethernet   encap type         :
ether-dot1q-pppoe
mode type       : 0x2    port type        : ethernet
mtu size        : 1500   cfg mtu size     : 1500
ipv6 mtu size   : 1500   ipv6 cfg mtu size: 1500
cct speed       : 100000 cct rx speed     : 0
cct flags(attr) : 0x0
slot mask       : 0x0    parent slot mask : 0x0 ppa cct clear:FALSE
if flags        : 0x0    aaa index        : 0x0
profile id      : 0      version          : 188
h node id       : 0
lg_id           : 0      spg_id            : 0
PPPOE State     : DOWN
internal handle : 5/1:1023:63/1/2/35
Summary:
total: 1
up: 0             down: 1
bound: 0          unbound: 1
auth: 0        interface: 0       subscriber: 0            bypass: 0
no-bind: 1           atm: 0            chdlc: 0            dot1q: 0
ether: 0            fr: 0              gre: 0
mpls: 0             ppp: 0          pppoe: 1
clips: 0             vpls: 0          ipip: 0
ipsec: 0       ipv6v4-man: 0      ipv6v4-auto: 0
```

Recommended Action:

1. Check the configuration on both endpoints and make sure they match.
2. Ping the ports to check for connectivity.
3. If they are up, begin debugging at the circuit level.

For information about PPPoE debug commands, see Debugging PPPoE.

4.14 Step 10: Checking the PPPoE Configuration

In Table 15 is a configuration checklist for troubleshooting configuration mismatches for PPPoE subscribers. Use the **`show configuration pppoe`** command to check the PPPoE configuration.

```
[local]Redback#show configuration pppoe
```

Table 15 PPPoE Common Configuration Mismatch Checklist

#	Task	Checked?
1	Does the PPPoE client's service name (if not blank) match the domain name of the server? To test authentication, use the **`test aaa authentication`** ***`username pppoe-login`*** **`password`** ***`password`*** in the correct context and verify the PPPoE account is correct. For information about authentication, see Checking Authentication. See also Troubleshooting the RADIUS Server.	
2	Are the maximum number of sessions correctly specified?	

4.15 Step 11: Checking PPPoE Process

Use the **`show pppoe process`** command to verify that the PPPoE process is running. For detailed information, use the **`detail`** keyword. If the PPPoE process is not running, use the **`show crashfiles`** command to check if there is a core dump. If there is, contact your local technical support representative.

```
[isp]Redback# show process pppoe
NAME   PID  SPAWN MEMORY TIME        %CPU  STATE UP/DOWN
pppoe  166  3     3436K  00:00:00.59 0.00% run   00:02:20

[isp]Redback# show crashfiles
4844 Jul 4 16:02 /md/pppoed_43.mini.core
5944456 Jul 4 16:02 /md/pppoed_43.core
4812 Jul 4 16:03 /md/pppoed_526.mini.core
5923992 Jul 4 16:03 /md/pppoed_526.core
```

4.16 Step 12: Displaying Subscriber Routes

Use the **`show ip route subscriber`** command to check where the subscriber is terminated. Make sure the IP address negotiated during the IPCP stage is correctly installed in the routing table.

```
[isp]Redback#show ip route subscriber
Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B
 - IBGP
       A,H - derived hidden
       O   - OSPF, IA - OSPF inter area, N1  - OSPF NSSA external type 1
       N2  - OSPF NSSA external type 2,  E1  - OSPF external type 1
       E2  - OSPF external type 2
       i   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2
       IPH - IP Host, SUB A - Subscriber address, SUB S - Subscriber
 static
       A - Derived Default
       >   - Active Route
Type    Network       Next Hop   Dist  Metric   UpTime     Interface
> SUB A 20.1.1.1/32               15      0     00:01:08   pppox
> SUB A 20.1.1.2/32               15      0     00:01:08   pppox
> SUB A 30.1.1.0/32               15      0     00:01:08   pppox
```

4.17 Step 13: Checking the RADIUS Server

If you have configured a RADIUS server, make sure the RADIUS attributes are configured correctly for your clients. For information about checking the RADIUS Server, see Section 15 on page 159, Troubleshooting the RADIUS Server.

4.18 Step 14: Debugging PPPoE

Use the **`debug pppoe`** command to enable the generation of debug messages for various types of PPP events on the system.

```
debug [boot {active | standby} | switchover] pppoe {all | cct |
discovery | exception | info | packet | timer}
```

```
no debug [boot {active | standby} | switchover] pppoe {all | cct |
discovery | exception | info | packet | timer}
```

`boot`	Optional. Enables the generation of debug messages during a system reload.
`active`	Enables the generation of debug messages for the active controller card.
`standby`	Enables the generation of debug messages for the standby controller card.
`switchover`	Optional. Enables the generation of debug messages during a switchover from the active to the standby controller.
`all`	Enables the generation of PPPoE debug messages for all types of events.
`cct`	Enables the generation of PPPoE debug messages for circuit-related events.
`discovery`	Enables the generation of PPPoE debug messages for discovery of protocol-related events.
`exception`	Enables the generation of PPPoE exception debug messages.
`info`	Enables the generation of PPPoE debug messages for PPPoE information.
`packet`	Enables the generation of PPPoE debug messages for packet input and output events.
`timer`	Displays timer-related debug messages.

Caution!

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

Note: The SmartEdge 100 router does not support the **`standby`** and **`switchover`** keywords.

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

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

Note: For more information about **`logging`** commands and the **`terminal monitor`** command, see the *Command List*.

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

The following example searched for a particular host and saves the output to a file called `test`:

```
[Redback]Redback#show subscribers log | grep 'user1@Redback' | save test
        Username = user1@Redback,
        Username = user1@Redback,
        Username = user1@Redback,
        Username = user1@Redback,
        Username = user1@Redback,
[Redback]Redback#cd /flash
Current directory is now /flash
[Redback2]Redback#dir test
Contents of /flash/test
-rw-r--r--  1 root  0  135 Jun 26 19:25 /flash/test
```

The following example shows how to verify the contents of the `test` file:

```
[Redback]Redback#more /flash/test
        Username = user1@Redback,
        Username = user1@Redback,
        Username = user1@Redback,
        Username = user1@Redback,
        Username = user1@Redback,
[Redback]Redback#
```

4.18.1 Using the Debug PPPoE Exception Command

Use the **debug pppoe exception** command to identify any unexpected events with PPPoE; for example, when a PPPoE daemon drops a packet because a session is restarting.

The following lists the different types of PPPoE exceptions:

- Dropping packet—The circuit is down (transmit path).

  Recommended Action: Check the circuit state and make sure the port or circuit is not shut down and that the link is working by using the **show configuration pppoe** and **show port detail** commands.

- Packet received on uninitialized circuit; dropped (receive path).

  Recommended Action: Check the circuit state and make sure the port or circuit is not shut down and that the link is working.

- Packet received on non-subscriber circuit; dropped—The circuit configuration is incomplete. For example, the `no bind auth` line or the card does not have a MAC address configured.

  Recommended Action: Check the circuit configuration by using the **show configuration pppoe** command.

- Session is going down; dropped—A packet got received while the session is in the process of being terminated. If it persists, an event might have been dropped due to a process restarting, such as ISM, PPP, or AAA.

  Recommended Action: Check the output and monitor recovery of that process.

- max sessions N reached— The maximum capacity on the circuit has been reached. The SmartEdge router knows how many sessions you can establish on a given circuit with the **bind auth pap max nn** statement, where ***nn*** can be up to `8000`. When that number is reached on the circuit, an error message is displayed.

- Dropping PADR, circuit with same MAC is starting—This message mostly applies to settings of `max-session > 1`. The PPPoE daemon has started bringing up a session with the same MAC address, and unless that session is up, no new session with the same MAC address is accepted.

```
[isp]Redback# debug pppoe exception
[isp]Redback#terminal monitor
[isp]Redback##show debug // Display enabled debug commands.
```

4.18.2 PPPoE Circuit Level Debug Commands

The following example show how to enable the generation of all PPPoE debug messages for all circuits on port `1` on the traffic card in slot `3`:

```
[isp]Redback#debug circuit handle 14/1:1023:63/2/2/1
[isp]Redback#debug circuit pppoe packet
```

The following example show how to enable the generation of all PPPoE debug messages on circuit handle `14/1:1023:63/2/2/1`:

```
[isp]Redback#debug circuit handle 14/1:1023:63/2/2/1
[isp]Redback#debug circuit pppoe all
[isp]Redback#show debug circuit  //Shows circuits that are being debugged.
Circuit debugging:
14/1:1023:63/2/2/1
```

5 L2TP

This section describes L2TP troubleshooting.

5.1 Terminology

The following are tunnel setup control messages:

- SCCRQ (Start-Control-Connection-Request)—Initializes a tunnel between an L2TP network server (LNS) and an L2TP access concentrator (LAC). It is sent by the LAC or the LNS during the tunnel establishment process.

- SCCRP (Start-Control-Connection-Reply)—Sent in reply to a received SCCRQ message. SCCRP is used to indicate that the SCCRQ was accepted and that establishment of the tunnel should continue.

- SCCCN (Start-Control-Connection-Connected)—Sent in reply to an SCCRP. SCCCN completes the tunnel establishment process.

- HELLO—L2TP keepalive mechanism.

- StopCCN (Stop-Control-Connection-Notification)—Sent by the LAC or LNS to notify its peer that the tunnel is being shut down and the control connection should be closed. All active sessions are cleared. The reason for this request is indicated in the Result Code AVP.

The following are session (call) setup control messages:

- ICRQ (Inbound-Call-Request)—Sent by the LAC to the LNS when an incoming call is detected.

- ICRP (Inbound-Call-Reply)—Sent by the LNS to the LAC in response to a received ICRQ message

- ICCN (Inbound-Call-Connected)—Sent by the LAC to the LNS in response to a received ICRP message.

- AVP (Attribute value pair)—Format for data that is sent inside L2TP control messages.

- Active Initiator—The peer sending the SCCRQ to establish the tunnel.

- Passive Initiator—The peer receiving the SCCRQ to establish the tunnel.

- CDN—Call-Disconnect-Notify— The LAC or LNS sends a Call-Disconnect-Notify (CDN) and notifies the LNS of the disconnection of the session. The CDN contains an AVP 1 result code, which has "Loss of carrier" as the reason for the disconnect.

- Local Abort—The local system decided to close the session because it cleared the subscriber, authentication failed, or as a result of a PPP idle timeout. When a session has been established, the SmartEdge router sends a CDN to the peer.
- Remote Abort—Received a CDN from the peer. If the peer provided a reason for the disconnect, you can display it in debug output.

  If a CDN is received on the LAC for a tunnel in a tunnel group, the tunnel group load-balancing algorithm marks the tunnel as unavailable (for example, because the LNS is busy or out of resource) and only periodically tries to set up requests.

5.2 Overview

The SmartEdge router functions as an L2TP access concentrator (LAC) or as an L2TP network server (LNS). In each context configured on the system, the SmartEdge router can function as a LAC to one or more LNSs, as an LNS to one or more LACs, or as both a LAC and an LNS. LNSs and LACs are collectively referred to as L2TP peers.

With the L2TP protocol, PPP and Layer 2 endpoints can reside in different devices. PPP users are connected to the LAC, and the LAC tunnels PPP sessions to the LNS. As a result, PPP sessions are processed in a central location (LNS), regardless of where PPP users are connected.

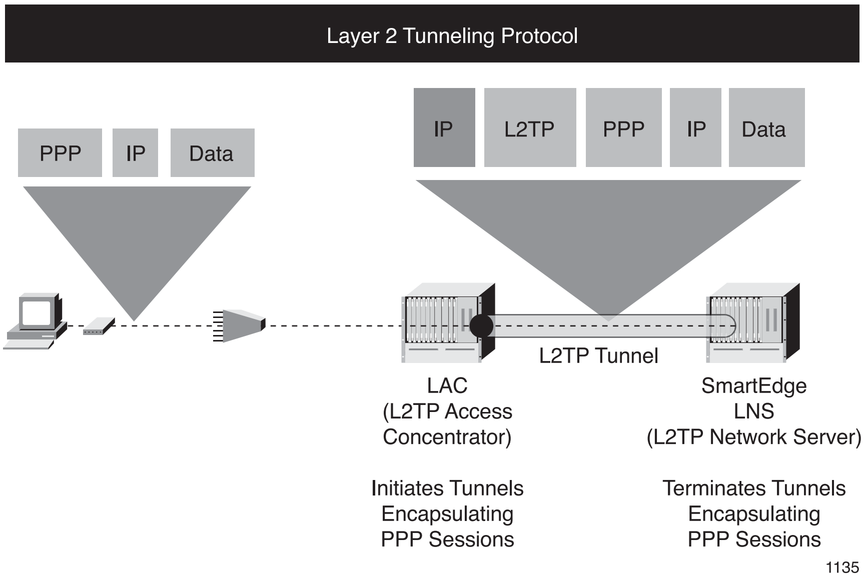


Figure 6 L2TP Tunneling Protocol Diagram

5.3 L2TP Tunnels and Peers

The router is designated as an LNS, LTS (tunnel switch), or a LAC, depending on its tunnel function: aggregating or switching. Subscriber sessions are tunneled from the LAC to the LNS through an optional LTS :

- When functioning as an LNS, the SmartEdge router accepts sessions from LACs in the network and can either terminate them or switch them to another LNS.
- When functioning as a LAC, the SmartEdge router tunnels subscriber PPP sessions to a number of LNSs.

5.4 Tunnel Switching

The SmartEdge OS can also act as an L2TP tunnel switch (LTS), accepting PPP sessions over one tunnel and relaying them to other LNSs over another tunnel. A tunnel switch has aspects of both LAC and LNS operation.

Figure 13 shows two LACs (`lac1.com` and `lac2.com`) feeding into a tunnel switch `(switch.com`), which provides upstream connectivity to each indicated LNS (`lns1.net` and `lns2.net`). Here, it is assumed that the two LACs are configured to tunnel appropriate PPP sessions (perhaps all of them) to `switch.com`. It is also assumed that each LNS is configured to accept an L2TP tunnel to the tunnel switch.

A tunnel switch can either consult RADIUS to determine the mapping of sessions to outgoing tunnels, or it rely on the fully qualified domain name of the subscriber. In the following example, sessions with domain names of `lns1.net` and `lns2.net` are tunneled from `lac1`. The tunnel switch then (when not consulting RADIUS) looks for a tunnel supporting these domains. In the simplest case, if the peer name is `lns1.net`, the tunnel switch switches `lns1.net` sessions to this tunnel. With `lns1.net` and `lns2.net`, sessions coming from `lac1`, the tunnel switch maps each to the outgoing tunnel.

Likewise, for `lns1.net` and `lns2.net` sessions coming from `lac2`, the tunnel switch maps the sessions to each of the outgoing tunnels.

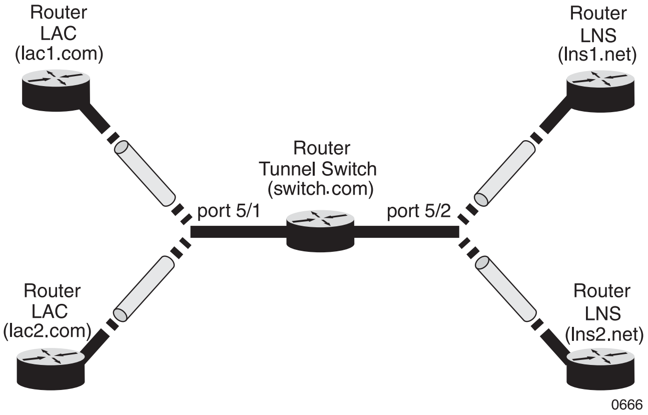


Figure 7 Tunnel Switching

5.5 L2TP Packet Exchange

The following diagram describes the L2TP packet exchange.

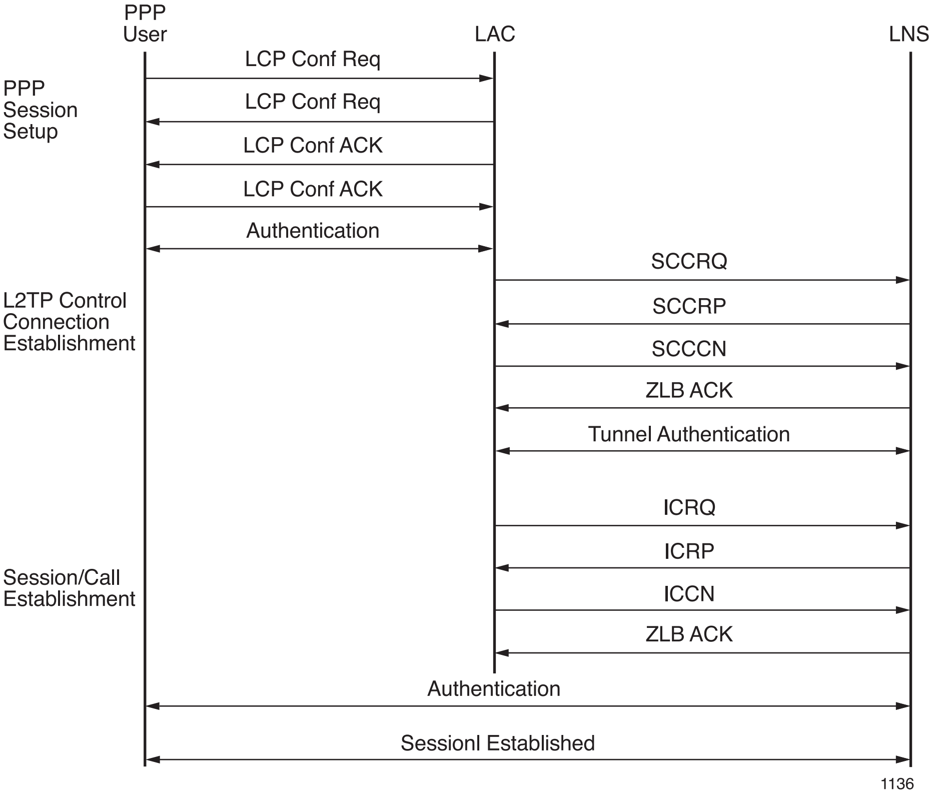
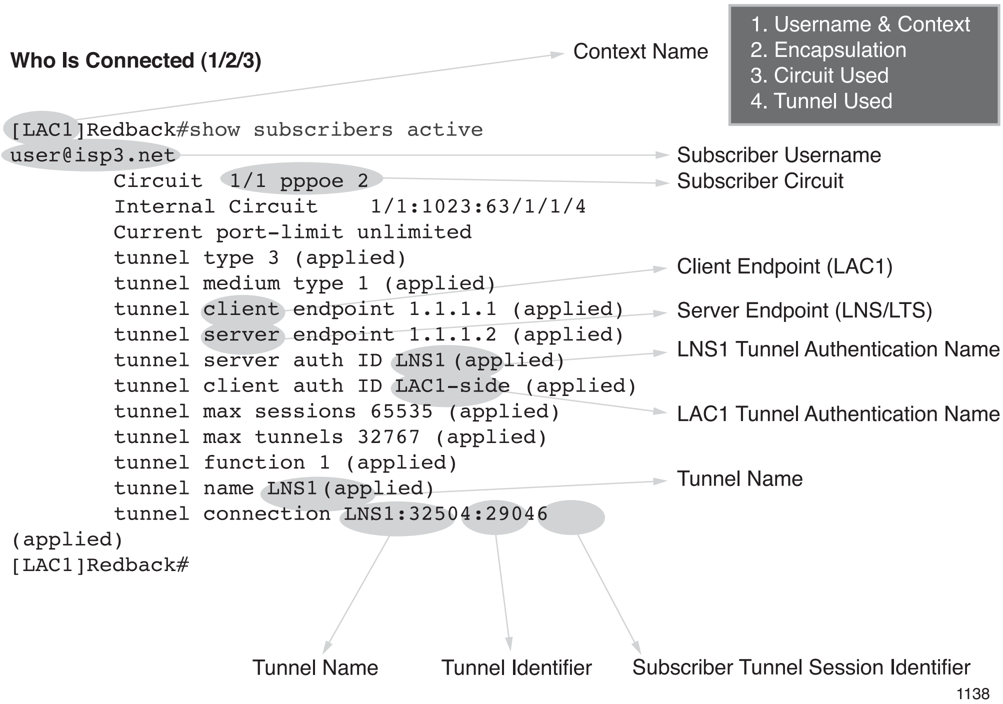


Figure 8 L2TP Packet Exchange

5.6 Understanding Tunnel Information on the LAC

The following illustration describes the tunnel information on the LAC when you issue the **`show subscribers active`** command.



