ERICSSON

Commands: show r through show z

COMMAND DESCRIPTION

24/190 82-CRA 119 1170/1-V1 Uen J

Contents

1 Command Descriptions

Commands starting with “show r” through commands starting with “show z” are included.

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

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

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

1.1 show radius control

`show radius control`

1.1.1 Purpose

Displays Remote Authentication Dial-In User Service (RADIUS) server control information.

1.1.2 Command Mode

All modes

1.1.3 Syntax Description

This command has no keywords or arguments.

1.1.4 Default

None

1.1.5 Usage Guidelines

Use the **`show radius control`** command to display RADIUS server control information.

Table 1 describes the information displayed in the output of the **show radius control** command. The display represents a snapshot of the current status of the message processing being handled by the RADIUS server or servers.

Table 1 Field Descriptions for the show radius control Command

Field	Description
Number of servers	Total number of RADIUS servers in the context or contexts
Total slots	Total number of possible outstanding requests for all servers in the context or contexts
Total in waiting queue	Number of requests waiting to be processed for all servers in the context or contexts
Total in process queue	Number of requests currently being processed for all servers in the context or contexts
Server status	Full means no more requests can be handled OK means not full

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.1.6 Examples

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

```
[local]Redback>show radius control

=========================================================
Context Name: local
---------------------------------------------------------
                         Authentication       Accounting
Number of servers:           1                    1
Total slots:                 256                  256
Total in hi_waiting queue:   0                    0
Total in low_waiting queue:  0                    0
Total in hi_process queue:   0                    0
Total in low_process queue:  0                    0
Total in waiting queue:      0                    0
Total in process queue:      0                    0
Server status:               Ok                   Ok
```

1.2 show radius counters

`show radius counters`

1.2.1 Purpose

Displays counters for Remote Authentication Dial-In User Service (RADIUS) access, accounting, Change of Authorization (CoA) messages, and counters related to route downloads.

1.2.2 Command Mode

All modes

1.2.3 Syntax Description

This command has no keywords or arguments.

1.2.4 Default

None

1.2.5 Usage Guidelines

Use the **`show radius counters`** command to display RADIUS access and accounting message counters. If the RADIUS server is configured as a CoA server, this command also displays CoA server counters.

Table 2 describes the counters that are displayed in the output of the **`show radius counters`** command.

Table 2 Field Descriptions for the show radius counters Command

Field	Description
`Access Messages`	
Requests sent	Number of access request messages sent
Requests retried	Number of access request retry messages sent
Requests send fail	Number of access request messages that were sent and failed
Requests timeout	Number of access request messages that timed out
Responses drop	Number of access request messages that were dropped
Accepts received	Number of access accept messages received
Rejects received	Number of access reject messages received

Table 2 Field Descriptions for the show radius counters Command

Field	Description
`Accounting Messages`	
Requests sent	Number of accounting request messages sent
Requests retry	Number of accounting request retry messages sent
Requests send fail	Number of accounting request messages that were sent and failed
Requests timeout	Number of accounting request messages that timed out
Responses drop	Number of accounting request messages that were dropped
Responses received	Number of accounting request message responses received
`CoA Messages`	
Requests received	Number of CoA and disconnect request messages received
Duplicate request	Number of duplicate CoA and disconnect request messages received
Response ACK	Number of CoA and disconnect requests that were successful
Response NAK	Number of CoA and disconnect requests that were unsuccessful

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

Note: By appending a space followed by the pipe (|) character at the end of a **`show`** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.2.6 Examples

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

```
[local]Redback>show radius counters

================================================================================
Server: 10.13.130.75      Port:  1812 Counter start time: May 23 17:55:30 2006
--------------------------------------------------------------------------------
  Access Messages:
--------------------------------------------------------------------------------
  Requests sent:            0
  Requests retried:         0
  Requests send fail:       0
  Requests timeout:         0
  Responses dropped:        0
  Accepts received:         0
  Rejects received:         0

================================================================================
Server: 10.13.130.75    Port: 1813  Counter start time: May 22 23:41:09 2006
--------------------------------------------------------------------------------
  Accounting Messages:
--------------------------------------------------------------------------------
  Requests sent:            356
  Requests retried:         1
  Requests send fail:       0
  Requests timeout:         0
  Responses dropped:        0
  Accepts received:         357
  Rejects received:         0

================================================================================
Server:  10.13.130.75     Port: 3799  Counter start time: May 22 23:52:35 2006
--------------------------------------------------------------------------------
  CoA Messages:
--------------------------------------------------------------------------------
  Requests received:        12
  Duplicate request:        0
  Response ACK:             6
  Response NAK:             6
```

This example displays the output for the **show radius counters** command with AAA route-download information.

```
[local]Redback>show radius counters


================================================================================
Server: 10.18.18.33      Port: 1850  Counter start time: Jun 15 23:28:07 2010
--------------------------------------------------------------------------------
  Route Download Messages:
--------------------------------------------------------------------------------
  Requests sent:             1335
  Requests retried:          0
  Requests send fail:        0
  Requests timeout:          0
  Responses dropped:         0
  Accepts received:          1334
  Rejects received:          1
```

1.3 show radius server

show radius server

1.3.1 Purpose

Displays Remote Authentication Dial-In User Service (RADIUS) server configuration, status information, and route download server information .

1.3.2 Command Mode

All modes

1.3.3 Syntax Description

This command has no keywords or arguments.

1.3.4 Default

None

1.3.5 Usage Guidelines

Use the **show radius server** command to display RADIUS server configuration and status information. If the RADIUS server is configured as a Change of Authorization (CoA) server, this command also displays CoA server information.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.3.6 Examples

The following example displays RADIUS server configuration information and status:

```
[local]Redback#show radius server

Authentication Server
================================================================================
  Address       Port      Key             State       State set time
================================================================================
155.53.129.64   1812      ********        Init     Fri Mar 12 19:07:33 2010

Algorithm:                first
Timeout (in sec.):        5
Max retry:                1
Max outstanding:          256
Server timeout (in sec.): 60
Deadtime (in min.):       5


Accounting Server
================================================================================
  Address       Port      Key             State       State set time
================================================================================
155.53.129.64   1813      ********        Alive    Fri Mar 12 19:08:02 2010

Algorithm:                first
Timeout (in sec.):        10
Max retry:                3
Max outstanding:          256
Server timeout (in sec.): 60
Deadtime (in min.):       5
Interim timeout:          0
Interim max retry:        0


CoA Server
================================================================================
  Address       Port      Key             State       State set time
================================================================================
1.1.1.1         3799      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.2         3800      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.3         3801      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.4         3802      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.5         3803      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.6         3804      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.7         3805      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.8         3806      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.9         3807      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.10        3808      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.11        3809      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.12        3810      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.13        3811      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.14        3812      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.15        3813      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.16        3814      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.17        3815      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.18        3816      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.19        3817      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.20        3818      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.21        3819      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.22        3820      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.23        3821      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.24        3822      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.25        3823      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.26        3824      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.27        3825      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.28        3826      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.29        3827      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.30        3828      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.31        3829      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.32        3830      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.33        3831      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.34        3832      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.35        3833      ********        Init     Fri Mar 12 19:07:33 2010
1.1.1.36        3834      ********        Init     Fri Mar 12 19:07:33 2010
```

The following example displays RADIUS server configuration information with AAA route download information:

```
[local]Redback>show radius server


Route Download Server
================================================================================
  Address        Port       Key             State        State set time
================================================================================
10.18.18.33      1850      ********         Alive     Tue Jun 15 23:28:39 2010

Algorithm:                 first
Timeout (in sec.):         10
Max retry:                 3
Server timeout (in sec.): 60
Deadtime (in min.):        5
```

1.4 show radius statistics

show radius statistics

1.4.1 Purpose

Displays Remote Authentication Dial-In User Service (RADIUS) server statistics and statistics related to route downloads.

1.4.2 Command Mode

All modes

1.4.3 Syntax Description

This command has no keywords or arguments.

1.4.4 Default

None

1.4.5 Usage Guidelines

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

Table 3 describes the counters that are displayed in the output of the **show radius statistics** command.

Table 3 Field Descriptions for the show radius statistics Command

Field	Description
Authentication Servers	
Requests send	Number of access request messages sent.
Requests re-send	Number of access-requests sent more than one time by the SmartEdge router to the RADIUS servers (NetOp™ PM) because the timeout set (command radius timeout) in the configuration is over
Requests timeout	Number of access request messages that timed out
Requests send fail	Number of access request messages that were sent and failed
Requests accepted	Number of access-accepts received by the SmartEdge router from the RADIUS servers (NetOp PM)

Table 3 Field Descriptions for the show radius statistics Command

Field	Description
Requests rejected	Number of access-rejects received by the SmartEdge router from the RADIUS servers (NetOp PM)
Response dropped	Number of access request messages that were dropped
Req in process	Total number of access-requests outstanding from the SmartEdge router .
Req in waiting	Number of subscribers waiting for an available slot to send the access-request to the RADIUS servers.
Server slots	Total number of simultaneous access-requests that can out stand from the SmartEdge router .
Capacity	Percentage of server slots currently in use.
Server marked dead	Number of RADIUS servers known as dead at the moment the show command was typed.
Accounting Servers	
Requests send	Number of access request messages sent.
Requests re-send	Number of access-requests sent more than one time by the SmartEdge router to the RADIUS servers (NetOp PM) because the timeout set (command radius timeout) in the configuration is over
Requests timeout	Number of access request messages that timed out
Requests send fail	Number of access request messages that were sent and failed
Requests accepted	Number of access-accepts received by the SmartEdge router from the RADIUS servers (NetOp PM)
Requests rejected	Number of access-rejects received by the SmartEdge router from the RADIUS servers (NetOp PM)
Response dropped	Number of access request messages that were dropped
Req in process	Total number of access-requests outstanding from the SmartEdge router .
Req in waiting	Number of subscribers waiting for an available slot to send the access-request to the RADIUS servers.
Server slots	Total number of simultaneous access-requests that can out stand from the SmartEdge router .
Capacity	Percentage of server slots currently in use.
Server marked dead	Number of RADIUS servers known as dead at the moment the show command was typed.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.4.6 Examples

The following example displays the output of the **show radius** command with the **statistics** keyword:

```
[local]Redback#show radius statistics
================================================================================
Server: 155.53.129.64    Port: 1812  Counter start time: Mar 12 20:50:57 2010
--------------------------------------------------------------------------------
  Access Messages:
--------------------------------------------------------------------------------
  Requests sent:            0
  Requests retried:         0
  Requests send fail:       0
  Requests timeout:         0
  Responses dropped:        0
  Accepts received:         0
  Rejects received:         0

================================================================================
Server: 155.53.129.64    Port: 1813  Counter start time: Mar 12 20:50:57 2010
--------------------------------------------------------------------------------
  Accounting Messages:
--------------------------------------------------------------------------------
  Requests sent:            0
  Requests retried:         1
  Requests send fail:       0
  Requests timeout:         0
  Responses dropped:        0
  Accepts received:         1
  Rejects received:         0

================================================================================
Server: 1.1.1.1          Port: 3799  Counter start time: Mar 12 20:50:57 2010
--------------------------------------------------------------------------------
  CoA Messages:
--------------------------------------------------------------------------------
  Requests received:        0
  Duplicate request:        0
  Response ACK:             0
  Response NAK:             0

================================================================================
Server: 1.1.1.2          Port: 3800  Counter start time: Mar 12 20:50:57 2010
--------------------------------------------------------------------------------
  CoA Messages:
--------------------------------------------------------------------------------
  Requests received:        0
  Duplicate request:        0
  Response ACK:             0
  Response NAK:             0

================================================================================
Server: 1.1.1.3          Port: 3801  Counter start time: Mar 12 20:50:57 2010
--------------------------------------------------------------------------------
  CoA Messages:
--------------------------------------------------------------------------------
  Requests received:        0
  Duplicate request:        0
```

The following example displays RADIUS statistics including AAA route download information:

```
[local]Redback>show radius ststistics


================================================================================
Context: local
================================================================================

Authentication Servers:

Requests send:                  0       Requests re-send:               0
Request timeout:                0       Requests send fail:             0
Requests accepted:              0       Requests rejected:              0
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                    0       Capacity:                       0%
Server marked dead:             0


Accounting Servers:

Requests send:                  0       Requests re-send:               0
Request timeout:                0       Requests send fail:             0
Requests accepted:              0       Requests rejected:              0
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                    0       Capacity:                       0%
Server marked dead:             0


Route Download Servers:

Requests send:                  1335    Requests re-send:               0
Request timeout:                0       Requests send fail:             0
Requests accepted:              1334    Requests rejected:              1
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                    256     Capacity:                       0%
Server marked dead:             0


CoA Servers:

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


Send Details:

Subscriber authentication:

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       No route:                       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       No route:                       0

Subscriber 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
No route:                       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
No route:                       0

Accounting On/Off:

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
No route:                       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
No route:                       0

Route download:

Request send:                   1335    Request retransmit:             0
Response received:              1335
Server busy:                    0       Server not ready:               0
No server:                      0       Server marked dead:             0
Bad attribute:                  0       Socket error:                   0
Send accept to AAAd:            1334    Send reject to AAAd:            0
Send meth fail to AAAd:         0       Internal error:                 0
Unknown attribute:              0       No route:                       0


Receive Details:

No match request:               0       No match server:                0
Invalid packet:                 0       Bogus packet:                   0
Dup response packet:            0

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

Global radius statistics:


Send Details:

Subscriber authentication:

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       No route:                       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       No route:                       0

Subscriber 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
No route:                       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
No route:                       0

Accounting On/Off:

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
No route:                       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
No route:                       0

Route download:

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       No route:                       0


Receive Details:

No match request:               0       No match server:                0
```

```
Invalid packet:                 0       Bogus packet:                   0
Dup response packet:            0
```

1.5 show rate-limit card

show rate-limit card {**all** | ***slot***} **dhcp** {**counter** | **log**}

1.5.1 Purpose

Displays dropped Dynamic Host Configuration Protocol (DHCP) packet information for one or more traffic cards.

1.5.2 Command Mode

All modes

1.5.3 Syntax Description

all Displays DHCP packet information for all traffic cards.

slot Slot number of a specific traffic card.

counter Displays the count of dropped DHCP packets for one or all traffic cards.

log Displays the log messages for dropped DHCP packets for one or all traffic cards.

1.5.4 Default

None

1.5.5 Usage Guidelines

Use the **show rate-limit card** command to display DHCP packet information for packets dropped because of rate limiting.

Use the **counter** keyword to display the count of dropped DHCP packets for one or all traffic cards.

Use the **log** keyword to display the log messages for dropped DHCP packets for one or all traffic cards.

Note: This command always displays a slot number unless no active traffic cards are present. If the resolution of the IP address is the Ethernet management port, the output might display a slot number.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

ejudlap - this note may not be necessary as it is not in all of these documents

1.5.6 Examples

The following example displays the count of dropped DHCP packets for the traffic card in slot `1`:

```
[local]Redback>show rate-limit card 1 dhcp counter
Slot 1 Ingress:
        card rate-limit 1060236 packets
```

The following example displays the log messages for the traffic card in slot `1`:

```
[local]Redback>show rate-limit card 1 dhcp log

Slot 1 Ingress:
current index: 103
000  src-ip-addr 2.1.1.2    src-mac-addr 00 00 03 00 03 00   circuit 1/3:1023:63/1/1/5
001  src-ip-addr 2.1.1.2    src-mac-addr 00 00 03 00 03 00   circuit 1/3:1023:63/1/1/5
002  src-ip-addr 2.1.1.2    src-mac-addr 00 00 03 00 03 00   circuit 1/3:1023:63/1/1/5
003  src-ip-addr 2.1.1.2    src-mac-addr 00 00 03 00 03 00   circuit 1/3:1023:63/1/1/5
004  src-ip-addr 2.1.1.2    src-mac-addr 00 00 03 00 03 00   circuit 1/3:1023:63/1/1/5
005  src-ip-addr 2.1.1.2    src-mac-addr 00 00 03 00 03 00   circuit 1/3:1023:63/1/1/5
```

1.6 show rcm

show rcm {**memory** | **session**}

1.6.1 Purpose

Displays Router Configuration Manager (RCM) information.

1.6.2 Command Mode

All configuration modes

1.6.3 Syntax Description

`memory` Displays RCM memory usage.

`session` Displays RCM session information.

1.6.4 Default

None

1.6.5 Usage Guidelines

Use the **`show rcm`** command to display RCM information.

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

Note: By appending a space followed by the pipe (|) character at the end of a **`show`** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.6.6 Examples

The following example displays output from the **`show rcm`** command with the **`memory`** keyword:

```
[local]Redback>show rcm memory
```

```
Displaying memory usage by RCM:
  Internal chunk memory                      : 125200 bytes
  Dynamically memory allocated by all        : 13844 bytes
  Memory allocated for msg by RCM components : 0 bytes
```

The following example displays output from the **show rcm** command with the **session** keyword:

```
[local]Redback>show rcm session

CLI pid      State                 Trans ID      Waiting on
-------------------------------------------------------------------
13117        Not in transaction    N/A           None
13059        Not in transaction    N/A           None
12610        In transaction        3062          None
```

1.7 show redundancy

show redundancy

1.7.1 Purpose

Displays the state of the standby controller card and verifies whether it is ready to become active. It also displays AAA route information.

1.7.2 Command Mode

All modes

1.7.3 Syntax Description

This command has no keywords or arguments.

1.7.4 Default

None

1.7.5 Usage Guidelines

Use the **show redundancy** command to display the state of the standby controller card and to verify whether it is ready to become active.

Note: The SmartEdge 100 router does not support this command; the chassis has only one controller carrier card.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.7.6 Examples

The following example displays the state of the controller cards:

```
[local]Redback>show redundancy

---------------------------------
This XCRP is active
---------------------------------
Firmware in sync? : YES
Software Release in sync? : YES
Database in sync? : YES
Mate-to-Mate link up? : YES
Standby Ready? : YES
```

If you have configured AAA route download, you will see AAA routes information when you issue the **show redundancy** command:

```
[local]Redback>show redundancy
```

```
--------------------------------
       This XCRP is active
--------------------------------
STANDBY XCRP READY?       : YES
VxWorks in sync?          : YES
Database in sync?         : YES
Software Release in sync? : YES
Firmware in sync?         : YES
Mate-to-Mate link up?     : YES

ARP                                SUCCESS
CSM                                SUCCESS
ISM                                SUCCESS
RDB                                SUCCESS
SM AAA DSLline                     SUCCESS
SM AAA RD Info                     SUCCESS
SM AAA Routes                      SUCCESS
SM AAA Session                     SUCCESS
SM AAA Strings                     SUCCESS
SM DOT1Q                           SUCCESS
SM ISM2                            SUCCESS
SM LDP ADJ                         SUCCESS
SM LDP CTX                         SUCCESS
SM LDP PEER                        SUCCESS
SM LM                              SUCCESS
SM OSPF                            SUCCESS
SM RCM                             SUCCESS
SM RIB                             SUCCESS
SM STATD                           SUCCESS
```

1.8 show release

`show release`

1.8.1 Purpose

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

1.8.2 Command Mode

All modes

1.8.3 Syntax Description

This command has no keywords or arguments.

1.8.4 Default

None

1.8.5 Usage Guidelines

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

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.8.6 Examples

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

```
[local]Redback>show release


Installed releases:

p02: active (will be booted after nextreload)
---------------------------------------------
Version SEOS-11.1.1.0.28-Release
Built on Wed Sep 21 16:14:58 PDT 2011
Copyright (C) 1998-2011, Redback NetworksInc. All rights reserved.

p01: alternate
--------------
Version SEOS-11.1.0.0.148-Release
Built on Wed Jun 15 00:00:59 PDT 2011
Copyright (C) 1998-2011, Redback NetworksInc. All rights reserved.
```

1.9 show rip debug

show rip debug

1.9.1 Purpose

Displays enabled Routing Information Protocol (RIP) debug settings.

1.9.2 Command Mode

All modes

1.9.3 Syntax Description

This command has no keywords or arguments.

1.9.4 Default

None

1.9.5 Usage Guidelines

Use the **show rip debug** command to display enabled RIP debug settings.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.9.6 Examples

The following example displays output from the **show rip debug** command:

```
[local]Redback>show rip debug

RIP debug flags: REQUEST_RECV REQUEST_SEND RESPONSE_RECV RESPONSE_SEND
PACKET_GENERAL

RIP debug detail flags:
```

1.10 show rip instance

show rip instance [*instance*]

1.10.1 Purpose

Displays information for all Routing Information Protocol (RIP) instances, or only for a particular RIP instance.

1.10.2 Command Mode

All modes

1.10.3 Syntax Description

instance Optional. RIP instance name.

1.10.4 Default

When entered without the optional ***instance*** argument, this command displays information for all configured RIP instances.

1.10.5 Usage Guidelines

Use the **show rip instance** command to display information for all RIP instances, or only for a particular RIP instance.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.10.6 Examples

The following example displays output from the **show rip instance** command:

```
[local]Redback>show rip instance
```

```
Fl - Instance Flags: (O - Default information originate), P - Maximum paths
TH - Flash update threshold, DM - Default metric, Dis - Admin distance
Dl - Output delay, TableVer - Routing table version, Upd - Update
Inv - Invalid, Hld - Holddown, Flu - Flush, Expr - Next flashupdate
GblFlg - Global flags: (I - ISM up, P - RPM up, R-RIB up)

InstanceName         Fl P TH DM Dis Dl   TableVer Expr Upd/Inv/Hld/Flu GblFlg
area1                -  8  5  0 120  0          1    2  30 180 180 240    IPR
area2                -  8  5  0 120  0          1    2  30 180 180 240    IPR
```

1.11 show rip interface

show rip interface [***instance***]

1.11.1 Purpose

Displays information for all Routing Information Protocol (RIP) interfaces, or only for RIP interfaces within a particular RIP instance.

1.11.2 Command Mode

All modes

1.11.3 Syntax Description

instance Optional. RIP instance name.

1.11.4 Default

When entered without the optional ***instance*** argument, this command displays information about all RIP interfaces.

1.11.5 Usage Guidelines

Use the **show rip interface** to display information for all RIP interfaces, or only for RIP interfaces within a particular RIP instance.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.11.6 Examples

The following example displays output from the **show rip interface** command:

```
[local]Redback>show rip interface

Interface Flags: U - Up, B - Bound, L - Listen, S - Supply, A-Admin up
V - have Valid addr, R-Registered with ISM, O - Default information originate
N - No default info orig, H - split Horizon, P - Poison reverse, Upd - Update
Inv - Invalid, Hld - Holddown, FLu - Flush, Expr - Next full update, Co - Cost

Interfaces of RIP instance: area1
Name                   Addr/MaskLen State    Upd/Inv/Hld/Flu Expr Co IntfId
ripint1                 10.1.1.1/24 LSRVH     30 180 180 240   29  1 10000001
Total 1 interfaces, 0 are up.
```

1.12 show ripng

show ripng {**all-instances** | **debug** | **instance** [***instance-id***] | **interface** [***if-name***] | **route** [***instance-id***]}

1.12.1 Purpose

Displays Routing Information Protocol next generation (RIPng) information.

1.12.2 Command Mode

All modes

1.12.3 Syntax Description

all-instances	Displays information for all RIPng instances.
debug	Displays RIPng debug settings.
instance	Displays RIPng instance information.
instance-id	Optional. Instance ID. When specified, displays RIPng instance or RIPng route information for a specific RIPng instance.
interface	Displays RIPng interface information.
if-name	Optional. Interface name. When specified, displays information for a specific RIPng interface.
route	Displays RIPng route information.