```
[LAC1]Redback#show subscribers active
user@isp3.net
        Circuit  1/1 pppoe 2
        Internal Circuit    1/1:1023:63/1/1/4
        Current port-limit unlimited
        tunnel type 3 (applied)
        tunnel medium type 1 (applied)
        tunnel client endpoint 1.1.1.1 (applied)
        tunnel server endpoint 1.1.1.2 (applied)
        tunnel server auth ID LNS1 (applied)
        tunnel client auth ID LAC1-side (applied)
        tunnel max sessions 65535 (applied)
        tunnel max tunnels 32767 (applied)
        tunnel function 1 (applied)
        tunnel name LNS1 (applied)
        tunnel connection LNS1:32504:29046
(applied)
[LAC1]Redback#
```

Figure 9 LAC Show Subscribers Active Command Output Fields

6 Troubleshooting Specific L2TP Issues

Before you get started, check Table 16 to determine if your have a specific L2TP issue. If so, use the associated procedure in this table as a guide to troubleshooting your specific issue.

If your issue is not listed in this section, go to the Troubleshooting General LAC Issues or Troubleshooting General LNS Issues sections.

Before you begin, get a description of the problem and check if you made any recent changes or upgrades to the network.

Note: When you troubleshoot specific L2TP issues, make sure you navigate to the correct context.

Table 16 Specific L2TP Issues

Issue	Command	Notes	Checked?

No Replies to SCCRQ	`ping`
	`l2tp admin test peer` *`name`* `tun-setup`
	`debug l2tp tun-setup`
		• Pings the configure remote address (LNS).
		• Verifies that the peer receives your SCCRQ and replies with the SCCRP.
		• Debugs stages in the L2TP setup.	

L2TP Tunnel Setup	`l2tp admin test peer` *`name`* `tun-setup`
	`debug l2tp all`
		• Checks for StopCCN tunnel setup control messages or SCCRP timeout message.
		• Debugs all L2TP events.
		For information about the `l2tp admin test peer` command, see Step 8: Testing L2TP Peers.	

Tunnel Authorization	`l2tp admin test peer` *`name`* `tun-setup`
	`debug l2tp avp`
		• Checks for a StopCCN message instead of SCCRP (active initiator) message, a StopCCN instead of SCCCN (passive initiator), or the RADIUS Tunnel-Server-Auth-Id attribute that does not match the peer hostname AVP.
		• Debugs attribute-value pairs (AVPs) transmitted or received in L2TP control messages.	

LAC 1-Pass RADIUS	`debug aaa rad-packet`
	`debug ses-abort`
	`debug tun-setup`
		Checks the RADIUS response for the appropriate tagging.	

L2TP Session Setup	`debug l2tp ses-abort`
	`l2tp admin test peer` *`name`* `ses-setup count` *`number`*
		• Debugs L2TP-related abnormal termination of session events.
		• Performs L2TP peer testing.
		• *`number`*is number of sessions to set up; the range of values is 1 to 10,000.	

Table 16   Specific L2TP Issues

Issue	Command	Notes	Checked?

CDN for an Unknown Session ID or A Duplicate Remote Session ID	`debug l2tp packet`
	`debug l2tp avp`
		• Debugs L2TP-related packet transmit (TX) and receive (RX) events for L2TP control messages.
		• Debugs L2TP attribute-value pairs (AVPs) transmitted or received in L2TP control messages.	

Stuck Sessions or Tunnels			
Scaling	`l2tp admin test peer` ***name*** `ses-setup count` ***number*** `debug l2tp ses-abort` `l2tp admin down peer` ***name*** `second` ***seconds***	• Performs L2TP peer testing. • Debugs L2TP-related abnormal termination of session events. • Marks the L2TP peer as “dead”; no new sessions are assigned to this peer.	

Fragmentation	`l2tp renegotiate mru`
	`ppp peer-options mru`
	`l2tp fragment l2tp packet`
	`l2tp fragment user packet`
		• Forces renegotiation on LNS
		• Configures the LAC to negotiate MRU correctly for L2TP
		• Verifies that the subscriber’s interface is set to clear-df.	

LNS PPP Session Setup	`debug ppp packet`	Use the `debug ppp packet` command on the LAC, LNS or client.	

6.1 No Replies to SCCRQ

Symptom:

There are no replies to the SCCRQ (a control message that initializes a tunnel between an LNS and an LAC) or the SCCRQ reaches the maximum retransmits.

Cause:

Table 17 No Replies to the SCCRQ Message Checklist

#	Cause	Checked?
1	Check for a bad remote address on the LNS. There might be no route to peer and as a result, no connectivity.	
2	Check for a bad local address. The local address might not match the remote address configured on the LNS, or the peer might not have a route back to your source address. This is a common problem with a loopback address, which is not announced using a routing protocol.	
3	Check for blocked L2TP control messages. The firewall or ACL might be blocking L2TP control messages.	

To troubleshoot no replies to the SCCRQ message:

1. Ping the configured remote address (the LNS) using the source address configured. For example:

```
local]Redback#l2tp-peer name lns media udp-ip remote ip 50.0.0.2 local 50.0.0.1
local-name chopin
function lac-only
[local]Redback#ping 50.0.0.2 source 50.0.0.1
PING 50.0.0.2 (50.0.0.2): source 50.0.0.1, 36 data bytes,
timeout is 1 second
!!!!!
```

2. Use the **`l2tp admin test`** command to verify that the peer receives the SCCRQ and replies with SCCRP. For examples on how to interpret results, see Step 8: Testing L2TP Peers.

3. If the peer does not respond, issue the **`debug l2tp tun-setup`** command to enable debug messages for L2TP-related tunnel setup events:

Caution!

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

```
[lns1]Redback#debug l2tp tun-setup
```

6.2 Basic L2TP Tunnel Setup Problems

Symptom:

L2TP tunnel setup problems when you receive StopCCN tunnel setup control messages or a SCCRP time-out message.

Cause:

Table 18 L2TP Tunnel Setup Checklist

#	Cause	Checked?
1	An invalid local name; it does not match the peer name on remote system.	
2	An invalid **`client-auth-id`** or **`server-auth-id`** attribute (RADIUS only).	
3	Your system is not configured in the remote system. There is no peer record.	
4	The maximum tunnel limit has been reached on the peer.	
5	If required, the peer is missing in the l2tp-peer unnamed configuration.	
6	There is no tunnel authorization key. (The SCCRQ is missing a challenge).	
7	There is no response to the challenge.	
8	The tunnel authentication key is not configured on the peer or local system.	
9	The hostname AVP does not match the RADIUS **`Tunnel-Server-Auth-Id`** attribute.	

To troubleshoot L2TP setup problems:

1. Use the **`l2tp admin test peer`** ***`name`*** **`tun-setup`** command. For an example about how to interpret the results of this test, see Step 8: Testing L2TP Peers

2. Use the **`debug l2tp all`** command. The system that sends the StopCCN tunnel setup control message should provide a reason for it in the debug output or in the result code AVP in the Stop CCN message.

Caution!

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

6.3 Tunnel Authorization Problems

Symptom:

Tunnel authorization problems when you receive the receive StopCCN control message instead of SCCRP (active initiator) message, a StopCCN control message instead of SCCCN (passive initiator) control message, or the RADIUS `Tunnel-Server-Auth-Id` attribute that does not match the peer hostname AVP.

The StopCCN control message indicates that the tunnel was not established. The SCCCN completes the tunnel establishment process.

Cause:

Table 19 L2TP Tunnel Authorization Checklist

#	Cause	Checked?
1	An invalid hostname AVP. The peer cannot identify the SmartEdge router.	
2	The **`local-name`** parameter is not configured. As a result, the SmartEdge software uses the system hostname by default.	
3	Only one endpoint might be configured for authorization. Make sure both sides are configured with tunnel authorization keys if required.	

To troubleshoot tunnel authorization problems:

1. Use the **`debug l2tp tun-setup`** command.

Caution!

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

2. Use the **`l2tp admin test peer`** ***`peer-name`*** **`tun-setup`** command. In the output, look for the end of the tunnel that sends the StopCCN tunnel control message. The test determines why it is sending this message.

3. Use the **`debug l2tp avp`** command and verify that both peers or neither peer sends a challenge attribute value pair (AVP) .

4. If the `Tunnel-Server-Auth-Id` parameter is supplied, the hostname AVP sent by the peer must match this attribute value. Compare the hostname AVP in output when you issue the **`debug l2tp avp`** command and the RADIUS record.

6.4 LAC 1-Pass RADIUS Problems

Symptom:

One or more peers out of a RADIUS set are never created, which might be caused by a missing `Tunnel-Server-Endpoint` attribute on any tag. This is different than being created and marked dead, which is associated with a SCCRQ timeout. If the peer can be seen in the output of the **`show l2tp peer`** command, this section does not apply.

Cause: Mistakes in RADIUS tagging.

To troubleshoot LAC 1-Pass Problems:

1. Issue the **`debug aaa rad-packet`** command to enable generation of RADIUS packet debug messages.

2. Check the RADIUS response for the appropriate tagging. RADIUS debugging is useful if there is no access to the user configuration in RADIUS (or it is not a regular RADIUS server).

3. For each RADIUS tag, make sure that the appropriate `Tunnel-Server-Endpoint`, `Tunnel-Assignment-ID`, and `Tunnel-Client-Endpoint` attributes are present.

   The following example shows a working 1-Pass RADIUS record:

```
wrr-5-0-100@local, Password = "user-password"
Service-Type = Framed-User,     /* usually required by RADIUS */
Tunnel-Preference:1 = 1,        /* optional peer preference */
Tunnel-Server-Endpoint:1 = "42.1.0.5", /* LNS's address */
Tunnel-Client-Endpoint:1 = "81.5.1.189", /* local addr on LAC */
Tunnel-Client-Auth-Id:1 = "lac01",    /* local-name on LAC */
Tunnel-Assignment-Id:1 = "primary", /* optional assignmentId */
Tunnel-Preference:2 = 2,
Tunnel-Server-Endpoint:2 = "42.1.0.6",
Tunnel-Client-Endpoint:2 = "81.5.1.189",
Tunnel-Client-Auth-Id:2 = "lac01",
Tunnel-Assignment-Id:2 = "backup
```

4. In the debug output, look for `StopCCN` control messages and check the Result-Code AVP for any messages indicating why you have LAC1-Pass problems. The `StopCCN` message indicates that the L2TP tunnel was not established.

5. Use the **`debug ses-abort`** and **`debug tun-setup`** to determine if the remote system was closed by administrator.

Caution!

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

6.5 L2TP Session Setup

Symptom:

If you are not receiving an ICRP control message from a LNS, or if the LAC receives the CDN from the LNS instead of the ICRP, you might have l2TP session setup issues.

Causes:

Table 20 L2TP Session Setup Causes

#	Cause	Checked?
1	The tunnel is not established state on both sides.	
2	The LNS `max-sessions` parameter is not correctly set.	
3	The LNS `function` parameter is not correct. It should be "lns".	
4	The LNS is throttling new sessions.	
5	There is no route to the LAC from the LNS.	

To troubleshoot L2TP session setup issues:

1. Use the **`ping`** and **`traceroute`** commands to check the connectivity on the L2TP tunnel.

2. Use the **`debug l2tp ses-abort`** command on the LAC and LNS. The sender of the CDN should have a debug message before sending the Call-Disconnect-Notify (CDN) message, and the CDN may have a result-code AVP with a disconnect reason message (or ppp-disconnect cause or Redback term cause). The Redback term causes are termination error codes (codes that identify what caused the error or what caused the subscriber to go down). They are in the L2TP disconnect messages (such as CDN, StopCCN), and are specific to Redback Networks.

   Caution!

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

3. Use the **`l2tp admin test peer`** ***`peer-name`*** **`ses-setup`** [**`count`** ***`number`***] to see if the LNS sends an ICRP. If the control channel is operating poorly, it can adversely impact session setups because of timing issues (and concurrency).

4. Check if the first packet from LNS is being dropped.

6.6 CDN for an Unknown Session ID or Duplicate Remote Session ID

Symptom: A CDN for an unknown session ID or a duplicate remote session ID (receiving an ICRQ).

Cause: Problems with peer software.

To troubleshoot a CDN for an unknown session ID or a duplicate remote session ID (receiving an ICRQ):

1. Use the **`debug l2tp packet`** command to enable debug messages for L2TP-related packet transmit (TX) and receive (RX) events for L2TP control messages.

   Caution!

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

2. Use the **`debug l2tp AVP`** command to enable debug messages on L2TP attribute-value pairs (AVPs) transmitted or received in L2TP control messages.

6.7 Stuck Sessions or Tunnels

Symptom: Session count is greater than 0 and no subscribers are up.

Recommended Action: On the LAC, perform the tasks listed at Tasks to Troubleshoot General LAC Issues. On the LNS, perform the tasks list at Tasks to Troubleshooting General LNS Issues.

6.8 Scaling Issues

Symptom:

You might have scaling issues if:

- The ICRQs are sent for sessions that have recently been shut down.
- There are FSM timeouts—The session is stuck in wait-ICRP on the LAC or wait-ICCN on the LNS.
- There is no response to the ICRQ, ICRP, or ICCN.
- On the LAC, you receive a Receive Term-Req from client before the ICRP from the LNS.

Cause:

The control channel might be operating too slowly.

To troubleshooting L2TP scaling issues:

1. Trace the session setup using the **`l2tp admin test peer`** ***`name`*** **`ses-setup count`** ***`number`*** command. Look at the output to determine how to address any issues.
2. If the tunnel remains up (it does not terminate from maximum retransmits), but symptoms are present, check the session setup debug output on the remote system.
3. Use the **`debug l2tp ses-abort`** command to check if the client sends a Term-Req attribute before the ICRP or if there are finite state machine (FSM) time-outs.

   Caution!

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

4. On the LAC, use the **`l2tp admin test`** command to trace a session setup and see if the LNS is sending the ICRP.
5. If the results for the test indicate that the control channel might be operating too slowly, use the **`l2tp admin down peer`** ***`name`*** **`seconds`** ***`seconds`*** command for several seconds to see if it fixes this issue. This command marks the L2TP peer as “dead”; no new sessions are assigned to this peer. If the control window is running poorly, this can help clean out the queue.

6.9 Fragmentation

Symptom:

If your subscribers can connect and log on, but certain sites are not accessible, you might have a fragmentation issue.

Cause:

The client TCP maximum segment size (MSS) is set too high for L2TP tunneling, forcing incorrect fragmentation or no fragmentation.

To troubleshoot fragmentation issues:

1. Check the maximum received unit (MRU) values negotiated with the client on the LAC and LNS by using the **`ppp debug packet`** command. Look for negotiated fragmentation mismatches.

Caution!

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

2. On the client, check that the appropriate TCP MSS is set.

3. Check the TAC FAQ for fragmentation issues.

Table 21 Recommended Actions to Correct Fragmentation Issues

Task	Command	Notes	Checked?
Force renegotiation to the LNS.	**`l2tp renegotiate lcp always`**	Context configuration mode.	
Configure the LAC to negotiate the MRU correctly for L2TP.	**`ppp peer-options mru`**	Global configuration mode.	

On the LAC, specify the type of fragmentation for used for L2TP packets that are sent downstream and need fragmentation.	**`l2tp fragment l2tp-packet`**
	`l2tp fragment user-packet`
		Context configuration mode. If you have enabled the **`l2tp fragment user-packet`** command, verify that the subscriber's interface is set to clear-df.	

6.10 LNS PPP Session Setup

Symptoms:

- The LNS sends the LCP Term-Req attribute after renegotiating the LCP.
- The client sends the LCP Term-Req attribute instead of renegotiating LCP.
- The call disconnects soon after the ICCN message is sent by the LAC.

Cause:

Table 22 LNS PPP Session Setup Problems

#	Cause	Checked?
1	The `session-auth` parameter is not configured to match the authorization protocols available on the client. As a result, the LNS rejects the call because the LNS and client cannot agree on an authentication protocol.	
2	The client does not want to renegotiate. If the client does not want to renegotiate, it might send a term-req. Renegotiation is being caused by the LNS but cannot be processed by the client	
3	There is a duplicate CHAP ID . If you have duplicate CHAP ID, compare the CHAP challenge sent by LAC with the challenge sent by LNS. If they are the same ID but the client does not see the LNS challenge, there might be a problem because the client responds to the LAC challenge; however, the LNS incorrectly determines that the client password is wrong. The symptom would look like authentication failed.	

To troubleshooting LNS PPP session setup problems:

1. Use the **`debug ppp lcp`** command to check the session setup on the LNS.
2. Troubleshoot AAA by using the commands listed in Troubleshooting the RADIUS Server.
3. Use the **`show l2tp configuration`** command to verify that the session authentication configuration on the LNS matches the authentication protocols available on the client. Make sure the LAC bind authentication protocols agree with the LNS session authentication configuration protocols.
4. Use the **`show configuration l2tp`** command and check for l2TP configuration mismatches in the MRU negotiation configuration (configured by using the **`ppp peer-options mru`** command in global configuration mode) and the LT2P renegotiation configuration on the LNS.
5. Use the **`debug ppp packet`** command on the LAC and LNS.

Recommended Actions:

- If you have enabled the **`l2tp renegotiate lcp on-mismatch`** command, change the value of the **`l2tp renegotiate mru`** to agree with client if you want to avoid renegotiation.
- Force renegotiation on the LNS by using the **`l2tp renegotiate lcp always`** command.

- On the LAC, prevent it from sending proxy AVPs by issuing the **`no l2tp proxy-auth`** command.

7 Troubleshooting General LAC L2TP Issues

This section describes how to troubleshoot general LAC L2TP Issues. Before you begin, get a description of the problem and check if you made any recent changes or upgrades to the network. For information about the operational commands, see the *Command List*.

The following is a sample configuration for a SmartEdge router that is acting as a LAC (a LNS peer), in context `LAC1`. The following configuration maps to the tasks listed in the Tasks to Troubleshoot LAC General L2TP Issues section.

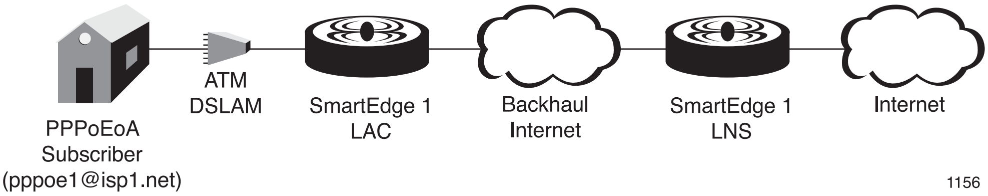


Figure 10 L2TP Network Topology