1.12.4 Default

None

1.12.5 Usage Guidelines

Use the **show ripng** command to display RIPng information.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.12.6 Examples

The following example displays information for all RIPng instances:

```
[local]Redback>show ripng all-instances

Fl - Flags: (O - Default information originate, M - Maximum routes reached)
P  - Maximum paths
TH - Flash update threshold, DM - Default metric, Dis - Admin distance
Dl - Output delay, TableVer - Routing table version, Upd - Update
Inv - Invalid, Hld - Holddown, Flu - Flush, Expr - Next flashupdate

InstanceName         Fl P TH DM Dis Dl   TableVer Expr Upd/Inv/Hld/Flu #Route
Context local:
1                    -  16  5   0 120  0          4    1  30 180 180 240      3
```

The following example displays the RIPng debug settings:

```
[local]Redback>show ripng debug

RIP debug flags: REQUEST_RECV REQUEST_SEND RESPONSE_RECV RESPONSE_SEND
 PACKET_GE
NERAL MEMORY INTERNAL PROTOCOL IPC TIMER INTERFACE LOCAL_RIB GLOBAL_RIB
 POLICY C
ONFIG IN_QUEUE OUT_QUEUE AUTHENTICATION THREAD SOCKIO ISM GENERAL
RIP debug detail flags:
```

The following example displays information for the RIPng instance, `4`:

```
[local]Redback>show ripng instance 4

Fl - Flags: (O - Default information originate, M - Maximum routes reached)
P  - Maximum paths
TH - Flash update threshold, DM - Default metric, Dis - Admin distance
Dl - Output delay, TableVer - Routing table version, Upd - Update
Inv - Invalid, Hld - Holddown, Flu - Flush, Expr - Next flashupdate

InstanceName         Fl P TH DM Dis Dl   TableVer Expr Upd/Inv/Hld/Flu #Route
Context local:
1                    -  16  5   0 120  0          4    3  30 180 180 240      3
```

The following example displays information for the RIPng interface, `88`:

```
[local]Redback>show ripng interface 88

Interface Flags: U - Up, B - Bound, L - Listen, S - Supply, A-Admin up
V - have Valid addr, R-Registered with ISM, O - Default information originate
N - No default info orig, H - split Horizon, P - Poison reverse, Upd - Update
Inv - Invalid, Hld - Holddown, FLu - Flush, Expr - Next full update, Co - Cost

Interfaces of RIP instance: 1
Name                   Addr/MaskLen State    Upd/Inv/Hld/Flu Expr Co IntfId
lo                       8001::1/128 ULVH      30 180 180 240   16  1 10000004
to-nbor                  7001::1/112 ULSVH     30 180 180 240   16  1 10000003
Total 2 interfaces, 2 are up.
```

The following example displays information for the RIPng route, 37:

```
[local]Redback>show ripng route 37

T - RouteType:(C - Connected, E - External, R - RIP, EB - External backup)
M - Metric, Exp - Expire time, PrFl - Prefix flags ( D - Delete, H - Holddown
A - Need flash, B - Need download to RIB, I - Inactive) NhFl - Next Hop Flags
(W - Withdrawn from RIB, H - Holddown, F - Flush expire before holddown)

Routing table for RIP instance: 1
T Prefix/PrefixLen     NextHop                   M  Exp PrFl|NhFl Intf     Peer
C 7001::/112           ::                        0   -     6|6    to-nbor
C 8001::1/128          ::                        0   -     6|6    lo
R 8001::2/128          fe80::230:88ff:fe00:3294  1  172    6|6    to-nbor
Total 3 prefixes 3 routes(1 intern 0 extern 2 connected)
```

1.13 show rip route

show rip route [***instance***] [***ip-addr/prefix-length*** [**longer-prefixes**]]

1.13.1 Purpose

Displays information about all Routing Information Protocol (RIP) routes, or only for routes within a particular RIP instance.

1.13.2 Command Mode

All modes

1.13.3 Syntax Description

instance	Optional. RIP instance name.
ip-addr/prefix-length	Optional. IP address (in the form ***A.B.C.D)*** and prefix length, separated by the slash (**/**) character. The range of values for the ***prefix-length*** argument is 0 to 32.
longer-prefixes	Optional. Displays all routes that fall into the range of the prefix; otherwise, only routes that exactly match are displayed.

1.13.4 Default

When entered without any optional arguments, this command displays information about all RIP routes.

1.13.5 Usage Guidelines

Use the **show rip route** command to display information about RIP routes, or only for routes within a particular RIP instance.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.13.6 Examples

The following example displays output from the **show rip route** command:

```
[local]Redback>show rip route
```

```
T - RouteType: (C - Connected, E - External, R - RIP, EB - External backup)
M - Metric, Exp - Expire time, PrFl - Prefix flags D - Delete, H - Holddown
A - Need flash, B - Need download to RIB, I - Inactive) NhFl - Next Hop Flags
(W - Withdrawn from RIB, H - Holddown, F - Flush expire before holddown)

Routing table for RIP instance: rip001
T          Prefix     NextHop          M   Exp PrFl|NhFl Intf     Peer
Total 0 prefixes 0 routes (0 intern 0 extern 0 connected)
```

1.14 show rmon

show rmon {**alarms** | **events**}

1.14.1 Purpose

Displays Remote Monitoring (RMON) information.

1.14.2 Command Mode

All modes

1.14.3 Syntax Description

alarms Displays RMON alarm records.

events Displays RMON event records.

1.14.4 Default

None

1.14.5 Usage Guidelines

Use the **show rmon** command to display RMON information.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.14.6 Examples

The following example displays RMON alarms:

```
[local]Redback>show rmon alarm


rmon alarm 5 ipInReceives.0 50 delta rising-threshold 5000 5
falling-threshold 200 6 owner "gold.isp.net"

rmon alarm 10 ipForwDatagrams.0 60 delta rising-threshold 3000000
1 falling-threshold 600000 2

rmon alarm 20 rbnCpuMeterOneMinuteAvg.0 5 absolute rising-threshold
 50 3 falling-threshold 10 4 owner "alarmDel6"
```

The following example displays RMON events:

```
[local]Redback>show rmon events


rmon event 1 log notify owner gold.isp.net description "packets
per second too high in context gold.isp.net"

rmon event 2 log notify owner gold.isp.net description "packets
per second is below 10000 in context gold.isp.net"

rmon event 3 log notify owner gold.isp.net description "One minute
average CPU usage on the device is above 50%"

rmon event 4 log notify owner gold.isp.net description "One minute
average CPU usage on the device is now below 10%"

rmon event 5 log notify owner gold.isp.net description "The total
number of input IP datagrams received from interfaces per second
is 100 and above"

rmon event 6 log notify owner gold.isp.net description "The total
number of input IP datagrams received from interfaces per second
is 4 and below"
```

1.15 show route-map

show route-map [*map-name*] [**summary**]

1.15.1 Purpose

Displays information about configured route maps.

1.15.2 Command Mode

All modes

1.15.3 Syntax Description

map-name Optional. Name of the route map.

summary Optional. Displays route map summary information.

1.15.4 Default

Displays all configured route maps.

1.15.5 Usage Guidelines

Use the **show route-map** command to display information about configured route maps.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.15.6 Examples

The following example displays all configured route maps:

```
[local]Redback>show route-map
route-map c1-a2-in:
 count: 6, sequences: 10 - 40, client count: 1
 modified: 2 day(s), 21 hour(s) ago
 sequence 10, permit (hits: 13, cache hits: 7)
   Match clauses:
     as-path (as-path filter): AS2686
   Set clauses:
     local-preference 80
     weight 65535
 sequence 15, permit (hits: 17667, cache hits: 17667)
   Match clauses:
     ip address (prefix list): /22-permit
   Set clauses:
     community local-AS
 sequence 20, permit (hits: 2, cache hits: 0)
   Match clauses:
     ip address (prefix list): slash9
   Set clauses:
     metric 80
 sequence 25, permit (hits: 3, cache hits: 0)
   Match clauses:
     ip address (prefix list): slash18
   Set clauses:
     community-list no-export/11:121-delete delete
     community 11:102 additive
     ip next-hop 10.255.255.254
 sequence 30, permit (hits: 307062, cache hits: 0)
   Match clauses:
     community (community list filter): 11:121-c1-wtn
   Set clauses:
     community 11:102 additive
 sequence 40, permit (hits: 0, cache hits: 0)
   Match clauses:
   Set clauses:
route-map a2-out-map:
 count: 4, sequences: 10 - 40, client count: 1
 modified: 2 day(s), 21 hour(s) ago
 sequence 40, permit (hits: 2227, cache hits: 0)
   Match clauses:
     community (community list filter): a2community
   Set clauses:
     metric-type internal
total route maps: 2
```

The following command displays a summary of all configured route maps:

```
[local]Redback>show route-map summary
route-map c1-a2-in:
 count: 6, sequences: 10 - 40, client count: 1
 modified: 2 day(s), 21 hour(s) ago
route-map a2-out-map:
 count: 4, sequences: 10 - 40, client count: 1
 modified: 2 day(s), 21 hour(s) ago
total route maps: 2
```

1.16 show rsvp counters

show rsvp counters [**global** | **lsp** | **packets**]

1.16.1 Purpose

Displays Resource Reservation Protocol (RSVP) counter information.

1.16.2 Command Mode

All modes

1.16.3 Syntax Description

global	Optional. Displays only global counters.
lsp	Optional. Displays only label-switched path (LSP) related counters.
packets	Optional. Displays only packet-related counters.

1.16.4 Default

Displays all RSVP counter information.

1.16.5 Usage Guidelines

Use the **show rsvp counters** command to display RSVP counter information.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.16.6 Examples

The following example displays packet-related output from the **show rsvp counters** command:

```
[local]Redback>show rsvp counters packets
```

```
                --- Global RSVP Counters ---
        Packet Counters


           Interval:  00:00:09
       Packets Sent:          0        Packets Recvd:          0
  Packets Tx dropped:          0   Packets Rx dropped:          0
  Packets Tx IO errs:          0   Packets Rx IO errs:          0
           PATH Sent:          0            PATH Recvd:          0
           RESV Sent:          0            RESV Recvd:          0
      PATH TEAR Sent:          0       PATH TEAR Recvd:          0
      RESV TEAR Sent:          0       RESV TEAR Recvd:          0
       PATH ERR Sent:          0        PATH ERR Recvd:          0
       RESV ERR Sent:          0        RESV ERR Recvd:          0
        CONFIRM Sent:          0         CONFIRM Recvd:          0
  Unknown Pkts Recvd:          0
```

The following example displays LSP-related output from the **show rsvp counters** command:

```
[local]Redback>show rsvp counters lsp

                --- Global RSVP Counters ---
        LSP Counters


      Total Sessions:         26            Total LSPs:         27
        Ingress LSPs:          7           Egress LSPs:         18
        Transit LSPs:          2           Backup LSPs:         1
             Up LSPs:         23             Down LSPs:         4
         Active LSPs:         23          Backup2 LSPs:         0
         Bypass LSPs:          0         Rerouted LSPs:         0
          Stale LSPs:          5 Stale LSPs Recovered:          5
```

In this example:

- Stale LSPs are the number of LSPs that moved to the Stale state due to local or neighbor restart events.
- Stale LSPs Recovered are the number of previously stale LSPs that moved back successfully to the Up state.

1.17 show rsvp debug

show rsvp debug

1.17.1 Purpose

Displays Resource Reservation Protocol (RSVP) debug information.

1.17.2 Command Mode

All modes

1.17.3 Syntax Description

This command has no keywords or arguments.

1.17.4 Default

None

1.17.5 Usage Guidelines

Use the **show rsvp debug** command to display RSVP debug information.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.17.6 Examples

The following example displays output from the **show rsvp debug** command:

```
[local]Redback>show rsvp debug
```

```
Event                    Filter

Packet
Packet Send
Path Send
Path Recv
Resv Send
Resv Recv
Path Error Send
Path Error Recv
Resv Error Send
Resv Error Recv
Path Tear Send
Path Tear Recv
Packet Confirm Send
Packet Confirm Recv
Packet Recv
```

1.18 show rsvp explicit-route

show rsvp explicit-route [*er-name*] [**detail**]

1.18.1 Purpose

Displays explicit route information.

1.18.2 Command Mode

All modes

1.18.3 Syntax Description

er-name	Optional. Name of the explicit route for which information is displayed.
detail	Optional. Displays detailed information for the specified explicit route or all explicit routes.

1.18.4 Default

Displays summary information for all explicit routes.

1.18.5 Usage Guidelines

Use the **show rsvp explicit-route** command to display explicit route information.

Use the ***er-name*** argument to display detailed information for a specific explicit route.

Use the **detail** keyword to display the detailed explicit route information; otherwise, the summary information is displayed.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.18.6 Examples

The following example displays summary information for all explicit routes:

```
[local]Redback>show rsvp explicit-route

Explicit Route       Hop Count
exp-rt1              2
```

The following example displays detailed information for the `exp-rt1` explicit route:

```
[local]Redback>show rsvp explicit-route exp-rt1

Explicit Route: exp-rt1              Hop Count: 2
  Length: 8 Addr: 10.1.1.1/32
  Length: 8 Addr: 10.2.1.2/32
```

1.19 show rsvp interface

show rsvp interface [*if-name* | **detail**]

1.19.1 Purpose

Displays Resource Reservation Protocol (RSVP) interface summary information.

1.19.2 Command Mode

All modes

1.19.3 Syntax Description

if-name	Optional. Name of the RSVP interface to be displayed.
detail	Optional. Displays detailed information.

1.19.4 Default

Displays all RSVP interface summary information.

1.19.5 Usage Guidelines

Use the **show rsvp interface** command to display all RSVP interface summary information.

Use the ***if-name*** argument to display information for only a specific RSVP interface.

Use the **detail** keyword to display detailed RSVP interface information; otherwise, summary information is displayed.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.19.6 Examples

The following example shows how to display information for all configured RSVP interfaces:

```
[local]Redback>show rsvp interface

         --- All RSVP Interfaces ---

Address/Mask       Name                 State  Bound to
1.1.1.1/24         one                  Up     7/4
3.1.1.1/24         two                  Up     7/2
```

The following example shows how to display information for the `IPst.14` RSVP interface:

```
[local]router#show rsvp interface IPst.14
--- RSVP Interface 10.18.241.74 ---

Name : IPst.14               Mask : 255.255.255.252
State                  : Down        Bound to                :
Refresh Interval (sec) : 30          Keep Multiplier         : 6
Hello Interval (sec)   : 0           Hello Keep Multiplier   : 3
Max Bandwidth (By/sec) : 0           TE metric : Use IGP metric
TE update threshold    : 5           TE advertisements       : 0
Tracking               : Enabled (tracking objects below)
Track-mtu
Allocated BW (By/sec)  : 0
Priority     Resv B/W (By/sec)      Last-Advertised   Available
0            0                      0                 0
1            0                      0                 0
2            0                      0                 0
3            0                      0                 0
4            0                      0                 0
5            0                      0                 0
6            0                      0                 0
7            0                      0                 0
```

1.20 show rsvp lsp

show rsvp lsp [*lsp-name* backup | bypass | detail | down | egress | ingress | label | protected | protection | track [lsp-name | detail] | transit | up]

1.20.1 Purpose

Displays Resource Reservation Protocol (RSVP) label-switched path (LSP) information.

1.20.2 Command Mode

All modes

1.20.3 Syntax Description

lsp-name	Optional. Name of LSP for which information is displayed.
backup	Optional. Displays only back-up LSPs.
bypass	Optional. Displays only bypass LSPs.
detail	Optional. Displays detailed information.
down	Optional. Displays only down LSPs.
egress	Optional. Displays only egress LSPs.
ingress	Optional. Displays only ingress LSPs.
label	Optional. Displays label information for RSVP LSPs.
protection	Optional. Displays only protection information.
protected	Optional. Displays only protected LSPs with back-ups configured.
transit	Optional. Displays only transit LSPs.
track	Optional. Displays information about the tracking-enabled label-switched paths (LSPs) that are currently configured on your system. Include the ***lsp-name*** argument after the **track** keyword to display tracking information for a specific LSP. Include the **detail** keyword after the track keyword to display detailed tracking information for a specific LSP.
up	Optional. Displays only up LSPs.

1.20.4 Default

Displays summary information for all LSPs.

1.20.5 Usage Guidelines

Use the **show rsvp lsp** command to display all RSVP LSP information.

Use the ***lsp-name*** argument to display information only for the specified LSP, or use any of the available keywords to display LSP information only for the specified keyword.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

Note: When the output fills a width of 80 characters or more, the column headings and contents are truncated or abbreviated.

1.20.6 Examples

The following example displays information for all RSVP LSPs:

```
[local]Redback>show rsvp lsp

LSP                     TID    Ingress         Endpoint        State FRR O Prtct
primary-dev4-backup     1      12.12.12.12     14.14.14.14     Up        I Back
primary-dev4            1      12.12.12.12     14.14.14.14     Up    3   I Prim
primary-dev4-bypass     3      12.12.12.12     13.13.13.13     Up        I Bypas
primary-dev2            1      14.14.14.14     12.12.12.12     Up        E None
primary-dev2_2          2      14.14.14.14     12.12.12.12     Up        E None
```

The **show rsvp lsp** command displays the following:

- LSP—Name of the LSP. Each RSVP LSP has a specific name.
- TID—Tunnel ID of the LSP (this ID is determined by the ingress node of the LSP).
- Ingress—IP address of the ingress of the LSP. Usually, this address is the IP address of the router from which the packet got its LSP, but the ingress address is configurable for SE RSVP LSPs; so, it can also be a loopback address.
- Endpoint—Destination address of the LSP. Usually, this address is the IP address of the destination router to which the packet has its last hop, but the address does not need to be the router ID of the destination router; it can be a loopback address configured at the destination router.

- `State`—State of the LSP. The state can be `Up`, `Down`, `Shut`, or `Stale`.
- `FRR`—If the LSP has an FRR bypass LSP that can protect it, then this field displays the tunnel ID of the bypass LSP that is protecting it. Otherwise, this field is empty.
- `0`—Origin, for the type of LSP relative to the location of the local switch in the path: I (or `Ingress`) for ingress, `E` (or `Egress`) for egress, or `T` (or `Transit`) for transit.
- `Prtct`—Protection characteristic of the LSP. For example, if an LSP does not protect other LSPs but is protected by other LSPs, `Prim` (for primary LSP) is listed. If an LSP protects other LSPs (a backup or backup of a backup), `Back` is listed. If an LSP has no protection characteristic, `None` is listed. If an LSP is a bypass LSP, it is preestablished to protect an LSP that traverses either a specific link (link bypass LSP) or node (node bypass LSP), and `Bypas` is listed.

The following example displays detailed information for all RSVP LSPs:

```
[local]Redback>show rsvp lsp detail


                --- RSVP LSP primary-dev4-backup (Tunnel ID: 1) ---

Ingress             : 12.12.12.12     Endpoint            : 14.14.14.14
Origin              : Ingress         LSP State           : Up
Extended Tunnel ID  : 12.12.12.12     LSP ID              : 32768
Traffic-Eng         : default         State Transitions   : 1
Downstream Nhop     : 16.1.1.2        Downstream Intf     : 16.1.1.1
Downstream Intf Name: to_dev3_2
Downstream Nbr      : 16.1.1.2        Downstream Label    : 458755
Setup Priority      : 7               Holding Priority    : 0
Last Downstream Tx  : 9               Last Downstream Rx  : 9
Next Timer in (sec) : 3               Lifetime (sec)      : 157
Time to Die (sec)   : 148             B/W (Bytes/sec)     : 0
LSP cct             : 255/3:511:63:31/0/1/1
IGP Shortcut        : Enabled         Exclusive Mapping   : No
Tunnel Shortcut     : Enabled
Nnhop Label         : 0
Nnhop Addr:         : 14.14.14.14
Session Attr        : Local-Protect Node-Protect May-Reroute Record-Label
Use Explicit Route  : Yes             Record Route        : Yes
Explicit Route      : primary-dev4-bypass
Backup LSP protecting LSP primary-dev4
Recorded Route (hops: 2):
        13.13.13.13/32  Label flags 1, value 458755
        14.14.14.14/32  Label flags 1, value 0

                --- RSVP LSP primary-dev4 (Tunnel ID: 1) ---

Ingress             : 12.12.12.12     Endpoint            : 14.14.14.14
Origin              : Ingress         LSP State           : Up
Extended Tunnel ID  : 12.12.12.12     LSP ID              : 1
Traffic-Eng         : default         State Transitions   : 1
Downstream Nhop     : 15.1.1.2        Downstream Intf     : 15.1.1.1
Downstream Intf Name: to_dev3_1
Downstream Nbr      : 15.1.1.2        Downstream Label    : 458753
Setup Priority      : 7               Holding Priority    : 0
Last Downstream Tx  : 33              Last Downstream Rx  : 10
Next Timer in (sec) : 3               Lifetime (sec)      : 157
Time to Die (sec)   : 146             B/W (Bytes/sec)     : 0
LSP cct             : 255/3:511:63:31/0/1/2
IGP Shortcut        : Enabled         Exclusive Mapping   : No
Tunnel Shortcut     : Enabled
FRR Protection      : Standby (Bypass)
FRR Adjacency ID    : 0x8300000       FRR Tunnel ID       : 3
```

```
Nnhop Label          : 0
Nnhop Addr:          : 14.14.14.14
Session Attr         : Local-Protect Node-Protect May-Reroute Record-Label
Use Explicit Route   : Yes              Record Route        : Yes
Explicit Route       : primary-dev4
LSP protected by LSP primary-dev4-backup
Recorded Route (hops: 2):
        13.13.13.13/32  Label flags 1, value 458753
        14.14.14.14/32  Label flags 1, value 0

                --- RSVP LSP primary-dev4-bypass (Tunnel ID: 3) ---

Ingress              : 12.12.12.12      Endpoint            : 13.13.13.13
Origin               : Ingress          LSP State           : Up
Extended Tunnel ID   : 12.12.12.12      LSP ID              : 1
Traffic-Eng          : default          State Transitions   : 1
Downstream Nhop      : 16.1.1.2         Downstream Intf     : 16.1.1.1
Downstream Intf Name: to_dev3_2
Downstream Nbr       : 16.1.1.2         Downstream Label    : 3
Setup Priority       : 7                Holding Priority    : 0
Last Downstream Tx   : 10               Last Downstream Rx  : 11
Next Timer in (sec)  : 26               Lifetime (sec)      : 157
Time to Die (sec)    : 145              B/W (Bytes/sec)     : 0
LSP cct              : 255/3:511:63:31/0/1/4
IGP Shortcut         : Disabled         Exclusive Mapping   : No
Tunnel Shortcut      : Disabled
Session Attr         : May-Reroute Record-Label
Use Explicit Route   : Yes              Record Route        : Yes
Explicit Route       : primary-dev4-bypass
Bypass LSP           : Protected rsvp interface 15.1.1.2, grid 0x10040003
Bypass LSP Attr      : Preferred Link-Bypass
Recorded Route (hops: 1):
        13.13.13.13/32  Label flags 1, value 3

                --- RSVP LSP primary-dev2 (Tunnel ID: 1) ---

Ingress              : 14.14.14.14      Endpoint            : 12.12.12.12
Origin               : Egress           LSP State           : Up
Extended Tunnel ID   : 14.14.14.14      LSP ID              : 1
Traffic-Eng          : None             State Transitions   : 1
Setup Priority       : 7                Holding Priority    : 0
Last Upstream Tx     : 6                Last Upstream Rx    : 9
Upstream Intf        : 16.1.1.1         Upstream Nhop       : 16.1.1.2
Upstream Intf Name   : to_dev3_2                            :
Upstream Nbr         : 16.1.1.2         Upstream Label      : 0
Next Timer in (sec)  : 15               Lifetime (sec)      : 157
Time to Die (sec)    : 147              B/W (Bytes/sec)     : 0
Session Attr         : Local-Protect Node-Protect May-Reroute Record-Label

                --- RSVP LSP primary-dev2_2 (Tunnel ID: 2) ---

Ingress              : 14.14.14.14      Endpoint            : 12.12.12.12
Origin               : Egress           LSP State           : Up
Extended Tunnel ID   : 14.14.14.14      LSP ID              : 1
Traffic-Eng          : None             State Transitions   : 1
Setup Priority       : 7                Holding Priority    : 0
Last Upstream Tx     : 26               Last Upstream Rx    : 7
Upstream Intf        : 16.1.1.1         Upstream Nhop       : 16.1.1.2
Upstream Intf Name   : to_dev3_2                            :
Upstream Nbr         : 16.1.1.2         Upstream Label      : 0
Next Timer in (sec)  : 5                Lifetime (sec)      : 157
Time to Die (sec)    : 150              B/W (Bytes/sec)     : 0
Session Attr         : Local-Protect Node-Protect May-Reroute Record-Label
```

The following example displays information for RSVP LSPs that are currently shut down:

```
[local]Redback>show rsvp lsp down
```

```
                RSVP LSPs

LSP       TID   Ingress      Endpoint     State  FRR O Prtct
W-E-lsp   1     10.1.1.2     10.2.1.2     Shut       I None
```

The following example displays information for RSVP LSPs that are currently up:

```
[local]Redback>show rsvp lsp up

                RSVP LSPs

LSP       TID  Ingress      Endpoint     State  FRR O Prtct
W-E-bkup  1    10.1.1.2     10.2.1.2     Up         I Backup
E-W-lsp   2    10.2.1.2     10.1.1.2     Up         E None
```

The following example displays information for egress RSVP LSPs:

```
[local]Redback>show rsvp lsp egress

                RSVP LSPs

LSP       TID   Ingress      Endpoint     State  FRR O Prtct
E-W-lsp   2     10.2.1.2     10.1.1.2     Up         E None
```

The following example displays information for ingress RSVP LSPs:

```
[local]Redback>show rsvp lsp ingress
LSP                  TID Ingress      Endpoint     State FRR O Prtct
R1-R5-backup         1   10.2.250.201 10.2.250.205 Up        I Back
R1-R5-prim           1   10.2.250.201 10.2.250.205 Up    8   I Prim
R1-R6-backup         3   10.2.250.201 10.2.250.206 Up        I Back
R1-R6-prim           3   10.2.250.201 10.2.250.206 Up    7   I Prim
R1-R3-bypass         4   10.2.250.201 10.2.250.203 Up        I Bypas
R1-R2-prim           6   10.2.250.201 10.2.250.202 Up    7   I None
R1-R2-bypass         7   10.2.250.201 10.2.250.202 Up        I Bypas
R1-R5-bypass-node-R3 8   10.2.250.201 10.2.250.205 Up        I Bypas
R1-R3-prim           9   10.2.250.201 10.2.250.203 Up    4   I None
R1-R4-prim           10  10.2.250.201 10.2.250.204 Up    7   I None
```

This example shows information on incoming packet in the local MPLS-enabled network where RSVP is used to communicate labels and their meaning among label-switched routers (LSRs). At each incoming (ingress) point of the network, packets are assigned a label by an edge label-switched router (LSR). Packets are forwarded along a label-switched path (LSP) where each LSR makes forwarding decisions based on the label information. At each hop, the LSR swaps the existing label for a new label that tells the next hop how to forward

the packet. At the outgoing (egress) point, an edge LSR removes the label, and forwards the packet to its destination.

The **show rsvp lsp ingress** command displays the following:

- LSP—The name of the LSP. All RSVP LSPs have a specific name.
- TID—The Tunnel ID. It is unique per originating node, for a given LSP, so the ID can be 1 to 40,000.
- Ingress—The IP address of the ingress of the LSP. Usually, this is the IP address of the router that the packet got its LSP from, but the ingress address is configurable for SE RSVP LSPs, so it can also be a loopback address.
- Endpoint—The destination address of the LSP. Usually, this is the IP address of the destination router that the packet has its last hop to, but the address does not need to be the destination router's router ID, it can be a loopback address configured at the destination router.
- State—The state of the LSP. The state can be Up, Down, Shut, or Stale.
- FRR—If the LSP has a Fast-Reroute (FRR) bypass LSP that can protect it, then this field displays the tunnel ID of the bypass LSP that is protecting it. Otherwise, this field is empty.
- O—Origin, for the type of LSP with regards to where the local switch is in the path: I for ingress, E for egress, or T for transit.
- Prtct—The protection characteristic of the LSP. For example, if it is an LSP that does not protect other LSPs but is protected by other LSPs, Prim (for primary LSP) is listed. If it is an LSP that protects other LSPs (a backup or backup of a backup), Back is listed. If it has no protection characteristic, None is listed. If it is a bypass LSP, it is preestablished to protect an LSP that traverses either a specific link (link bypass LSP) or node (node bypass LSP), and Bypas is listed.

The following example displays label information for all RSVP LSPs:

```
[local]Redback>show rsvp lsp label

LSP             State  Upstream lbl  Downstream lbl
W-E-bkup        Up     N/A           262144
W-E-lsp         Shut   N/A           0
E-W-lsp         Up     3             N/A
```

The following example displays information for RSVP LSPs protected with a backup LSP:

```
[local]Redback>show rsvp lsp protected
```

```
LSP             ID      Ingress       Endpoint      State   Backed up by
W-E-lsp         1       10.1.1.2      10.2.1.2      Shut    W-E-bkup
```

The following example displays protection information for all RSVP LSPs:

```
[local]Redback>show rsvp lsp protection

Primary         State  Active Backup         State  Active
W-E-lsp         Shut   No     W-E-bkup       Up     Yes
```

The following example displays information for transmit RSVP LSPs:

```
[local]Redback>show rsvp lsp transit

                RSVP LSPs

LSP        TID   Ingress       Endpoint      State  FRR O Prtct
W-E-bkup   1     10.1.1.2      10.2.1.2      Up          T None
E-W-lsp    2     10.2.1.2      10.1.1.2      Up          T None
```

The following example shows how to display summary information about all tracking-enabled LSPs currently configured on the router:

```
[local]Redback#show rsvp lsp track

LSP                       TID  Ingress         Endpoint        State FRR
O Prtct
AC1_MTU1_azul             13   10.18.241.3     10.18.241.6     Down
(tracking)
I None
AC1_AC2_rojo              22   10.18.241.3     10.18.241.4     Down
(tracking)
I Prim
```

The following example shows how to display information about the `AC1_MTU1_azul` tracking-enabled LSP:

```
[local]Redback#show rsvp lsp track AC1_MTU1_azul

--- RSVP LSP AC1_MTU1_azul (Tunnel ID: 13) ---
Ingress             : 10.18.241.3     Endpoint            : 10.18.241.6
Origin              : Ingress         LSP State           : Down (tracking)
Extended Tunnel ID  : 10.18.241.3     LSP ID              : 1
Traffic-Eng         : default         State Transitions   : 2
Downstream Nhop     : 0.0.0.0         Downstream Intf     : 0.0.0.0
Downstream Intf Name:
Downstream Nbr      : 0.0.0.0         Downstream Label    : 0
Setup Priority      : 7               Holding Priority    : 0
Last Downstream Tx  : 58761           Last Downstream Rx  : 0
Next Timer in (sec) : 1271218063      Lifetime (sec)      : 0
Time to Die (sec)   : 0               B/W (Bytes/sec)     : 0
LSP cct             : Cct invalid
IGP Shortcut        : Disabled
Session Attr        : Local-Protect Node-Protect May-Reroute Record-Label
Use CSPF Route      : Yes             Record Route        : Yes
Dynamic Route       :
Tracking            : Track-mtu       Tracking State      : Down
CSPF Route          : Pending
```

The following example shows how to display detailed information about all tracking-enabled LSPs currently configured on the router:

```
[local]Redback#show rsvp lsp track detail

--- RSVP LSP AC1_MTU1_azul (Tunnel ID: 13) ---
Ingress             : 10.18.241.3     Endpoint            : 10.18.241.6
Origin              : Ingress         LSP State           : Down (tracking)
Extended Tunnel ID  : 10.18.241.3     LSP ID              : 1
Traffic-Eng         : default         State Transitions   : 2
Downstream Nhop     : 0.0.0.0         Downstream Intf     : 0.0.0.0
Downstream Intf Name:
Downstream Nbr      : 0.0.0.0         Downstream Label    : 0
Setup Priority      : 7               Holding Priority    : 0
Last Downstream Tx  : 59130           Last Downstream Rx  : 0
Next Timer in (sec) : 1271217694      Lifetime (sec)      : 0
Time to Die (sec)   : 0               B/W (Bytes/sec)     : 0
LSP cct             : Cct invalid
```

```
IGP Shortcut         : Disabled
Session Attr         : Local-Protect Node-Protect May-Reroute Record-Label
Use CSPF Route       : Yes              Record Route         : Yes
Dynamic Route        :
Tracking             : Track-mtu        Tracking State       : Down
CSPF Route           : Pending
--- RSVP LSP AC1_AC2_rojo (Tunnel ID: 22) ---
Ingress              : 10.18.241.3      Endpoint             : 10.18.241.4
Origin               : Ingress          LSP State            : Down (tracking)
Extended Tunnel ID   : 10.18.241.3      LSP ID               : 1
Traffic-Eng          : default          State Transitions    : 2
Downstream Nhop      : 0.0.0.0          Downstream Intf      : 0.0.0.0
Downstream Intf Name:
Downstream Nbr       : 0.0.0.0          Downstream Label     : 0
Setup Priority       : 7                Holding Priority     : 0
Last Downstream Tx   : 59764            Last Downstream Rx   : 0
Next Timer in (sec)  : 1271217694       Lifetime (sec)       : 0
Time to Die (sec)    : 0                B/W (Bytes/sec)      : 0
LSP cct              : Cct invalid
IGP Shortcut         : Disabled
Session Attr         : Local-Protect Node-Protect May-Reroute Record-Label
Use CSPF Route       : Yes              Record Route         : Yes
Dynamic Route        :
LSP protected by LSP AC1_AC2_verde which is protected by LSP AC1_AC2_3camino
Tracking             : Track-mtu        Tracking State       : Down
CSPF Route           : Pending (21 retries)
```

1.21 show rsvp neighbor

show rsvp neighbor [*ip-addr* | **detail**]

1.21.1 Purpose

Displays Resource Reservation Protocol (RSVP) neighbor information.

1.21.2 Command Mode

All modes

1.21.3 Syntax Description

ip-addr	Optional. Neighbor IP address. Displays detailed information for specified neighbor.
detail	Optional. Displays detailed information for all neighbors.

1.21.4 Default

Displays summary RSVP information for all neighbors.

1.21.5 Usage Guidelines

Use the **show rsvp neighbor** command to display RSVP neighbor information.

If the RSVP neighbor's transport IP address differs from its router ID, the IP address specified in the **neighbor** ***ip-addr*** construct must be the RSVP neighbor's transport IP address.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.21.6 Examples

The following example displays summary RSVP neighbor information for all RSVP interfaces:

```
[local]Redback>show rsvp neighbor
```

```
    --- All RSVP Neighbors ---

Nbr Address     GR      Rest-Time      Recov-Time     State
17.1.1.3        Yes     60             120            Up
20.1.1.1        Yes     30             60             Up
27.27.27.1      No      30             60             Hello Disabled
28.28.28.1      No      30             60             Hello Disabled
31.1.1.2        No      30             60             Hello Disabled
```

The summary includes the following information for all RSVP neighbors:

- `Nbr Address`—Neighbor address: IP Address
- `GR`—Graceful Restart Enabled: Yes/No
- `Rest-Time`—Number of seconds that Nbr has to send “Hello” after restarting.
- `Recov-Time`—Number of seconds that Nbr has to refresh LSPs after restarting.
- `State`—`Up`, `Down`, `Hello Disabled`, or `Restarting`

The following example displays detailed information for neighbor 17.1.1.3:

```
[local]Redback>show rsvp neighbor 17.1.1.3

    --- RSVP Neighbor 17.1.1.3 ---
Intf Name         :to-nbrA      GR Enabled         :Yes
Restart Time      :60 (sec)     Recovery Time      :120 (sec)
Nbr Restart Time :20 (sec)      Nbr Recovery Time :40 (sec)
Restart TTD       :14 (sec)     Recovery TTD       :54 (sec)
Hello Status      :Restarting   Nbr Restart Cnt    :9
Last Nbr Restart :09:48:21 Wed Oct 15 2008
Nbr flags         :0x0010       Nbr Reference Cnt :300
```

The detailed display includes the following information:

- `Intf Name`—Interface Name GR Enabled = Graceful Restart Enabled: Yes/No
- `Restart Time`—Number of seconds that the local node has to send “Hello” after restarting. Recovery Time = Number of seconds that the local node has to refresh LSPs after restarting. (Restart/Recovery Time is available only if RSVP Hello messages are enabled.)

- `Nbr Restart Time`—Number of seconds that Nbr has to send “Hello” after restarting. Nbr Recovery Time = Number of seconds that Nbr has to refresh LSPs after restarting. (Restart/Recovery Time is available only if RSVP Hello messages are enabled.)
- `Restart TTD`—Number of seconds remaining for Nbr to send “Hello”. Recovery TTD = Number of seconds remaining for Nbr to refresh LSPs.
- `Hello Status`—Enabled/Disabled/Restarting Nbr Restart Cnt = Number of restarts since Nbr discovery.
- `Last Nbr Restart`—Time and date of the last Nbr restart.
- `Nbr flags`— Nbr flags.
- `Nbr Reference Cnt` —The number of structures currently referencing the nbr structure. Both path state blocks and resv state blocks can reference the nbr structure, so there is not always a 1-to-1 relationship between the number of LSPs and the Nbr Reference Cnt.

1.22 show rsvp track

show rsvp track [*object-name* | **detail**]

1.22.1 Purpose

Displays information about a specific RSVP tracking object or for all RSVP tracking objects currently configured on the router.

1.22.2 Command Mode

All modes

1.22.3 Syntax Description

object-name	Optional. Tracking object.
detail	Optional. Displays detailed information about all tracking objects currently configured on the router.

1.22.4 Default

Displays summary information about all RSVP tracking objects that are currently configured on the router.

1.22.5 Usage Guidelines

Use the **show rsvp track** command to display information about a specific RSVP tracking object or for all RSVP tracking objects currently configured on the router.

1.22.6 Examples

The following example shows how to display summary information about all tracking objects currently configured on the router:

```
[local]Redback#show rsvp track
Track Object          Member Count Observer Count Status
object1               1            0              DOWN
Track1                1            0              UP
Track-mtu             3            2              UP
```

The following example shows how to display information about a tracking object called `object1`:

```
[local]Redback#show rsvp track object1
Track Object object1 is DOWN
Number of members: 1
RSVP interface:1 is DOWN
Tracked by 0 observers
```

The following example shows how to display detailed information about all tracking objects currently configured on the router:

```
[local]Redback#show rsvp track detail

Track Object Track10 is DOWN
        Number of members: 0
        Tracked by 2 observers
         RSVP LSP:AC1MTU2AZUL
         RSVP LSP:AC1AG1VERDE

Track Object Track3 is DOWN         Number of members: 0
        Tracked by 0 observers

Track Object Track4 is DOWN
        Number of members: 0
        Tracked by 0 observers
```

```
Track Object Track5 is DOWN
        Number of members: 0
        Tracked by 0 observers

Track Object Track6 is DOWN
Number of members: 0
Tracked by 0 observers

Track Object Track7 is DOWN
Number of members: 0
Tracked by 0 observers

Track Object Track8 is DOWN
Number of members: 0
Tracked by 0 observers

Track Object Track9 is DOWN
        Number of members: 0         Tracked by 0 observers

Track Object Track-mtu is UP
        Number of members: 6
RSVP interface:IPst.2 is UP
RSVP interface:IPst.14 is DOWN
RSVP interface:abc3 is DOWN
RSVP interface:IPst.4 is UP
RSVP interface:abc is DOWN
RSVP interface:IPst.3 is DOWN
Tracked by 1 observers
RSVP LSP:AC1_MTU1_azul
Track Object Track-new is UP
Number of members: 1
        Tracked by 0 observers
```

1.23 show secured-arp

show secured-arp

1.23.1 Purpose

Displays secured Address Resolution Protocol (ARP) information.

1.23.2 Command Mode

All modes

1.23.3 Syntax Description

This command has no keywords or arguments.

1.23.4 Default

None

1.23.5 Usage Guidelines

Use the **show secured-arp** command to display secured ARP information.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.23.6 Examples

The following example displays secured ARP information:

```
[local]Redback>show secured-arp

Total number of Secured ARP entries in cache: 1

Host                Interface           i/f grid      Circuit
20.1.1.187/32       to-dhcpclient       0x1000000b    11/1 vlan-id 11
20.2.10.0/24        test                0x10000002    11/2
```

1.24 show service

show service [**filter**]

1.24.1 Purpose

Displays enabled and disabled services.

1.24.2 Command Mode

All modes

1.24.3 Syntax Description

`filter` Optional. Displays service filter information.

1.24.4 Default

None

1.24.5 Usage Guidelines

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

Use the optional **`filter`** keyword to display service filter information.

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

Note: By appending a space followed by the pipe (|) character at the end of a **`show`** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.24.6 Examples

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

```
[local]Redback>show service
```

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

1.25 show snmp

show snmp {accesses | communities | server | targets | views}

1.25.1 Purpose

Displays Simple Network Management Protocol (SNMP) information, including usage, configured contexts, communities, SNMP daemon status, targets, and views.

1.25.2 Command Mode

All modes

1.25.3 Syntax Description

accesses Optional. Displays usage.

communities Optional. Displays the communities.

server Optional. Displays the current state of the SNMP daemon and the User Datagram Protocol (UDP) port on which it is currently configured to listen.

targets Optional. Displays configured SNMP targets (notification receivers).

views Optional. Displays the configured Management Information Base (MIB) views.

1.25.4 Default

None

1.25.5 Usage Guidelines

Use the **show snmp** command to display SNMP statistics, including usage, configured contexts, communities, notifications, SNMP daemon status, targets, and views.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.25.6 Examples

The following example displays output from the **show snmp** command with the **views** keyword:

```
[local]Redback>show snmp views

restricted system - included non-volatile
restricted snmp - included non-volatile
restricted snmpEngine - included non-volatile
restricted snmpMPDstats - included non-volatile
restricted usmStats - included non-volatile
```

1.26 show snmp alarm

show snmp alarm {active | cleared | model | stats}

1.26.1 Purpose

Displays Simple Network Management Protocol (SNMP) information for SNMP alarms.

1.26.2 Command Mode

All modes

1.26.3 Syntax Description

active	Display active alarms in Alarm MIB
cleared	Display cleared alarms
model	Display SNMP alarm model table
stats	Display statistics

1.26.4 Default

None

1.26.5 Usage Guidelines

Use the **show snmp alarm** command to display SNMP alarm statistics, alarm model configuration, and lists of active and cleared alarms.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.26.6 Examples

The following example displays output from the **show snmp alarm** command with the **cleared** keyword:

```
[local]Redback>show snmp alarm cleared

=========================================================================
Object name                  : Value
=========================================================================

alarmClearIndex              : 3
alarmClearDateAndTime        : 2009-4-9, 12:28:19, -8:0
alarmClearEngineID           : 80.0.9.30.83.0.0.30.88.1.45.8d [hex]
alarmClearEngineAddressType  : ipv4(1)
alarmClearEngineAddress      : 10.12.49.19
alarmClearContextName        : local
alarmClearLogIndex           : 0
alarmClearNotificationID     : interfaces.3.3.4.5
alarmClearResourceId         : 0.0
alarmClearModelPointer       : 0.0
```

1.27 show snmp ping

show snmp ping [**status** {**name** *ping-test-name*} {**details**} | {**result** {**name** *ping-test-name*}{**success** | **failed** {**history**} {**details**}} {*output*}]

1.27.1 Purpose

Displays information about that status and results of scheduled ping tests.

1.27.2 Command Mode

All modes

1.27.3 Syntax Description

status	Displays the status of scheduled ping tests.
result	Displays the result of the ping test.
name *ping-test-name*	Limits displayed information to the ping test with the name you identify in the *ping-test-name* argument.
success	Displays ping tests that ran successfully.
failed	Displays ping tests that failed.
history	Displays a history of ping test results up to 12 ping tests.
details	Displays a detailed listing of ping test results.

1.27.4 Default

None

1.27.5 Usage Guidelines

Use this command to display the status and results of the scheduled ping tests. If a hostname is used as the ping target, the details keyword shows the resolved IP address of the hostname; otherwise, it shows the ping target IP address.

When you run the command from a non-local context, only the ping tests defined within that context will display. If you run the commands from the local context, you can view all defined ping tests and the output is organized by context.

1.27.6 Examples

The following example displays output from the **show snmp ping** command with the **result** and **history** keywords:

```
[local]Redback>show snmp ping result history
Context: local, Owner: CLI
     name             idx status  sent recv min/max/avg rtt (ms) jitter
--------------------- --- ------- ---- ---- -------------------- ----
ip test #3             1 success     15     15     1000/1000/1000     0
ip test #3             2 success     15     15     1000/1000/1000     0
ip test #3             3 failed      15     0         0/0/0           0
ip test #4             1 failed      15     0         0/0/0           0
ip test #4             2 failed      15     0         0/0/0
```

The following example displays output from the **show snmp ping** command with the **status** and **details** keywords:

```
[local]Redback>show snmp ping status details
Context: local, Owner: CLI
name              status   protocol         target        freq  cnt
------------------- -------- ---------- -------------------- ----- ---
ip test             enabled   ip/icmp   ipaddr-or-hostname   86400 15
 timeout=60, df, size=nn, pattern=0xff, tos=0xff, ttl=255, src=1.2.3.4

Context: local, Owner: SNMP(test1)
name              status   protocol         target        freq  cnt
------------------- -------- ---------- -------------------- ----- ---
ip test             enabled   ip/icmp   ipaddr-or-hostname   86400 15
 timeout=60, df, size=nn, pattern=0xff, tos=0xff, ttl=255, src=1.2.3.4
```

1.28 show snmp traceroute

show snmp traceroute { **result** ***traceroute-test-name*** **details** | ***traceroute-test-name*** **details** }

1.28.1 Purpose

Displays the status of the current SNMP traceroute tests. If SNMP traceroute tests are configured by SNMP set requests and the value of the traceRouteCtlCreateHopsEntries object is set to FALSE, traceroute hop related information will not be displayed when the “detail” option is enabled.

1.28.2 Command Mode

All modes

1.28.3 Syntax Description

traceroute-test-name	Limits displayed information to the traceroute test with the name you identify in the ***traceroute-test-name*** argument. String used to filter in the tests using this string as the test name.
result	Displays the result of the traceroute test.
details	Displays additional traceroute configurations.

1.28.4 Default

None

1.28.5 Usage Guidelines

This command displays the results of the current SNMP traceroute tests. The option ***traceroute-test-name*** is used as a test name filter. The **detail** option is used to display additional hop related information, including hop index, hop IP address, number of probe sent, number of probes received, minimum RTT, max RTT, and average RTT.

1.28.6 Examples

The following example displays output from the **show snmp traceroute** command with the ***traceroute-test-name*** **test_1** and **details** keyword:

```
[local]Redback>show snmp traceroute test_1 details

Context: local      Owner: CLI
Name                    status   protocol   target              freq  cnt
----------------------- -------- ---------- ------------------- ----- ---
test_1                  enabled  ip/udp     1.1.1.1               600   5

df       init-ttl max-ttl  port  size  source           timeout tos
-------- -------- ------- ------ ----- ---------------- ------- ----
disabled 1        30      33434  0     n/a              3       0x0


Totals: 1 test
```

The following example displays the results from the **show snmp traceroute** command with the ***traceroute-test-name*** **test_1** and the **result** and **details** keywords:

```
[local]Redback>show snmp traceroute result test_1 details

Context: local      Owner: CLI
                                hop    test      test
Name                    status  count  attempts  successes  last good path
----------------------- ------- ------ --------- ---------- ---------------
test_1                  running 3      10        10         Jun 21 18:31:12

IP address = 3.3.3.3
                        Hop  hop IP address       sent recv min/max/avg (ms)
                        ---- -------------------- ---- ---- --------------------
                         1   1.1.1.1                3    3                0/1/1
                         2   2.2.2.2                3    3                1/1/1
                         3   3.3.3.3                3    3                0/1/1
Totals: 1 tests
```

1.29 show spanning-tree

show spanning-tree ***bridge-name*** [**details**]

1.29.1 Purpose

Shows the spanning-tree information for the bridge instance.

1.29.2 Command Mode

Exec

1.29.3 Syntax Description

bridge-name Name of the bridge.

details Show detailed spanning-tree information.

1.29.4 Default

None

1.29.5 Usage Guidelines

Use the show spanning-tree to show the spanning-tree information for the bridge instance; that is, use the command to show the spanning-tree information that applies to the whole bridge.

1.29.6 Examples

The following example shows detailed spanning-tree information for the `brdgrp1` bridge:

```
[local]Redback#show spanning-tree brdgrp1 details
```

1.30 show spanning-tree circuit

show spanning-tree *bridge-name* **circuit** *circuit-id* [**details**]

1.30.1 Purpose

Shows the spanning-tree information for specific circuits on the bridge.

1.30.2 Command Mode

Exec

1.30.3 Syntax Description

bridge-name	Name of the bridge.
circuit *circuit-id*	Specifies circuits on the bridge. See Table 4 for the expanded syntax for the circuit-id argument.
details	Provide detailed spanning-tree information.

1.30.4 Default

None

1.30.5 Usage Guidelines

Use the show spanning-tree to show the spanning-tree information for specific circuits on the bridge on the SmartEdge router.

The *circuit-id* argument is composed of the keywords and arguments as described in the following syntax:

slot/port {**ethernet** | **vlan** *vlan-id*}

Table 4 describes the components of the *circuit-id* argument:

Table 4 Building Blocks of the circuit-id Argument

Field	Description
slot	Chassis slot number of the traffic card with the bridged circuits.
port	Port number of the port with the bridged circuits.

Table 4 Building Blocks of the circuit-id Argument

Field	Description
ethernet	Clears all the circuits on the specified Ethernet port.
vlan ***vlan-id***	A filter that limits the command to a specified virtual LAN (VLAN) 802.1Q tunnel or PVC. The ***vlan-id*** argument is one of the following constructs: • ***pvc-vlan-id***—VLAN tag value of a PVC that is not within an 802.1Q tunnel. • ***tunl-vlan-id***—VLAN tag value of an 802.1Q tunnel. • ***tunl-vlan-id*:*pvc-vlan-id***—VLAN tag value of an 802.1Q tunnel followed by the VLAN tag value for the PVC within the tunnel. If you specify the VLAN tag value for an 802.1Q tunnel, this command clears subscriber sessions on all the PVCs in the tunnel. The range of values for any VLAN tag value is 1 to 4095.

1.30.6 Examples

The following example shows detailed spanning-tree information specific to the circuits in the Ethernet port `2/1` in the `brdgrp1` bridge:

```
[local]Redback#show spanning-tree brdgrp1 circuit 2/1 ethernet details
```

1.31 show spanning-tree track

show spanning-tree track {***master-bridge-name context*** | **all** | **all-master**

1.31.1 Purpose

Displays the names of the RSTP master bridge or bridges and the names of their non-RSTP client bridges.