```
context LAC1
 domain isp1.net                        <-Assign a domain alias for this context.
 interface loop1 loopback
  ip address 1.1.1.1/32
 interface toLNS1
  ip address 192.168.6.2/30
 ip route 0.0.0.0/0 192.168.6.1
 l2tp-peer name LNS1 media udp-ip remote ip 1.1.1.2 local 1.1.1.1
  session-auth pap
  function lac-only                     <-Specify the role as a LAC.
  local-name LAC1                       <-Name of LAC
  aaa authentication subscriber local   <-This line is normally hidden because
 subscriber name pppoe1                 <-it is the default behavior.
  password test3
  tunnel name LNS1                      <-Static peer selection for subscriber sessions.
!
atm profile ubr
 shaping ubr
!
port atm 1/1
 no shutdown
 atm pvc 1 32 profile ubr encapsulation pppoe
  bind authentication pap context LAC1
!
port eth 5/1
 no shutdown
 encap dot1q
 dot1 pvc 100
  bind interface toLNS1 LAC1
```

7.1 Tasks to Troubleshoot General LAC L2TP Issues

Use the following table as a guide to troubleshooting general L2TP issues on the LAC.

Note: When working with technical support representatives, use the **`show tech-support`** command on your router and have the output available for technical support representatives to assist in troubleshooting.

Table 23 Tasks to Troubleshoot LAC General L2TP Issues

Task	Command	Notes	Checked?
Step 1: Checking the Troubleshooting Specific L2TP Issues section		Check if you have a specific LAC issue listed in Troubleshooting Specific L2TP Issues section. If you do, use the procedure in this section to resolve your issue. If not, go to step 2.	

Step 2: Navigating to the Correct Context	`show context all`
	`context` *`context-name`*
		Display all the contexts on your router in the local context and then navigate to the context you want to troubleshoot.	

Step 3: Checking LAC Port Counters	`show port counters live`
	`show port counters detail`
		Check port counter performance.	

Step 4: Displaying LAC Tunnel-Level Counters	`show l2tp counters peer`	Display all statistics for tunnel-level control packet counters for all tunnels under specific L2TP peers on the system.	
Step 5: Displaying LAC IPC Counters	`show l2tp global` *`group-name`*	Display L2TP interprocess communication (IPC) counters.	
Step 6: Checking LAC Interfaces	`show ip interface brief`	Make sure the interfaces are up.	

Step 7: Verifying LAC L2TP Establishment	`ping`
	`traceroute`
	`show l2tp peer`
		Test peers for tunnels and session setup on L2TP control packets.	

Step 8: Checking the LAC Status of L2TP Peers	`show l2tp peer`		
Step 9: Performing LAC L2TP Tunnel and Session Testing	`l2tp admin test peer` *`peer-name`* `tun-setup`	Set up an administrative tunnel for testing.	
Step 10: Displaying LAC L2TP Groups	`show l2tp group`	Displays L2TP group configuration information. If you have configured an L2TP group, issue this command.	
Step 11: Displaying LAC Summary Peer Information	`show l2tp summary`	Display information about all peers in all the contexts.	
Step 12: Checking LAC Bindings	`show bindings summary`	Display the configured bindings for one or more subscribers, ports, channels, or PVCs on the system.	

Table 23 Tasks to Troubleshoot LAC General L2TP Issues

Task	Command	Notes	Checked?
Step 13: Checking LAC IP Route Summary Information	`show ip route summary`	Display summary information for all IP routes on the LAC.	
Step 14: Verifying LAC Routes	`show ip route`	Display information about all IP routes or routes for only the specified IP address or IP prefix.	

Step 15: Displaying LAC PPP Summary Information	`show ppp summary`
	`show ppp down`
	`show circuit ppp down detail`
		• Display summary information for all PPP sessions in the current context.
		• Specifies that only PPP sessions for which the LCP is in the INITIAL, CLOSED, or STOPPED state are to be displayed.
		• Display detailed information about PPP circuits that are down. See Troubleshooting PPP.	

Step 16: Checking the LAC L2TP Process	`show process l2tp`
	`show-crashfiles`
		Verify that the L2TP process is running.	

Step 17: Checking the LAC L2TP Configuration	`show configuration l2tp`	Check for L2TP configuration errors.	
Step 18: Checking the RADIUS Server		If you have configured a RADIUS server, make sure the RADIUS attributes are configured correctly for your clients. For information about checking the RADIUS Server, see Troubleshooting the RADIUS Server.	
Step 19: Debugging L2TP			

7.2 Step 1: Checking Specific LAC Issues

Check if you have a specific LAC issue listed in the Troubleshooting Specific L2TP Issues section. If you do, use the procedure in this section to resolve your issue. If not, go to step 2.

7.3 Step 2: Navigating to the Correct Context

Use the **`show context all`** command and display all the contexts on your router and then navigate to the context you want to troubleshoot, in this case, the `LAC1` context.

The following example shows how to view all contexts on your router and then navigate to context `LAC1`:

```
[local]Redback#show context all
Context Name          Context ID       VPN-RD   Description
-----------------------------------------------------------
local                 0x40080001
LAC1                  0x40080002

[local]Redback#
[local]Redback#context LAC1
[LAC1]Redback#
```

7.4 Step 3: Checking LAC Port Counters

Use the **`show port counters live`** command to check the port counters on the LAC in real time. Use the **`detail`** keyword to display detailed port counter information. For more information about this command, see Checking Port Performance.

```
[LAC1]Redback#show port counters live
please wait...
Port             Type
1/1              ATM
packets sent       : 15000            bytes sent    : 20000
packets recvd      : 10000            bytes recvd   : 50000
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
5/1            ethernet
packets sent       : 25000            bytes sent    : 40000
packets recvd      : 60000            bytes recvd   : 80000
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
```

7.5 Step 4: Displaying LAC Tunnel-Level Counters

Use the **`show l2tp counters peer`** command to display all statistics for tunnel-level control packet counters for all tunnels under specific L2TP peers on the system.

Use the **`tunnel`** ***`tunl-id`*** construct to display counters for a specific L2TP tunnel.

Use the **`detail`** keyword to display detailed information for each L2TP counter. Use the optional **`tunnel`** ***`tunl-id`*** construct to display all statistics for tunnel-level control packet counters for all tunnels with a specific tunnel ID.

The following example show you how to display detailed information for counters for L2TP tunnel **28561**:

```
[LAC1]Redback#show l2tp counters peer LAC1 tunnel 28561 detail
Local ID:            28561      Remote ID:           30416
Local IP:            1.1.1.1    Remote IP:           1.1.1.2
Local Name:          LAC1       Remote Name:         LNS1
Session Count:       101        Active Sessions:     100
Total Est Sessions:  120        Total Fail Sessions: 2
Max Sessions Ever:   100
Uptime :             50 mins 2 secs

Control Statistics
Tx Control Packets:  165031     Rx Control Packets:  165031
Tx Control Bytes:    2862224    Rx Control Bytes:    3015284020
Tx Hello Packets:    234        Rx Hello Packets:    235
Ns:                  2445       Nr:                  2457
Tx Cwnd:             3          Remote Window Size:  10
Resend Q Size:       8          Unsent Q Size:       6
Max Resend Q Size:   8          Max Unsent Q Size:   8
Control Errors:      2
Control Message Times
Last Msg sent:       Tue 16:34:06 (9 mins 19 secs ago)
Last Msg recved:     Tue 16:34:06 (9 mins 19 secs ago)
Last Hello sent:     Tue 16:34:06 (9 mins 19 secs ago)
Last Hello rcvd:     Tue 16:34:06 (9 mins 19 secs ago)
Last Control Error:  Tue 16:34:06 (9 mins 19 secs ago)
Data Statistics
Tx Data Packets:     4              Rx Data Packets:     3
Tx Data Bytes:       43             Rx Data Bytes:       36
```

7.6 Step 5: Displaying LAC IPC Counters

Use the **`show l2tp global`** ***`group-name`*** command to view IPC counters for all L2TP peers and groups on the LAC.

The following example displays the IPC counters for 16,000 subscriber circuits on each of two traffic cards in slots `12` and `13`:

```
[LAC1]Redback#show l2tp global ipc
L2TP IPC Stats


Up since:...........Fri 08:13:05 (3 hours 30 mins 25 secs ago)
Last clock tick:.....Fri 11:43:30 (0 secs ago)


ISM MBE:
Sessions Recovered/Failed:......0/0
Tunnels Recovered/Failed:.......0/0
Idle Session Cleanups:..........0
Couldn't Allocate Msg:..........0
TX Circuit Tunnel-Start:........91867
TX Circuit Tunnel-Stop:.........0
TX Circuit Stale Kills:.........0
TX Sub-Sess-Down:...............26
Tunnel Start/Stop Errors:.......0


PPP:
RX Start request:...............0


AAA:
TX Tunnel Author:...............0
RX Tunnel Author:...............0
PPAs:
Registrations:..................12
Stale Registrations:............0
Registration Errors:............0
TX Tunnel Create:...............16179
TX Tunnel Delete:...............95
IPC Errors:.....................0


Registered PPAs:
Slot 01 02 03 04 05 06 07 08 09 10 11 12 13 14
I  I  I  I  .  .  .  .  .  .  .  I  I  .
E  E  E  E  .  .  .  .  .  .  .  E  E  .


PPA Name     Registration Time    Chg#  Ccts Tun-Cr   Tun-Del
------------ -------------------- ---- ----- -------- -------
Slot  1 IPPA Fri Nov 05 08:13:39     2     1    16179     95
Slot  1 EPPA Fri Nov 05 08:13:40     4     1    16179     95
Slot  2 IPPA Fri Nov 05 08:13:41     6     2    16179     95
Slot  2 EPPA Fri Nov 05 08:13:42    16     2    16179     95
Slot  3 IPPA Fri Nov 05 08:13:41     8     4    16179     95
Slot  3 EPPA Fri Nov 05 08:13:42    18     4    16179     95
Slot  4 IPPA Fri Nov 05 08:13:41    10     0    16179     95
Slot  4 EPPA Fri Nov 05 08:13:42    20     0    16179     95
Slot 12 IPPA Fri Nov 05 08:13:41    12 16004    16179     95
Slot 12 EPPA Fri Nov 05 08:13:42    22 16004    16179     95
Slot 13 IPPA Fri Nov 05 08:13:42    14 16002    16179     95
Slot 13 EPPA Fri Nov 05 08:13:42    24 16002    16179     95
```

7.7 Step 6: Checking LAC Interfaces

On the LAC, check that the interfaces are up by using the **`show ip interface brief`** command.

```
[LAC1]Redback#show ip interface brief
Mon Jun 27 06:38:05 2009
Name       Address              MTU    State    Bindings
1/1        4.2.13.4/16          1500   Up       ATM
5/1        10.13.49.166/24      1500   Up       ethernet
```

Recommended Action: If the interfaces are down, see Verifying Interfaces and Checking Port Performance.

7.8 Step 7: Verifying LAC L2TP Establishment

To verify LAC L2TP establishment, use the **`ping`** and **`traceroute`** commands to verify that links between the LAC and LNS are operational. If a ping between routers is not successful, the link is not functioning properly and you need to troubleshoot it. Use the **`source`** ***`address`*** option, because loopbacks are often used:

```
[LAC1]Redback#ping 1.1.1.2 source 1.1.1.3
[LAC1]Redback#traceroute 1.1.1.2
```

7.9 Step 8: Checking the LAC Status of L2TP Peers

On the LAC, check the status of L2TP peers by using the **`show l2tp peer`** command.

If the session count = 0, there is no PPP session. If the session count is > 1, PPP sessions have been established. If the tunnel count = 0, the tunnel is down. If the tunnel count is > 1, the tunnel has been established. In Conf. source, Local indicates a local configuration; RADIUS indicates a RADIUS configuration.

```
[LAC1]Redback# show l2tp peer
                                    Conf.   Tun   Ses
Peer Name   Local Name       Role Source    Count Count
----------  ---------------- ------------ ----  -----
LNS1        LAC1             LAC  Local     1     1
[LAC1]Redback#

[LAC1]Redback#show l2tp peer LNS1
Peer Name:        LNS1
Admin State:      Up
Local Name:       LAC1
Vendor:           RedBack Networks (Firmware: 0x0600)
Local IP Address: 1.1.1.1     Remote IP Address:  1.1.1.2
Local Role:       LAC Only    DNIS:               Disabled
Hello Timer:      300         Preference:         10
Maximum Tunnels:  32767       Maximum Ses/Tunnel: 65535
Control Timeout:  3           Retry:              10
Tunnel Count:     1           Session Count:      1
Domains: isp1.net #Peer name LNS1 is assigned domain isp1.net
[LAC1]Redback#
```

7.10 Step 9: Performing LAC L2TP Tunnel and Session Testing

7.10.1 Step 1: Tunnel and Session Testing

On the LAC, use the **`l2tp admin test peer`** command to perform L2TP peer testing. You can test any idle tunnels to a peer using Hello messages, test the tunnels, and test sessions on tunnels. Check for StopCCN control messages.

Use the **`ses-setup`** keyword to test if an L2TP network server (LNS) peer allows a session to be set up without a client connecting to it. The L2TP session is established, but the Point-to-Point Protocol (PPP) is not negotiated for the session with the peer; as a result, the peer times out and closes the session.

Use the **`tun-setup`** keyword to test if a tunnel can be created to a peer; this test validates the remote IP address (LNS) and, if configured, the local IP address specified by the **`l2tp-peer`** command (in context configuration mode), and the tunnel authorization key specified by the **`tunnel-auth key`** command (in L2TP peer configuration mode).

The following is an example of an unsuccessful L2TP peer test:

```
[LAC1]Redback#l2tp admin test peer LNS1 tun-setup
Apr 12 17:00:02: %L2TP-7-TUN: Choosing endpoints for tunnel LNS1:30947
Apr 12 17:00:03: %L2TP-7-TUN: LNS1:30947 local address dynamic:
50.0.0.2:1701/50.0.0.1:1701
Apr 12 17:00:03: %L2TP-7-TUN: LNS1:30947 endpts cfg: 50.0.0.2:1701/50.0.0.1:1701
Apr 12 17:00:03: %L2TP-7-TUN: Sending SCCRQ to LNS1:30947 at 50.0.0.2
Apr 12 17:00:03: %L2TP-7-TUN: LNS1:30947 Sent SCCRQ
Apr 12 17:00:03: %L2TP-7-TUN: LNS1:30947 No response from peer to our SCCRQ
Apr 20 12:40:05: %L2TP-7-AVP:  M  Len=46 IETF Result-Code=(2,6):
Control channel timeout - Remote peer dead
Apr 12 17:00:03: %L2TP-7-TUN: Choosing endpoints for tunnel LNS1:30947
Apr 12 17:00:03: %L2TP-7-TUN: LNS1:30947 endpts cfg:50.0.0.2:1701/50.0.0.1:1701
Apr 12 17:00:03: %L2TP-7-TUN: LNS1:30947 Sending Stop SCCCN
```

Recommended Action: Ping the LNS from the LAC context. Verify the IP routes using the **`show ip route`** command.

In the following example, the No response from peer to the SCCRQ message indicates that the LNS was not reachable; the Stop SCCN message indicates that the L2TP tunnel was not established.

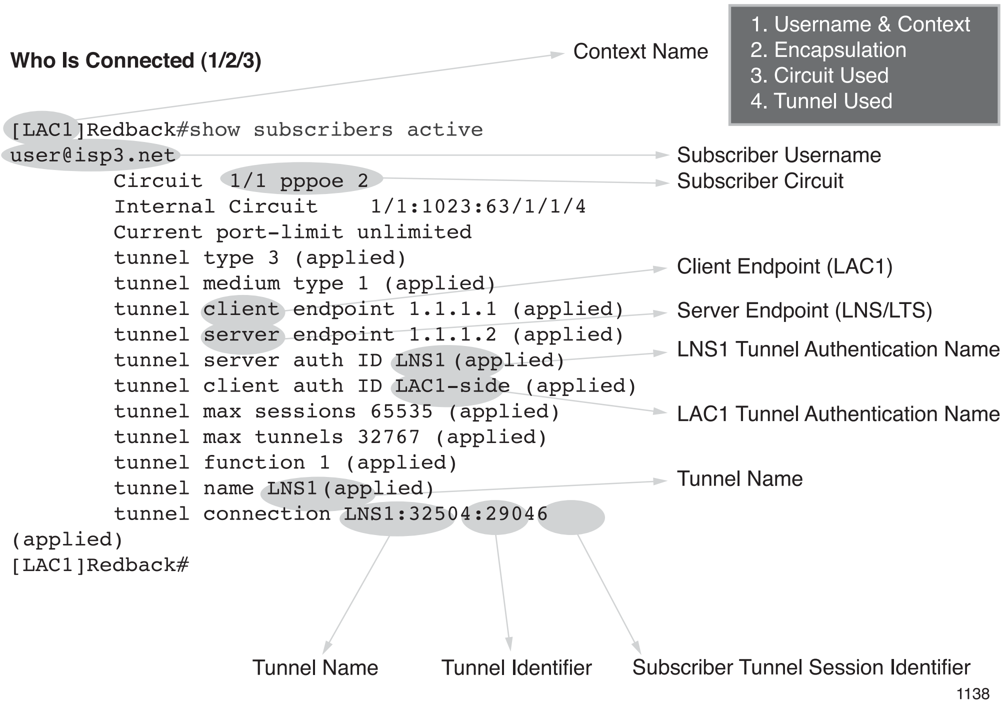
1. Ping the LNS from the LAC context.

2. Verify the IP routes using the **`show ip route`** command.

7.10.2 Step 2: Verifying Subscriber Attributes on the LAC

On the LAC, verify subscriber attributes by using the **`show subscribers active`** command.

The following illustration describes the tunnel information on the LAC when you issue this command:



Who Is Connected (1/2/3)

```
[LAC1]Redback#show subscribers active
user@isp3.net
        Circuit  1/1 pppoe 2
        Internal Circuit    1/1:1023:63/1/1/4
        Current port-limit unlimited
        tunnel type 3 (applied)
        tunnel medium type 1 (applied)
        tunnel client endpoint 1.1.1.1 (applied)
        tunnel server endpoint 1.1.1.2 (applied)
        tunnel server auth ID LNS1 (applied)
        tunnel client auth ID LAC1-side (applied)
        tunnel max sessions 65535 (applied)
        tunnel max tunnels 32767 (applied)
        tunnel function 1 (applied)
        tunnel name LNS1 (applied)
        tunnel connection LNS1:32504:29046
(applied)
[LAC1]Redback#
```

Figure 11 LAC Subscriber Attributes

To view some examples on how to use **`show subscribers`** commands, see Troubleshooting PPP, Step 9: Checking Subscribers.

7.10.3 Step 3: Verifying Where Subscribers are Terminated on the LAC

On the LAC, verify where the subscribers are terminated by using the **`show subscribers all`** command:

```
[LAC1]Redback# show subscribers all
[TYPE    CIRCUIT                   SUBSCRIBER    CONTEXT  START  TIME
-----------------------------------------------------------------------
pppoe   13/1:1 vpi-vci 0 100 pppoe  user@isp3.net LAC1     Jan 4 15:25:12
-----------------------------------------------------------------------
Total=1
```

7.11 Step 10: Displaying L2TP Group Information on the LAC

If you have configured a L2TP group, use the **`show l2tp group`** command to view the redundancy algorithm and deadtime of one specific L2TP group or for all groups in the current context. When you display information for a specific group, the names of the peer members of the group and information about each peer are also displayed.

Note: The LAC1 sample configuration does not have L2TP groups.

The following example displays output from the **`show l2tp group`** command without specifying a group name:

```
[local]Redback#show l2tp group
Group Name       Algorithm    Deadtime
---------------- ------------ --------
l2tp             Load-balance 10
l2tp2            Load-balance 5
l2tp3            Load-balance 10
```

The following example displays the output when you use the **`show l2tp group`** command to display a particular group (l2tp). The asterisk (*) in front of the peer, `l2tp-1`, indicates that the peer is down (“dead”).

```
[LAC1] Redback#show l2tp group l2tp
Group name:      l2tp  RADIUS:  YES
Algorithm        Load-balance  Deadtime: 10
Peers:          *l2tp-1
                 l2tp-2

Domains: vpn
                            Max  Tun    Max   Ses
Peer Name  Local Name Med  Tuns  Cnt    Ses   Cnt  Stat LAC  LNS  Named
--------- ----------  ---  ----  ---    ---   ---- ---- ---  ---  -----
l2tp-1     tgrp1       UDP   1     0     20     0  NO   YES  YES   YES
l2tp-2     tgrp2       UDP   1     1     65535  6  NO   YES  YES   YES
```

7.12 Step 11: Displaying LAC Summary Peer Information

On the LAC, use the **`show l2tp summary`** command to display information about all peers in all the contexts:

```
[LAC1]Redback#show l2tp summary
Context Name   Peer Name    Local Name    Tun      Ses
                                          Count    Count
-------------  ----------   ----------    -----    -----
LNS1            LAC1        LNS1            1        0
LAC1            LNS1        LAC1            1        0
```

7.13 Step 12: Checking LAC Bindings

On the LAC, use the **`show bindings summary`** command to verify your bindings. For information about this command, see Checking Bindings.

7.14 Step 13: Checking the LAC IP Route Summary Information

On the LAC, use the **show ip route summary** command to display summary information for all IP routes.

7.15 Step 14: Verifying the LAC Routes

On the LAC, use the **show ip route** command to display information about all IP routes or routes for only the specified IP address or IP prefix. For information about this command, see the *Command List*.

7.16 Step 15: Displaying LAC PPP Summary Information

On the LAC, use the **show ppp summary** command to display summary information for all PPP sessions in the current context: `LAC1`. For more information about this command, see Displaying Summary of PPP Information.

7.17 Step 16: Checking LAC L2TP Process

On the LAC, use the **show process l2tp** command to verify that the L2TP process is running. Use the **detail** keyword to view detailed information about the L2TP process. If the process is not running, use the **show crashfiles** command to check if there is a core dump. If there is, contact your local technical support representative.

```
[LAC1]Redback#show process l2tp
NAME PID  SPAWN  MEMORY TIME        %CPU  STATE  UP/DOWN
l2tp  166 3      3436K  00:00:00.59 0.00% run    00:02:20
```

7.18 Step 17: Checking the LAC L2TP Configuration

On the LAC, use the **show configuration l2tp** command and the following table as a guide to check for common configuration mismatches.

```
[LAC1]Redback# show configuration l2tp
```

Table 24 L2TP LAC Configuration Mismatch Checklist

#	LAC Configuration Mismatch	Checked?
1	The tunnel authentication key is not configured on the peer or local system.	
2	The hostname AVP does not match the RADIUS Tunnel-Server-Auth-Id attribute.	
3	The local-name parameter is not configured. As a result, the SmartEdge software uses the system hostname by default.	
4	Only one endpoint might be configured for authorization. Make sure both sides are configured with tunnel authorization keys if required.	

#	LAC Configuration Mismatch	Checked?
5	Check for a bad local address. The local address might not match the remote address configured on the LNS or the peer might now have a route back to your source address. This is a common problem with a loopback address, which is not announced using a routing protocol.	
6	Check for blocked L2TP control messages. The firewall or ACL might be blocking L2TP control messages. Check UDP port 1701.	

7.19 Step 18: Checking the RADIUS Server

If you have configured a RADIUS server, make sure the RADIUS attributes are configured correctly for your clients. For information about checking the RADIUS Server, see Section 15 on page 159, Troubleshooting the RADIUS Server.

7.20 Step 19: Debugging the LAC

For information about debugging L2TP, see Using L2TP Debug Commands.

8 Troubleshooting LNS General L2TP Issues

This section shows you how to troubleshooting general L2TP issues.

The following is a sample LNS configuration for the SmartEdge router acting as a LNS for a LAC peer in the context `LNS1`.

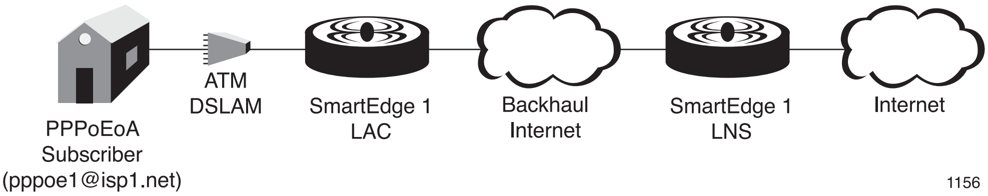


Figure 12 L2TP Network Topology

```
context LNS1
  domain isp1.net            //Domain alias for the context to use the LAC peer.
    interface loop1 loopback
    ip address 1.1.1.2/32
 interface toLAC1
   ip address 192.168.6.1/30
 interface toInternet
  ip address 2.1.1.2/24
   ip route 0.0.0.0/0 2.1.1.1.254
   ip route 1.1.1.1/32 192.168.6.2
 l2tp-peer name LAC1 media udp-ip remote ip 1.1.1.1 local 1.1.1.2
   session-auth pap
   function lns-only         //Specify that this tunnel definition will act as a LNS.
   local-name LNS1
!
  interface forSubs multibind
   ip address 10.1.1.1/24
   ip pool 10.1.1.1/24
 aaa authentication subscriber none
 subscriber default
  ip address pool
!
 port ethernet 2/1
  encap dot1q
  no shutdown
  dot1 pvc 100
      bind inter toLAC1 LNS1
!
port ethernet 2/4
 no shutdown
bind interface toInternet LNS1
```

8.1 Tasks to Troubleshoot General LNS Issues

Use the following table as a guide to troubleshooting general L2TP issues on the LNS. Before you begin, get a description of the problem and check if you made any recent changes or upgrades to their network.

For information about operational commands, see the *Command List*.

Note: When working with technical support representatives, use the **`show tech-support`** command on your router and have it available to your technical support representative to assist in troubleshooting.

Table 25 Tasks to Troubleshoot LNS General L2TP Issues

Task	Command	Notes	Checked?
Step 1: Checking Specific L2TP Issues		Check if you have a specific LNS issue listed at the Troubleshooting Specific L2TP Issues section. If you do, use the procedure in this section to resolve your issue. If not, go to step 2.	

Step 2: Navigating to the Correct Context	`show context all`
	`context` *`context-name`*
		Display all the contexts on your router in the local context and then navigate to the context you want to troubleshoot.	

Step 3: Checking LNS Port Counters	`show port counters`
	`show port counters detail`
		Check port performance.	

Step 4: Checking LNS Circuit Counters	`show circuit counters l2tp all`
	`show circuit counters l2tp lns`
		• Display summary information for all circuits.
		• Display the circuit counters for specific circuit handle on the LNS.	

Step 5: Displaying LNS Tunnel-Level Counters	`show l2tp counters peer` *`name`* `tunnel`	Display tunnel-level counters.	
Step 6: Displaying LNS IPC Counters	`show l2tp global` *`group-name`*	Display IPC counters for all L2TP peers and groups on the LNS.	

Step 7: Verifying LNS L2TP Establishment	`ping`
	`traceroute`
	`show subscribers active`
	`show l2tp peer`		

Step 8: Check the LNS Status of L2TP Peers	`show l2tp peer`		
Step 9: Displaying LNS Summary Information	`show l2tp summary`	Display information about all peers in all the contexts.	
Step 10: Checking LNS Bindings	`show bindings`		

Table 25 Tasks to Troubleshoot LNS General L2TP Issues

Task	Command	Notes	Checked?
Step 11: Checking LNS Interfaces	`show ip interface brief`	Make sure the interfaces are up.	

Step 12: Displaying LNS PPP Summary Information	`show ppp summary`
	`show ppp down`
	`show circuit ppp down detail`
		• Display summary information for all PPP sessions in the current context.
		• Specifies that only PPP sessions for which the LCP is in the INITIAL, CLOSED, or STOPPED state are to be displayed.
		• Display detailed information about PPP circuits that are down.	

Step 13: Checking the LNS IP Routes	`show ip route summary`	Display summary information for all IP routes.	
Step 14: Displaying LNS Subscriber Routes	`show ip route subscriber`	Verify where the subscriber is terminating. Make sure the IP address negotiated during the IPCP stage is correctly installed in the routing table.	
Step 15: Verifying the LNS Routes	`show ip route`	Display information about all IP routes or routes for only the specified IP address or IP prefix.	

Step 16;: Checking the LNS L2TP Process	`show process l2tp`
	`show-crashfiles`
		Verify that the L2TP process is running.	

Step 17: Checking the LNS Configuration	`show configuration l2tp`	Check for configuration mismatches.	
Step 18: Checking the RADIUS Server		If you have configured a RADIUS server, make sure the RADIUS attributes are configured correctly for your clients. For information about checking the RADIUS Server, see Troubleshooting the RADIUS Server.	
Step 19: Debugging the LNS			

8.2 Step 1: Checking Specific LNS Issues

Check if you have a specific LNS issue listed in the Checking Troubleshooting Specific L2TP Issues section. If you do, use the procedure in this section to resolve your issue. If not, go to step 2.

8.3 Step 2: Navigating to the Correct Context on the LNS

Use the **`show context all`** command to display all the contexts on the SmartEdge router and then navigate to the context in which you have configured the LNS—in this case, the `LNS1` context.

```
[local]Redback#show context all
Context Name  Context ID    VPN-RD    Description
-------------------------------------------------
local         0x40080001
LNS1          0x40080002

[local]Redback#
[local]Redback#context LNS1
[LAC1]Redback#
```

8.4 Step 3: Checking LNS Port Counters

On the LNS, use the **`show port counters`** command to check the port counters. Use the **`detail`** keyword to displayed detailed information about the port counters. For more information about this command, see Checking Port Performance.

```
[LNS1]Redback#show port counters live
please wait...
Port            Type
2/1             ethernet
packets sent       : 15000      bytes sent     : 20000
packets recvd      : 10000      bytes recvd    : 50000
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
2/4             ethernet
packets sent       : 25000      bytes sent     : 40000
packets recvd      : 60000      bytes recvd    : 80000
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
```

8.5 Step 4: Checking LNS Circuit Counters

On the LNS, use the **show circuit counters l2tp all** command to display summary information for all circuits.

```
[LNS1]Redback#show circuit counters l2tp all
Circuit        Packets/Bytes Sent    Packets/Bytes Received
L2TP LNS 1
                        0                     0
                        0                     0
```

On the LNS, use the **show circuit counters l2tp lns** ***circuit_ID*** command to display information on a specific circuit handle:

```
[LNS1]Redback#show circuit counters l2tp lns 1
Circuit      Packets/Bytes Sent    Packets/Bytes Received
L2TP LNS 1
                   10                          9
                  534                        229
```

8.6 Step 5: Displaying LNS Tunnel-Level Counters

On the LNS, use the **show l2tp counters peer** ***peer-name*** **tunnel** command to display tunnel-level counters for L2TP control packets.

Use the **tunnel** ***tunl-id*** construct to display counters for a specific L2TP tunnel. Use the detail keyword to display detailed information for each L2TP counter.

Use the optional **tunnel** ***tunl-id*** construct to display all statistics for tunnel-level control packet counters for all tunnels with a specific tunnel ID.

The following displays tunnel-level counters on the LNS:

```
[LNS1]Redback#show l2tp counter peer tr069 tunnel
Local ID:             13127        Remote ID:   6934
Local IP:            1.1.1.2       Remote IP     1.1.1.1
Local Name:          tr069-tunnel-client  Remote Name:  l2tp-tr069
Session Count:       4             Active Sessions:     4
Total Est Sessions:  15            Total Fail Sessions: 2
Max Sessions Ever:   5
Uptime :             11 hours 25 mins 18 secs
Control Statistics
Tx Control Packets:  191           Rx Control Packets:  173
Tx Control Bytes:    7669          Rx Control Bytes:    3025
Tx Hello Packets:    126           Rx Hello Packets:    0
Ns:                  166           Nr:                  25
Tx Cwnd:             130           Remote Window Size:  20050
Resend Q Size:       0             Unsent Q Size:       0
Max Resend Q Size:   2             Max Unsent Q Size:   0
 Control Errors:     0
```

8.7 Step 6: Displaying LNS IPC Counters

Use the **`show l2tp global`** ***`group-name`*** command to view IPC counters for all L2TP peers and groups on the LNS.

The following example displays the IPC counters for 16,000 subscriber circuits on each of two traffic cards in slots `12` and `13`:

```
[LNS1]Redback#show l2tp global ipc
L2TP IPC Stats

Up since:............Fri 08:13:05 (3 hours 30 mins 25 secs ago)
 Last clock tick:.....Fri 11:43:30 (0 secs ago)

ISM MBE:
  Sessions Recovered/Failed:......0/0
  Tunnels Recovered/Failed:.......0/0
  Idle Session Cleanups:..........0
  Couldn't Allocate Msg:..........0
  TX Circuit Tunnel-Start:........91867
  TX Circuit Tunnel-Stop:.........0
  TX Circuit Stale Kills:.........0
  TX Sub-Sess-Down:...............26
  Tunnel Start/Stop Errors:.......0

 PPP:
  RX Start request:...............0

 AAA:
  TX Tunnel Author:...............0
  RX Tunnel Author:...............0

 PPAs:
  Registrations:..................12
  Stale Registrations:............0
  Registration Errors:............0
  TX Tunnel Create:...............16179
  TX Tunnel Delete:...............95
  IPC Errors:.....................0

  Registered PPAs:

Slot 01 02 03 04 05 06 07 08 09 10 11 12 13 14
      I  I  I  I  .  .  .  .  .  .  .  I  I  .
      E  E  E  E  .  .  .  .  .  .  .  E  E  .

 PPA Name     Registration Time   Chg# Ccts  Tun-Cr  Tun-Del
 ------------ ------------------- ---- ----- -------- ------
 Slot  1 IPPA Fri Nov 05 08:13:39    2     1    16179   95
 Slot  1 EPPA Fri Nov 05 08:13:40    4     1    16179   95
 Slot  2 IPPA Fri Nov 05 08:13:41    6     2    16179   95
 Slot  2 EPPA Fri Nov 05 08:13:42   16     2    16179   95
 Slot  3 IPPA Fri Nov 05 08:13:41    8     4    16179   95
 Slot  3 EPPA Fri Nov 05 08:13:42   18     4    16179   95
 Slot  4 IPPA Fri Nov 05 08:13:41   10     0    16179   95
 Slot  4 EPPA Fri Nov 05 08:13:42   20     0    16179   95
 Slot 12 IPPA Fri Nov 05 08:13:41   12 16004    16179   95
 Slot 12 EPPA Fri Nov 05 08:13:42   22 16004    16179   95
 Slot 13 IPPA Fri Nov 05 08:13:42   14 16002    16179   95
 Slot 13 EPPA Fri Nov 05 08:13:42   24 16002    16179   95
```

8.7.1 Verifying Session Mapping to the Context and Tunnel

PPP sessions are mapped to contexts in the following ways:

1. Global RADIUS is used, and the context to map the subscriber session is returned from RADIUS.

2. The fully qualified domain name is used to map a subscriber PPP session to a context. The context name as well as additional domain statements in each context are used to map the sessions.

   The global configuration statement **`aaa last-resort context`** ***`context-name`*** assigns sessions to the named context if no matching domain-name statement is found.

3. The circuit bind statement can force or override the domain switching logic. For example, the **`bind authentication pap context LAC1`** command forces every session to context “LAC1”, regardless of the subscriber session domain.

Once mapped to a context, PPP sessions can be mapped to a tunnel in the following ways:

1. Based on domain; for example, the name or domain statement on the tunnel peer or peer group (by using the aaa auth subscriber none command or tunnel domain in the subscriber default).

2. By using the **`tunnel name`** ***`tunnel_name`*** command under the **`subscriber default`** command or under the local subscriber record.

3. By RADIUS returning tunnel peer name local authentication and tunnel assignment in the subscriber record.

8.8 Step 7: Verifying LNS L2TP Establishment

8.8.1 Step 1: Checking Connectivity

From the LNS, ping the LAC to test connectivity.

Use the `ping` and `traceroute` commands to verify that links between LNS and LAC are operational. If a ping between routers is not successful, the link is not functioning properly, and you need to troubleshoot it. Use the `source` *`address`* option because loopbacks are often used.

```
[LNS1]Redback#ping 1.1.1.1 source 1.1.1.3
[LNS1]Redback#traceroute 1.1.1.1
```

8.8.2 Step 2: Verify Where Subscribers are Terminated

On the LNS, use the `show subscribers all` command to verify where the subscribers are terminated:

```
[LNS1]Redback# show subscribers all
TYPE CIRCUIT           SUBSCRIBER    CONTEXT START TIME
-----------------------------------------------------------
ppp  L2TP LNS 5245747  user@isp1.net ISP3    Jan 4 15:25:12
-----------------------------------------------------------
Total=1
```

8.8.3 Step 3: Verifying Subscribers Attributes

On the LNS, use the `show subscribers active` command to make sure the subscriber attributes were applied correctly.

```
[LNS1]Redback#context ISP3
[ISP3]Redback#show subscribers active
user@isp3.net
Circuit L2TP LNS 6587802
Internal Circuit 255/16:1023:63/5/2/6587802
Current port-limit unlimited
timeout idle 36000 (applied)
ip address 10.1.1.2 (applied from pool)
tunnel type 3 (applied)
tunnel medium type 1 (applied)
tunnel server endpoint 1.1.1.2 (applied)
tunnel client endpoint 1.1.1.1 (applied)
tunnel server auth ID LNS1 (applied)
tunnel client auth ID LAC1 (applied)
tunnel max sessions 65535 (applied)
tunnel max tunnels 32767 (applied)
tunnel function 2 (applied)
tunnel connection LAC1:27201:54912 (applied)
tunnel vendor avp (applied)
tunnel vendor avp (applied
[ISP3]Redback#
```

For more examples on how to use `show subscribers` commands, see Checking Subscribers in the Troubleshooting PPP section.

8.9 Step 8: Checking L2TP Peers on LNS

On the LNS, check the status of L2TP peers by using the **show l2tp peer** command. Check the number of tunnels, profiles, session count (number of subscribers for the tunnel) and the attributes (Auth Method, Domains, Session-Context, maximum sessions and tunnels) applied to the tunnels:

```
[LNS1]Redback# show l2tp peer
                                               Conf.  Tun   Ses
Peer Name              Local Name        Role  Source Count Count
--------------------   ----------------  ----  ------ ----- -----
LAC1                   LNS1              LNS   Local  1     0

[LNS1]Redback#show l2tp peer LAC1
Peer Name:             LAC1
Admin State:           Up
Local Name:            LNS1
Vendor:                RedBack Networks
Local IP Address:      1.1.1.2         Remote IP Address:  1.1.1.1
Local Role:            LNS Only        DNIS:               Disabled
Hello Timer:           300             Preference:         10
Maximum Tunnels:       32767           Maximum Ses/Tunnel: 65534
Control Timeout:       3               Retry:              10
Tunnel Count:          1               Session Count:      2
Authen Method:         CHAP-PAP        Session-Context:    <Any>
Domains: (NO DOMAINS)
[LNS1]Redback#


[LNS1]Redback# show l2tp peer
                                               Conf.  Tun   Ses
Peer Name              Local Name        Role  Source Count Count
--------------------   ----------------  ----  ------ ----- -----
LAC1                   LNS1              LNS   Local  1     0
```

```
[LNS1]Redback# show l2tp peer LAC1 tunnel
Loc    Rem    Remote          Rem    Ses   Act   Total   Total
ID     ID     IP Address      Port   Count Ses   Estab   Fail
-----  -----  --------------- ------ ----- ----- ------- -------
29048  29047  1.1.1.1         1701   0     0     1       0

[LNS1]Redback# show l2tp peer LAC1 tunnel 29048
State:                 Established
Last change:           Wed 14:42:27 (7 mins 7 secs ago)
Local ID:              29048          Remote ID:          29047
Local IP:              1.1.1.2        Remote IP:          1.1.1.1
Local Name:            LNS1           Remote Name:        LAC1
Session Count:         0              Active Sessions:    0
Total Est Sessions:    1              Total Fail Sessions: 0
Control Channel:
Window current-tx:     3 max-tx: 8 rx: 8
Forwarding:
Next-Hop Circuit:      11/2
Peer-facing Card(s):   11
Tunnel PPA Table:
Slot 01 02 03 04 05 06 07 08 09 10 11 12 13 14
       . . I . . . . . . . I . I .
       . . E . . . . . . . E . E .


[LNS1]Redback# show l2tp peer LAC1 tunnel
Loc    Rem    Remote          Rem    Ses   Act   Total   Total
ID     ID     IP Address      Port   Count Ses   Estab   Fail
-----  -----  --------------- ------ ----- ----- ------- -------
23734  23733  1.1.1.1         1701   1     1     1       0


[LNS1]Redback# show l2tp peer LAC1 tunnel 23734 session
Ses   Rem
ID    ID     State          Port/Circuit
----- ----- -----------    --------------------------------------
60847 34635 Established    L2TP LNS 3027653


[LNS1]Redback# show circuit count l2tp LAC1 tunnel 23734 session 60847
Circuit          Packets/Bytes Sent  Packets/Bytes Received
L2TP LNS 3027653       22359               22357
                       1073261             447140

[LNS1]Redback#
[LNS1]Redback# show circuit count l2tp LAC1 tunnel 23734 session 60847
detail
Circuit: L2TP LNS 3027653, Internal id: 5/2/3027653, Encap: l2tp-lns
Packets                              Bytes
----------------------------------------------------------------------
Receive           :            22397  Receive           :      447940
Receive/Second    :             0.00  Receive/Second    :        0.00
Transmit          :            22399  Transmit          :     1075181
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
```

8.10 Step 9: Displaying LNS L2TP Summary Information

On the LNS, use the **show l2tp summary** command to display information about all peers in all the contexts.

```
[LNS1]Redback#show l2tp summary
Context Name     Peer Name    Local Name     Tun      Ses
                                             Count    Count
-------------    ---------    -----------    -----    ----
LNS1             LAC1         LNS1           1        0
LAC1             LNS1         LAC1           1        0
```

8.11 Step 10: Checking LNS Bindings

On the LNS, use the **show bindings** command to verify your bindings. For information about this command, see Section 2.7 on page 20.

8.12 Step 11: Checking LNS Interfaces

On the LNS, use the **show ip interface brief** command to verify that your interfaces are up.