1.31.2 Command Mode

Exec

1.31.3 Syntax Description

master-bridge-name Name of the RSTP master bridge.

context Name of the context in which the RSTP master bridge exists.

all	Display the names of all the spanning-tree master bridges in all contexts and each of their clients.
all-master	Display the names of all the spanning-tree master bridges in all contexts.

1.31.4 Default

None

1.31.5 Usage Guidelines

Use the `show spanning-tree track` command to display the names of the RSTP master bridge or bridges and the names of their non-RSTP client bridges.

1.31.6 Examples

The following example shows the use of the `show spanning-tree tracking` command to display the clients of the spanning tree master bridge `ted` in the context `local`:

```
[local]Redback#show spanning-tree track ted local
Role   Bridge Group                      Context

Master ted                               local
clients : 1   master cct count : 0  master pw count : 0
client cct count : 0   client pw count : 0

Client bob                               local
client cct count : 0     client pw count : 0
```

1.32 show sse

show sse {group | partition} [*group_name* [*partition_name*]] [detail]

1.32.1 Command Mode

All modes

1.32.2 Syntax Description

group	Display SSE group information.
partition	Displays SSE card partition information.
group_name	Optional. Name of the SSE group.

partition_name	Optional. Name of the partition.
detail	Optional. Display detailed information for the specified SSE group or partition.

1.32.3 Usage Guidelines

Displays SSE group or SSE partition information.

See Table 5 for a description of the fields displayed in the output of the command.

Table 5 Command Output Field Descriptions

Output Field	Description
Group	SSE group name.
ID	SSE group ID: 1 to 32.
Description	Group description.
State	Service state of the SSE group: • Up • Partial • Down • Stale—At least one of the partition's NFS mounts was not removed due to the card going out of service. You cannot modify a stale group until the state is corrected. Recover the group by inserting an SSE card with disks in any slot to which the group is bound, or by reloading the system.
Redundancy	SSE group redundancy setting: Network or Disk.
Revert	Switch mode configured: Enabled or Disabled.
Disk Mode	Configured disk mode: RAID-0, RAID-1, or Independent.
Switch Trigger Reason	If applicable, trigger reason for redundancy switch: N/A, Manual, or Auto.
Switch Failed Reason	If applicable, switch failed reason: Alarm events.
Partition(s)	Number of partitions configured.
Name	Name of each partition configured.
ID	Partition ID: 1 to 16.
Group Name	Name of group.
Group ID	Group ID: 1 to 32.
State	Operational status of the partition: Up, Down, Stale.

Table 5 Command Output Field Descriptions

Output Field	Description
Size (GB)	Configured size of the partition.
Percent Used (%)	Data used on the partition, expressed as a percentage.
Disk	Disk number, if designated: 1, 2, or All.
Mirrored	Mirror data to standby disk, if network redundancy is configured: Enabled, Disabled, N/A.
Alarm Low Space	Alarm for low partition space: Enabled or Disabled.
Trigger Percentage	Triggering disk space in percentage; clear percentage in brackets.
Alarm(s)	Alarms triggered on the partition.
Primary	Primary slot assigned to the group: **slot *slot_num***.
Secondary	If redundancy is configured, the secondary slot assigned to the group: **slot *slot_num***.
Disk Mode	Configured disk mode for the group: RAID-0, RAID-1, or Independent.
Redundancy State	The acting status of the redundancy group. Standalone is assigned for nonredundant groups: Active, Standby, or Standalone.
Disk ID(s) Ready	Indicates which disks are ready for service: 1, 2, All, or None.
Total Disk Size	Total disk size available on the slot/disk, rounded to the nearest GB.
Data Status	The redundancy status of the data on the disk. Sync-in-progress means that the redundancy data is being synchronized from the current active slot/disk: Up-to-date or Sync-in-progress.
Alarm(s)	Alarm(s) raised for the slot/disk.
Sync Progress	If synchronization is happening, it shows the progress as a status bar with percentage completed, as well as size synchronized and total to be synchronized.
Time Remaining	Estimated time remaining for the sync to complete: HH:MM:SS.
Speed	Current speed of the sync in KB/sec.
Mean Speed	Mean speed of the sync in KB/sec.

1.32.4 Examples

```
[local]Redback#show sse group
Group            ID Redundancy        Disk Mode   Slot    State
-----------------------------------------------------------------
grp1             1  network-redundant Independent 2 (5)   Down
```

```
[local]Redback#show sse group detail
Name                : grp1
ID                  : 1
Description         :
------------------------------------------------------------------------
State               : Up
Redundancy          : network-redundant
Disk Mode           : Independent
Revert              : no revert
Switch Reason       : Standby INS
Switch Failed Reason: No Reason
Alarms              : NONE

Partition(s)        :
-----------------------------------------
Name                : ptn1              ID                  : 1
Group Name          : grp1              Group ID            : 1
State               : Up
Size (GB)           : 2                 Percent Used        : 9
Disk                : 1                 Mirrored            : Enabled
Alarm Low Space     : Enabled           Trigger Percentage  : 80 (clear 70)
Alarms              : NONE

Name                : ptn2              ID                  : 2
Group Name          : grp1              Group ID            : 1
State               : Up
Size (GB)           : 2                 Percent Used        : 2
Disk                : 1                 Mirrored            : Disabled
Alarm Low Space     : Enabled           Trigger Percentage  : 80 (clear 70)
Alarms              : NONE


Primary Slot        : 2
-----------------------------------------
Redundancy State    : Active            Slot State          : Up
Disk ID(s) Ready    : All               Total Size (GB)     : 268
Data Status         : Up-To-Date
Active Alarms       : NONE

Secondary Slot      : 5
-----------------------------------------
Redundancy State    : Standby           Slot State          : Up
Disk ID(s) Ready    : 1                 Total Size (GB)     : 134
Data Status         : Up-To-Date
Active Alarms       : NONE


[local]Redback#show sse partition
Group            ID Partition        ID Size (GB) Disk   State
-----------------------------------------------------------------
grp1             1  ptn1             1  2         1      Up
grp1             1  ptn2             2  2         1      Up


[local]Redback#show sse partition detail
Name                : ptn1              ID                  : 1
Group Name          : grp1              Group ID            : 1
State               : Up
Size (GB)           : 2                 Percent Used        : 9
Disk                : 1                 Mirrored            : Enabled
Alarm Low Space     : Enabled           Trigger Percentage  : 80 (clear 70)
Alarms              : NONE

Name                : ptn2              ID                  : 2
Group Name          : grp1              Group ID            : 1
State               : Up
Size (GB)           : 2                 Percent Used        : 2
Disk                : 1                 Mirrored            : Disabled
Alarm Low Space     : Enabled           Trigger Percentage  : 80 (clear 70)
Alarms              : NONE
```

1.33 show sse counters

show sse {group | partition} counters [*group_name* [*partition_name*]]

1.33.1 Command Mode

All modes

1.33.2 Syntax Description

group	Display SSE group information.
partition	Display SSE card partition information.
group_name	Optional. Name of the SSE group.
partition_name	Optional. Name of the partition.

1.33.3 Usage Guidelines

Displays SSE group or SSE partition counters.

1.33.4 Examples

```
[local]Redback#show sse group counters
Name                : grp1
ID                  : 1
Redundancy          : network-redundant
Primary Slot        : 2                 Redundancy State    : Active
Secondary Slot      : 5                 Redundancy State    : Standby

Partition(s)        :
------------------------------------------------------------------------
timestamp: 11486967468
timestamp secs: 11486  timestamp usecs: 967468

Name                : ptn1              ID                  : 1
Group Name          : grp1              Group ID            : 1
Disk Allocated      : 1                 Partition Size (GB) : 2
Percent Used        : 9                 Percent Available   : 91
Network Send        : 2097100
Network Received    : 0
Disk Write (KB)     : 12
Disk Read (KB)      : 2097826
Activity Log        : 1
Bit Map             : 128
Local Count         : 0
Local Pending       : 0
Unacknowledged      : 0
Application Pending : 0

timestamp: 11486968702
timestamp secs: 11486  timestamp usecs: 968702

Name                : ptn2              ID                  : 2
Group Name          : grp1              Group ID            : 1
Disk Allocated      : 1                 Partition Size (GB) : 2
Percent Used        : 2                 Percent Available   : 98
Network Send        : 0
Network Received    : 0
Disk Write (KB)     : 32
Disk Read (KB)      : 738
Activity Log        : 2
Bit Map             : 0
Local Count         : 0
Local Pending       : 0
Unacknowledged      : 0
Application Pending : 0
```

1.34 show ssh-attributes

show ssh-attributes

1.34.1 Purpose

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

1.34.2 Command Mode

All modes

1.34.3 Syntax Description

This command has no keywords or arguments.

1.34.4 Default

None

1.34.5 Usage Guidelines

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

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.34.6 Examples

The following example displays SSH attributes:

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

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

1.35 show static route

show static route [**print-prefix**] [**all**] [**ipv6**]

1.35.1 Purpose

Displays static route information.

1.35.2 Command Mode

All modes

1.35.3 Syntax Description

`print-prefix` Optional. Displays the IP address and prefix length for static routes with multiple next hops. By default, entries in the prefix field are left blank.

`all` Optional. Displays static route information for all contexts.

[**`ipv6`**] Optional. Displays IPv6 static route information.

1.35.4 Default

None

1.35.5 Usage Guidelines

Use the **`show static route`** command to display static route information.

Note: By default, most show commands display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can precede the **`show`** command with the **`context`** ***`ctx-name`*** construct to view output for the specified context without entering that context. For more information about using the **`context`** ***`ctx-name`*** construct, see the **`context`** command description.

Note: To filter the output, at the end of the **`show`** command, append a space followed by a pipe (|) and the keywords and arguments for filtering. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

Table 6 describes the **`show static route`** command output fields.

Table 6 Field Descriptions for the show static route Command

Field	Description
Prefix	IP address and prefix length.

Table 6 Field Descriptions for the show static route Command

Field	Description
Best	• Yes—Indicates that the next hop or path is considered the best path. • No—Indicates that it is not the best next hop or path. A hyphen (-) is attached if the prefix has not been advertised into the Router Information Base (RIB).
NType	Next-hop type. The types can be addr (IP address), intf (interface), dvsr, or cntx (context). The dvsr next-hop type is a special type of IP address.
Addr/Intf/Cntx	Detailedl next-hop information. The information displayed can be an IP address, interface name, context name, or null0 (a special interface name).
NS	Next-hop status. The status is either up or dn (down). It reflects the status of either the next-hop IP address reachability, the next-hop interface status, or the next-hop context.
Dist	Route distance to be advertised into the RIB.
P	An asterisk (*) indicates that the route is a permanent announced route.
Tag	Tag value of the prefix.

1.35.6 Examples

The following example displays output from the **show static route** command:

```
[local]Redback>show static route

  Prefix             Best  NType Addr/Intf/Cntx    NS  Dist  P  Tag
  8.1.1.1/30         yes   dvsr  165.63.39.15      up  1        0x0
  10.1.1.0/24        yes   intf  ether3/1          up  1        0x0
                     no    intf  op-net-lan        up  10       0x0
  10.1.2.0/24        yes   intf  to-redback       up  1        0x0
  10.11.12.0/24      yes   cntx  foo               up  1        0x0
  20.0.0.0/8         yes   intf  to-redback       up  1        0x0
                     yes   addr  165.63.39.1       up  1        0x0
  30.0.0.0/8         yes   intf  null0             up  1        0x0
  40.1.0.0/16        no-   cntx  vpn-abc           dn  1        0x0
  50.1.2.0/24        yes   addr  165.63.39.2       up  1     *  0x0

  Total static route in context local: 8, total path: 10
```

The following examples display output from the **show static route** and **show static route ipv6** commands with BFD enabled:

```
[local]Redback#show static route
Prefix              Best  NType Addr/Intf/Cntx    NS  Dist  F  Tag BFD
2.2.2.1/32          yes   addr  12.1.1.2          up  1        0x0 yes
2.2.2.2/32          yes   addr  13.1.1.2          up  1        0x0 no


[local]Redback#show static route ipv6
Prefix              Best  NType Addr/Intf/Cntx    NS  Dist  F  Tag BFD
3000::/64           yes   addr  2000::2           up  1        0x0 yes
```

1.36 show subscribers

To display the basic subscriber status fields:

show subscribers [{**active** | **agent-circuit-id** *id* | **agent-remote-id** *id* | **all** | {**session** *slot/port*[**:***chan-num*[**:***sub-chan-num*]] [*circuit-id*]} | **session l2tp lns** *id* | **username** *subscriber*}]

To display the digital subscriber line (DSL) attributes associated with subscribers:

show subscribers access-line [{**agent-circuit-id** *id* | **agent-remote-id** *id* | **all** | {**session** *slot/port*[**:***chan-num*[**:***sub-chan-num*]] [*circuit-id*]} | **session l2tp lns** *id* | **username** *subscriber*}]

To display the attributes of active subscriber sessions:

show subscribers active [{**agent-circuit-id** *id* | **agent-remote-id** *id* | **all** | {**session** *slot/port*[**:***chan-num*[**:***sub-chan-num*]] [*circuit-id*]} | **session l2tp lns** *id* | **username** *subscriber*}]

To display the Mobile IP attributes associated with subscribers:

show subscribers mobile-ip [{**agent-circuit-id** *id* | **agent-remote-id** *id* | **all** | {**session** *slot/port*[**:***chan-num*[**:***sub-chan-num*]] [*circuit-id*]} | **session l2tp lns** *id* | **username** *subscriber*}]

To display the authentication, authorization, and accounting (AAA) logs of subscribers:

show subscribers log *[{{***session** *slot/port[:chan-num[:sub-chan-num]]* [*circuit-id*]} | **session l2tp lns** *id* | **username** *subscriber}]*

To display a summary of subscriber information:

show subscribers summary [[**ipv4** | **ipv4-only** | **ipv6** | **ipv6-only** | **dual-stack**] **all**]

To display information about the subscriber licenses currently being used by the system:

show subscribers license summary

To display IP information associated with subscribers:

show subscribers address username ***subscriber***

1.36.1 Purpose

Displays subscriber information.

1.36.2 Command Mode

All modes

1.36.3 Syntax Description

agent-circuit-id ***id***	Optional. A filter that limits the information displayed to the subscriber specified by the agent circuit ID in a subscriber record. Enter the ***id*** argument as a structured subscriber username in the form subscriber@context.
agent-remote-id ***id***	Optional. A filter that limits the information displayed to the subscriber specified by the agent remote ID in a subscriber record. Enter the ***id*** argument as a structured subscriber username in the form **subscriber@context**.
all	Optional. Displays information about all subscribers in all contexts. This keyword is available only to administrators in the local context.
session	Optional. Limits the command output to the specified session or circuit.
slot	Optional. Chassis slot number for a traffic card.
port	Optional. Port number on the specified traffic card.
circuit-id	Optional. A subscriber session identifier, or a subscriber username that filters which subscriber information this command displays. See Table 7 for information about the ***circuit-id*** argument.
l2tp lns ***id***	Optional. Limits the output of the command output to the specified Layer 2 Tunneling Protocol (L2TP) network server (LNS) circuit.
username ***subscriber***	Optional. Limits the command output to subscribers specified by a subscriber name. Enter the ***subscriber*** argument as a structured subscriber username in the form **subscriber@context**.
access-line	Optional. Displays the DSL attributes.
active	Optional. Displays the attributes of active subscriber sessions.
mobile-ip	Optional. Displays the Mobile IP attributes for the specified subscriber sessions.

log	Optional. Displays the AAA log.
summary	Optional. Displays the total number of subscribers and their encapsulations in the current context.
ipv4	Optional. Displays all IPv4 subscriber sessions on the system (single and dual-stack). Information is displayed for the current context only; to display information for all contexts, include the **all** keyword in the command string.
ipv4-only	Optional. Displays ipv4 subscriber sessions only (for subscribers that are authorized to carry IPv4 traffic only). Information is displayed for the current context only; to display information for all contexts, include the **all** keyword in the command string. Be aware that this keyword does not display information about dual-stack subscribers that have only the IPv4 stack active.
ipv6	Optional. Displays all IPv6 subscriber sessions on the system (single and dual-stack). Information is displayed for the current context only; to display information for all contexts, include the **all** keyword in the command string.
ipv6-only	Optional. Display IPv6 subscriber sessions only (for subscribers that are authorized to carry IPv6 traffic only). Information is displayed for the current context only; to display information for all contexts, include the **all** keyword in the command string. Be aware that this keyword does not display information about dual-stack subscribers that have only the IPv6 stack active.
dual-stack	Optional. Displays dual-stack subscriber sessions only (for subscribers that are authorized for both IPv4 and IPv6, and can simultaneously support both IPv4 and IPv6 traffic). Information is displayed for the current context only; to display information for all contexts, include the **all** keyword in the command string. Be aware that this keyword only displays information for dual-stack subscribers that have both stacks (IPv4 and IPv6) active.
license	Optional. Displays information about the subscriber licenses currently configured on the system.
address	Optional. Displays the IP information.

1.36.4 Default

Displays information for all active subscribers in the current context.

1.36.5 Usage Guidelines

Use the **show subscribers** command to display subscriber information. This includes basic subscriber status fields, DSL attributes, attributes of active

subscriber sessions, Mobile IP attributes, AAA log or logs, a summary of subscriber information, and IP addresses associated with subscribers.

The ***circuit-id*** argument represents the following keywords and arguments; see Table 7:

clips [***clips-session***] | **pppoe** [***pppoe-session***] | **vlan-id** ***vlan-id*** [**pppoe** [***pppoe-session***] | **clips** [***clips-session***]] | **vpi-vci** ***vpi vci*** [**pppoe** [***pppoe-session***] | **clips** [***clips-session***]]

Table 7 Building Blocks of the circuit-id Argument

Construct	Description
clips ***clips-session***	A filter that limits the command to a specified CLIPS circuit on a port, channel, 802.1Q PVC, or ATM PVC. If the CLIPS circuit is on an 802.1Q or ATM PVC, also specify the circuit identifier for the 802.1Q or ATM PVC. If the session is not specified, the command applies to all CLIPS sessions in the context. The range of values for the ***clips-session*** argument is 1 to 262,144.
pppoe ***pppoe-session***	A filter that limits the command to a specified PPPoE session. If the ***pppoe-session*** argument is not specified, the command applies to all PPPoE sessions in the context.
vlan-id ***vlan-id***	A filter that limits the command to a specified virtual LAN (VLAN) 802.1Q tunnel or PVC. The ***vlan-id*** argument is one of the following constructs: • **vlan-id** ***pvc-vlan-id***VLAN tag value of a PVC that is not within an 802.1Q tunnel. • **vlan-id** ***tunl-vlan-id***VLAN tag value of an 802.1Q tunnel. • **vlan-id** ***tunl-vlan-id:pvc-vlan-id***VLAN tag value of an 802.1Q tunnel followed by the VLAN tag value for the PVC within the tunnel. If you specify the VLAN tag value for an 802.1Q tunnel, this command clears subscriber sessions on all the PVCs within the tunnel. The range of values for any VLAN tag value is 1 to 4,095.
vpi-vci ***vpi vci***	A filter that limits the command to a specified ATM PVC. The ATM PVC is specified by the virtual path identifier (VPI) and virtual circuit identifier (VCI). The range of values is 0 to 255 and 1 to 65,534, respectively.

The slot and port assignments for the SmartEdge routers are described in their respective hardware guides.

Use the **access-line** keyword to display information about DSL line attributes for each subscriber. The output information includes the parameters learned from the DSL attribute extension Type, Length, Value (TLV) in the General Switch Management Protocol (GSMP) Port Up message for the DSL.

The DSL attributes are learned from the DSL access multiplexer (DSLAM). They can be learned by GSMP messages and from PPPoE or DHCP tags during a subscriber session setup. Each learned attribute is preceded by the words Access Node Control Protocol (ANCP) or DSL Forum (DSLF) when printed. This indicates the mechanism by which it was learned. For example, ANCP means it was learned by ANCP; DSLF was learned from a tag during subscriber session setup; and so forth.

Table 8 lists the types of DSL data and the values that this command can display.

Table 8 Data Displayed by the access-line Keyword

Type of Data	Value
Agent-Circuit-ID	This includes DSLAM slot, port and channel number.
Internal Circuit	This includes the internal circuit number, slot, port and channel numbers.
Neighbor ID	Neighbor ID number
DSL Line State	• SHOWTIME (DSL is active) • IDLE (DLS is down) • SILENT (DSL is down)
DSL Data Rates	• Actual data rates upstream (inbound to the SmartEdge router) and downstream (outbound from the SmartEdge router) in Kbps • Minimum and maximum data rates upstream and downstream in Kbps • Attainable data rates upstream and downstream in Kbps • Minimum low-power data rates upstream and downstream in Kbps • Actual and maximum interleaving delay upstream and downstream in msec
ACI/ARI Global-session-limit	The current maximum number of sessions enforced for the ACI/ARI. This field is only displayed if the **`aaa global suppress-authentication slid-session-limit`** command is configured.
ACI/ARI Total-sessions-up	The total number of sessions that are UP. This field is only displayed if the **`aaa global suppress-authentication slid-session-limit`** command is configured.
ACI/ARI Total-sessions-in-progress	The total number of sessions that are authenticating. This field is only displayed if the **`aaa global suppress-authentication slid-session-limit`** command is configured.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

Use the **show bindings** command to get the binding information that optionally can be specified in the **show subscribers** command. For information on the **show bindings** command, see the *Command List*.

The **show subscribers** command used with the **active** keyword, provides information on the dynamic policy rules applied to active subscriber sessions.

The slot and port numbering rules for the SmartEdge 100, SmartEdge 400, and SmartEdge 800 routers are described in their respective hardware guides.

Use the **show subscribers summary** command to display information about the subscriber sessions on the system. The following information is displayed:

- The type of subscriber sessions whose information is displayed
- The number of subscriber sessions currently being authenticated.
- The number of active subscriber sessions.
- The number of subscriber sessions currently disconnecting.

Note: The **ipv4-only** and **ipv6-only** keywords do not display information about dual-stack sessions that have only the specified stack active. For example, the **ipv4-only** keyword does not display information for dual-stack sessions that have only the IPv4 stack active.

Use the **show subscribers license summary** command to display the subscriber licenses currently being used by the system. Usage information for following types of subscribers is displayed:

- LAC
- IPv4
- IPv6
- Dual-stack

Subscriber licenses are applicable to LAC, IPv4, and dual-stack subscribers only, and IPv6 licenses are applicable to IPv6 and dual-stack subscribers.

Dual-stack subscribers must have an IPv4 license and an IPv6 license configured.

1.36.6 Examples

The following example shows typical output:

```
[local]Redback>show subscribers

Type     CIRCUIT  SUBSCRIBER          CONTEXT     START TIME
-------------------------------------------------------------------------
PPPOE    00001   pppoe@redback.com    company1    JUN 30 17:46:49 2005
VIPSRC   00002   00:dd:00:00:00:01    isp1        JUN 30 00:03:11 2005
VIPSRC   00003   00:dd:00:00:00:02    isp1        JUN 30 00:03:01 2005
VIPSRC   00004   00:dd:00:00:00:03    isp1        JUN 30 00:03:01 2005
VIPSRC   00005   00:dd:00:00:00:04    isp1        JUN 30 00:03:11 2005
VIPSRC   00006   00:dd:00:00:00:05    isp1        JUN 30 00:03:11 2005
-------------------------------------------------------------------------
Total=6

Type            Authenticating          Active          Disconnecting
PPP                          0               0                      0
PPPoE                        0               1                      0
DOT1Q                        0               0                      0
CLIPs                        0               5                      0
ATM-B1483                    0               0                      0
ATM-R1483                    0               0                      0
```

The following example displays the information for an active subscriber; it includes both the `absolute timeout 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
        session time left 3215
        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)
```

The following example shows the dynamic policy access control lists (ACLs) applied in the forward direction to the active subscriber session `usr1@local`. For information on the dynamic policy fields displayed in both **`show`** commands, see **`show access-group`** command in the *Command List*:

```
[local]Redback>show subscribers active
usr1@local
        Circuit   2/1 clips 1
        Internal Circuit   2/1:1023:63/4/2/1
        Interface bound  clips1
        Current port-limit unlimited
        session time left 3215
        ip address 11.1.0.1 (applied)
        forward policy in forpol (applied)
        dynamic policy acl  (applied in: fwd)
           ip in forward srcip 11.1.0.51/32 tos 0x08 0x1e class c1 fwd
           ip in forward srcip 11.1.0.51/32 tos 0x40 0xe0 class c1 fwd
           ip in forward srcip 11.1.0.51/32 tos 0x48 0xfe class c1 fwd
           ip in forward srcip 11.1.0.51/32 tos 0x0c 0x1e class c1 fwd
           ip in forward srcip 11.1.0.51/32 dscp af41 class c1 fwd
```

Use the **show subscribers active all** command to view if the RFlow profile is applied to the subscriber in the ingress direction (in), egress direction (out), or bi-directionally (both). In the following example, the flow ip profile has been applied at ingress:

```
[local]Redback# show subscribers active all
client2162833@local
Circuit 4/1:1 vpi-vci 33 145 pppoe 2450
Internal Circuit 4/1:1:63/1/2/8193
Interface bound subs
Current port-limit unlimited
session time left 3215
ip pool subs (applied from sub_default)
ip source-validation 1 (applied from sub_default)
ip address 2.2.0.1 (applied from pool)
flow ip profile ingress-flow:in (applied)
```

The following example includes DSL fields in the command output:

```
[local]Redback>show subscribers access-line
test@local
        Agent Circuit ID "DSLAM1-slot0-port0-channel2"
        Internal Circuit   4/3:1023:63/1/2/6
        Neighbor ID 10.13.16.98:6068
        ANCP Line State    SHOWTIME
        ANCP Actual Data Rate Downstream (kbps)    7777 (applied)
```

The following example shows the vendor-class-identifier (`dhcp vendor class id`) is applied to the user session and used by the system for context selection.