```
[LNS1]Redback#show ip interface brief

Mon Jun 27 06:38:05 2009
Name    Address              MTU    State    Bindings
2/1     4.2.13.4/16          1500   Up       ethernet 2/1
2/4     10.13.49.166/24      1500   Up       ethernet 2/4
```

Recommended Action: If the interfaces are down, see Verifying Interfaces and Checking Port Performance.

8.13 Step 12: Displaying LNS PPP Summary Information

On the LNS, use the **show ppp summary** command to display summary information for all PPP sessions in the current context. For information about this command, see Displaying PPP Summary Information.

8.14 Step 13: Checking LNS IP Routes

On the LNS, use the **show ip route summary** command to display summary information for all IP routes.

8.15 Step 14: Displaying LNS Subscriber Routes

On the LNS, use the **`show ip route subscriber`** command to check where the subscriber is being terminated. Make sure that the correct routes are installed in the routing table during IPCP negotiation.

```
[LNS1]Redback#show ip route subscriber
Codes:C-connected,S - static,S dv - dvsr, R - RIP, e B - EBGP,i B
- IBGP
    A,H - derived hidden
    O  - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1
    N2 - OSPF NSSA external type 2,  E1 - OSPF external type 1
    E2 - OSPF external type 2
    I  - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2
    IPH - IP Host, SUB A - Subscriber address, SUB S - Subscriber
 static
       A - Derived Default
       >   - Active Route
Type    Network       Next Hop  Dist  Metric   UpTime      Interface
> SUB A 20.1.1.1/32              15      0     00:01:08    LNS1
> SUB A 20.1.1.2/32              15      0     00:01:08    LNS1
> SUB A 30.1.1.0/32              15      0     00:01:08    LNS1
```

8.16 Step 15: Verifying LNS Routes

On the LNS, use the **`show ip route`** command to display information about all IP routes or routes for only the specified IP address or IP prefix.

8.17 Step 16: Checking the LNS L2TP Process

Use the **`show process l2tp`** command to verify that the L2TP process is running on the LNS. For detailed information, use the **`detail`** keyword. If the process is not running, use the **`show crashfiles`** command to check if there is a core dump. If one exists, contact your local technical support representative.

```
[LNS1]Redback#show process l2tp

NAME PID SPAWN MEMORY TIME         %CPU  STATE UP/DOWN
l2tp 166  3    3436K  00:00:00.59  0.00% run   00:02:20
```

8.18 Step 17: Checking the LNS Configuration

On the LNS, use the **`show configuration l2tp`** command to check for common configuration mismatches. Use the following table as a guide to checking LNS configuration mismatches.

```
[LNS1]Redback#show configuration l2tp
```

Table 26 L2TP LNS Configuration Mismatch Checklist

#	LNS Configuration Mismatch	Checked?
1	The LNS function parameter is not correct. It should be `lns-only` because the default is `lac-only`. This is common misconfiguration.	
2	The `session-auth` parameter is not configured to match the authorization protocols available on the client. As a result, the LNS rejects the call since the LNS and client cannot agree on an authentication protocol.	
3	The client does not want to renegotiate. If the client does not want to renegotiate, it might send a term-req. Renegotiation is being caused by the LNS but cannot be processed by the client	
4	There is a duplicate CHAP ID . If you have duplicate CHAP ID, compare the CHAP challenge sent by LAC with the challenge sent by LNS. If they are the same ID, but the client does not see the LNS challenge, there might be a problem. The client responds to the LAC challenge; however, the LNS incorrectly determines that the client password is wrong. The symptom would look like an authentication failure.	
5	The LNS `max-sessions` parameter is not correctly set.	
6	The tunnel authentication key is not configured on the peer or local system.	
7	The `local-name` parameter is not configured. As a result, the SmartEdge software uses the system hostname by default.	
8	Only one endpoint might be configured for authorization. Make sure both sides are configured with tunnel authorization keys if required.	
9	Check for a bad remote address on the LNS. There might be no route to the peer and, as a result, no connectivity.	
10	Check for a bad local address. The local address might not match the remote address configured on the LNS, or the peer might not have a route back to your source address. This is a common problem with a loopback address, which is not announced using a routing protocol.	
11	Check for blocked L2TP control messages. The firewall or ACL might be blocking L2TP control messages.	

8.19 Step 17: Checking the RADIUS Server

If you have configured a RADIUS server, make sure the RADIUS attributes are configured correctly for your clients. For information about checking the RADIUS Server, see Section 15 on page 159, Troubleshooting the RADIUS Server.

8.20 Step 18: Debugging the LNS

For information about debug the LNS, see Using L2TP Debug Commands.

9 L2TP Debug Commands

Use the **`debug l2tp`** command to enable the generation of debug messages for L2TP-related events.

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

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

Note: The SmartEdge 100 router does not support the **`standby`** and **`switchover`** keywords.

Caution!

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

Table 27 L2TP Event Types

Event	Description
aaa	L2TP-related authentication, authorization, and accounting (AAA) events.
all	All L2TP-related events.
avp	L2TP attribute-value pairs (AVPs) transmitted or received in L2TP control messages.
circuit	L2TP-related circuit events.
group	L2TP-related group events, including the selection of a peer for a given session.
ipc	L2TP-related interprocess communication (IPC) events.
ism both	L2TP-related Interface and Circuit State Manager (ISM) messages in both directions.
ism in	L2TP-related ISM incoming messages.
ism out	L2TP-related ISM outgoing messages.
misc	L2TP-related miscellaneous events.
packet	L2TP-related packet transmit (TX) and receive (RX) events for L2TP control messages.
peer	L2TP-related peer events.
ppa	L2TP-related Packet Processing ASIC (PPA) events.
ppp	L2TP-related Point-to-Point Protocol (PPP) events.
rcm	L2TP-related Router Configuration Manager (RCM) events.
route	L2TP routes to peers events.

Event	Description
ses-abort	L2TP-related abnormal termination of session events.
ses-fsm	L2TP-related session finite-state-machine events.
ses-setup	L2TP-related session setup events.
tun-fsm	L2TP-related tunnel finite-state-machine events.
tun-setup	L2TP-related tunnel setup events.
window	L2TP-related control window events, including out-of-order or retransmitted control messages.

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

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

Note: For more information about **`logging`** commands and the **`terminal monitor`** command, see the *Command List*.

Issue the **`no`** form of this command to disable the generation of debug messages for L2TP-related events.

The following example show how to enable the generation of all PPP debug messages for all circuits on port **`1`** on the traffic card in slot **`3`** on the `LAC1` context:

```
[LAC1]Redback#debug circuit handle 14/1:1023:63/2/2/1
[LAC1]Redback#debug circuit ppp packet
```

The following example show how to enable the generation of all L2TP debug messages on circuit handle **14/1:1023:63/2/2/1** on the LNS1 context:

```
[LNS1]Redback#debug circuit handle 14/1:1023:63/2/2/1
[LNS1]Redback#debug circuit l2tp all
[LNS1]Redback#show debug circuit  //Shows circuits
Circuit debugging:                //being debugged.
14/1:1023:63/2/2/1
```

Note: To find a circuit handle, use the **`show circuit`** ***`circuit-type`*** **`detail | grep [`*`ip-address`*` | `*`username`*` | `*`mac-address`*`]`** command. When you use this command, make sure the encapsulation type is correct.

10 Overview of DHCP

10.1 About DHCP

DHCP dynamically configures IP address information for subscriber hosts. The SmartEdge OS provides three types of DHCP support:

- **DHCP relay server**—The SmartEdge router acts as an intermediary between an external DHCP server and the subscriber (client). The router relays requests from the subscriber to the DHCP server and relays the server responses back to the subscriber.
- **DHCP proxy server**—The SmartEdge router provides responses directly to subscriber requests. Each subscriber sees the router as the DHCP server, and as such, sends all DHCP requests, including IP address release and renewal, to the router, which then proxies the information to the external DHCP server. The proxy feature enables the router to maintain IP address leases.
- **Internal DHCP server**—The SmartEdge router provides the functions of the DHCP server; no external DHCP server is required.

11 Troubleshooting Subscriber Connectivity on the Proxy or Relay

Use Table 28 as a guide to troubleshooting specific DHCP relay or proxy issues—that is, to determine where the packets are dropping.

Table 28 Tasks to Troubleshoot Why Subscribers are Not Coming Up.

Issue	Command	Checked?
Troubleshooting Specific CLIPS Issues	show port counters show ip interface show configuration port show circuit counters show dhcp relay stats show ip route show configuration dhcp show arp	
DHCP Relay is Not Receiving Offers	show dhcp relay stats detail show dhcp relay server show ip route show subscribers active	
SmartEdge Router is not Sending Offers to Subscribers	debug aaa show dhcp relay stats show dhcp relay stats detail show ip route all	
Subscribers Are Not Receiving Offers	show bridge table show spanning-tree *name-of-bridge* circuit show configuration	
Subscriber Request Is Not Receiving an Acknowledgement	show dhcp relay stats detail show port counters	
Subscribers Coming Through Relay or Proxy Lose Connectivity	show dhcp relay stats show arp	
Subscribers Cannot Access the Network	show subscribers active *username* show clips | grep *mac-address* debug aaa all show arp	

11.1 Troubleshooting Specific CLIPS Issues

When you troubleshooting specific CLIPS issues, check the following areas:

1. The relay or proxy (SmartEdge router)
2. The external DHCP server
3. The subscriber system

11.1.1 Checking the DHCP Relay or Proxy

On the SmartEdge router acting as a DHCP relay or proxy:

1. Check if overall packets are being sent and received by using the **`show port counters`** ***`slot/port`*** command.

2. Make sure that the IP interfaces are up by using the **`show ip interface`** command.

3. Check if the relevant CLIPS session is sending and receiving packets by using the **`show circuit counters`** ***`slot/port`*** command. This command displays the parent and child circuit counters.

4. Check if the DHCP relay or proxy is receiving DHCP discovers by using the **`show dhcp relay stats`** command. Make sure the DHCP discover counters are increasing.

   If the results are as expected, make sure the DHCP relay or proxy is relaying discovery messages to the external DHCP server. Look at the sent counters field to see if they are increasing. If the sent counter is not increasing, check if authentication is successful.

5. Ping the external DHCP server to see if it is reachable.

6. Ping the IP address of a remote IP host. If this fails, check the route table entries by using the **`show ip route`** command.

7. Check the configuration by using the **`show configuration`** command.

8. Examine the ARP entries by using the **`show arp`** command.

11.1.2 Checking the External DHCP Server

On the external DHCP server:

1. Check that it has available IP addresses to assign to the subscribers.

2. Verify that the external DHCP server responds to the subscriber request and that the subscriber DHCP client receives this response.

11.1.3 Checking the Subscriber System

1. On the subscriber system, check the IP configuration and verify the correct values for your host.

2. Check if the subscriber system has a static address that is outside the pool range of the external DHCP server.

11.2 DHCP Relay Is Not Receiving Offers

If the SmartEdge router acting as a DHCP relay is not receiving offers:

1. Check if the DHCP relay is dropping discover packets in the TX error counter by using the **`show dhcp relay stats detail`** command.

2. Validate the server status by using the **`show dhcp relay server`** command.

3. Validate the network configuration by using the **`show ip route`** command.

4. Determine if the DHCP relay is selecting the correct multibind interface for using gi_addr.

   If the subscriber is bound to an interface, issue the **`show subscribers active`** command to get information about the interface it is bound to.

5. Check the external DHCP server. Make sure the network range is configured correctly.

11.3 SmartEdge Router Is Not Sending Offers to Subscribers

If the SmartEdge router is not sending offers to subscribers:

1. On the SmartEdge router that is acting as the DHCP relay or proxy, check if the received offer has a valid IP address for subscribers (the IP address must match the subnet configured on the multibind interface to which the subscriber is bound) or on the interface by using the **`debug aaa`** and then the **`terminal monitor`** commands and look for the following line:

   ```
   dhcp rtn_add failed for iphost add
   ```

2. Use the **`show dhcp relay stats`** command to check the `Offers Sent` counter. If this counter is not increasing, then the offer is invalid or multibind interface configuration is not correct.

3. Use the **`show dhcp relay stats detail`** command several times and see if the `Send Client Error` counter is increasing. If the counter is increasing, the DHCP relay is not able to send packets out.

4. Use the **show ip route all** command and check the routing towards the subscriber. A route must exist for the subscriber network (if coming through another relay or proxy), which is active.

11.4 Subscribers Are Not Receiving Offers

If the SmartEdge router acting as a relay or proxy is sending offers to the subscriber, but the subscriber is not able to receive them:

1. Determine if the subscriber is directly connected to the relay or proxy (through a Layer 2 network) or that the subscriber is connecting through a relay or proxy.

2. In a directly connected case, check if the switch is enabled with broadcast rate limiting (this might be blocking the client from receiving offers) and other related configuration that might be blocking the client from receiving the offer.

3. On the relay or proxy, check the Layer 2 configuration, such as VLAN and STP. If present, check if the port is in a forwarding state by using the **show bridge table** and **show spanning-tree *name-of-bridge* circuit** commands.

4. Capture the packets at the subscriber side for further debugging.

5. If the subscriber is connecting through the DHCP relay or proxy, check the SmartEdge router configuration by using the **show configuration** command.

11.5 Subscriber Request Is Not Receiving An Acknowledgement

To determine why the subscriber is not receiving an acknowledgement from the relay or proxy:

1. On the relay or proxy (SmartEdge router), check that it is receiving requests by using the **show dhcp relay stats detail** command.

2. Check if the bad circuit counter is incrementing by using **show port counters** command. If this counter is not incrementing:

- The subscriber circuit is deleted, due to an attribute failure or because the interface was deleted.

- The request is received on a port other than the one discovered.

11.6 Subscribers Coming Through the Relay or Proxy Lose Connectivity

If the subscribers coming through a SmartEdge router that is acting as a DHCP relay or proxy lose connectivity to the network:

1. Check the DHCP relay or proxy statistics by using the **`show dhcp relay stats`** command.

2. On the DHCP relay or proxy, check that the ARP entries are correct for both the client and DHCP server by using the **`show arp`** command.

3. On the external DHCP server, check that the ARP entries are correct.

4. On the subscriber system, ping the DHCP relay or proxy and the external DHCP server to check connectivity.

5. If the ping is successful, on the subscriber system, check the ARP entries to make sure they are correct.

11.7 Subscribers Cannot Access the Network

After receiving an IP address lease, if the subscriber cannot ping to the default gateway or cannot reach any other destination:

1. On the relay or proxy, verify that the subscriber has a valid lease and has a circuit by using the **`show subscribers active`** ***`username`***. ***`username`*** is the MAC address of the subscriber, if it is a CLIPS session, which can be obtained from the subscriber IP address by using **`show clips`** | **`grep`** ***`mac-address`***.

2. If the subscriber has a valid circuit, check if any policies or ACLs are applied by default and validate them. The policies or ACLs might be blocking the subscriber from accessing the network. Correct these policies or ACLs to allow your subscriber to access the network.

Caution!

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

3. If there is no circuit for this subscriber even though lease is granted, check the output from the **`debug aaa all`** command for any failure related to applying attributes by the AAA server.

4. Check that the subscriber MAC address and that the circuit is bound to the correct interface and port by using the **`show arp`** command. The subscriber should have an entry pointing to the correct port and interface.

5. Validate the ARP entries for subscriber IP access.

12 Troubleshooting General DHCP Relay or Proxy Issues

When you verify the DHCP relay or proxy server, check the following:

1. The DHCP connection towards the subscriber (subscriber connection).

2. The DHCP proxy or relay function within the SmartEdge router.

3. The external DHCP server.

The following is a sample configuration for the SmartEdge router that is acting as a DHCP Proxy, in context `dhcp-proxy`. This configuration maps to the tasks listed in Tasks to Troubleshoot the DHCP Relay or Proxy.

```
context dhcp-proxy
!
 no ip domain-lookup
!
 interface toExtDHCPServer
  ip address 10.0.0.1/24
!
 interface subs multibind
  ip address 192.168.1.1/24
  dhcp proxy 254     //Specify that this is a DHCP Proxy.
                     //The number indicates the number of IP addresses
                     //available for assignment.
  no logging console
 aaa authentication administrator local
 aaa authentication administrator maximum sessions 1
 aaa authentication subscriber none
!
!
 subscriber default
   dhcp max-addrs 1
 service ssh client
!
 dhcp relay server 10.0.0.2
!
```

12.1 Tasks to Troubleshoot the DHCP Relay or Proxy

Use Table 29 as a guide to troubleshooting general DHCP relay or proxy server (SmartEdge router) issues. Use the **`show dhcp relay`** and **`debug dhcp-relay`** commands to troubleshoot the relay or proxy. Check each task that you have completed and document your results.

Before you begin, get a description of the problem and check if were any recent changes or upgrades to the network.

Note: When working with technical support representatives, use the **`show tech-support`** command on your router and have the output available for technical support representative to assist in troubleshooting.

When you reload the SmartEdge router, the external micro-drive must be present to preserve leases.

Table 29 Tasks to Troubleshoot DHCP General Relay or Proxy Issues

Task	Command	Notes	Checked?
Step 1: Checking for Specific DHCP Relay or Proxy Issues		Check if you have a specific DHCP proxy or relay issue listed in the Troubleshooting Subscriber Connectivity on the Proxy or Relay section. If you do, use the procedure in this section to resolve your issue. If not, go to step 2.	

Step 2: Navigating to the Correct Context	**`show context all`**
	`context` ***`context-name`***
		• Display all the contexts in the local context and then navigate to the context you want to troubleshoot.
		• Most of these commands must be executed in the context where the DHCP proxy or relay server is configured.	

Step 3: Checking DHCP Relay or Proxy Statistics	**`show dhcp relay stats`**	Display DHCP relay or proxy statistics.	
Step 4: Checking Relay or Proxy Port Counters	**`show port counters live`**	Check port performance.	

Step 5: Verifying the Status of Existing Sessions on the Relay or Proxy	**`show subscribers active`**
	`ping`
		• Display active subscribers.
		• The ping may not work if a subscriber firewall is blocking pings. Make sure you are in the appropriate context by using the **`context`** ***`context-name`*** command.	

Step 6: Testing the DHCP Client Address and External DHCP Server Connectivity	**`ping`**	Ping the client IP address and the DHCP server IP address.	
Step 7: Checking Relay or Proxy Interfaces	**`show ip interface brief`**	Check for to see if the interface is up.	

Table 29 Tasks to Troubleshoot DHCP General Relay or Proxy Issues

Task	Command	Notes	Checked?
Step 8: Checking Relay or Proxy Bindings	`show bindings`	Display the configured bindings for one or more subscribers, ports, channels, or PVCs on the system.	
Step 9: Checking Subscribers	`show subscribers`	Display information about subscribers.	

Step 10: Checking the External DHCP IP Address on the SmartEdge router	`show dhcp relay server`
	`show dhcp relay server detail`
		Display summary or detailed DHCP relay or proxy statistics.	

Step 11: Displaying Subscriber Routes and the Route to the External DHCP Server	`show ip route subscriber`
	`show ip route`
		• Display subscriber IP addresses and routes.
		• Verify the route to the external DHCP server on the DHCP relay (SmartEdge router).	

Step 12: Checking All IP Routes on the Relay or Proxy	`show ip route summary`	Display summary information for all IP routes. If the "Act-Routes" are the same as "Max Ever Reached", the system is behaving correctly.	
Step 13: Verifying Hosts (DHCP clients) on the Relay or Proxy	`show dhcp relay hosts`	Display DHCP host clients on the DHCP relay or proxy. The `detail` option displays the internal and external circuit handle associated with the entry, the giaddr used to select the interface in the case of CLIPS hosts.	
Step 14: Examining ARP Entries	`show arp`	Display ARP entries.	
Step 15: Checking the Configuration	`show configuration dhcp`	Check the DHCP relay or proxy server configuration.	

Step 16:: Checking the DHCP Process on the Relay or Proxy	`show process dhcp`
	`show crashfiles`
		• Make sure the DHCP process is running on the relay or proxy
		• If the DHCP process is not running, check for a core dump.	

Step 17: Checking the RADIUS Server		If you have configured a RADIUS server, make sure the RADIUS attributes are configured correctly for your clients. For information about checking the RADIUS Server, see Troubleshooting the RADIUS Server.	
Step 18: Debugging the Relay or Proxy		**Caution**: Enabling the generation of debug messages can severely affect system performance.	

12.2 Step 1: Checking Specific Troubleshooting DHCP Proxy or Relay Issues

Check if you have a specific DHCP proxy or relay issue listed in the Troubleshooting Subscriber Connectivity on the Proxy or Relay section. If you do, use the procedure in this section to resolve your issue. If not, go to step 2.

12.3 Step 2: Navigating to the Correct Context

Use the **`show context all`** command and display all the contexts on your SmartEdge router and then navigate to the context you want to troubleshoot—in this case, the proxy in the `dhcp-proxy` context.

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

```
[local]Redback#show context all
Context Name    Context ID    VPN-RD     Description
----------------------------------------------------
local            0x40080001
dhcp-proxy       0x40080002

[local]Redback#
[local]Redback#context dhcp-proxy
[dhcp-proxy]Redback#
```

12.4 Step 3: Checking DHCP Relay or Proxy Statistics

Use the **`show dhcp relay stats`** command and check that DHCP discovery sent and DHCP offer received counters are about even. The SmartEdge router acting as a DHCP relay or proxy should normally receive an offer for every valid discovery message sent to the external DHCP server.

If, on the DHCP proxy or relay, the Discovery Sent counter is showing a number much less than the Offers Received counter, see Section 11 on page 113.

12.4.1 External DHCP Issues

The following section lists external DHCP issues:

- **Overloaded**—If the sent discover count is much larger than received offer count, investigate client retries on the DHCP proxy or relay.
- **Out of IP addresses**—If you are trying to bring up more clients than the number of addresses available, try adding more subnets or IP addresses.
- **Not Receiving Discovers**—When the external DHCP server is not receiving discovery messages, check the following:
  - The connectivity between the proxy or relay (SmartEdge router), and the external DHCP server.

- The subscriber links and any intermediate devices where the subscriber is connected.

- The DISCOVER messages between the proxy or relay (SmartEdge) and the external DHCP server are unicast, so they are routed; ensure the routing is correct. If the routing is not correct, check the configuration.

12.4.2 Relay or Proxy is Not Forwarding Discovery Messages to the External DHCP Server

Normally, the subscriber discovery messages are forwarded to the external DHCP server. When the SmartEdge router is acting as a relay or proxy and is not forwarding discovers to the external DHCP server, check the following on the DHCP relay or proxy:

- The configuration. If the bind subscriber command is used, check the status of the subscriber sessions by using **`show subscribers summary`** command in the correct context.

- That the SmartEdge router is not servicing the discovers; for example, due to an authentication failure.

- That the MAC address in the discover messages correspond with the devices in the network.

12.4.3 Example: Displaying DHCP Relay or Proxy Statistics

```
[dhcp-proxy]Redback#show dhcp relay stats

Current time: Wed Jul 29 08:44:20 2009
Last cleared: Wed Jul 29 08:21:10 2009
Packets Received      : 1865            Packets Relayed       : 1835

Packet received---------------------------------------------------------
DHCP Discover         : 104             DHCP Offer            : 100
DHCP Request          : 830             DHCP Decline          : 0
DHCP Ack              : 802             DHCP Nack             : 0
DHCP Release          : 0

Packet Sent-------------------------------------------------------------
DHCP Discover         : 103             DHCP Offer            : 100
DHCP Request          : 830             DHCP Decline          : 0
DHCP Ack              : 802             DHCP Nack             : 0
DHCP Release          : 0               Unknown Packet        : 0
BOOTP Request         : 0               BOOTP Reply           : 0
Tx server error       : 0               Tx client error       : 0

Split Lease-------------------------------------------------------------
Request handled       : 0               Ack sent              : 0
Lease misconfiguration: 0               Renewal failed        : 0
No server id for ack  : 0               No subnet mask for ack: 0
Sub lease timer expiry: 0

-----------------------------------------------------------------------

Dropped packets--------------------------------------------------------
Bad Ack               : 0               Internal Error        : 0
Bad Length            : 0               Bad Circuit           : 0
Bad Circuit UP        : 0               Bad Circuit Kern      : 0
Bad Circuit EOF       : 0               Bad Circuit slot      : 29
Bad Context           : 0                 Bad Server IP         : 0
No Server             : 0                 No Interface          : 0
Unbound Circuit       : 0                 Disabled Interface    : 0
Min Wait Error        : 0                 Max Hops Error        : 0
Bad IP                : 0                 Unknown Packet Type   : 0
Dropped Discover      : 0                 Dropped Request       : 0
Dropped Offer         : 0                 Dropped Ack           : 0
Dropped Release       : 0
del_pending_dropped   : 0                 EP Down               : 0
Error in Options      : 0                 max-addr dropped      : 0
non-clips mac         : 0                 Invalid mac-addr      : 0
MAC entry not found   : 0                 Dup cct-cfg entry     : 0
Mismatch ip/mac       : 0                 No renewal marked     : 0
Dropped invalid server: 0                 Bcast/Mcast mac       : 0
Context  not found    : 0                 Interface not found   : 0
Circuit not found     : 0                 Request entry not found: 0
Drop dup disc/del req : 0                 Drop dup discover     : 0
Throttle dropped disc : 0


Timers----------------------------------------------------------------
Server timeout        : 5                 Del Req               : 907
Lease timer exp       : 0                 cfg lease exp         : 0
Timer started         : 1936              Timer start failed    : 0
Timer stopped         : 1809

Input pack Q full (packet drops):: 0
Input pack Q (enqueued) count:: 1836
Input pack Q (dequeued) count:: 1836

Recovery Signalled count:: 0
Packet Receive Blocked count:: 0
Packet Processing Blocked count:: 0


[dhcp-proxy]Redback#show dhcp relay stats detail

Current time: Wed Jul 29 08:44:39 2009
Last cleared: Wed Jul 29 08:21:10 2009

Packets Received      : 1877              Packets Relayed       : 1847

Packet received--------------------------------------------------------
DHCP Discover         : 104               DHCP Offer            : 100
DHCP Request          : 836               DHCP Decline          : 0
DHCP Ack              : 808               DHCP Nack             : 0
DHCP Release          : 0

Packet Sent------------------------------------------------------------
DHCP Discover         : 103               DHCP Offer            : 100
DHCP Request          : 836               DHCP Decline          : 0
DHCP Ack              : 808               DHCP Nack             : 0
DHCP Release          : 0                 Unknown Packet        : 0
BOOTP Request         : 0                 BOOTP Reply           : 0
Tx server error       : 0                 Tx client error       : 0

Split Lease-----------------------------------------------------------
Request handled       : 0                 Ack sent              : 0
Lease misconfiguration: 0                 Renewal failed        : 0
No server id for ack  : 0                 No subnet mask for ack: 0
Sub lease timer expiry: 0

----------------------------------------------------------------------

Dropped packets------------------------------------------------------
Bad Ack               : 0                 Internal Error        : 0
Bad Length            : 0                 Bad Circuit           : 0
Bad Circuit UP        : 0                 Bad Circuit Kern      : 0
Bad Circuit EOF       : 0                 Bad Circuit slot      : 29
Bad Context           : 0                 Bad Server IP         : 0
No Server             : 0                 No Interface          : 0
Unbound Circuit       : 0                 Disabled Interface    : 0
Min Wait Error        : 0                 Max Hops Error        : 0
Bad IP                : 0                 Unknown Packet Type   : 0
Dropped Discover      : 0                 Dropped Request       : 0
Dropped Offer         : 0                 Dropped Ack           : 0
Dropped Release       : 0
del_pending_dropped   : 0                 EP Down               : 0
Error in Options      : 0                 max-addr dropped      : 0
non-clips mac         : 0                 Invalid mac-addr      : 0
MAC entry not found   : 0                 Dup cct-cfg entry     : 0
Mismatch ip/mac       : 0                 No renewal marked     : 0
Dropped invalid server: 0                 Bcast/Mcast mac       : 0
Context  not found    : 0                 Interface not found   : 0
Circuit not found     : 0                 Request entry not found: 0
Drop dup disc/del req : 0                 Drop dup discover     : 0
Throttle dropped disc : 0


Timers---------------------------------------------------------------
Server timeout        : 5                 Del Req               : 913
Lease timer exp       : 0                 cfg lease exp         : 0
Timer started         : 1948              Timer start failed    : 0
Timer stopped         : 1821

AAA------------------------------------------------------------------
IPH ADD sent          : 100               IPH DEL Sent          : 0
cct-cfg ADD sent      : 0                 cct-cfg DEL sent      : 0
IPH Reject rcvd       : 0                 Pending Del sent      : 0

Clips----------------------------------------------------------------
clips msg add         : 101               clips msg del         : 2
clips msg enq         : 103               clips throttle        : 0
clips resp msg        : 0                 clips del on resp     : 0
clips cct del mrk     : 0                 clips cct del         : 0
clips delete resp     : 0

ISM------------------------------------------------------------------
IPH Add Rcvd          : 100               IPH Del Rcvd          : 0
ism cct create        : 102               ism cct delete        : 1
ism cct up            : 103               ism cct down          : 9
ism cct bind          : 101               ism cct unbind        : 1
dhcp_cct_del          : 1                 IPH ADD matched       : 100
ism if create         : 9                 ism if delete         : 0
ism if down           : 0                 ism if up             : 9
ism port down         : 0                 ism port delete       : 0
ism clips group down  : 1                 ism clips group up    : 0
ism clips group delete: 0                 ism throttle hit      : 0

Interface Stale Processing:
 Create Stale Mark    : 0                  Create Stale Clear   : 0
 Up Stale Mark        : 0                  Up Stale Clear       : 0
 Bind Stale Mark      : 0                  Bind Stale Clear     : 0
 I/F Bind Stale       : 0                  I/F Up Stale         : 0
 I/F Create Stale     : 0

Circuit Stale Processing:
 Create Stale Mark    : 0                  Create Stale Clear   : 0
 Up Stale Mark        : 0                  Up Stale Clear       : 0
 Bind Stale Mark      : 0                  Bind Stale Clear     : 0
 Cct Bind Stale       : 0                  Cct Up Stale         : 0
 Cct Create Stale     : 0

ARP-----------------------------------------------------------------
Router id add sent    : 0                 Router id del sent    : 0
Router id add failed  : 0                 Router id del failed  : 0

Input pack Q full (packet drops):: 0
Input pack Q (enqueued) count:: 1848
Input pack Q (dequeued) count:: 1848

Recovery Signalled count:: 0
Packet Receive Blocked count:: 0
Packet Processing Blocked count:: 0
```

12.5 Step 4: Checking Relay or Proxy Port Counters

Use the **show port counters live** command to check port counters in real time on the SmartEdge router. Use the **detail** keyword to display detailed port counter information. For more information about this command, see Checking Port Status.

```
[dhcp-proxy]Redback#show port counters live

please wait...
Port Type
1/3 ethernet
packets sent : 25000 bytes sent : 40000
packets recvd : 60000 bytes recvd : 80000
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
2/4 ethernet
packets sent : 29000 bytes sent : 20000
packets recvd : 70000 bytes recvd : 30000
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
```

12.6 Step 5: Verifying the Status of Existing Sessions on the Relay or Proxy

Use the **show subscriber active** and **ping** commands to verify the status of existing sessions on the DHCP relay or proxy.

Note: When you ping the subscriber, it might not work because most subscribers have a firewall.

```
[dhcp-proxy]Redback#show subscribers active
00:0e:7b:d4:7f:93
        Circuit   2/6 clips 131096
        Internal Circuit   2/6:1023:63/7/2/24
        Interface bound  subs
        Current port-limit unlimited
        dhcp max-addrs 1 (applied)
        dhcp vendor class id MSFT 5.0 (applied)
        dhcp option client id 0x3d0701000e7bd47f93 (applied)
        dhcp option hostname 0x0c0a525249504c2d4d335850 (applied)
          IP host entries installed by DHCP: (max_addr 1 cur_entries 1)
                192.168.1.10    00:0e:7b:d4:7f:93

[dhcp-proxy]Redback#ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10): source 192.168.1.1, 36 data bytes,
timeout is 1 second
!!!!!

----192.168.1.10 PING Statistics----
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.592/2.907/5.351/1.486 ms
```

12.7 Step 6: Testing the DHCP Client and External DHCP Server

Ping the external DHCP server and client address (from the correct context) on the DHCP relay or proxy.

```
[dhcp-proxy]Redback#ping 10.0.0.1
PING 10.0.0.2 (10.0.0.1): source 10.0.0.1, 36 data bytes,
timeout is 1 second
!!!!!

----10.0.0.2 PING Statistics----
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.592/2.907/5.351/1.486 ms
```

12.8 Step 7: Checking Relay or Proxy Interfaces

Use the **show ip interface brief** to display what host IP addresses have been assigned and corresponding interface names on the DHCP relay or proxy. Make sure the interfaces are up.

```
[dhcp-proxy]Redback#show ip interface brief

Name              Address         MTU   State  Bindings
subs              192.168.1.1     1500  Up
toExtDHCPServer   10.0.0.1        1500  Up     ethernet 2/2
```

Recommended Action: If the interfaces are down, see Verifying Interfaces and Checking Port Performance.

12.9 Step 8: Checking Bindings on the Relay or Proxy

Use the **show bindings** command to check the configured bindings for one or more subscribers, ports, channels, or PVCs on the system. For information about this command, see Checking Bindings.

12.10 Step 9: Checking Subscribers on the Relay or Proxy

For information about how to check subscribers, see Displaying Information About My Subscribers.

12.11 Step 10: Checking the External DHCP Server IP Address on the SmartEdge Router

Use the **show dhcp relay server detail** command to display detailed information about the external DHCP server. Make sure that the SmartEdge router has the correct IP address. When you look at the output, make sure the "Server is available" and the "Route to the server available" status is "Yes". If it is not, the external DHCP server is not accessible to the DHCP proxy or relay.

```
[dhcp-proxy]Redback#show dchp relay server detail
DHCP Relay server     : 10.0.0.1
Minimum wait          : 0         Maximum hops    : 4
Server Group grid     : 0x1
Server group          : default
Server is available                    : Yes  // Make sure the state is set to Yes.
 Time of last reply                    : May 29 15:23:05
Route to the server available          : Yes  // Make sure the state is set to Yes.
Source ipaddress for server bound pkts: 10.0.0.1
Dhcp relay option (82) enabled         : FALSE
Stats-----------------------------------------------------
Discover Tx           : 10       Request Tx          : 1
Release Tx            : 0        Decline Tx          : 0
Offer Rx              : 2        Ack Rx              : 1
Nack Rx               : 0        No. of leases       : 2
```

12.12 Step 11: Displaying Subscriber Routes and the Route to the External DHCP Server

Use the **show ip route subscriber** command to display subscriber IP addresses and routes on the DHCP relay or proxy. Check where the subscriber is terminated. Make sure the IP address assigned to the subscriber is correctly installed in the routing table.

```
[dhcp-proxy]Redback#show ip route subscriber
Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
   A,H - derived hidden
   O    - OSPF, O3   - OSPFv3, IA - OSPF(v3) inter-area,
   N1   - OSPF(v3) NSSA external type 1, N2   - OSPF(v3) NSSA external type 2
   E1   - OSPF(v3) external type 1, E2   - OSPF(v3) external type 2
   I    - IS-IS, L1 - IS-IS level-1,  L2   - IS-IS level-2, N - NAT
   IPH - IP Host, SUB A - Subscriber address, SUB S - Subscriber static
   MIP F - Mobile-IP Foreign Agent, MIP H - Mobile-IP Home Agent
   A - Derived Default, MH - Media Nexthop
   >    - Active Route, * - LSP

Type     Network         Next Hop      Dist  Metric  UpTime   Interface
> SUB A  192.168.1.10/32 192.168.1.10  15    0       00:00:45 subs
```

Use the **show ip route** command to verify the route to the external DHCP server on the SmartEdge router. If the routes are statically configured, validate the configuration by using the **show configuration** command.

Confirm connectivity by pinging the IP address of the external DHCP server. For further confirmation, use the **show dhcp relay server detail** command.

```
[dhcp-proxy]Redback##show ip route 10.1.1.1

Longest match Routing entry for 10.1.1.1/24 is 10.1.1.1/24,
version 53
Route Uptime 03:22:05
Paths: total 1, best path count 1
Route has been downloaded to following slots 01/0
Path information :
Active path :
Known via adjacency, type-hidden route, distance 254,
metric 0, Tag 0, Next-hop 30.1.1.1, NH-ID 0x3110000B,
Adj ID: 0x5, Interface  Server_Int
Circuit 1/10:1023:63/1/1/12085
```

12.13 Step 12: Checking All IP Routes on the Relay or Proxy

Use the **show ip summary** command to display summary information for all IP routes on the DHCP relay or proxy. If the "Act-Routes" are the same as "Max Ever Reached", the SmartEdge router is working correctly.

```
[dhcp-proxy]Redback#show ip summary

load-balance: Use the built-in default hash function
Rt Tbl Version:      87, Nh Tbl Version: 42
FIB Rt Tbl Version:  87
Route Source  Tot-Routes   Act-Routes  Max Ever Reached
Connected     2            2           2
IP Host       1            1           1
```

12.14 Step 13: Verifying DHCP Clients on the Relay or Proxy

Use the **show dhcp relay hosts** command to verify DHCP clients on the DHCP relay or proxy. Use the **detail** keyword to view detailed information.

```
[dhcp-proxy]Redback#show dhcp relay host
Circuit          Host          Hardware address  Lease Ttl
2/6 clips 131075 192.168.1.10  00:0e:7b:d4:7f:93 600   382

Timestamp                Type  Context
Fri Aug 7 14:50:52 2009 Proxy dhcp-proxy


[dhcp-proxy]Redback##show dhcp relay hosts detail
-----------------------------------------------------
Displaying information for host: 100.1.1.50
MAC Address       : aa:bb:cc:00:00:00
Circuit           : 1/11
Context           : dhcp-proxy
Circuit Handle    : 1/11:1023:63/1/1/12083
Create time       : Fri Nov  4 05:53:08 2005
Type              : Proxy
Server            : 30.1.1.1
Lease             : 3600
giaddr            : 0.0.0.0  flags:            : 0x5805
helper flags      : 0xa    Standby helper flags: 0xa
Act. File Page #  : 0      Act. File Page Elem : 0
Sby. File Page #  : 0      Sby. File Page Elem : 0
```

12.15 Step 14: Examining ARP Entries on the Relay or Proxy

Use the **show arp** command to verify ARP entries on the DHCP relay or proxy.

12.16 Step 15: Checking Relay or Proxy Configuration Issues

Use the **show configuration dhcp** commands to check for DHCP relay or proxy configuration mismatches listed in Table 30. Make sure that you are in the correct context.

Table 30 Configuration DHCP Relay and DHCP Proxy Server Mismatch Checklist

#	Task	Checked?
1	Make sure that the external DHCP server has a route to the SmartEdge router multibind interface address/giaddr.	
2	Is the DHCP relay or proxy enabled on an interface?	
3	The interface used for binding the subscriber must have the multi-bind attribute.	

12.17 Step 16: Checking the DHCP Process on the Relay or Proxy

Use the **show process dhcp** command to verify that the DHCP process is running on the DHCP relay or proxy. For detailed information, use the **detail** keyword. If the DHCP process is not running, use the **show crashfiles** command to check if there is a core dump. If there is, contact your local technical support representative.