```
[local]Redback>show subscribers active
        00:00:68:0d:01:02@pacbell.net
        Session state Up
        Circuit   10/1 vlan-id 10:10 clips 131100
        Internal Circuit   10/1:1023:63/7/2/28
        Interface bound  subs
        Current port-limit unlimited
        dhcp vendor class id pacbell.net (not applied)
        dhcp max-addrs 1 (applied)
        context-name pacbell.net (not applied)
        dhcp vendor class id pacbell.net (applied)
          IP host entries installed by DHCP: (max_addr 1 cur_entries 1)
            30.30.30.10    00:00:68:0d:01:02
```

The following example shows how to display information about the dual-stack sessions on the system:

```
[local]Redback#show subscribers summary dual-stack


--------------------------------------------------------------------------------
Total=0

Type            Authenticating          Active          Disconnecting
PPP                          0               0                      0
PPPoE                        0               1                      0
DOT1Q                        0               0                      0
CLIPs                        0               0                      0
ATM-B1483                    0               0                      0
ATM-R1483                    0               0                      0
Mobile-IP                    0               0                      0
```

The following example shows how to display the number of subscriber licenses that are in use for each type of subscriber:

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

Subscriber-Type         Subscriber-License    IPv6-License
                             Used                  Used

LAC                          0                   0
IPv4 Only                    1                   0
IPv6 Only                    0                   0
Dual-Stack                   0                   0
```

The following example shows the output of the **`show subscribers access-line agent-circuit-id`** command when the **`aaa global suppress-authentication slid-session-limit`** command is configured. Similar output is provided for the **`agent-remote-id`** option.

```
[local]Redback#show subscribers access-line agent-circuit-id test
user@local
Agent Circuit ID "test"
        Internal Circuit   1/1:511:63:31/6/2/1
        ACI Global session-limit       :     4
        Total ACI Sessions Up          :     2
        Total ACI Sessions In-Progress :     0
```

1.37 show system alarm

For SSE cards, the syntax is:

show system alarm [all | **sse [***group_ID* **[***partition_ID***]]]**

For ports on Asynchronous Transfer Mode (ATM) OC, Ethernet, or Packet over SONET/SDH (POS) traffic cards, the syntax is:

show system alarm [**all** | ***slot***[**/***port*]]

1.37.1 Purpose

Displays system-level, card-level, or port-level alarms.

1.37.2 Command Mode

All modes

1.37.3 Syntax Description

all	Optional. Displays alarms at all levels.
slot	Optional. Chassis slot number of the traffic card for which card-, port-, channel-, and subchannel-level alarms are displayed.
port	Optional. Card port number of the port for which port-, channel-, and subchannel-level alarms are displayed.
chan-num	Optional. Channel number for which channel- and subchannel-level alarms are displayed. The range of values depends on the type of port.
sub-chan-num	Optional. Subchannel number for which subchannel-level alarms are displayed. The range of values depends on the type of port.
sse	Optional. Displays alarm information for all SSE group and partition alarms.
group_ID	Optional. Displays alarm information for the specified SSE group ID. See the output of the **show sse group** command for valid values.
partition_ID	Optional. Displays alarm information for the specified partition ID. See the output of the **show sse partition** command for valid values.

1.37.4 Default

Displays system-level alarms only.

1.37.5 Usage Guidelines

Use the **show system alarm** command to display system-level, card-level, port-level, channel-level, or subchannel-level alarms.

Each succeeding argument restricts the display to the alarms at that level and below and to the alarms for that card, or port, channel, or subchannel.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

Use the **show port detail** command (in any mode) to view the alarms for a port. See the *Command List* for more information.

Use the **show diag** command (in any mode) to view the results of the power-on diagnostics (POD) or on-demand diagnostics (ODD).

1.37.6 Examples

The following example displays system-level alarms only:

```
[local]Redback>show system alarm


Timestamp       Type              Source      Severity  Descriptions
-------------------------------------------------------------------------------
Dec 16 19:32:01 chassis                       Minor     Chassis power failure - side B
```

The following example displays all system-level alarms:

```
[local]Redback#show system alarm all
Timestamp       Type              Source         Severity  Description
-------------------------------------------------------------------------
Jul 27 13:24:35 chassis                          Minor     Chassis power failure - side A1
Jul 27 13:24:35 chassis                          Minor     Chassis power failure - side A2
Jul 27 16:27:32 sse               5d2            Major     Hard disk missing
Jul 27 13:24:36 xcrp4-base        7              Major     Backup fail: peer dead
Jul 27 13:24:36 xcrp4-base        8              Critical  Controller missing
Jul 27 13:24:46 xcrp4-base        8              Major     Controller auto switch completed
```

The following example displays alarms at the traffic card level and below only; in this case, the traffic card is not installed:

```
[local]Redback#show system alarm 4
```

```
Timestamp       Type              Source         Severity  Descriptions
------------------------------------------------------------------------
Dec 10 18:48:33 oc3e-8-port 4                 Critical  Circuit pack missing
```

The following example displays alarms at the port-level and below only; in this case, only a channel alarm is present:

```
[local]Redback#show system alarm 13/2
Timestamp       Type          Source    Severity  Descriptions
------------------------------------------------------------------------
Dec 10 18:48:49 oc12e-4-port   13/2:1    Major     Path alarm indication signal (AIS-P)
```

1.38 show system nvlog

show system nvlog

1.38.1 Purpose

Displays the contents of nonvolatile memory (NVRAM) on the controller card to which you are connected.

1.38.2 Command Mode

All modes

1.38.3 Syntax Description

This command has no keywords or arguments.

1.38.4 Default

None

1.38.5 Usage Guidelines

Use the **show system nvlog** to display the contents of NVRAM on the controller card to which you are connected. The NVRAM stores logs of trap- and panic-related messages from the operating system and can be used to help debug system crashes in the absence of a local console (connected to the Craft 2 port). If your system does not support NVRAM, you receive the following error message: `This XCRP doesn't support this feature`.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.38.6 Examples

The following example displays the contents of the NVRAM on the active controller card:

```
[local]Redback>show system nvlog

panic: testing
Redback: dumpsys called
dumping to dev 10,33 offset 8
dump succeeded
!!!vxWorks sent REBOOT intr, will shutdown BSD!!!
!!!vxWorks sent REBOOT intr, will shutdown BSD!!!
!!!vxWorks sent REBOOT intr, will shutdown BSD!!!
```

1.39 show tacacs+ server

show tacacs+ server [{{*ip-addr* | *hostname*} [**port** *tcp-port*]}]

1.39.1 Purpose

Displays information for one or all Terminal Access Controller Access Control System Plus (TACACS+) servers in the current context.

1.39.2 Command Mode

All modes

1.39.3 Syntax Description

ip-addr	Optional. IP address of the TACACS+ server for which more detailed information is to be displayed. Additional information includes detailed error and status counters, such as packets received and transmitted.
hostname	Optional. Hostname of the TACACS+ server.
port ***tcp-port***	Optional. TACACS+ server Transmission Control Protocol (TCP) port. The range of values is 1 to 65,536. If no port is specified, TCP port number 49 is used.

1.39.4 Default

None

1.39.5 Usage Guidelines

Use the **show tacacs+ server** command to display information for one or all TACACS+ servers in the current context, including the IP address and the key set by the **tacacs+ server** command (in context configuration mode), and the values set by the **tacacs+ max-retries** and **tacacs+ timeout** commands (in context configuration mode).

Use the ***ip-addr*** or ***hostname*** argument to display detailed information for a particular server; otherwise, the system displays summary information for all servers in the context.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.39.6 Examples

The following example displays summary information for all TACACS+ servers in the context:

```
[local]Redback#show tacacs+ server
```

```
IP Address/Hostname Port Timeout/Max-Tries Key
------------------------------------------------------------------
10.12.121.211       49   5/1               mykey
10.12.209.171       49   5/1               otherkey
```

The following example displays information for a specific TACACS+ server:

```
[local]Redback#show tacacs+ server 10.12.211.121

IP Address/Hostname     Port    State           In-svc          Key
------------------------------------------------------------------------
10.12.211.121           49      untried         alive           mykey

Counter                          Value
-------                         ----------
Current sessions                         0
Transmitted packets                      8
Received packets                         8
Dropped packets                          0
Connection errors                        0
Connection timeouts                      0
Host unreachable errors                  0
Transmission errors                      0
Reception errors                         0
Authentication timeouts                  0
Authorization timeouts                   0
Accounting timeouts                      0
```

1.40 show tcp

show tcp [{**brief** [**all**] | **md5** | **statistics** | **tcb** ***tcpcb-addr***}]

1.40.1 Purpose

Displays Transmission Control Protocol (TCP) Internet connections, statistics, and keepalive settings.

1.40.2 Command Mode

All modes

1.40.3 Syntax Description

brief	Optional. Displays active Internet connections.
all	Optional. Displays active Internet connections, including servers. Used with the brief keyword.
md5	Optional. Displays Message Digest 5 (MD5) entries.
statistics	Optional. Displays TCP statistics.
tcb ***tcpcb-addr***	Optional. TCP connection for which details are to be displayed.

1.40.4 Default

None

1.40.5 Usage Guidelines

Use the **show tcp** command to display TCP Internet connections, statistics, and keepalive settings.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.40.6 Examples

The following example displays output when the statistics keyword is specified:

```
[local]Redback>show tcp statistics

tcp:
        85778 packets sent
                33921 data packets (934491 bytes)
                323 data packets (91638 bytes) retransmitted
                26522 ack-only packets (77668 delayed)
                0 URG only packets
```

```
        0 window probe packets
        24871 window update packets
        141 control packets
123389 packets received
        33053 acks (for 936341 bytes)
        537 duplicate acks
        0 acks for unsent data
        102667 packets (37396219 bytes) received in-sequence
        132 completely duplicate packets (189 bytes)
        0 old duplicate packets
        167 packets with some dup. data (232 bytes duped)
        39 out-of-order packets (13 bytes)
        0 packets (0 bytes) of data after window
        0 window probes
        7 window update packets
        1 packet received after close
        0 discarded for bad checksums
        0 discarded for bad header offset fields
        0 discarded because packet too short
26 connection requests
75 connection accepts
82 connections established (including accepts)
98 connections closed (including 24 drops)
18 embryonic connections dropped
32255 segments updated rtt (of 32538 attempts)
333 retransmit timeouts
        1 connection dropped by rexmit timeout
0 persist timeouts (resulting in 0 dropped connections)
110 keepalive timeouts
        86 keepalive probes sent
        24 connections dropped by keepalive
6023 correct ACK header predictions
89333 correct data packet header predictions
224 PCB hash misses
64 dropped due to no socket
0 connections drained due to memory shortage
1 bad connection attempt
79 SYN cache entries added
```

```
                0 hash collisions
                75 completed
                0 aborted (no space to build PCB)
                0 timed out
                0 dropped due to overflow
                0 dropped due to bucket overflow
                4 dropped due to RST
                0 dropped due to ICMP unreachable
          1 SYN,ACK retransmitted
          1 duplicate SYN received for entries already in the cache
          0 SYNs dropped (no route or no space)
```

The following example displays output when a TCP connection address is specified:

```
[local]Redback>show tcp tcb 0xe091a630
```

```
TCP Protocol Control Block at 0xe091a630:

Timers:         REXMT: 1430     PERSIST: 0      KEEP: 15827     2MSL: 0

State: ESTABLISHED, flags 0x38a0, inpcb 0xe090ca80

rxtshift 0, rxtcur 3, dupacks 0
peermss 498, ourmss 8152, segsz 498

snd_una 2215311423, snd_nxt 2215311425, snd_up 2215311423
snd_wl1 16681764, snd_wl2 2215311423, iss 2215310590, snd_wnd 8271

rcv_wnd 24456, rcv_nxt 16681766, rcv_up 16681764, irs 16681574
rcv_adv 16706222, snd_max 2215311425, snd_cwnd 51294, snd_ssthresh
1073725440
max_sndwnd 8466

idle 0, rtt 1, rtseq 2215311423, srtt 35, rttvar 3, rttmin 2

oobflags 0, iobc 0, softerror 0

snd_scale 0, rcv_scale 0, req_r_scale 0, req_s_scale 0
ts_recent 0, ts_regent_age 0, last_ack_sent 16681766
```

The following example displays the output of this command when no keywords or arguments are specified:

```
[local]Redback>show tcp

Active Internet connections
PCB      Recv-Q Send-Q Local Address         Foreign Address        State
99e1a28       0      0 10.12.49.56.23        155.53.44.159.38903    ESTABLISHED
99e1960       0      0 10.12.49.56.23        155.53.44.159.43022    ESTABLISHED
99e1898       0      0 127.0.2.5.64524       127.0.2.3.6667         ESTABLISHED
99e17d0       0      0 127.0.2.5.56326       *.*                    LISTEN
99e1708       0      0 127.0.2.5.57435       127.0.2.3.6667         ESTABLISHED
99e1640       0      0 127.0.2.5.51241       127.0.2.3.6666         ESTABLISHED
99e1578       0      0 127.0.2.5.54221       127.0.2.3.6666         ESTABLISHED

IP Path MTU discovery is enabled
TCP keep-alive idle = 14400
TCP keep-alive interval = 150
TCP keep-alive count = 8
```

1.41 show tech-support

show tech-support [aaa | ase | ase2 | atm | bfd | bgp | dhcp | dot1q | flowd | gre | igmp | ipv6 | isis | l2tp | ldp | mobile-ip | ospf | ospf3 | pim | ppp | pppoe | qos | rdb | snmp]

1.41.1 Purpose

Collects system information to enable customer support to resolve issues; includes both basic and module-related versions..

1.41.2 Command Mode

All modes

1.41.3 Syntax Description

aaa Collects Authentication, Authorization, and Accounting configuration and events

ase Connects to each ASP in the system and collects debug and status information for use by technical support.

ase2	Connects to each ASP in the system and collects debug and status information for use by technical support.
atm	Collects Asynchronous Transfer Mode (ATM) information
bfd	Collects Bidirectional Forwarding Detection (BFD) information
bgp	Collects Border Gateway Protocol (BGP) information
dhcp	Collects Dynamic Host Configuration Protocol (DHCP) server and relay information
dot1q	Collects 802.1Q permanent virtual circuit (PVC) information
flowd	Collects Flow process information for Flow Admission Control
gre	Collects Generic Routing Encapsulation (GRE) tunnels and tunnel circuit information
igmp	Collects Internet Group Management Protocol (IGMP) information
ipv6	Collects IPv6 subscriber services information, concentrating on IPv6 and ND; the basic command collects data about DHCPv6
isis	Collects Intermediate System-to-Intermediate System (IS-IS) routing information
l2tp	Collects Layer 2 Tunneling Protocol (L2TP) peer and group information
ldp	Collects Label Distribution Protocol (LDP) signalling information
mobile-ip	Collects Mobile IP information
ospf	Collects Open Shortest Path First (OSPF) information
ospf3	Collects Open Shortest Path First (OSPF) version 3 information
pim	Collects Protocol Independent Multicast (PIM) information
ppp	Collects Point-to-Point Protocol (PPP) information
pppoe	Collects PPP over Ethernet (PPPoE) information
qos	Collects Quality of Service (QoS) information
rdb	Collects SmartEdge database information
snmp	Simple Network Management Protocol (SNMP) information

1.41.4 Default

None

1.41.5 Usage Guidelines

Use the basic **show tech-support** command (without any keywords) to collect troubleshooting information for technical support; see Table 9 for the areas covered by the basic command. The output of this command must be attached to all customer support requests.

If you know that your problem is related to an ASE or ASE2 card or one of the modules covered by the keywords, use the command with a keyword.

To save the output in memory, use the **show tech-support | save /md/*filename*** command. Then, to send the output to a remote location, use the **copy /md/*filename* ftp://*username@hostname*/*filename*** command.

Table 9 Areas Covered by Basic show tech-support Command

Startup and software revision
System hardware details
Configuration
Core system statistics
Process and memory status and crashes
Core system processes
IP routes
Subscriber details (basic)
Shared memory routing
DHCPv6

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

For more information on using the **show tech-support** command to collect troubleshooting data, see *Data Collection Guideline for the SmartEdge Router*.

1.41.6 Examples

Note: Some commands in the **show tech-support** macro do not appear in the CLI and are used by customer support for troubleshooting. They are not supported for customer use outside the macro.

The following example displays entering the **show tech-support** command for PPP problems. For brevity, some of the command output has been truncated.

```
[local]Redback#show tech-support ppp

[10] (ppp-debug)# term len 0

[20] (ppp-debug)# show system status process pppd
History for Process: pppd
  Date/Time            Status          Message
  -------------------  --------------  -------
  Dec 15 06:49:57.345  Starting        Init
  Dec 15 06:49:57.574  Starting        Initializing after reload
  Dec 15 06:49:57.712  Starting        Started thread pkt-out
  Dec 15 06:49:57.730  Starting        Started thread auth
  Dec 15 06:50:01.570  Starting        Started thread ppp-ppa-tx_thread
  Dec 15 06:50:01.570  Starting        Started thread worker
  Dec 15 06:50:01.571  Starting        Sent EOF to AAA
  Dec 15 06:50:01.610  Starting        Started thread ism
  Dec 15 06:50:01.615  Starting        ISM FSM state: MBE-EP-up
  Dec 15 06:50:01.730  Starting        Started thread cfg
  Dec 15 06:50:01.735  Starting        Received EOF from RCM
  Dec 15 06:50:01.750  Starting        Awaiting EOF from ISM
  Dec 15 06:50:01.840  Starting        ISM FSM state: All-EP-up
  Dec 15 06:50:01.844  Starting        Received EOF from ISM
  Dec 15 06:50:01.860  Starting        Sent EOF to ISM
  Dec 15 06:50:01.860  Starting        Awaiting MBE-All-EOF from ISM
  Dec 15 06:50:11.285  Starting        Received MBE ALL EOF from ISM
  Dec 15 06:50:11.300  Starting        Started thread ipc
  Dec 15 06:50:11.330  Running         Ready

[30] (ppp-debug)# show process ppp diagnose
Current time: Thu Jan  6 08:22:47 2011
Diagnostics for ppp found no issues

[40] (ppp-debug)# show process ppp chunk-statistics
                Elements                                  Chunks
  Size    InUse  MaxUse    Alloc     Free    Size InUse MaxUse Alloc  Free  U% Name
    40        1       1        1        0    4096     1      1     1     0   1 id free list
    40        3       3        3        0   40960     1      1     1     0   0 radix node
    48        3       3        3        0    8192     1      1     1     0   1 ft-mc
    64       35      39      114       79    8192     1      1     1     0  27 ipc
    64        1       1        1        0    4096     1      1     1     0   1 pkt
   ...
[50] (ppp-debug)# show process ppp ipc-pack-statistics
                       Max              Start Flush       New   Chain
                       Per Imm.  Force  Flush Timer Buf   ReqId Too   Q     Block
Endpoint IPCs   Msgs   IPC Send  Send   Timer Exp.  Full  Flush Short Count Count
-------- ------ ------ --- ----- ------ ----- ----- ----- ----- ----- ----- -----
l2tp          0      0   0     0      0     0     0     0     0     0     0     0
aaad          1      1   1     1      0     0     0     0     0     0     0     1
ism mbe       1      1   1     1      0     0     0     0     0     0     0     1
ism           2      2   1     1      0     0     0     0     0     1     0     0
pppoe         0      0   0     0      0     0     0     0     0     0     0     0
09/0          1      1   1     1      0     0     0     0     0     0     0     1

[60] (ppp-debug)# show process ppp throttle-statistics
Throttle statistics for process: ppp

Throttle Enabled        : Yes         Throttle Debug Enabled  : No
Throttle Active         : No
Min-starting            : 540         Max-starting            : 600
Min-authenticating      : 675         Max-authenticating      : 750
Min-sess-up             : 540         Max-sess-up             : 600
Low watemark            : 90%

[70] (ppp-debug)# show process ppp termination-cause

[80] (ppp-debug)# show ppp counters detail
Current time: Thu Jan  6 08:22:47 2011
Last cleared: Never

Packet------------------------------------------------------------
 In                        0      Out                        0
  ConfReq                  0       ConfReq                   0
  ConfAck                  0       ConfAck                   0
  ConfNak                  0       ConfNak                   0
  ConfRej                  0       ConfRej                   0
```

```
  TermReq                  0       TermReq                  0
  TermAck                  0       TermAck                  0
  Authen Proto             0       Authen Proto             0
  other                    0       other                    0
Session-------------------------------------------------------
 LCP Up                    0      LCP Down                  0
 IPCP Up                   0      IPCP Down                 0
 IPV6CP Up                 0      IPV6CP Down               0
 Authen Success            0      Authen Failure            0
 Session Up                0      Session Down              0
SessionControl------------------------------------------------
 Starting                  0      Authenticating            0
 Pended (current)          0      Pended (total)            0
 Session up start          0
 Packet Drop:
 Session pended            0      At Limit                  0
Timeout-------------------------------------------------------
 ConfReq                   0      TermReq                   0
 CHAP Challenge            0      UPAP Listen               0
 CHAP Response             0      UPAP Request              0
 Passive                   0      Auto start                0
 Sess phase                0
DownCause-----------------------------------------------------
 Rcvd TermReq              0      Rcvd PPPoE PADT           0
 No ConfReq Resp           0      No Echo Resp              0
 Authen Failed             0      Session Down              0
 LCP Down                  0      Circuit Down              0
 Port Down                 0      Port Delete               0
 Stale Sessions            0      Circuit Unbound           0
 ICR Down                  0

[90] (ppp-debug)# show ppp counters debug
Current time: Thu Jan  6 08:22:47 2011
Last cleared: Never

Circuit/Unit--------------------------------------------------
 Circuit Create            0      Circuit Delete            0
 Circuit Up                0      Circuit Down              0
 Unit Create               0      Unit Delete               0
 Queued up msgs            0      Processed q msgs          0
Session control-----------------------------------------------
 Auto starting             0      Ccod starting             0
 Pppoe starting            0      Tunnel starting           0
 Pppoa starting            0      Sync Pkt Pended           0
Throttling state----------------------------------------------
 Pppoa                    No      Auto                     No
 System                   No      Ccod                     No
 Pppoe                    No      Tunnel                   No
 Max pended               No      Auth at max              No
 Sess up starting         No
Throttling counters-------------------------------------------
 auto throttle             0      ccod throttle             0
 pppoa throttle            0
 ism throttle              0      ism ipc blocked           0
 aaa throttle              0      aaa ipc blocked           0
IPC-----------------------------------------------------------
 IPCs from PPPoE           0      Msgs from PPPoE           0
 Bad PPPoE IPC msg         0      Bad IPC msg               0
 IPCs from ISM            17      Msgs from ISM           125
 IPCs from AAA             0      Msgs from AAA             0
 EOF from RCM            Yes      EOF to ISM              Yes
ISM-----------------------------------------------------------
 EOF from ISM            Yes      ALL EOF from ISM        Yes
 ISM MBE EP Up           Yes      ISM Client EP Up        Yes
 ISM Client Births         1      ISM Client Deaths         0
 ISM MBE Births            1      ISM MBE Deaths            0
 IPv4 wait UP cplt         0      IPv6 wait UP cplt         0
 Sess Up recover           0
AAA-----------------------------------------------------------
 Authen Req Sent           0      Authen Resp Rcvd          0
 Sess Up Sent              0      Sess Down Sent            0
 IPv4 Up Sent              0      IPv4 Down Sent            0
 IPv6 Up Sent              0      IPv6 Down Sent            0
 Verify Sub Sent           0      EOF Sent                  1
 Slot change Sent          0      Dropped                   0
PPPoE---------------------------------------------------------
```

```
 PADS rest drops            0      PADS stale drops           0
 KA restart drops           0      KA ignore: sess up         0
 KA stuck: down             0      KA no lcp: down            0
 PPPoE sync drops           0      Timeout w/ no sync         0
L2TP------------------------------------------------------------
 Tunnel start sent          0      Tunnel start rcvd          0
 Tunnel stop rcvd           0      Session stop sent          0
 LNS-Start no cct           0      LNS-Start no unit          0
 LNS-Start rcvd             0      Unit ready sent            0
 LAC-Stop no cct            0      LAC-Stop no unit           0
 LAC-Stop rcvd              0      LAC verify sent            0
MP--------------------------------------------------------------
 Bundle sess Limit          0      Encap mismatch             0
 Slot mismatch              0      Slot no support            0
 Card sess Limit            0      MP neg reject              0
 No MP Master               0      No MP Bundle               0
 No MP Acct                 0
PPA-------------------------------------------------------------
 Drop ctrl                  0      Pass ctrl                  0
 Install ctx                1      Uninstall ctx              0
 Msgs alloc                 0      Msgs freed                 0
 Conf walk iter             1      Conf walk restart          0
 Sent msgs                  0      Recv msgs                  1
 Enqueued msgs              0      Dequeued msgs              0
 Requeued msgs              0
Process---------------------------------------------------------
 Thread Yield               0

Packet processing-----------------------------------------------
 LCP Creq rxmits            0      IPCP Creq rxmits           0
 IPv6CP Creq rxmits         0

 Buffer management statistics:
  enqueued 0, dequeued 0, freed 0
  canceled 0, cleaned 0

ISM_In----------------------------------------------------------

 ISM Statistics:
  Total events: ipc rcvd: 0, ipc err 0, unknown event 0

   ID: I/F   : state 47, cfg 25, IP cfg 21,
       Cct   : state 0, Cct cfg 0, Cct grp 0
       Port  : state 2, Port cfg 0
       Lg    : cfg 0
       L2tp  : sesscfg 0
       Hdr   : only 1
       GrpMac: cfg 0
       Card  : state 8
       Peer  : 0

   CCT SUBID: down 0, up 0, create 0, del 0, par_up 0
         CFG: eth 0, ocn 0, 1q 0, tun 0, fr 0, ppp 0
              atm 0, lm 0, l2tp 0, cfg 0
         SUB: clear 0, down 0, down_cplt 0
         GRP: join 0, leave 0

   I/F SUBID: down 10, up 15, create 11, del 0, bind 11, unbind 0
         CFG: cfg 25, ipcfg 21

   PORT SUBID: down 2, up 0, del 0
          CFG: eth 0, stsn 0

   LG SUBID: grp cfg 0, ungrp cfg 0, prot grp cfg 0
             prot cct cfg 0, prot grp action 0

   L2TPSESS SUBID: cfg 0

   GRPMAC: UCAST: reg 0, dereg 0
           MCAST: reg 0, dereg 0

   CARD SUBID: create 2, down 0, up 2, del 0
               rate cfg 1, mic 0
ISM_Out---------------------------------------------------------

 ISM Statistics:
```

```
  Total events: ipc rcvd: 0, ipc err 0, unknown event 0

   ID: I/F   : state 0, cfg 0, IP cfg 0,
       Cct   : state 0, Cct cfg 0, Cct grp 0
       Port  : state 0, Port cfg 0
       Lg    : cfg 0
       L2tp  : sesscfg 0
       Hdr   : only 0
       GrpMac: cfg 0
       Card  : state 0
       Peer  : 0

   CCT SUBID: down 0, up 0, create 0, del 0, par_up 0
         CFG: eth 0, ocn 0, 1q 0, tun 0, fr 0, ppp 0
              atm 0, lm 0, l2tp 0, cfg 0
         SUB: clear 0, down 0, down_cplt 0
         GRP: join 0, leave 0

   I/F SUBID: down 0, up 0, create 0, del 0, bind 0, unbind 0
         CFG: cfg 0, ipcfg 0

   PORT SUBID: down 0, up 0, del 0
          CFG: eth 0, stsn 0

   LG SUBID: grp cfg 0, ungrp cfg 0, prot grp cfg 0
             prot cct cfg 0, prot grp action 0

   L2TPSESS SUBID: cfg 0

   GRPMAC: UCAST: reg 0, dereg 0
           MCAST: reg 0, dereg 0

   CARD SUBID: create 0, down 0, up 0, del 0
               rate cfg 0, mic 0

[100] (ppp-debug)# show ppp counters all-contexts
Context   :local                          Context id  : 0x40080001
-------------------------------------------------------------------
 Last cleared: Never
     received: bytes 0, packets 0,
               unsupported packets 0
         sent: bytes 0, packets 0
LCP echo request      : received 0, sent 0, dropped 0
LCP echo response     : received 0, sent 0, dropped 0
LCP protocol reject   : received 0, sent 0, dropped 0
Context   :two                          Context id  : 0x40080003
-------------------------------------------------------------------
 Last cleared: Never
     received: bytes 0, packets 0,
               unsupported packets 0
         sent: bytes 0, packets 0
LCP echo request      : received 0, sent 0, dropped 0
LCP echo response     : received 0, sent 0, dropped 0
LCP protocol reject   : received 0, sent 0, dropped 0
Context   :three                        Context id  : 0x40080004
...
[110] (ppp-debug)# show ppp summary all

[120] (ppp-debug)# show ppp multilink summary
Bundle Count = 0, Link Count = 0
Total Bundles = 0, Total Links = 0


[130] (ppp-debug)# show ppp global
fast disconnect   : No                pppoe large mru   : No
pppoe-src-mac vld : No                pppoe send-padt   : No
sub MP enabled    : No                sync control      : No
LCP no padt       : No                disc no peer-ip   : No
Our MP ED set     : No                send ipv6cp-creq  : No

max conf reqs     : 11
our init mru      : 1500              our max mru       : 12800
peer min mru      : 256               peer max mru      : 12800
delay lcp-confreq : 3 (secs)

[140] (ppp-debug)# show log | grep "PPP-"
```

```
[150] (ppp-debug)# show proc ppp detail

Process (PID)        : ppp (1934)

Spawn count          : 1
Memory               : 7172K
Time                 : 00:04:05.08
%CPU                 : 0.00%
State                : run
Up time              : 3w1d
Heart beat           : Enabled
Spawn time           : 2 seconds
Max crashes allowed : 5
Crash thresh time    : 86400 seconds
Total crashes        : 0
Fast restart         : DISABLED
Critical process     : NO / NO

Images: (Spawns, Max spawns, Version, Path)
  (*)  1, 4, v1, /usr/siara/bin/pppd

Client IPC Endpoints:
    EP 7f000205 f2640006 - PPP SLOT 09/0:00000000
    EP 7f000205 f264000a - PPPOE-IPC-EP-NAME:00000000
    EP 7f000205 f2640008 - ISM2-CLIENT-EP-NAME:00000000
    EP 7f000205 f2640008 - ISM2-MBE-EVIN-EP-NAME:00000000
    EP 7f000205 f2640005 - AAA-IPC-MSG-EP-NAME:00000000
    EP 7f000205 f2640005 - L2TP-PPP-EP-NAME:00000000

Server IPC Endpoints:
    EP 7f000205 f264000a - PPP-IPC-EP-NAME:00000000
      Dependent process pppoe (1938) EP 7f000205 e6820007
      Dependent process l2tp (1873) EP 7f000205 f94d0005
      Dependent process IPPA IPC SLOT 9 (-2146893823) EP 7f000a09 0001001e
    EP 7f000205 f2640009 - PPP-CONF-EP-NAME:00000000
      Dependent process rcm (1846) EP 7f000205 e8ac0001
    EP 7f000205 f2640008 - PPP-ISM-EP-NAME:00000000
      Dependent process ism (1848) EP 7f000205 ddab000c
      Dependent process ism (1848) EP 7f000205 ddab000a
    EP 7f000205 f2640005 - PPP-AUTH-EP-NAME:00000000
      Dependent process aaad (1964) EP 7f000205 f5d70009
```

1.42 show terminal

show terminal

1.42.1 Purpose

Displays terminal settings for the current session.

1.42.2 Command Mode

All modes

1.42.3 Syntax Description

This command has no keywords or arguments.

1.42.4 Default

None

1.42.5 Usage Guidelines

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.42.6 Examples

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

```
[local]Redback>show terminal


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

1.43 show transaction

show transaction

1.43.1 Purpose

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

1.43.2 Command Mode

All modes

1.43.3 Syntax Description

This command has no keywords or arguments.

1.43.4 Default

None

1.43.5 Usage Guidelines

Use the **`show transaction`** command to display information about outstanding configuration database transactions made by other administrators in all configuration modes, or created by internal processes. Outstanding transactions are those that have been configured by other administrators or started by an internal process, but have not yet been committed to the configuration database. Table 10 lists the possible states that might be displayed for a transaction.

Table 10 Transaction States

State	Description
Active	Transaction is active for configuration changes.
Ready	Transaction just got the lock it was waiting for and is ready to proceed.
Blocked	Transaction is blocked waiting for a lock. The information field displays the transaction ID that holds the lock.
Blocked on User	Transaction is blocked by administrator input on whether to continue waiting for the lock to clear. The information field displays the transaction ID that holds the lock.
Pending Rollback	Administrator has requested to stop waiting for the lock and the system is preparing to rollback the current command.
Abort	Transaction is being erased.
Committing	Transaction is marked for commit.
Commit - Duplicated	Transaction is duplicated to the standby controller card. (1)
Commit - Duplicated	Transaction is duplicated to the standby controller card.
Commit - Synched	Transaction is committed on the standby controller card.(2)
Commit - Synched	Transaction is committed on the standby controller card.
Committed	Transaction has completed the committing on the active controller card.
Commit - Blocked	Commit is held up because of a global database lock. Waiting to commit after the lock is clear.

Table 10 Transaction States

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

(1) The SmartEdge 100 router has a single controller card. The Commit-Duplicated and Commit-Synched transaction states apply only to SmartEdge routers with dual controller cards.
(2) The SmartEdge 100 router has a single controller card. The Commit-Duplicated and Commit-Synched transaction states apply only to SmartEdge routers with dual controller cards.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.43.6 Examples

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

```
[local]Redback>show transaction
```

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

1.44 show tunnel

To show information about Generic Routing Encapsulation (GRE) tunnels, the syntax is:

show tunnel gre [**name** *tunl-name* | **peer** *peer-name* | **remote** *remote-IP*] [**detail**]

To show information about IP-in-IP tunnels, the syntax is:

show tunnel ipip [**name** *tunl-name* | **remote** *remote-IP*] [**detail**]

To show information about automatic IP Version 6 (IPv6) tunnels, the syntax is:

show tunnel ipv6-auto [**name** *tunl-name* | **remote** *remote-IP*] [**detail**]

To show information about manual IPv6 tunnels, the syntax is:

show tunnel ipv6-manual [**name** *tunl-name* | **remote** *remote-IP*] [**detail**]

1.44.1 Purpose

Displays information about tunnels currently configured in the SmartEdge router.

1.44.2 Command Mode

All modes

1.44.3 Syntax Description

gre	Displays information for GRE tunnels.
ipip	Displays information for IP-in-IP tunnels
ipv6-auto	Displays information for automatic IPv6 tunnels.
ipv6-manual	Displays information for manual IPv6 tunnels.
name *tunl-name*	Optional. The name of the tunnel for which information is displayed.
peer *peer-name*	Optional. The name of the GRE peer for which information is displayed.
remote *remote-IP*	Optional. The IP address of the remote interface to a tunnel for which information is displayed.
detail	Optional. Specifies the output provides fullest details.

1.44.4 Default

When the tunnel type is specified, but the name, remote address. and peer name are not specified, all tunnels of that type are displayed.

1.44.5 Usage Guidelines

Use the **show tunnel** command to display information about tunnels currently configured in the SmartEdge router. Use the **show tunnel client** command on Section 1.45 on page 111 to find information about dynamic tunnel clients that are registered with the tunnel manager.

The following fields can appear in the output of the **show tunnel** command.

Table 11 Fields Descriptions for the show tunnel Command

Field	Description
Name	Name of the tunnel.
Context	Context in which the tunnel was created.
Type	IPv6-auto, IPv6-manual, IP-in-IP, or GRE tunnel.
MTU	MTU of tunnel.
Local IP	Local IP address of the tunnel.
Remote IP	Remote IP address of the tunnel.

Table 11 Fields Descriptions for the show tunnel Command

Field	Description
State	The tunnel states can be: • Shut—Tunnel is disabled by the **shutdown** command (in GRE peer configuration mode). • Up—Tunnel can send and receive traffic. • Down—Tunnel cannot send and receive traffic.(1)
Bound to	Interface and context to which tunnel circuit is bound.

*(1) If the GRE tunnel has no circuits configured, the state is always down, even after you have entered the **no shutdown** command (in GRE peer configuration mode).*

Use the **uptime** keyword to display the amount of time the tunnel circuit is in the Up state.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.44.6 Examples

(Example 1) The following example shows how to display information for the GRE peer named `toBoston`:

```
[local]Redback>show tunnel gre peer toBoston

Name      Context    Type      MTU       Local-IP        Remote-IP   State
toBoston  local      gre       1468      11.1.1.1        11.1.1.1    Down
```

(Example 2) The following example shows how to display detailed information for the `toChicago` GRE tunnel in the local context:

```
[local]Redback>show tunnel name gre toChicago detail

::::: Tunnel : toChicago
   Key       : -
   Remote IP : 2.2.2.2     Local IP    : 192.168.1.5
   Tnl Type  : GRE
   State     : Down        Bound to    :
   Circuit ID: 1           Internal Hdl: 255/4:1023:63/0/1/1
   Tunnel is User Configured
   local-ip 192.168.1.5, context-for-local-ip: local
   mtu 1468
   log-state-changes no
  clear-df no
  Keep-alive 0 seconds, retries 0
   destination DOWN on nhop mgmt interface
   resolved on  grid 0x10000000
   Tunnel ID: gre 1
   Circuit ID Internal: 255/4:1023:63/0/1/1
```

1.45 show tunnel client

show tunnel client ***client-name*** [**context** ***ctx-name***] [**detail**]

1.45.1 Purpose

Displays information about dynamic tunnel clients that are registered with the tunnel manager.

1.45.2 Command Mode

All modes

1.45.3 Syntax Description

client-name	Name of client.
context ***ctx-name***	Optional. Name of context.
detail	Optional. Displays detailed information about dynamic tunnel clients that are registered with the tunnel manager.

1.45.4 Default

When entered without any optional syntax, the **show tunnel client** command displays all dynamic tunnel clients that are registered with the tunnel manager.

1.45.5 Usage Guidelines

Use the **show tunnel client** command to information about dynamic tunnel clients registered with the tunnel manager.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.45.6 Examples

The following example shows how to display information about all dynamic tunnel clients that are registered with the tunnel manager in all contexts:

```
[local]Redback>show tunnel client
Tunnel client information summary
---------------------------------------------------------
Client Name       : mobile-ip  (client-id 2
Context Name      : local
IPIP Tunnel Count : 0
GRE Tunnel Count  : 0
Register State    : Registered         Restart State    : Alive
---------------------------------------------------------
Client Name       : mobile-ip  (client-id 2)
Context Name      : fa-ctx
IPIP Tunnel Count : 0                  GRE Tunnel Count : 0
Register State    : Registered         Restart State    : Alive
```

The following example shows how to display information about dynamic tunnel client named `mobile-ip` in all contexts that it has registered with tunnel manager:

```
[local]Redback>show tunnel client mobile-ip
Tunnel client information summary
---------------------------------------------------------
Client Name       : mobile-ip  (client-id 2)
Context Name      : local
IPIP Tunnel Count : 0                  GRE Tunnel Count : 0
Register State    : Registered         Restart State    : Alive
---------------------------------------------------------
Client Name       : mobile-ip  (client-id 2)
Context Name      : fa-ctx
IPIP Tunnel Count : 0                  GRE Tunnel Count : 0
Register State    : Registered         Restart State    : Alive
```

The following example shows how to display information about dynamic tunnel client named `mobile-ip`, that is registered with the tunnel manager in the `fa-ctx` context:

```
[local]Redback>show tunnel client mobile-ip context fa-ctx
Tunnel client information summary
---------------------------------------------------------
Client Name       : mobile-ip          (client-id 2)
Context Name      : fa-ctx
IPIP Tunnel Count : 0                  GRE Tunnel Count : 0
Register State    : Registered         Restart State    : Alive
```

The following example shows how to display detailed information tunnel information about all dynamic tunnel clients that are registered with the tunnel manager in all contexts:

```
[local]Redback>show tunnel client detail

Tunnel client detailed information
----------------------------------------------------------
Client Name       : mobile-ip         (client-id 2)
Context Name      : local
IPIP Tunnel Count : 0                  GRE Tunnel Count : 0
Register State    : Registered         Restart State    : Alive
Counters
Registration requests received       :   1
Deregistration requests received     :   0
Reregistration requests received     :   0
Tunnel add requests received         :   0
Tunnel delete requests received      :   0
Tunnel modify requests received      :   0
Tunnel verify requests received      :   0
Tunnel registration responses sent   :   0
Client information responses sent    :   0
Tunnel verification responses sent   :   0
Failed to get state - no client      :   0
Invalid config requests received     :   0
Reg info req rcvd no client          :   0
Client free fail bad client id       :   0
Client add fail-bad client id        :   0
Client add fail-no memory            :   0
Client add fail-due to tree insert   :   0
Client add fail-no id available      :   0
Client add fail-duplicate insert     :   0
Reg resp not sent not registered     :   0
Reg resp not sent no memory          :   0
Client info not sent-not registered  :   0
Client info not sent-no memory       :   0
Client IPC xmit queue count          :   0
----------------------------------------------------------
Client Name       : mobile-ip   (client-id 2)
Context Name      : fa-ctx
IPIP Tunnel Count : 0                  GRE Tunnel Count : 0
Register State    : Registered         Restart State    : Alive
Counters
Registration requests received       :   1
Deregistration requests received     :   0
Reregistration requests received     :   0
Tunnel add requests received         :   0
Tunnel delete requests received      :   0
Tunnel modify requests received      :   0
Tunnel verify requests received      :   0
Tunnel registration responses sent   :   0
Client information responses sent    :   0
Tunnel verification responses sent   :   0
Failed to get state - no client      :   0
Invalid config requests received     :   0
Reg info req rcvd no client          :   0
Client free fail bad client id       :   0
Client add fail-bad client id        :   0
Client add fail-no memory            :   0
Client add fail-due to tree insert   :   0
Client add fail-no id available      :   0
Client add fail-duplicate insert     :   0
Reg resp not sent not registered     :   0
Reg resp not sent no memory          :   0
Client info not sent-not registered  :   0
Client info not sent-no memory       :   0
Client IPC xmit queue count          :   0
```

1.46 show udp

show udp {**sockets** | **statistics**}

1.46.1 Purpose

Displays User Datagram Protocol (UDP) socket and statistical information.

1.46.2 Command Mode

All modes

1.46.3 Syntax Description

sockets Displays UDP socket information.

statistics Displays UDP statistics.

1.46.4 Default

None

1.46.5 Usage Guidelines

Use the **show udp** command to display UDP socket and statistical information.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.46.6 Examples

The following example displays output when the **statistics** keyword is specified:

```
[local]Redback>show udp statistics
```

```
udp:
        95808 datagrams received
        0 with incomplete header
        0 with bad data length field
        0 with bad checksum
        875 dropped due to no socket
        94931 broadcast/multicast datagrams dropped due to no socket
        0 dropped due to full socket buffers
        2 delivered
        875 PCB hash misses
        875 datagrams output
```

The following example displays output when the **sockets** keyword is specified:

```
[local]Redback>show udp sockets

Active Internet connections (including servers)
PCB      Recv-Q Send-Q Local Address         Foreign Address
f07cbb80      0      0 127.0.0.1.64721       *.* vc
f07cb958      0      0 127.0.0.1.64741       *.*
f07cb8a0      0      0 127.0.0.1.64746       *.*
f07cbcf0      0      0 127.0.0.1.64773       *.*
f07cb730      0      0 127.0.0.1.64790       *.*
f07cbc38      0      0 127.0.0.1.64876       *.*
f07cba6c      0      0 127.0.0.1.123         *.*
f07cb7e8      0      0 127.0.0.1.64914       *.*
f07cb78c      0      0 127.0.0.1.64915       *.*
f07cb6d4      0      0 127.0.0.1.64917       *.*
f07cb678      0      0 127.0.0.1.64918       *.*
f07cbbdc      0      0 127.0.0.1.64919       *.*
f07cbe60      0      0 127.0.0.1.64920       *.*
f07cbf18      0      0 127.0.0.1.64921       *.*
f07cbf74      0      0 127.0.0.1.64922       *.*
f07cbebc      0      0 127.0.0.1.6000        *.*
```

1.47 show version

show version

1.47.1 Purpose

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

1.47.2 Command Mode

All modes

1.47.3 Syntax Description

This command has no keywords or arguments.

1.47.4 Default

None

1.47.5 Usage Guidelines

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

For the SmartEdge 100 router with one or both ATM OC media interface cards (MICs), the command output includes, at or near its end, several lines dedicated to the MICs.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.47.6 Examples

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

```
[local]Redback#show version

Redback Networks SmartEdge OS Version SEOS-11.1.1.0.28-Release
Built by sysbuild@SWB-node06 Wed Sep 21 16:14:58PDT 2011
Copyright (C) 1998-2011, Redback NetworksInc. All rights reserved.
System Bootstrap version is Mips,rev2.0.2.44
Installed minikernel version is 11.7
Router Up Time -   19 days, 23 hours 34minutes 32 secs
```

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

```
[local]Redback#show version


Redback Networks SmartEdge OS Version SEOS-7.0.0.0-Release

Built by sysbuildd@lx-lsf401 Wed Nov 22 10:05:57 PST 2006

Copyright (C) 1998-2006, Redback Networks Inc. All rights reserved.

System Bootstrap version is PowerPC,rev2.0.1.2 Installed minikernel
version is 2.6

...

Linecard 2 MIC _mic_ sarc Version SEOS-7.0.0.0-Release

Built by  sysbuildd@lx-lsf401 Wed Nov 22 10:21:45 PST 2006

Copyright (C) 1998-2006, Redback Networks Inc. All rights reserved.