```
[dhcp-proxy]Redback# show process dhcp
NAME PID  SPAWN MEMORY TIME        %CPU  STATE UP/DOWN
dhcp 166  3     3436K  00:00:00.59 0.00% run   00:02:20
[local]Redback# show crashfiles
4844 Jul 4 16:02 /md/dhcpd_43.mini.core
5944456 Jul 4 16:02 /md/dhcpd_43.core
4812 Jul 4 16:03 /md/dhcpd_526.mini.core
5923992 Jul 4 16:03 /md/dhcpd_526.core
```

12.18 Step 17: Checking the RADIUS Server

If you have configured a RADIUS server, make sure the RADIUS attributes are correctly configured for your subscribers. For information about checking the RADIUS Server, see Troubleshooting the RADIUS Server.

12.19 Step 18: Debugging the DHCP Proxy or Relay

Use the **debug dhcp-relay** commands to enable the generation of debug messages for the SmartEdge router acting as a DHCP relay or proxy.

debug [{**boot** {**active** | **standby**} | **switchover**}] **dhcp-relay** {**aaa** | **all** | **arp** | **clips** | **configuration** | **exception** | **file** | **general** | **helper** | **ipc** | **ism** | **packet** | **rcm** | **show** | **timer**}

no debug [{**boot** {**active** | **standby**} | **switchover**}] **dhcp-relay** {**aaa** | **all** | **arp** | **clips** | **configuration** | **exception** | **file** | **general** | **helper** | **ipc** | **ism** | **packet** | **rcm** | **show** | **timer**}

Table 31 DHCP relay or proxy events

Keyword	Description
`boot`	Optional. Enables the generation of debug messages during a system reload.
`active`	Enables the generation of debug messages for the active controller card.
`standby`	Enables the generation of debug messages for the standby controller card.
`switchover`	Optional. Enables the generation of debug messages during a switchover from the active to the standby controller.
`aaa`	Enables the generation of debug messages for authentication, authorization, and accounting (AAA) events.
`all`	Enables the generation of debug messages for all DHCP relay or proxy events.
`arp`	Enables the generation of debug messages for DHCP relay or proxy Address Resolution Protocol (ARP) events.
`clips`	Enables the generation of debug messages for DHCP relay or proxy clientless IP service selection (CLIPS) events.
`configuration`	Enables the generation of debug messages for the DHCP relay or proxy configuration.
`exception`	Enables the generation of debug messages for DHCP relay or proxy exception events.
`file`	Enables the generation of debug messages for DHCP relay or proxy file events.
`general`	Enables the generation of debug messages for DHCP relay or proxy general events.
`helper`	Enables the generation of debug messages for DHCP relay or proxy helper events.
`ipc`	Enables the generation of debug messages for DHCP relay or proxy interprocess communication (IPC) events.
`ism`	Enables the generation of debug messages for DHCP relay or proxy Interface and Circuit State Manager (ISM) events.
`option`	Enables the generation of debug messages for option events for the DHCP relay or proxy.
`packet`	Enables the generation of debug messages for DHCP relay or proxy packet events.
`rcm`	Enables the generation of debug messages for DHCP relay or proxy Router Configuration Manager (RCM) events.
`show`	Enables the generation of debug messages for DHCP relay or proxy for show commands related events.
`timer`	Enables the generation of debug messages for DHCP relay or proxy timer events.

Note: The SmartEdge 100 router does not support the **`standby`** and **`switchover`** keywords.

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

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

Note: For more information about **`logging`** and the **`terminal monitor`** commands, see the *Command List*.

Caution!

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

Use the **`no debug`** command to disable debug messages.

12.19.1 Debugging the SmartEdge Router Acting as a Relay or Proxy

Use the **`debug dhcp-relay exception`**, **`debug dhcp-relay all`**, and **`debug dhcp-relay packet`** commands to verify that the relay packets are reaching the DHCP relay or proxy.

When you issue these debug commands, check for the following messages in the log files:

- The DHCP relay or proxy received the DHCP request from the subscriber.
- Cannot get server IP address or no route.
- Packets are being dropped.

To debug the SmartEdge router acting as a DHCP relay or proxy:

1. Connect by Telnet to the SmartEdge router acting as a DHCP relay or proxy.
2. Navigate to the correct context.
3. Enable the **`terminal monitor`** command to view messages on your Telnet session.

Warning!

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

4. Use the **`debug dhcp-relay exception`** command.

5. Capture and examine the log file for exceptions.

6. If you need more information about the cause of the exceptions, use the **`debug dhcp-relay all`** command.

7. If the output does not provide enough information about the cause of the exception, turn off debugging for DHCP relay events using the **`no debug dhcp-relay all`** command.

8. Use the **`debug dhcp-relay packet`** command to enable debugging messages on DHCP relay packets.

9. Capture and examine the log file.

12.19.2 Checking for Proxy or Relay Exceptions

The following example displays results from the **`debug dhcp-relay exception`** command:

```
[dhcp-proxy]Redback#debug dhcp-relay exception
[dhcp-proxy]Redback#terminal monitor
Mar 4 15:46:03: %CSM-6-PORT: ethernet 3/11 link state DOWN, admin is UP
Mar 4 15:46:03: %LOG-6-PRI_STANDBY:
Mar 4 15:46:03: %CSM-6-PORT : ethernet 3/11 link state DOWN, admin is UP
Mar 4 15:46:37: [0002]: [3/2:1023:63/1/2/48]: %DHCP-7-PKT_E:
Can't get server IP addressr or no route
Mar 4 15:46:41: [0002]: [3/2:1023:63/1/2/48]: %DHCP-7-PKT_E:
Can't get server IP addressr or no route
Mar 4 15:46:49: [0002]: [3/2:1023:63/1/2/48]: %DHCP-7-PKT_E:
Can't get server  IP addressr or no route
Mar 4 15:46:59: %LOG-6-PRI_STANDBY: Mar 4 15:46:59: %CSM-6-PORT:
 ethernet 3/11 link state UP, admin is UP
Mar 4 15:46:59: %CSM-6-PORT: ethernet 3/11 link state UP, admin is UP
```

12.19.3 Using the Circuit Level Debug Command

The following example show how to enable the generation of all DHCP relay or proxy debug messages on circuit handle `14/1:1023:63/2/2/1`:

```
[local]Redback#debug circuit handle 14/1:1023:63/2/2/1
[local]Redback#debug circuit dhcp-relay all
[local]Redback#show debug circuit     //Shows circuits that
Circuit debugging:                    //have debug messages enabled.
14/1:1023:63/2/2/1
```

Note: To find a circuit handle, use one of the following commands:

- **`show subscribers active username`** ***`username`***
- **`show circuit username`** ***`username`*** **`detail`**

13 Troubleshooting the Internal DHCP Server

When you troubleshoot the SmartEdge router acting as an internal DHCP server, there are two main areas to investigate:

1. The DHCP connection towards the subscriber (subscriber connection).

2. The internal DHCP server function within the SmartEdge router.

Note: When you reload the SmartEdge router, the external micro-drive must be present to preserve leases.

The following is a sample configuration for the SmartEdge router that is acting as an internal DHCP server, in context `internal-DHCP`. This configuration maps to the tasks listed in Tasks to Troubleshoot Internal DHCP Server Issues.

```
context internal-DHCP
 interface forSubs multibind
  ip address 1.1.1.1/24
  ip address 1.1.2.1/24 secondary
  dhcp server interface
  ip arp secured-arp
 aaa authentication subscriber none
 subscriber default
   dhcp max-addrs 1
!
dhcp server policy
   default-lease-time 900
   maximum-lease-time 900
   subnet 1.1.1.0/24
     range 1.1.1.1 1.1.1.20
     default-lease-time 1000
     option router 1.1.1.1
   subnet 1.1.2.0/24
     range 1.1.2.100 1.1.2.200
     option router 1.1.2.1
     mac-address 00:dd:00:00:00:01 ip-address 1.1.2.210
port ethernet 1/3
 no shutdown
 encapsulation dot1q
 dot1q pvc 501
  bind subscriber  user1@internal-DHCP
 dot1q pvc 502
  bind interface forSubs internal-DHCP
 dot1q pvc 503
  service clips dhcp maximum 1000 context internal-DHCP
```

13.1 Tasks to Troubleshoot Internal DHCP Issues

Use Table 32 as a guide to troubleshooting internal DHCP server issues when the SmartEdge router is acting as an internal DHCP server. When your are troubleshooting the internal DHCP server on the SmartEdge router, there are two main areas to investigate:

1. The DHCP connection towards the subscriber (subscriber connection).

2. The internal DHCP server function within the SmartEdge router.

Before you begin, get a description of the problem and check if you (or the customer) made any recent changes or upgrades to the network. For information about troubleshooting specific DHCP issues on the proxy or relay, see Troubleshooting Subscriber Connectivity on the Proxy or Relay.

Note: When you reload the SmartEdge router, the external micro-drive must be present to preserve leases.

Table 32 Tasks to Troubleshoot Internal DHCP Issues

Task	Command	Notes	Checked?

Step 1: Navigating to the Correct Context	`show context all`
	`context` *`context-name`*
		Display all the contexts on your router and then navigate to the context you want to troubleshoot.	

Step 2: Verifying Internal DHCP Statistics	`show dhcp server stats`	Check that the DHCP discovers received and offers sent are increasing.	
Step 3: Checking Port Counters	`show port counters`	Verify the packets are received and sent to the port.	
Step 4: Checking Interfaces	`show ip interface brief`	Make sure the interfaces are up.	
Step 5: Checking Bindings	`show bindings summary`	Display the configured bindings for one or more subscribers, ports, channels, or PVCs on the system.	
Step 6: Verifying that the Circuit is Present on the Internal DHCP Server	`show dhcp server host`	Verify if the circuit is present and if it is waiting for the IP address	
Step 7: Verifying Leases on the Internal DHCP Server	`show dhcp server lease count`	Determine if you are receiving enough leases for all your clients.	
Step 8: Checking Subscribers	`show subscribers`	Display information about subscribers.	
Step 9: Displaying Summary IP Route Information on the Internal DHCP Server	`show ip summary`	Display summary information for all IP routes on the Internal DHCP server.	

Step 10: Displaying Subscriber Routers and the Route to the Internal DHCP Server	`show ip route subscriber`
	`show ip route`
		Verify subscriber routes and the route to the internal DHCP server.	

Step 11: Verifying ARP Entries	`show arp`	Examine ARP entries.	

Table 32 Tasks to Troubleshoot Internal DHCP Issues

Task	Command	Notes	Checked?

Step 12: Checking the DHCP Process on the Internal DHCP Server	`show process dhcp`
	`show crashfiles`
		• Check DHCP process.
		• Displays the size, location, and name of any crash files located on the system. Check for a core dump.	

Step 13: Checking the Internal DHCP Server Configuration	`show configuration dhcp`
	`show subscribers active`
		• Check configuration.
		• Check the status of active subscribers.	

Step 14: Checking the RADIUS Server		If you have a RADIUS server configured, make sure the RADIUS attributes are configured correctly for your clients. For information about checking the RADIUS Server, see Troubleshooting the RADIUS Server.	
Step 15: Debugging the Internal DHCP Server		**Caution**: Enabling the generation of debug messages can severely affect system performance.	

13.2 Step 1: Navigating to the Correct Context

Use the **show context all** command and display all the contexts on the SmartEdge router that is acting as an internal DHCP server and then navigate to the context you want to troubleshoot—in this case, the `internal-DHCP` context.

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

```
[local]Redback#show context all
Context Name          Context ID    VPN-RD   Description
-------------------------------------------------------
local                 0x40080001
internal-DHCP         0x40080002

[local]Redback#
[local]Redback#context internal-DHCP
[internal-DHCP]Redback#
```

13.3 Step 2: Verifying Internal DHCP Server Statistics

Use the **show dhcp server stats** command on the SmartEdge router acting as an internal DHCP server and check that the DHCP discovery messages received and offer messages sent are increasing. The SmartEdge router should normally send an offer for every valid discover received.

The following lists reasons why the SmartEdge router is not receiving, responding, or servicing discovery messages:

- Not Receiving Discovers—This is typically a Layer 2 issue on the access network, or the expected interface to receive DHCP discovers is not configured for DHCP.

- Not Responding to the Discovers—Misconfiguration on the SmartEdge router; for example, incorrect subnet definition on the DHCP server policy.

- Is the SmartEdge router not servicing discovers; for example, due to an authentication failure?

If the Discover Received counter is much larger than the Offers Sent counter, the SmartEdge router could be:

- Overloaded—Verify that the process to see if the DHCP daemon is using too much of the CPU; client links could be flapping (coming up and down continuously), which can spike the process.

- Out of IP Addresses—Add either more multibind interfaces with additional subnets for the internal DHCP server.

Use the **show dhcp server stats** command to display internal DHCP server statistics.

The following example displays internal DHCP server statistics for the specified circuit:

```
[internal-DHCP]Redback#show dhcp server stats circuit 11/4 vlan-id 10
Current time: Fri Aug  4 17:49:44 2006

Last cleared: Never
Internal Circuit Handle: 11/5:1023:63/1/2/10
Discovers Received    : 0          Requests Received     : 0
Releases Received     : 0          Declines Received     : 0
Renewal REQs Received : 0
Offers Sent           : 0          ACKs Sent             : 0
Renewal ACKs Sent     : 0
```

The following example displays internal DHCP server statistics for the specified interface:

```
[internal-DHCP]Redback#show dhcp server stats context c1 interface i1
Current time: Fri Aug  4 17:49:46 2006
Last cleared: Never
Discovers Received    : 0            Requests Received     : 0
Release Received      : 0            Decline Received      : 0
Renewal REQs Received : 0
Offers Sent           : 0            ACKs Sent             : 0
Renewal ACKs Sent     : 0
```

13.4 Step 3: Checking Port Counters

Use the **show port counters live** command to check the port counters in real time on the internal DHCP server. Use the **detail** keyword to display detailed port counter information. For more information about this command, see Checking Port Performance.

```
[internal-DHCP]Redback#show port counters live
please wait...
Port Type
1/3 ethernet
packets sent : 25000 bytes sent : 40000
packets recvd : 60000 bytes recvd : 80000
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
2/4 ethernet
packets sent : 29000 bytes sent : 20000
packets recvd : 70000 bytes recvd : 30000
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
```

13.5 Step 4: Checking Interfaces on the Internal DHCP Server

On the internal DHCP server, use the **show ip interface brief** to display what host IP addresses have been assigned and corresponding interface names. Make sure the interfaces are up.

```
[internal-DHCP]Redback#show ip interface brief
Name  Address      MTU  State  Bindings
subs  192.168.1.1  1500 Up
```

Recommended Action: If the interfaces are down, see Verifying Interfaces and Checking Port Performance.

13.6 Step 5: Checking Bindings

Use the **`show bindings`** command verify your bindings on the internal DHCP server. For information about this command, see Section 2.7 on page 20.

13.7 Step 6: Verifying that the Circuit is Present on the Internal DHCP Server

Use the **`show dhcp server host`** command to display information about the hosts (subscribers) and their leases. Check that the circuit is present and whether it is waiting for the IP address. When the circuit you are examining is not present, the DHCP session is not up.

For example, if the ATM PVC is down, examine the fault at the circuit level by using the **`show subscribers log username`** ***`username`*** to determine if the circuit has been created and authenticated.

If the circuit is present, the circuit is up. If there is no IP address, and the circuit is up but no IP has been assigned, check the internal DHCP server. If the IP address is present, there is no fault because the IP has been sent to the subscriber.

```
[internal-DHCP]Redback#show dhcp server host
Circuit          Host        Hardware address   Lease Ttl
2/6 clips 131078 192.168.2.2 00:0e:7b:d4:7f:93  7200  7131

Timestamp               Type   Context
Fri Aug 7 15:01:06 2009 Server internal-DHCP
```

13.8 Step 7: Verifying Leases on the Internal DHCP Server

Use the **`show dhcp server lease count`** command to determine if the number of leases matches the expected number for your subscribers. If you do not have the expected number of leases, begin debugging the SmartEdge router acting as an internal DHCP server.

For information about debugging the internal DHCP server, see Debugging the Internal DHCP Server.

```
[internal-DHCP]Redback##show dhcp server lease count
Number of leases is 150
```

13.9 Step 8: Checking Subscribers

For information about how to check subscribers, see Displaying Information About My Subscribers.

13.10 Step 9: Displaying Summary IP Route Information on the Internal DHCP Server

Use the **`show ip summary`** command to display summary information for all IP routes on the internal DHCP server. If "Act-Routes" is the same as "Max Ever Reached", the system is working correctly:

```
[internal-DHCP]Redback#show ip summary

load-balance: Use the built-in default hash function
Rt Tbl Version:      87, Nh Tbl Version: 42
FIB Rt Tbl Version:  87
Route Source Tot-Routes  Act-Routes  Max Ever Reached
Connected    2           2           2
IP Host      1           1           1
```

13.11 Step 10: Displaying Subscriber Routes and the Route to the Internal DHCP Server

Use the **`show ip route`** command to verify the route to the internal DHCP server and to ensure that routes have been learned from the other parts of the network. If the routes are statically configured, validate the configuration by using the **`show configuration`** command.

```
[internal-DHCP]Redback##show ip route 30.1.1.1
Longest match Routing entry for 30.1.1.1/32 is 30.1.1.1/32, version 53
Route Uptime 03:22:05
Paths: total 1, best path count 1
Route has been downloaded to following slots
01/0
Path information :
Active path :
Known via adjacency, type-hidden route, distance 254, metric 0,
Tag 0, Next-hop 30.1.1.1, NH-ID 0x3110000B, Adj ID: 0x5, Interface   Server_Int
Circuit 1/10:1023:63/1/1/12085
```

Use the **`show ip route subscriber`** command to display subscriber IP addresses and routes. Check where the subscriber is terminated. Make sure that the assigned IP address is correctly installed in the routing table.

```
[internal-DHCP]Redback#show ip route subscriber
Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
   A,H - derived hidden
   O   - OSPF, O3  - OSPFv3, IA - OSPF(v3) inter-area,
   N1  - OSPF(v3) NSSA external type 1, N2  - OSPF(v3) NSSA external type 2
   E1  - OSPF(v3) external type 1, E2  - OSPF(v3) external type 2
   I   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2, N - NAT
   IPH - IP Host, SUB A - Subscriber address, SUB S - Subscriber static
   MIP F - Mobile-IP Foreign Agent, MIP H - Mobile-IP Home Agent
   A - Derived Default, MH - Media Nexthop
   >   - Active Route, * - LSP

Type     Network         Next Hop      Dist  Metric  UpTime   Interface
> SUB A  192.168.1.10/32 192.168.1.10  15    0       00:00:45 subs
```

13.12 Step 11: Verifying ARP Entries

Use the **show arp** command to examine ARP entries related to circuits on the internal DHCP server. Check that the subscriber MAC address and the circuit are bound to the correct interface and port.

```
[internal-DHCP]Redback#show arp
```

13.13 Step 12: Checking the DHCP Process on the Internal DHCP Server

Use the **show process dhcp** command to verify that the DHCP process is running on the internal DHCP server. For detailed information, use the **detail** keyword . If the DHCP process is not running, use the **show crashfiles** command to check for a core dump. If one exists, contact your technical support representative.

```
[internal-DHCP]Redback# show process dhcp
NAME PID  SPAWN MEMORY TIME        %CPU  STATE UP/DOWN
dhcp 166  3     3436K  00:00:00.59 0.00% run   00:02:20

[internal-DHCP]Redback# show crashfiles
4844 Jul 4 16:02 /md/dhcpd_43.mini.core
5944456 Jul 4 16:02 /md/dhcpd_43.core
4812 Jul 4 16:03 /md/dhcpd_526.mini.core
5923992 Jul 4 16:03 /md/dhcpd_526.core
```

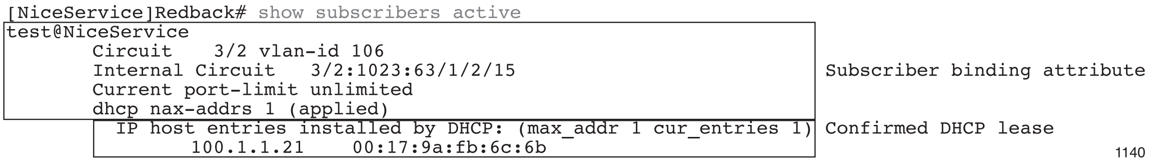
13.14 Step 13: Checking the Internal DHCP Server Configuration

Use the **show configuration dhcp** command to check for DHCP server configuration mismatches listed in Table 33. Make sure that you are in the correct context.

Table 33 Internal DHCP Server Configuration Checklist

#	Task	Checked?
1	Is the DHCP server enabled on an interface?	
2	Is a DHCP server configured in the correct context?	
3	Does the interface used for binding the subscriber have the multi-bind attribute?	
4	If the server is configured to give out leases from a shared network pool, is the corresponding interface in the SmartEdge router configured with the primary and or secondary IP addresses in that range?	

The following illustration identifies the **show subscribers active** command output fields for a DHCP lease for subscriber that has no issues.



```
[NiceService]Redback# show subscribers active
test@NiceService
        Circuit    3/2 vlan-id 106
        Internal Circuit   3/2:1023:63/1/2/15
        Current port-limit unlimited
        dhcp nax-addrs 1 (applied)
          IP host entries installed by DHCP: (max_addr 1 cur_entries 1)
                100.1.1.21    00:17:9a:fb:6c:6b
```

Figure 13 Show Subscribers Active Command Output Fields—DHCP Lease

Recommend Action: If this command does not display any IP addresses:

1. Check if the DHCP daemon knows about any leases for this subscriber by using the **show dhcp server hosts mac-address *mac-address*** command.

2. If the DHCP daemon also does not have a lease for this subscriber, the DHCP session for this subscriber is not up; debug the DHCP session for this subscriber.

13.15 Step 14: Checking the RADIUS Server

If you have configured a RADIUS server, make sure the RADIUS attributes are correctly configured for your subscribers. For information about checking the RADIUS server, see Section 15 on page 159.

13.16 Step 15: Debugging the Internal DHCP Server

Use the **debug dhcp-server** command to enable tdebug messages for internal DHCP server events.

debug [{**boot** {**active** | **standby**} | **switchover**}] **dhcp-server** {**aaa** | **all** | **arp** | **clips** | **configuration** | **exception** | **file** | **general** | **helper** | **ipc** | **ism** | **packet** | **rcm** | **timer**}

no debug [{**boot** {**active** | **standby**} | **switchover**}] **dhcp-server** {**aaa** | **all** | **arp** | **clips** | **configuration** | **exception** | **file** | **general** | **helper** | **ipc** | **ism** | **packet** | **rcm** | **timer**}

Table 34 Internal DHCP Debugging Commands

Event	Description
boot	Optional. Enables the generation of debug messages during a system reload.
active	Enables the generation of debug messages for the active controller card.
standby	Enables the generation of debug messages for the standby controller card.
switchover	Optional. Enables the generation of debug messages during a switchover from the active to the standby controller.
aaa	Enables the generation of debug messages for authentication, authorization, and accounting (AAA) events for internal DHCP servers.
all	Enables the generation of debug messages for all internal DHCP server events.
arp	Enables the generation of debug messages for internal DHCP server Address Resolution Protocol (ARP) events.
clips	Enables the generation of debug messages for internal DHCP server clientless IP service selection (CLIPS) events.
configuration	Enables the generation of debug messages for the internal DHCP server configuration.
exception	Enables the generation of debug messages for internal DHCP server exception events.
file	Enables the generation of debug messages for internal DHCP server file events.
general	Enables the generation of debug messages for internal DHCP server general events.
helper	Enables the generation of debug messages for internal DHCP server helper events.
ipc	Enables the generation of debug messages for internal DHCP server interprocess communication (IPC) events.
ism	Enables the generation of debug messages for internal DHCP server Interface and ISM events.
option	Enables the generation of debug messages for internal DHCP server option events.
packet	Enables the generation of debug messages for internal DHCP server packet events.
rcm	Enables the generation of debug messages for internal DHCP server Router Configuration Manager (RCM) events.
timer	Enables the generation of debug messages for internal DHCP server timer events.

Caution!

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

Note: The SmartEdge 100 router does not support the **`standby`** and **`switchover`** keywords.

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

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

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

Note: For more information about **`logging`** commands and the **`terminal monitor`** command, see the *Command List*.

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

13.16.1 Circuit Level Debug Internal DHCP Server Commands

The following example show how to enable the generation of all internal DHCP server debug messages on circuit handle `14/1:1023:63/2/2/1`:

```
[local]Redback#debug circuit handle 14/1:1023:63/2/2/1
[local]Redback#debug circuit dhcp-server packet
[local]Redback#show debug circuit  //Shows circuits that have debug messages enabled.
Circuit debugging:
14/1:1023:63/2/2/1
```

13.16.2 Debugging an Internal DHCP Server

To debug an internal DHCP server:

1. Connect by Telnet to the SmartEdge router acting as an internal DHCP server.

2. Navigate to the correct context.

3. Enable the **`terminal monitor`** command to view messages on your Telnet session.

Warning!

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

4. Use the **`debug dhcp-server exception`** command.

   Examine the log for exceptions; look for failed log messages.

5. If the debug output does not provide enough information about the cause of the exception, use the **`debug dhcp-server all`** command to obtain more information about the cause. This command enables the generation of debug messages for all internal DHCP server events.

6. Use the **`show debug`** command to display which debug features are enabled.

7. Use the **`show log | grep dhcp`** command to filter your results so that you view only internal DHCP server messages.

8. If the debug output does not provide enough information about the cause of the exception, use the **`no debug dhcp-server all`** command to disable debugging.

9. Use the **`debug dhcp-server packet`** command to enable debugging for internal DHCP server packet events.

10. Examine the log for exceptions; look for failed log messages.

11. Capture and examine the log file for exceptions and the cause of the failure.

13.17 Claiming Back a DHCP IP Address

To claim back a DHCP IP address:

1. Navigate to the context in which the SmartEdge router is configured to act as an internal DHCP server or proxy.

2. If the IP address for the subscriber MAC is not known, use the **`show dhcp [server | relay] host mac-address`** ***`mac-addr`*** command to get the IP address.

3. Clear the host and reclaim the IP address by using **`clear dhcp host`** ***`ip-address`*** command.

Caution!

When the IP address is reclaimed back, all subscriber traffic associated with this IP address is discarded.

14 Troubleshooting General CLIPS Issues

This section shows you how to troubleshoot general CLIPS issues.

The following is a sample CLIPS configuration. This configuration maps to the tasks listed in Tasks to Troubleshoot CLIPS Issues.

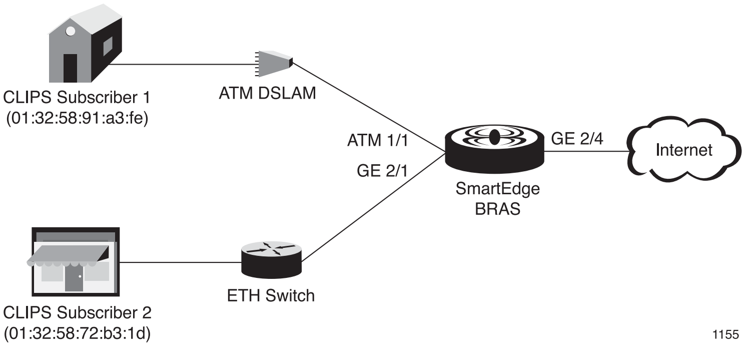


Figure 14 CLIPS Network Topology

```
context isp2.net
 interface forSubs multibind
  ip address 1.2.1.1/24
  dhcp server interface
  ip arp secured-arp
 interface toInternet
  ip address 2.1.1.2/24
 ip route 0.0.0.0/0 2.1.1.1.254
 aaa authentication subscriber local
 subscriber default
   dhcp max-addrs 1
 subscriber name 01:32:58:72:b3:1d
  password Redback
 subscriber name 01:32:58:91:a3:fe
  password Redback
 dhcp server policy
  default-lease-time 900
  maximum-lease-time 900

  subnet 1.2.1.0/24
   range 1.2.1.2 1.2.1.200
   default-lease-time 1000
   option router 1.2.1.1
!
atm profile ubr
 shaping ubr
port atm 1/1
 no shutdown
 atm pvc 1 34 profile ubr encapsulation bridge1483
  service clips dhcp maximum 1 context isp2.net
port ethernet 2/1
 no shutdown
 encapsulation dot1q
 dot1q pvc 33
  service clips dhcp maximum 10 context isp2.net
port ethernet 2/4
 no shutdown
 bind interface toInternet isp2.net
```

14.1 Tasks to Troubleshoot CLIPS Issues

Use Table 35 as a guide to troubleshooting CLIPS issues. Before you begin, get a description of the problem and check if any recent changes or upgrades were made to the network.

Table 35 Tasks to Troubleshoot CLIPS Issues

Task	Command	Notes	Checked?

Step 1: Navigating to the Correct Context	`show context all`
	`context context-name`
		Display all the contexts on your router and then navigate to the context you want to troubleshoot.	

Step 2: Checking Port Counters	`show port counters live`	Check packet counters on the port.	

Step 3: Displaying CLIPS Counters	`show clips counters`
	`show clips counters detail`
		• Display counters for a single static CLIPS PVC
		• Displays detailed counters CLIPS information.	

Step 4: Checking CLIPS Circuit Counters	`show circuit counters clips`	Display packet statistics for CLIPS circuits.	
Step 5: Checking Interfaces	`show ip interface brief`	Make sure the interfaces are up.	
Step 6: Checking Bindings	`show bindings`	Display the configured bindings for one or more subscribers, ports, channels, or PVCs on the system.	
Step 7: Displaying Summary of CLIPS Sessions	`show clips summary`	Check for a large number of CLIPS sessions that are starting, down, or awaiting IP address.	
Step 8: Displaying All Dynamic CLIPS Sessions	`show clips dhcp`	Display dynamic CLIPS sessions.	
Step 9: Displaying CLIPS Sessions that are Down	`show clips all down`	Display CLIPS sessions that are down.	
Step 10: Check Why CLIPS is Not Coming Up	`show dhcp server lease mac-address mac-address`		
Step 11: Checking Subscribers	`show subscribers`	Display subscriber information.	
Step 12 Checking All IP Routes	`show ip route summary`	Display summary information for all IP routes.	
Step 13: Displaying CLIPS Group	`show clips-group`	If you have configured a CLIPS group, issue show clips-group command.	
Step 14: Checking ARP Entries	`show arp`	Display ARP entries.	

Step 15: Checking CLIPS Process	`show process clips`
	`show crashfiles`
		• Verify that the CLIPS process is running.
		• If CLIPS is not running, check for a core dump.	

Step 16: Checking the Configuration	`show configuration`	Display the configuration.	

Table 35 Tasks to Troubleshoot CLIPS Issues

Task	Command	Notes	Checked?
Step 17: Checking the RADIUS Server		If you have configured a RADIUS server, make sure the RADIUS attributes are correctly are configured for your subscribers. For information about checking the RADIUS server, see Troubleshooting the RADIUS Server.	
Step 18: Debugging CLIPS		**Caution**: Enabling the generation of debug messages can severely affect system performance.	

14.2 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 isp2.net.

The following example shows how to view all contexts on your router and then navigate to context isp2.net:

```
[local]Redback#show context all
Context Name        Context ID     VPN-RD  Description
------------------------------------------------------
local               0x40080001
isp2.net            0x40080002
[local]Redback#
[local]Redback#context isp2.net
[isp2.net]Redback#
```

14.3 Step 2: Checking Port Counters

Use the **show port counter live** command to check port statistics. For information about this command, see Checking Port Status.

```
[isp2.net]Redback#show port counters live

please wait...
Port            Type
1/1             ATM
packets sent       : 15000          bytes sent     : 20000
packets recvd      : 10000          bytes recvd    : 50000
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
2/1           ethernet
packets sent       : 25000          bytes sent     : 40000
packets recvd      : 60000          bytes recvd    : 80000
send packet rate   : 0.00       send bit rate      : 0.00
recv packet rate   : 0.00       recv bit rate      : 0.00
2/4           ethernet
packets sent       : 25000          bytes sent     : 40000
packets recvd      : 60000          bytes recvd    : 80000
send packet rate   : 0.00       send bit rate      : 0.00
recv packet rate   : 0.0        recv bit rate      : 0.00
rate refresh interval : 60 seconds
```

14.4 Step 3: Displaying CLIPS Counters

Use the **`show clips counter`** command to display CLIPS information. To view detailed CLIPS information, use the **`detail`** keyword.

```
[isp2.net]Redback#show clips counters detail

Mon Jun 28 18:56:16 2005
Authen Success          12405      Authen Failure      0
 Session Up             12405      Session Down        0
DHCP---------------------------------------------------
 Create Rcvd            13525      Delete Rcvd         0
 Re-Create Rcvd          1012
SessionThrottling--------------------------------------
 Starting                 108      DHCP Denied      1012
DHCP_CreateFail-----------------------------------------
 Denied (limit)          1012      Parent Not Found     0
 Circ. Create fail          0      No Memory            0
 Duplicate MAC              0
DHCP_DeleteFail------------------------------------------
Circ. not found             0
Circuit--------------------------------------------------
 Create                 12513      Delete               0
CircuitCreateFail----------------------------------------
 No Memory                  0      Parent Limit         0
 Handle Create              0      Table Insert         0
 Retry Authen               0      Reserve Handle       0
 Bad Parent Encaps          0
ISM------------------------------------------------------
 Msg Ignored                0
```

14.5 Step 4: Checking CLIPS Circuit Counters

Display circuit counters for all CLIPS sessions within a port:

```
[isp2.net]Redback#show circuit counters 3/1 clips

Circuit               Packets/Bytes Sent  Packets/Bytes Received
3/1 clips 131074      124                 128
                      6114                7962
```

Display circuit counters for a specific CLIPS session within a port:

```
[isp2.net]Redback#show circuit counters 3/1 clips 131074

Circuit               Packets/Bytes Sent  Packets/Bytes Received
3/1 clips 131074      127                 131
                      6240                8142
```

14.6 Step 5: Checking Interfaces

Use the **`show ip interface brief`** command to check that your interfaces are up. When a CLIPS subscriber interface has no active subscribers, the interface is shown as unbound.

Recommended Action: If the interfaces are down, see Verifying Interfaces and Checking Port Performance.

14.7 Step 6: Checking Bindings

Use the **show bindings** command to verify your bindings. For information about this command, see Checking Bindings.

14.8 Step 7 Displaying Summary of CLIPS Sessions

Use the **show clips summary** command to check if there are large number of CLIPS sessions that are starting, down, or awaiting an IP address. This might indicate significant network churn, or the DHCP server might be responding slow:

```
[ip2.net]Redback#show clips summary

Wed Mar 12 19:23:05 2008
Dynamic circuits  1       Static circuits       0
Sessions up       1       Sessions down         0
Sessions starting 0       Sessions awaiting IP  0
```

14.9 Step 8: Displaying All Dynamic CLIPS Sessions

Use the **show clips dhcp** command to display all dynamic CLIPS sessions.

14.10 Step 9: Displaying CLIPS Sessions that are Down

Use the **show clips down** command to display CLIPS sessions that are down.

14.11 Step 10: Checking Why CLIPS Sessions Are Not Up

Use the **show dhcp server lease mac-address *mac-address*** command to determine why CLIPS is not coming up. For information about how to troubleshoot the internal DHCP server proxy, or relay, see:

- Troubleshooting the Internal DHCP Server
- Troubleshooting General DHCP Proxy or Relay Issues
- Troubleshooting Subscriber Connectivity on the Proxy or Relay

The following example shows expected output when CLIPS is coming up. If CLIPS is not coming up, the output displays an error message indicating the cause.

```
[isp2.net]Redback#show dhcp server lease mac-address 00:dd:00:00:00:01
---------------------------------------------------------------------
Displaying information for host: 1.2.1.16
MAC Address          : 00:dd:00:00:00:01
Circuit              : 5/1 vlan-id 10 clips 131079
Context              : isp2.net
Circuit Handle       : 5/1:1023:63/7/2/7
Create time          : Thu Sep  1 13:28:47 2005
Type                 : Server
Server               : 1.2.1.1
Lease                : 3000          Ttl                 : 2180
giaddr               : 0.0.0.0       flags               : 0x411805
helper flags         : 0xa           Standby helper flags: 0xa
Act. File Page #     : 384           Act. File Page Elem : 0
Sby. File Page #     : 359           Sby. File Page Elem : 0

[isp2.net]Redback#
```

14.12 Step 11: Checking Subscribers

Use the **show subscribers** commands to check your subscribers.

Table 36 Show Subscriber Command Examples

Command	Description
show subscribers all | grep “***time***"	Display all subscribers starting at a certain time.
show subscribers all |grep “@context”| count	Display how many subscribers are online for a particular context.
show subscribers active username ***mac-address***	Displays the individual CLIPS session, including the CLIPS circuit handle. This is the easiest way to get the CLIPS circuit handle. The subscriber could be up, but is not getting an IP address.
show subscribers active | begin before 3 after 5 “*mac-address@context*"	Display three lines prior and five lines after the match of the "***mac-address@context***". Normally, the grep shows a single line of the match.
show subscribers summary	Display summary information about CLIPS subscribers
show subcribers all | grep ***mac-address***	Display information about the binding, context, and subscriber.

For information about how to check subscribers, see Displaying Information About My Subscribers.

14.13 Step 12: Displaying IP Route Summary Information

Use the **show ip route summary** command to display summary information for all IP routes.

```
[isp2.net]Redback# show ip route summary
```

14.14 Step 13: Displaying CLIPS Groups

Use the **`show clips-group`** command to display information about a configured CLIPS group.

14.15 Step 14: Checking ARP Entries

Use the **`show arp`** command to verify ARP entries.

14.16 Step 15: Checking the CLIPS Process

Use the **`show process clips`** command to verify that the CLIPS process is running. For detailed information, use the **`detail`** keyword. If the CLIPS process is not running, use the **`show crashfiles`** command to check if there is a core dump. If there is, contact your local technical support representative.

```
[isp2.net]Redback#show process clips
NAME   PID    SPAWN  MEMORY    TIME         %CPU  STATE   UP/DOWN
clips  166    3      3436K    00:00:00.59  0.00% run     00:02:20

[isp2.net]Redback# show crashfiles
4844 Jul 4 16:02 /md/clipsd_43.mini.core
5944456 Jul 4 16:02 /md//clipsd_43.core
4812 Jul 4 16:03 /md//clipsd_526.mini.core
5923992 Jul 4 16:03 /md//clipsd_526.core
```

14.17 Step 16: Checking the CLIPS Configuration

Use the **`show configuration`** command and check for common CLIPS configuration and provisioning issues.

Table 37 CLIPS Configuration and Provisioning Issues Checklist

#	CLIPS Configuration and Provision Issue	Checked?
1	For dynamic CLIPS, is the **`dhcp max-addr 1`** setting configured under the subscriber configuration record?	
2	For static CLIPS, the subscriber must not have the **`dhcp max-addr`** attribute.	
3	The interface used for binding the subscriber must have the multibind attribute.	
4	For dynamic CLIPS clients connected to the SmartEdge through a relay, check the following: • The route pointing to the client network and the giaddr of the DHCP relay should exist in the context of the parent circuit. • The DHCP server should be not be configured to assign the IP address of the interface used in SmartEdge and that of the relay. • The interface matching the interface of the giaddr in the packet should exist with the **`multibind`** attribute configured and dhcp proxy enabled.	

14.18 Step 17: Checking the RADIUS Server

If you have configured a RADIUS server, make sure the RADIUS attributes are correctly configured for your clients. For information about checking the RADIUS server, see Troubleshooting the RADIUS Server.

14.19 Step 18: Debugging CLIPS

Use the **`debug clips`** command to enable the generation of debug messages for various types of CLIPS events on the system.

The following table lists the types of CLIPS events for which you can enable debug messages:

`boot`	Optional. Enables the generation of debug messages during a system reload.
`active`	Enables the generation of debug messages for the active controller card.
`standby`	Enables the generation of debug messages for the standby controller card.
`switchover`	Optional. Enables the generation of debug messages during a switchover from the active to the standby controller.
`all`	Enables the generation of debug messages for all CLIPS events.
`authentication`	Enables the generation of debug messages for CLIPS session authentication.
`be-cli`	Enables the generation of debug messages for CLIPS backend command-line interface (CLI) events.
`cct`	Enables the generation of debug messages for CLIPS circuit events.
`cli`	Enables the generation of debug messages CLIPS CLI events.
`dhcp`	Enables the generation of debug messages for CLIPS DHCP events.
`fsm`	Enables the generation of debug messages for CLIPS Finite State Machine (FSM) events.
`ism`	Enables the generation of debug messages for CLIPS Interface and Circuit State Manager (ISM) events.
`rcm`	Enables the generation of debug messages for CLIPS Router Configuration Manager (RCM) events.
`timer`	Enables the generation of debug messages for CLIPS timer events.

Use the **`debug clips exception`** command to list only CLIPS events that are considered exceptions. This can help you investigate a session bring-up problem as it is occurring. Exception events include:

- Process endpoint dies or becomes alive
- Unable to reserve a circuit handle
- Receipt of a circuit event for an unknown circuit
- Receipt of an unknown message

- Failure to recover a session during restart of clipsd process
- Authentication Failure
- Circuit creation failures
- DHCP create and delete failures

```
[local]Redback#debug clips exception
```

Recommended Action: If the output displays a CLIPS exception but does not display the cause of the failure, use the **debug clips all** command to determine the cause of the exception.

Caution!

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

Note: The SmartEdge 100 router does not support the **standby** and **switchover** keywords.

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

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

Note: For more information about **logging** commands and the **terminal monitor** command, see the *Command List*.

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

15 Troubleshooting the RADIUS Server

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

15.1 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 status of the port 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.

15.2 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 Action: If you find an issue in the RADIUS statistics output:

- Use the **`debug aaa all`** command from the local context.

15.3 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 38 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
```

15.4 Debugging RADIUS Attributes

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

15.5 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 `Commands Lists Document`.

```
[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
```

15.6 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.

Caution!

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

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
```