Router Up Time - 3 minutes 42 secs
```

1.48 show vpls

show vpls [***bridge-name***] [**detail**]

1.48.1 Purpose

Displays Virtual Private LAN Services (VPLS)-enabled bridge information.

1.48.2 Command Mode

All modes

1.48.3 Syntax Description

bridge-name	Optional. Name of the VPLS-enabled bridge instance name. Displays information for the specified bridge instance.
detail	Optional. Displays detailed information.

1.48.4 Default

None

1.48.5 Usage Guidelines

Use the **show vpls** command to display VPLS-enabled bridge information.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*. For information about troubleshooting VPLS, see *Troubleshooting VPLS*.

1.48.6 Examples

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

```
[local]Redback>show vpls

VPLS Bridge          Pseudo-wire ID       Peers(Up)  State
BridgeName           1                    1(1 )      Enable
```

The following example displays output from the **show vpls detail** command:

```
[local]Redback>show vpls detail

VPLS instance name           : vplsA
 Context name                : local
 Admin state                 : Enable
 Bridge identifier           : 0x1
 Context identifier          : 0x40080001
 Default PW-identifier       : <none>
 Number of peers             : 1 (Up:1, hub:1, spoke:0)
 Number of standby peers     : 1 (local PE-rs) 0 (local MTU-s)
```

1.49 show vpls peer

To display Virtual Private LAN Services (VPLS) peer information for a specific bridge, the syntax is:

show vpls *bridge-name* **peer** [*ip-addr* | **profile** *prof-name* | **pw-id** *pw-num* | **pw-name** *pw-name*] [**detail**]

To display VPLS peer information for all bridges, the syntax is:

show vpls peer *ip-addr* {**pw-id** *pw-num* | **pw-name** *pw-name*} [**detail**]

1.49.1 Purpose

Displays VPLS peer information.

1.49.2 Command Mode

All modes

1.49.3 Syntax Description

bridge-name	VPLS-enabled bridge instance name. Displays information for the VPLS peers on the specified bridge instance.
ip-addr	VPLS peer IP address in the form A.B.C.D. Displays information for the specified VPLS peer. Optional when displaying peer information for a specific bridge.
profile *prof-name*	VPLS profile name. Displays information for the VPLS peers in the specified VPLS profile. Optional when displaying peer information for a specific bridge.
pw-id *pw-num*	Pseudo-wire number. Displays information for the VPLS peers that use the specified pseudo-wire number. Optional when displaying peer information for a specific bridge.
pw-name *pw-name*	Pseudo-wire name. Displays information for the VPLS peers that use the specified pseudo-wire name. Optional when displaying peer information for a specific bridge.
detail	Optional. Displays detailed information.

1.49.4 Default

None

1.49.5 Usage Guidelines

Use the **show vpls peer** command to display VPLS peer information.

When the root command is used without any additional syntax, information for all the VPLS peer instances is displayed. If additional syntax is used to match a single VPLS peer instance, then the detailed version of the output is displayed.

If additional syntax is used to help filter the set of VPLS peers, then the brief version of the output is displayed.

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

Note: By appending a space followed by the pipe (|) character at the end of a **`show`** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*. For information about troubleshooting VPLS, see *Troubleshooting VPLS*

Table 12 describes the **`show vpls peer`** command output fields.

Table 12 Field Descriptions for the show vpls peer Command

Field	Description
Admin state	Computed administrative state for the peer: • disable—Peer is administratively disabled. This is the case when either the VPLS instance is administratively disabled or if the **`clear vpls peer disable`** command (in exec mode) was issued. • enable—Peer is administratively enabled.
Bridge id	System-generated bridge ID.
Circ cfg changes	Circuit configuration change count.
Circ delete cnt	Circuit delete count.
Circ error cnt	Circuit error count.
Circ up/down cnt	Circuit up and down count.
Circuit ID	Circuit ID, represented as VPLS ***`circuit-id,`*** which is used by a peer in the system. A circuit is allocated for each peer, except standby peers. A standby peer uses the circuit associated with the primary peer on switchover.
Context id	Context ID.
Context name	Name of the context in which VPLS is configured.

Table 12 Field Descriptions for the show vpls peer Command

Field	Description
Last error	Last error logged by the system: • error—An error occurred in the previous event handling. • no error—No error occurred in the previous event handling. • pw-exists—Pseudo-wire already associated with another peer. • pw-create-err—Error during pseudo-wire creation. • pw-alloc-err—Error during allocation of resources for pseudo-wire. • no-primary—Primary peer does not exist. • no-peid—Internal ID allocated for a provider edge (PE) router is missing (in the process restart case). • cct-alloc-err—Error during allocation of a circuit for the peer. • ism-err—Error when registering a circuit with the system. • clear—Previous operation was a **`clear`** command. • admin-down—Previous operation administratively disabled a peer. • stby-cfg-incomp—Standby peer configuration was incomplete for hierarchical VPLS (HVPLS). • switchover-err—Error during switchover between primary and standby pseudo-wires.
MAC flush received	MAC flush received count.
MAC flush sent	MAC flush sent count.

Table 12 Field Descriptions for the show vpls peer Command

Field	Description
Oper State/State	Operational state of the peer: • Deleted—Peer has been deleted, but pending clean up of the entry. • Disable—Peer is administratively disabled, either by disabling the VPLS instance or issuing the **`clear vpls peer disable`** command (in exec mode). The peer retains its allocated circuit ID, if it is not a standby peer. When a peer is in this state, a standby peer is activated for it, if configured. • Down—Peer is operationally down. The peer is waiting for a pseudo-wire to be established. • Init—Peer is initializing. It remains in this state if any basic resources can not be allocated, including a circuit. • Standby—Peer is ready as a standby peer. A peer in this state has a pseudo-wire established and is on standby. If the primary peer goes down, then the standby peer is ready to take over, without any disruptions by using the same circuit as the primary peer and the same set of learned entries mapped to the new pseudo-wire. • Up—Peer is operationally active. The pseudo-wire established for the peer is participating in data forwarding.
PE local mode	Local mode of operation for the neighbor connection: • MTU-s—Multitenant unit switch. This local mode is used when the local router is participating in hierarchical VPLS by using a pseudo-wire connected to a core provider edge router (PE-rs) device, and when the local VPLS instance does not have a mesh of pseudo-wire to all the core PE devices. • PE-rs—Provider edge routers. This local mode is used at a core VPLS PE device that is providing hierarchical VPLS connectivity to other MTU-s routers.

Table 12 Field Descriptions for the show vpls peer Command

Field	Description
PE peering Type/Type	VPLS peering type: • Hub—Hub peering indicates that two PE routers are participating a full mesh of connections. This peering constitutes one of the connections of this mesh. • Sp—Spoke connection at a PE-rs. This peer is connected to an MTU-s to provide a hierarchical VPLS functionality. This peer may be a standby link (PE-rs is not explicitly aware). • Sp Pri—Spoke connection at an MTU-s connecting to a primary PE-rs for providing hierarchical VPLS functionality. • Sp Sby—Spoke connection at an MTU-s connecting to a secondary or standby PE-rs for providing hierarchical VPLS functionality. This field describes the configuration, and not necessarily the operation state.
Peer config changes	Peer configuration change count.

Table 12 Field Descriptions for the show vpls peer Command

Field	Description
Peer flags	Run-time bit flags maintained by a peer to capture the state as it understands it: • active—Peer is operationally active. This flag is set when the peer is operational. When primary and standby peers are configured, only one of them can be active at the same time. • debug—A peer is marked for debug logging. This flag is set using the **`debug vpls peer`** command (in exec mode) to log all events related to this peer. • delete—A peer is marked for deletion. This flag is set if either the VPLS instance or bridge instance is deleted, an applied profile is removed for the VPLS instance, or a PE entry in the profile is removed. In all such configuration changes, a peer is marked for deletion using this flag and an event is queued for processing. • disable—A peer is administratively disabled. This flag is set using the **`clear vpls peer disable`** command (in exec mode). • pri—Peer is configured as a primary peer. It indicates that it has a successful binding relationship with another (standby) peer. This flag is not applicable for peers that do not have a standby peer configured. This flag is not set if the standby peer or the primary peer are not successfully initialized. • proc-restart—Peer is recovering from a restart operation. This flag is used when the Label Manager (LM) has restarted or the controller card has switched over. The information about all active peers is recovered so that the same circuit ID and other resource IDs are used by the peer, because these resources are still active. This flag is set when the peer instance is created with the recovered information and is waiting initialization. After the initialization of the peer is complete, this flag is reset.(1) • pw-up—Pseudo-wire for the peer was successfully established and bidirectional label-switched paths (LSPs) exist. • Reset-pndg—A peer reset or restart operation is partially complete (pending). This flag is normally set if processing a reset or restart requires withdrawing a pseudo-wire label and the peer is waiting for a notification from the LM that the signaling is complete. It is used to ensure a new pseudo-wire is not signaled before the previous one was withdrawn.

Table 12 Field Descriptions for the show vpls peer Command

Field	Description
	• restart—Peer restart flag. The peer is marked for restart operation and an event is queued. Either of the following conditions can mark a peer for restart: • Configuration changes that require the peer to completely shut down (go back to the init state) and come back up with a new set of attributes • Issuing the **`clear vpls peer restart`** command (in exec mode) • stby—Peer is configured as a standby peer. It indicates that it has a successful binding relationship with another (primary) peer. This flag is not set if the primary peer does not exist or either of the peers were not successfully initialized. • tmr-restart—A delayed restart operation is scheduled for a peer. This flag is used for certain reconfiguration operations that require restarting many peers. This flag is set to indicate a delay is introduced for restarting a peer. It is cleared when processing the restart.
Peer ID	VPLS peer ID, which is the neighbor IP address.
Peer proc restarts	Peer process restart count.
Peer reset cnt	Peer reset count.
Peer restart cnt	Peer restart count.
Peer state changes	Peer state change count.
Peer up/down cnt	Peer up and down count.
Prev event	Previous peer flag event: • admin-enable—Peer administratively enabled. • admin-disable—Peer administratively disabled. • init—Peer initialized. • delete—Peer deleted. • reset—Peer reset (operational state changed to down and then back to up). • activate—Peer activated to assume operational role. • cct-cfg-change—Circuit attributes changed. • pw-up—Pseudo-wire associated with the peer is up. • pw-down—Pseudo-wire associated with the peer is down.

Table 12 Field Descriptions for the show vpls peer Command

Field	Description
Prev state	Previous operational state: • Deleted—Peer has been deleted, but pending clean up of the entry. • Disable—Peer is administratively disabled, either by disabling the VPLS instance or issuing the **`clear vpls peer disable`** command (in exec mode). The peer retains its allocated circuit ID if it is not a standby peer. When a peer is in this state, a standby peer is activated for it, if configured. • Down—Peer is operationally down. The peer is waiting for a pseudo-wire to be established. • Init—Peer is initializing. It remains in this state if any basic resources can not be allocated, including a circuit. • Standby—Peer is ready as a standby peer. A peer in this state has a pseudo-wire established and is on standby. If the primary peer goes down, the standby peer is ready to take over, without any disruptions, by using the same circuit as the primary peer and the same set of learned entries mapped to the new pseudo-wire. • Up—Peer is operationally active. The pseudo-wire established for the peer is participating in data forwarding.
Primary PE	Primary neighbor's IP address.
Primary PE state	Primary neighbor's operational state. For more information about the values for this field, see the Prev State field.
Profile name	VPLS profile name.
Pseudo-wire ID	Pseudo-wire ID. The ID can be the pseudo-wire name or number.
PW encap type	Pseudo-wire encapsulation type: • Ethernet—Ethernet encapsulation. • VLAN—Ethernet VLAN encapsulation.
PW error cnt	Pseudo-wire error count.
PW exp bits	Pseudo-wire EXP bits.

Table 12 Field Descriptions for the show vpls peer Command

Field	Description
PW flags	Run-time bit flags maintained by a peer for a pseudo-wire: • in-rib—Route entry is associated with this pseudo-wire. • delete-sig—Received a pseudo-wire delete message from the remote PE device. • delete-cfg—Local request to remove the pseudo-wire association. • in-lblmap—LFIB entry is associated with this pseudo-wire. • update—Received a pseudo-wire update. • up—Pseudo-wire state is up. • in-ldp—Pseudo-wire was signaled using LDP. • from-ldp—Received LDP message for this pseudo-wire association. • from-cfg—Received local request from this pseudo-wire association. • ldp-stale—Previous LDP request for the pseudo-wire is stale. • exp-set—Pseudo-wire is transporting EXP bits. • peer-up—VPLS peer state is up. • remote-encap—Pseudo-wire encapsulation signaled by the remote PE device. • local-cbit—Control word flag signaled by the remote PE device. • remote-cbit—Control word flag signaled by the remote PE device.
PW In label	MPLS label used for packets received over the pseudo-wire.
PW local MTU	Pseudo-wire local MTU.
PW Out label	MPLS label used for packets transmitted over the pseudo-wire.
PW remote MTU	Pseudo-wire remote MTU.
PW restart cnt	Pseudo-wire restart count.
PW state	Pseudo-wire state: • Down—Pseudo-wire is down. • Up—Pseudo-wire is established, but not used. • Up, Active—Pseudo-wire is up and is in service.
PW up/down cnt	Pseudo-wire up and down count.
Standby PE	Standby neighbor's IP address.

Table 12 Field Descriptions for the show vpls peer Command

Field	Description
Standby PE state	Standby neighbor's operational state. For more information about the values for this field, see the Prev State field.
VPLS Bridge	VPLS bridge name.
VPLS peer	VPLS peer is uniquely identified by the following three values: • Bridge name • Peer ID (neighbor IP address) • Pseudo-wire ID (name or number)

(1) If the process restart occurred when a standby peer was operational, then the states for the primary and standby peers are recovered.

1.49.6 Examples

The following example displays output from the **`show vpls peer`** command:

```
[local]Redback>show vpls peer
VPLS Bridge      Peer ID         Pseudo-wire ID  Circuit ID  Type     State
corpA            22.22.22.22     100             VPLS 3      Hub      Up
corpA            33.33.33.33     100             VPLS 4      Hub      Up
corpA            55.55.55.55     100             VPLS 6      Sp       Up
```

The following example displays output from the **`show vpls peer`** command:

```
[local]Redback>show vpls peer detail

VPLS peer (bridge/ip:pwid):  vplsA/22.22.22.22:10
 Oper State          : Up                    Context name      : local
 Admin State         : Enable                Circuit id        : VPLS 3
 Peer Flags          : active, pw-up
 Bridge id           : 0x1                   Context id        : 0x40080001
 PE peering type     : Hub                   PE local mode     : PE-rs
 Prev state          : Down                  Profile name      : forvplsA
 Prev event          : pw-up                 Last error        : no error
 PW state            : Up, Active
 PW up/down cnt      : 1
 PW error cn         : 0                     PW restart cnt    : 1
 PW In label         : 131072                PW encap type     : Ethernet
 PW Out label        : 131072                PW Exp bits       : 0x0
 PW local MTU        : 1500                  PW remote MTU     : 1500
 PW flags            : in-rib, in-lblmap, in-ldp, from-ldp, from-cfg,
                       ism-up, peer-up
```

The following example displays output from the **show vpls peer** command when primary and standby neighbors are configured:

```
[local]Redback>show vpls peer

VPLS Bridge       Peer ID         Pseudo-wire ID  Circuit ID  Type     State
corpA-MTU         11.11.11.11     100             VPLS 3      Sp Pri   Up
corpA-MTU         33.33.33.33     100             VPLS 3      Sp Sby   Stby
```

The following example displays output from the **show vpls peer detail** command when primary and standby neighbors are configured:

```
[local]Redback>show vpls peer detail

VPLS peer (bridge/ip:pwid):  corpA-MTU/11.11.11.11:100
 Oper State          : Up             Context name        : local
 Admin State         : Enable         Circuit id          : VPLS 1
 Peer Flags          : pri, active, pw-up
 Bridge id           : 0x1            Context id          : 0x40080001
 PE peering type     : Spoke          PE local mode       : MTU-s
```

```
 Standby PE          : 33.33.33.33    Standby PE state    : Stby
 Prev state          : Down           Profile name        : p1
 Prev event          : cct-cfg-change Last error          : no error
 Peer up/down cnt    : 1              Peer state changes  : 2
 Peer reset cnt      : 0              Peer config changes : 0
 Peer restart cnt    : 0              Peer proc restarts  : 0
 MAC flush sent      : 0              MAC flush received  : 0
 Circ up/down cnt    : 0              Circ cfg changes    : 2
 Circ error cnt      : 0              Circ delete cnt     : 0
 PW state            : Up, Active
 PW up/down cnt      : 1
 PW error cnt        : 0              PW restart cnt      : 1
 PW In label         : 131072         PW encap type       : Ethernet
 PW Out label        : 131072         PW Exp bits         : 0x0
 PW local MTU        : 1500           PW remote MTU       : 1500
 PW flags  : in-rib, in-lblmap, in-ldp, from-ldp, from-cfg
             peer-up

VPLS peer (bridge/ip:pwid):  corpA-MTU/33.33.33.33:100
 Oper State          : Stby           Context name        : local
 Admin State         : Enable         Circuit id          : VPLS 1
 Peer Flags          : stby, pw-up
 Bridge id           : 0x1            Context id          : 0x40080001
 PE peering type     : Spoke          PE local mode       : MTU-s
 Primary PE          : 11.11.11.11    Primary PE state    : Up
 Prev state          : Down           Profile name        : p1
 Prev event          : pw-up          Last error          : no error
 Peer up/down cnt    : 0              Peer state changes  : 2
 Peer reset cnt      : 0              Peer config changes : 0
 Peer restart cnt    : 0              Peer proc restarts  : 0
 MAC flush sent      : 0              MAC flush received  : 0
 Circ up/down cnt    : 0              Circ cfg changes    : 0
 Circ error cnt      : 0              Circ delete cnt     : 0
 PW state            : Down, Standby, In-active
 PW up/down cnt      : 1
 PW error cnt        : 0              PW restart cnt      : 1
 PW In label         : 131073         PW encap type       : Ethernet
 PW Out label        : 131072         PW Exp bits         : 0x0
```

```
PW local MTU        : 1500           PW remote MTU       : 1500
PW flags  : in-lblmap, in-ldp, from-ldp, from-cfg
            peer-up
```

1.50 show vpls profile

show vpls profile [*prof-name* [**pe** *ip-addr*]] [**detail**]

1.50.1 Purpose

Displays Virtual Private LAN Services (VPLS) profile information.

1.50.2 Command Mode

All modes

1.50.3 Syntax Description

prof-name	Optional. VPLS profile name. Displays information for the specified VPLS profile.
pe ***ip-addr***	Optional. VPLS neighbor IP address in the form A.B.C.D. Displays VPLS profile information for the specified VPLS peer.
detail	Optional. Displays detailed information.

1.50.4 Default

None

1.50.5 Usage Guidelines

Use the **show vpls profile** command to display VPLS profile information.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*. For information about troubleshooting VPLS, see *Troubleshooting VPLS*.

1.50.6 Examples

The following example displays output from the **show vpls profile** command:

```
[local]Redback>show vpls profile

 VPLS Profile          PE ID           Bridge Profile  Type  Peers(Up)
 test                  1.2.1.1                         Hub   1   (1)
 test                  1.2.1.2                         Hub   1   (1)
```

The following example displays output from the **show vpls profile detail** command:

```
[local]Redback>show vpls profile detail

VPLS profile (name/pe-id) : test/1.2.1.1
 PE peering type       : Hub            PE local mode       : PE-rs
 Number of peers       : 1              Active peers        : 1
 Standby for           : none           Bridge profile      : forvplsA
 Enacp type            : Ethernet       MAC limit           : 16002
 Bcast rate-limit      : 0              Bcast burst-size    : 1
 Mcast rate-limit      : 1              Mcast burst-size    : 0
 Unknown rate-limit    : 0              Unknown burst-size  : 0
 Bridge flags          : 0x8004
```

1.51 show vrrp

show vrrp [**debug** | **routers** [*if-name* [*vrrp-id*]] | **statistics** [*if-name* [*vrrp-id*]]

1.51.1 Purpose

Displays Virtual Router Redundancy Protocol (VRRP) information.

1.51.2 Command Mode

All modes

1.51.3 Syntax Description

debug	Optional. Displays debug options and filters.
routers	Optional. Displays state information pertaining to virtual routers.
if-name	Optional. Interface name. Displays the specified information for only the named interface.
vrrp-id	Optional. Virtual router ID. The range of values is 1 to 255. Displays the specified information for only the VRRP ID indicated.
statistics	Optional. Displays VRRP statistics.

1.51.4 Default

When entered without specifying any options, this command displays all VRRP statistics information.

1.51.5 Usage Guidelines

Use the **show vrrp** command to display VRRP information. Router and statistics information may be limited to virtual routers on a single interface or a single virtual router on a single interface.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.51.6 Examples

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

```
[local]Redback>show vrrp
```

```
  --- VRRP Virtual Router vrrp1/2 (Backup) ---

State              : Backup            Last Event        : Interface Up
Priority           : 100               Advertise Int     : 22
Last Adv Source    : 0.0.0.0           Up Time           : 5d 05:24:04
Preempt            : No                Master Down Int   : 66
Skew Time (u-sec)  : 218750
Auth Type:         : None              Key Chain         :
Address List:
1.1.1.1

  --- VRRP Virtual Router vrrp1/3 (Backup) ---

State              : Init              Last Event        : None
Priority           : 100               Advertise Int     : 1
Last Adv Source    : 0.0.0.0           Up Time           : N/A
Preempt            : No                Master Down Int   : 3
Skew Time (u-sec)  : 609375
Auth Type:         : None              Key Chain         :
Address List:
2.2.2.2
```

The following example displays output from the **show vrrp statistics** command:

```
[local]Redback>show vrrp statistics

  --- VRRP Global Statistics ---

Virtual Routers    : 3                 Interfaces        : 1
Packets Sent       : 0                 Packets Received  : 0
Packet Dropped     : 0                 No Router Errors  : 0
Checksum Errors    : 0                 Version Errors    : 0

  --- VRRP Virtual Router vrrp1/1 (Backup) ---

Master Transitions: 0
Advertisement Recv: 0                  Advertisement Sent: 0
Priority 0 Recv    : 0                 Priority 0 Sent   : 0
```

```
Bad Type Errors    : 0                 Wrong Owner Errors: 0
IP TTL Error       : 0                 Pkt Length Errors : 0
Interval Errors    : 0                 Address Errors    : 0
Auth Type Errors   : 0                 Auth Mismatchs    : 0
Auth Failures      : 0                 Auth Header Errors: 0


  --- VRRP Virtual Router vrrp1/2 (Backup) ---

Master Transitions: 0
Advertisement Recv: 0                  Advertisement Sent: 0
Priority 0 Recv    : 0                 Priority 0 Sent   : 0
Bad Type Errors    : 0                 Wrong Owner Errors: 0
IP TTL Error       : 0                 Pkt Length Errors : 0
Interval Errors    : 0                 Address Errors    : 0
Auth Type Errors   : 0                 Auth Mismatchs    : 0
Auth Failures      : 0                 Auth Header Errors: 0

  --- VRRP Virtual Router vrrp1/3 (Backup) ---

Master Transitions: 0
Advertisement Recv: 0                  Advertisement Sent: 0
Priority 0 Recv    : 0                 Priority 0 Sent   : 0
Bad Type Errors    : 0                 Wrong Owner Errors: 0
IP TTL Error       : 0                 Pkt Length Errors : 0
Interval Errors    : 0                 Address Errors    : 0
Auth Type Errors   : 0                 Auth Mismatchs    : 0
Auth Failures      : 0                 Auth Header Errors: 0
```

1.52 show xc

show xc

1.52.1 Purpose

Displays a list of all cross-connects (XCs) currently configured on the system.

1.52.2 Command Mode

All modes

1.52.3 Syntax Description

This command has no keywords or arguments.

1.52.4 Default

None

1.52.5 Usage Guidelines

Use the **show xc** command to display a list of all XCs currently configured on the system.

Note: The **show xc** command output displays information for both bypass and L2VPN XCs.

1.52.6 Examples

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

```
[local]Redback>show xc

              LDP L2VPN Circuits

L2 Circuit                     L2 State Peer address    VC Id    L-Label  State
lg id 25 vlan-id 58            Down     3.3.3.3         102      131072   Down
lg id 25 vlan-id 54:1          Down     3.3.3.3         103      131073   Down
lg id 25 vlan-id 3501          Down     3.3.3.3         3501     131074   Down
lg id 25 vlan-id 3502          Down     3.3.3.3         3502     131075   Down
lg id 25 vlan-id 3503          Down     3.3.3.3         3503     131076   Down
lg id 25 vlan-id 3504          Down     3.3.3.3         3504     131077   Down
lg id 25 vlan-id 3505          Down     3.3.3.3         3505     131078   Down
lg id 25 vlan-id 3506          Down     3.3.3.3         3506     131079   Down
lg id 25 vlan-id 3507          Down     3.3.3.3         3507     131080   Down
lg id 25 vlan-id 3508          Down     3.3.3.3         3508     131081   Down
lg id 25 vlan-id 3509          Down     3.3.3.3         3509     131082   Down
lg id 25 vlan-id 3510          Down     3.3.3.3         3510     131083   Down
lg id 25 vlan-id 3511          Down     3.3.3.3         3511     131084   Down
lg id 25 vlan-id 3512          Down     3.3.3.3         3512     131085   Down
lg id 25 vlan-id 3513          Down     3.3.3.3         3513     131086   Down
lg id 25 vlan-id 3514          Down     3.3.3.3         3514     131087   Down
lg id 25 vlan-id 3515          Down     3.3.3.3         3515     131088   Down
lg id 25 vlan-id 3516          Down     3.3.3.3         3516     131089   Down
lg id 25 vlan-id 3517          Down     3.3.3.3         3517     131090   Down
lg id 25 vlan-id 3518          Down     3.3.3.3         3518     131091   Down
lg id 25 vlan-id 3519          Down     3.3.3.3         3519     131092   Down
lg id 25 vlan-id 3520          Down     3.3.3.3         3520     131093   Down
lg id 25 vlan-id 3521          Down     3.3.3.3         3521     131094   Down
lg id 25 vlan-id 3522          Down     3.3.3.3         3522     131095   Down
lg id 25 vlan-id 3523          Down     3.3.3.3         3523     131096   Down
lg id 25 vlan-id 3524          Down     3.3.3.3         3524     131097   Down
lg id 25 vlan-id 3525          Down     3.3.3.3         3525     131098   Down
lg id 25 vlan-id 3526          Down     3.3.3.3         3526     131099   Down
lg id 25 vlan-id 3527          Down     3.3.3.3         3527     131100   Down
lg id 25 vlan-id 3528          Down     3.3.3.3         3528     131101   Down
lg id 25 vlan-id 3529          Down     3.3.3.3         3529     131102   Down
lg id 25 vlan-id 3530          Down     3.3.3.3         3530     131103   Down
lg id 25 vlan-id 3531          Down     3.3.3.3         3531     131104   Down
lg id 25 vlan-id 3532          Down     3.3.3.3         3532     131105   Down
lg id 25 vlan-id 3533          Down     3.3.3.3         3533     131106   Down
lg id 25 vlan-id 3534          Down     3.3.3.3         3534     131107   Down
lg id 25 vlan-id 3535          Down     3.3.3.3         3535     131108   Down
lg id 25 vlan-id 3536          Down     3.3.3.3         3536     131109   Down
lg id 25 vlan-id 3537          Down     3.3.3.3         3537     131110   Down
lg id 25 vlan-id 3538          Down     3.3.3.3         3538     131111   Down
lg id 25 vlan-id 3539          Down     3.3.3.3         3539     131112   Down
lg id 25 vlan-id 3540          Down     3.3.3.3         3540     131113   Down
lg id 25 vlan-id 3541          Down     3.3.3.3         3541     131114   Down
lg id 25 vlan-id 3542          Down     3.3.3.3         3542     131115   Down
---(more)---
```

Table 1 describes the fields in the **show xc** command output.

Table 13 show xc Command Output

Field	Description
L2 Circuit	Displays the circuit type and identifier for the physical (Layer 2) circuit hosting the local end of the XC, in the following format: • Link group ID or physical circuit location. The physical circuit is defined in the following format: ***slot*** /***port***[:***chan-num***[:***sub-chan-num***]] • Circuit type and virtual circuit ID. The circuit type can be a VLAN, VPI-VCI, or PPPoE session.
L2 State	Current state of the circuit. Can be Up (circuit is active) or Down (circuit is inactive).

Table 13 show xc Command Output

Field	Description
Peer address	IP address of the peer router.
VC Id	Virtual circuit (XC) identifier.
L-Label	Inner label associated with the local end of the XC.
State	Current state of the VC. Can be Up (circuit is active) or Down (circuit is inactive).

1.53 show xc (circuit)

To display information about all XCs configured on a specific port:

show xc ***circuit*** [**detail**]

To display information about an XC configured on a specific DLCI:

show xc ***circuit*** **dlci** ***dlci*** [**detail**]

To display information about an XC configured on a specific Point-to-Point Protocol (PPP) over Ethernet (PPPoE) session:

show xc ***circuit*** **pppoe** ***pppoe-session***] [**detail**]

To display information about an XC configured on a specific VLAN:

show xc ***circuit*** **vlan-id** ***vlan-id*** [**ipv6oe** | **pppoe*****pppoe-session***] [**detail**]

To display information about an XC configured on a specific VPI and VCI:

show xc ***circuit*** **vpi-vci** ***vpi vci*** [**ipv6oe** | **pppoe** ***pppoe-session***] [**detail**]

1.53.1 Purpose

Displays information about an XC configured specific circuit.

1.53.2 Command Mode

All modes

1.53.3 Syntax Description

circuit	Physical circuit identifier for the XC whose bypass information is to be displayed. The ***circuit*** format is defined as follows: • ***slot*** /***port***—Chassis slot and card port number for the XC whose bypass information is to be displayed. A slash (/) is required. • :***chan-num***—Optional. Channel number on the port for which a cross-connection is to be specified. • :***sub-chan-num***—Optional. Subchannel number on the port for which a cross-connection is to be specified.
dlci ***dlci***	Data-link connection identifier (DLCI) for the Frame Relay PVC.
pppoe ***pppoe-session***	PPPoE session identifier.
vlan-id ***vlan-id***	Specifies a Virtual LAN (VLAN).
ipv6oe	Specifies an IP Version 6 over Ethernet (IPv6oE)-encapsulated circuit.
vpi-vci ***vpi vci***	Virtual path identifier (VPI) and virtual circuit identifier (VCI) for an ATM PVC. The range of values for the VPI is 0 to 255. The range of values for the VCI is 1 to 65535.
detail	Displays detailed information about the specified XC.

1.53.4 Default

None

1.53.5 Usage Guidelines

Use the **show xc** (circuit) command to display information about an XC configured on a specific circuit.

1.53.6 Examples

The following example displays output from the **show xc** command for the XCs whose local endpoint is configured on slot 5, port 9:

```
[local]Redback>show xc 5/9

Circuit                   State   XC Circuit                State
5/9 vlan-id 500:50        Up      lg 26 vlan-id 500:50      Up
lg 26 vlan-id 32          Up      5/9 vlan-id 32            Up
lg 26 vlan-id 500:40      Up      5/9 vlan-id 500:40        Up
lg 26 vlan-id 500:41      Up      5/9 vlan-id 500:41        Up
lg 26 vlan-id 500:42      Up      5/9 vlan-id 500:42        Up
lg 26 vlan-id 501:1       Up      5/9 vlan-id 501:1         Up
lg 26 vlan-id 501:2       Up      5/9 vlan-id 501:2         Up
lg 26 vlan-id 501:3       Up      5/9 vlan-id 501:3         Up
lg 26 vlan-id 501:4       Up      5/9 vlan-id 501:4         Up
lg 26 vlan-id 501:5       Up      5/9 vlan-id 501:5         Up
lg 26 vlan-id 501:6       Up      5/9 vlan-id 501:6         Up
lg 26 vlan-id 501:7       Up      5/9 vlan-id 501:7         Up
lg 26 vlan-id 501:8       Up      5/9 vlan-id 501:8         Up
lg 26 vlan-id 501:9       Up      5/9 vlan-id 501:9         Up
lg 26 vlan-id 501:10      Up      5/9 vlan-id 501:10        Up
lg 26 vlan-id 501:11      Up      5/9 vlan-id 501:11        Up
lg 26 vlan-id 501:12      Up      5/9 vlan-id 501:12        Up
lg 26 vlan-id 501:13      Up      5/9 vlan-id 501:13        Up
lg 26 vlan-id 501:14      Up      5/9 vlan-id 501:14        Up
lg 26 vlan-id 501:15      Up      5/9 vlan-id 501:15        Up
lg 26 vlan-id 501:16      Up      5/9 vlan-id 501:16        Up
lg 26 vlan-id 501:17      Up      5/9 vlan-id 501:17        Up
---(more)---
```

Table 14 describes the fields in the **show xc** (circuit) command output.

Table 14 show xc (circuit) Command Output

Field	Description
Circuit	Displays the circuit type and identifier for the physical (Layer 2) circuit hosting the local end of the XC, in the following format: • Link group ID or physical circuit location. The physical circuit is defined in the following format: ***slot*** /***port***[:***chan-num***[:***sub-chan-num***]] • Circuit type and virtual circuit ID. The circuit type can be a VLAN, VPI-VCI, or PPPoE session.
State	Current state of the circuit. Can be Up (circuit is active) or Down (circuit is inactive).
XC Circuit	Displays the circuit type and identifier for the XC circuit, in the following format: • Link group ID or physical circuit location. The physical circuit is defined in the following format: ***slot*** /***port***[:***chan-num***[:***sub-chan-num***]] • Circuit type and virtual circuit ID. The circuit type can be a VLAN, VPI-VCI, or PPPoE session.
State	Current state of the XC. Can be Up (circuit is active) or Down (circuit is inactive).

The following example shows sample output from the show xc command for a specific XC. In this example, detailed information is displayed for the XC configured on port 9 on the card in slot 5, on the VLAN 501:17:

```
[local]Redback>show xc 5/9 vlan-id 501:17 detail

Displaying circuit: 5/9 vlan-id 501:17, State: Up
------------------------------------------------------------
Circuit handle    : 5/9:1023:63/1/2/7591
Encapsulation     : ether-dot1q-tunnel
FSM State         : Crossconnected
Group's grid      : 0x0
Adj id            : 0xff480015        NH Grid           : 0x3fb0002a
rcm range cfg rcvd: Yes               rcm expl cfg rcvd : No
ism cfg rcvd      : Yes               pending ism cfg   : No
hole punched      : No                rcm cfg deleted   : No
inbound           : No                crossconnected    : Yes
interworking      : No                group name set    : No
prot acct         : No                prot ccct         : No
prot active       : No                prot economical   : No
slot mask cfg     : 0x10              slot mask run     : 0x10
slot mask set     : 0x0               slot mask clear   : 0x0
ppas registered   : Yes

Displaying Peer circuit: lg 26 vlan-id 501:17, State: Up
------------------------------------------------------------
Circuit handle    : 255/22:1:27/1/2/2549
Encapsulation     : ether-dot1q-tunnel
FSM State         : Crossconnected
---(more)---
```

Table 15 describes the fields in the **show xc detail** (circuit) command.

Table 15 show xc detail (circuit) Command Output

Field	Description
Displaying circuit	Circuit type and identifier for the physical (Layer 2) circuit hosting the local end of the XC, in the following format: • link group ID or physical circuit location. The physical circuit is defined in the following format: ***slot*** /***port***[:***chan-num***[:***sub-chan-num***]] • circuit type and virtual circuit ID. The circuit type can be a VLAN, VPI-VCI, or PPPoE session.
State	Current state of the circuit. Can be Up (circuit is active) or Down (circuit is inactive).
Circuit handle	Handle internally assigned to the L2VPN circuit.
Encapsulation	Type of encapsulation on the local end of the XC. Can be: • Frame Relay over MPLS • Ethernet VLAN (dot1Q) • Ethernet • ATM AAL5 • ATM cell-mode • ATM RFC 1483 routed
FSM State	Current state of the internal finite state machine (FSM).

Table 15 show xc detail (circuit) Command Output

Field	Description
Group's grid	Group that the XC is configured under. This ID corresponds to the XC group name.
Adj id	Adjacency ID for this endpoint.
rcm range cfg rcvd	Indicates whether ranged cross connect configuration has been received for this endpoint.
ism cfg rcvd	Indicates whether this endpoint is bound to a bypass circuit (using the **`bind bypass`** command).
hole punched	Indicates a there is a hole punched in the range for this XC, and the non-ranged XC is the active XC for this endpoint. This occurs when ranged and non-ranged configuration is received for an XC.
inbound	Indicates whether this circuit was the first circuit listed when the XC was configured with the **`xc`** command.
prot acct	Indicates whether this circuit is the aggregate circuit for a link-group.
prot active	Indicates whether the link-group for this circuit is active (configured on one or more ports).
slot mask cfg	Configured slot mask, in hexadecimal format.
slot mask set	Slot mask that XCD needs to process for this endpoint. The slot mask is displayed in hexadecimal format.
ppas registered	Indicates whether the PPA for this endpoint is registered with XCD.
NH Grid	Next-hop grid from this endpoint, in hexadecimal format.
rcm expl cfg rcvd	Indicates whether non-ranged XC configuration was received for this endpoint.
pending ism cfg	Indicates whether a configure message for this endpoint is waiting to be sent to ISM. This field is specific to interworking XCs.
rcm cfg deleted	Indicates whether non-ranged XC configuration for an endpoint is deleted. This field is always set to No.
crossconnected	Indicates whether this XC is installed on the PPA.
group name set	Indicates whether the group name is set. This fields is always set to No.
prot ccct	Indicates whether this circuit is a constituent circuit in a link group.
prot economical	Indicates whether this circuit is economical.
slot mask run	Configured slot mask, in hexadecimal format.
slot mask clear	Slot mask bits that need to be cleared, in hexadecimal format.

Table 15 show xc detail (circuit) Command Output

Field	Description
Displaying Peer circuit	Displays information for Layer 2 (physical) circuit hosting the remote end of the XC, in the following format: • link group ID or physical circuit location. The physical circuit is defined in the following format: ***slot*** **/** ***port*** [**:** ***chan-num*** [**:** ***sub-chan-num***]] • circuit type and virtual circuit ID. The circuit type can be a VLAN, VPI-VCI, or PPPoE session.
State	Current state of the circuit. Can be Up (circuit is active) or Down (circuit is inactive).
Circuit handle	Handle internally assigned to the L2VPN circuit.
FSM State	Current state of the internal finite state machine (FSM) for this endpoint.

1.54 show xc bypass

To display a list of all bypass cross-connects (XCs) configured on the system:

show xc bypass

To display information about the XCs configured on under a specific link group:

show xc bypass lg {***name*** | ***num***} [**vlan-id** ***vlan-id*** [**ipv6oe** |**pppoe** ***pppoe-session***] | **vpi-vci** ***vpi vci*** [**ipv6oe** |**pppoe** ***pppoe-session***] | **pppoe** ***pppoe-session***] [**detail**]

To display information about the bypass XCs configured on a specific circuit:

show xc ***circuit*** [**vlan-id** ***vlan-id*** [**ipv6oe** | **pppoe** ***pppoe-session***] | **vpi-vci** ***vpi vci*** [**ipv6oe** | **pppoe** ***pppoe-session***] | **pppoe** ***pppoe-session***] [**detail**]

To display information about the active (up) bypass XCs configured on the system:

show xc bypass up [**lg** {***name*** | ***num***} | ***circuit***] [**vlan-id** ***vlan-id*** [**ipv6oe** | **pppoe** ***pppoe-session***] | **vpi-vci** ***vpi vci*** [**ipv6oe** | **pppoe** ***pppoe-session***] | **pppoe** ***pppoe-session***] [**detail**]

To display information about the inactive (down) bypass XCs configured on the system:

show xc bypass down [**lg** {***name*** | ***num***} | ***circuit***] [**vlan-id** ***vlan-id*** [**ipv6oe** | **pppoe** ***pppoe-session***] | **vpi-vci** ***vpi vci*** [**ipv6oe pppoe** ***pppoe-session***] | **pppoe** ***pppoe-session***]| [**detail**]

To display brief (summarized) information about all bypass XCs configured on the system:

show xc bypass summary

1.54.1 Purpose

Displays information about the bypass XCs configured on this system.

1.54.2 Command Mode

All modes

1.54.3 Syntax Description

lg	Displays bypass information for a specific link group XC.
name	Specifies the name of an access link group XC whose bypass information to display.
num	Specifies the ID of an access link group XC whose bypass information to display. The link-group ID is automatically assigned by the SmartEdge router, and is displayed when you enter the **show link-group detail** command.
circuit	Physical circuit identifier for the XC whose bypass information is to be displayed. The ***circuit*** format is defined as follows: • ***slot*** /***port***—Chassis slot and card port number for the XC whose bypass information is to be displayed. A slash (/) is required. • :***chan-num***—Optional. Channel number on the port for which a cross-connection is to be specified. • :***sub-chan-num***—Optional. Subchannel number on the port for which a cross-connection is to be specified.
vlan-id ***vlan-id***	Specifies an 802.1Q Virtual LAN (VLAN) whose bypass information to display.
vpi-vci ***vpi vci***	Specifies a virtual path identifier (VPI) and virtual circuit identifier (VCI) for the bypass (ATM) XC whose information you want to display. The range of values is 0 to 255 and 1 to 65535.
ipv6oe	Displays bypass XC information for an IP Version 6 over Ethernet (IPv6oE)-encapsulated circuit.
pppoe ***session-id***	Specifies the PPPoE encapsulation session whose bypass XC information to display.
up	Displays bypass information about the active (up) XCs on the system.

down	Displays bypass information about the inactive (down) XCs on the system.
detail	Displays more detailed output about the specified bypass XC.
summary	Displays summarized information about the specified bypass XC.

1.54.4 Default

None

1.54.5 Usage Guidelines

Use the **show xc bypass** command to display bypass information about the XCs configured on this system.

1.54.6 Examples

The following example displays output from the **show xc bypass** command:

```
[local]Redback>show xc bypass

Circuit                  State   XC Circuit               State
5/9 vlan-id 500:50       Up      lg 26 vlan-id 500:50     Up
lg 26 vlan-id 32         Up      5/9 vlan-id 32           Up
lg 26 vlan-id 500:40     Up      5/9 vlan-id 500:40       Up
lg 26 vlan-id 500:41     Up      5/9 vlan-id 500:41       Up
lg 26 vlan-id 500:42     Up      5/9 vlan-id 500:42       Up
lg 26 vlan-id 501:1      Up      5/9 vlan-id 501:1        Up
lg 26 vlan-id 501:2      Up      5/9 vlan-id 501:2        Up
lg 26 vlan-id 501:3      Up      5/9 vlan-id 501:3        Up
lg 26 vlan-id 501:4      Up      5/9 vlan-id 501:4        Up
lg 26 vlan-id 501:5      Up      5/9 vlan-id 501:5        Up
lg 26 vlan-id 501:6      Up      5/9 vlan-id 501:6        Up
lg 26 vlan-id 501:7      Up      5/9 vlan-id 501:7        Up
lg 26 vlan-id 501:8      Up      5/9 vlan-id 501:8        Up
lg 26 vlan-id 501:9      Up      5/9 vlan-id 501:9        Up
lg 26 vlan-id 501:10     Up      5/9 vlan-id 501:10       Up
lg 26 vlan-id 501:11     Up      5/9 vlan-id 501:11       Up
lg 26 vlan-id 501:12     Up      5/9 vlan-id 501:12       Up
lg 26 vlan-id 501:13     Up      5/9 vlan-id 501:13       Up
lg 26 vlan-id 501:14     Up      5/9 vlan-id 501:14       Up
lg 26 vlan-id 501:15     Up      5/9 vlan-id 501:15       Up
lg 26 vlan-id 501:16     Up      5/9 vlan-id 501:16       Up
lg 26 vlan-id 501:17     Up      5/9 vlan-id 501:17       Up
---(more)---
```

Table 2 describes the fields in the **show xc bypass** command output.

Table 16 show xc bypass Command Output

Field	Description
Circuit	Displays the circuit type and identifier for the physical (Layer 2) circuit hosting the local end of the XC, in the following format: • Link group ID or physical circuit location. The physical circuit is defined in the following format: ***slot*** /***port***[:***chan-num***[:***sub-chan-num***]] • Circuit type and virtual circuit ID. The circuit type can be a VLAN, VPI-VCI, or PPPoE session.
State	Current state of the circuit. Can be Up (circuit is active) or Down (circuit is inactive).
XC Circuit	Displays the circuit type and identifier for the XC circuit, in the following format: • link group ID or physical circuit location. The physical circuit is defined in the following format: ***slot*** /***port***[:***chan-num***[:***sub-chan-num***]] • circuit type and virtual circuit ID. The circuit type can be a VLAN, VPI-VCI, or PPPoE session.
State	Current state of the XC. Can be Up (circuit is active) or Down (circuit is inactive).

The following example displays output from the **show xc bypass** command. In this example, the command output displays information about the bypass XC on port 9 on the card in slot 5 on VLAN 501:16:

```
[local]Redback>show xc bypass 5/9 vlan-id 501:16
Circuit                 State   XC Circuit              State
lg 26 vlan-id 501:16    Up      5/9 vlan-id 501:16      Up
```

The **show xc bypass** command output is described in Table 2.

The following example displays summarized output from the **show xc bypass** command:

```
[local]Redback>show xc bypass summary

     Endpoints total: 9019, Up: 9019, Down: 0
 Crossconnects total: 4505, Up: 4505, Down: 0
```

Table 3 describes the fields in the **show xc bypass** summary command output.

Table 17 show xc bypass summary Command Output

Field	Description
Endpoints total:	Total number of active and inactive XC endpoints on this system that are bound to bypass LSPs.
Crossconnects total:	Total number of active and inactive XCs configured on this system. This field is typically one-half of the Endpoints total.

1.55 show xc detail

`show xc detail`

1.55.1 Purpose

Displays detailed information about all cross-connects (XCs) configured on the system.

1.55.2 Command Mode

All modes

1.55.3 Syntax Description

This command has no keywords or arguments.

1.55.4 Default

None

1.55.5 Usage Guidelines

Use the **`show xc detail`** command to display detailed information about all XCs configured on this system.

Note: The **`show xc detail`** command output displays information for both bypass and L2VPN XCs.

1.55.6 Examples

The following example displays output from the **`show xc detail`** command:

```
[local]Redback>show xc detail

    LDP L2VPN Circuit lg id 25 vlan-id 58

L2 State         : Up               Peer             : 3.3.3.3
VC ID            : 102              XC state         : Up
Local Label      : 131072           Access Circuit   : 255/22:1:26/1/2/6
Remote Label     : 131126           L2VPN Circuit    : 255/12:103:63/0/1/1
EXP bits         : 0                Local Encap      : dot1q tsp
Remote Group ID  : 0                Remote Encap     :
Local VC Type    : VLAN             Remote VC Type   : VLAN
Local VC MTU     : 1500             Remote VC MTU    : 1500
Local VC Status  : forwarding       Remote VC Status : forwarding
XC group         : default          Negotiated cbit  : no
LSP Configured   :                  LSP Used         :
XC profile       :
Flags 0x800819e9: in-rib, in-lblmap, in-ldp, from-ldp, from-cfg
                : peer-up

    LDP L2VPN Circuit lg id 25 vlan-id 54:1

L2 State         : Up               Peer             : 3.3.3.3
VC ID            : 103              XC state         : Up
Local Label      : 131073           Access Circuit   : 255/22:1:26/1/2/15
Remote Label     : 131127           L2VPN Circuit    : 255/12:104:63/0/1/2
EXP bits         : 0                Local Encap      : dot1q-1q tu-tsp
Remote Group ID  : 0                Remote Encap     :
Local VC Type    : VLAN             Remote VC Type   : VLAN
Local VC MTU     : 1500             Remote VC MTU    : 1500
Local VC Status  : forwarding       Remote VC Status : forwarding
XC group         : default          Negotiated cbit  : no
---(more)---
```

Table 18 describes the fields in the **`show xc detail`** command.

Table 18 show xc detail Command Output

Field	Description
L2 State	Current state of the layer 2 (physical) circuit. Can be Up (active), Standby, or Down (inactive).
VC ID	Identifies the virtual circuit on which this XC is configured.
Local Label	Inner label associated with the local end of a cross-connection.
Remote Label	Inner label associated with the remote end of a cross-connection.
EXP bits	EXP bits to be used for transport. Range is from 0 through 7.
Remote Group ID	Identifies the link group hosting this XC at the remote end (if the XC is configured under a link group).
Local VC Type	Type of circuit hosting the local end of the XC.
Local VC MTU	MTU on the local end of the XC.
Local VC Status	Current forwarding status of the VC hosting the local end of the XC. The status can be Forwarding, Forwarding Standby, Receive, or Transmit.
XC group	Identifies the group under which the local end of the XC is configured.
LSP Configured	Name of the LSP mapped to the XC (if the XC is configured on an LSP).
XC profile	Identifies any XC profile that is attached to this XC. The XC profile determines the configuration used by the XC.

Table 18 show xc detail Command Output

Field	Description
Peer	IP address of the peer hosting the remote end of the XC.
XC state	Current state of the XC. Can be Up (active), Standby, or Down (inactive).
Access Circuit	Circuit handle internally assigned to the local access circuit on the XC.
L2VPN Circuit	Circuit handle internally assigned to the L2VPN circuit.
Local Encap	Type of encapsulation on the local end of the XC. Can be: • Frame Relay over MPLS • Ethernet VLAN (dot1Q) • Ethernet • ATM AAL5 • ATM cell-mode • ATM RFC 1483 routed
Remote Encap	Type of encapsulation on the remote end of the XC. Can be: • Frame Relay over MPLS • Ethernet VLAN (dot1Q) • Ethernet • ATM AAL5 • ATM cell-mode • ATM RFC 1483 routed
Remote VC Type	Type of virtual circuit hosting the remote end of the XC. Can be VLAN, VPI-VCI, or PPPoE.
Remote VC MTU	MTU on the circuit hosting the remote end of the XC.
Remote VC Status	Current forwarding status of the VC hosting the remote end of the XC. The status can be Forwarding, Forwarding Standby, Receive, or Transmit.
Negotiated cbit	Indicates whether the control word is present in the pseudowire PDU. The presence of a sequence number indicates that the control word is present in the pseudowire PDU. If the negotiated value is set to yes, then only the control word is present in the PDU that is carried over the pseudowire.
LSP Used	Displays whether the primary or bypass (backup) LSP is currently active.
Flags 0x800819e9:	Identifies the current running state of the XC.

1.56 show xc down

show xc down [**detail**]

1.56.1 Purpose

Displays information about the inactive (down) bypass cross-connects (XCs) configured on this system.

1.56.2 Command Mode

All modes

1.56.3 Syntax Description

detail Displays more detailed output about the inactive bypass XCs configured on this system.

1.56.4 Default

None

1.56.5 Usage Guidelines

Use the **show xc down** command to display information about the inactive (down) bypass XCs configured on this system.

Note: The **show xc down** command displays information for bypass XCs only; the **show xc down** command output does not display information for L2VPN XCs.

1.56.6 Examples

The following example displays output from the **show xc down** command:

```
[local]Redback>show xc down
               LDP L2VPN Circuits

L2 Circuit                    L2 State Peer address    VC Id    L-Label  State
lg id 25 vlan-id 3501         Up       3.3.3.3         3501     131074   Down
lg id 25 vlan-id 3502         Up       3.3.3.3         3502     131075   Down
lg id 25 vlan-id 3503         Up       3.3.3.3         3503     131076   Down
lg id 25 vlan-id 3504         Up       3.3.3.3         3504     131077   Down
lg id 25 vlan-id 3505         Up       3.3.3.3         3505     131078   Down
lg id 25 vlan-id 3506         Up       3.3.3.3         3506     131079   Down
lg id 25 vlan-id 3507         Up       3.3.3.3         3507     131080   Down
lg id 25 vlan-id 3508         Up       3.3.3.3         3508     131081   Down
lg id 25 vlan-id 3509         Up       3.3.3.3         3509     131082   Down
lg id 25 vlan-id 3510         Up       3.3.3.3         3510     131083   Down
lg id 25 vlan-id 3511         Up       3.3.3.3         3511     131084   Down
lg id 25 vlan-id 3512         Up       3.3.3.3         3512     131085   Down
lg id 25 vlan-id 3513         Up       3.3.3.3         3513     131086   Down
lg id 25 vlan-id 3514         Up       3.3.3.3         3514     131087   Down
lg id 25 vlan-id 3515         Up       3.3.3.3         3515     131088   Down
lg id 25 vlan-id 3516         Up       3.3.3.3         3516     131089   Down
lg id 25 vlan-id 3517         Up       3.3.3.3         3517     131090   Down
lg id 25 vlan-id 3518         Up       3.3.3.3         3518     131091   Down
lg id 25 vlan-id 3768         Up       3.3.3.3         3768     131341   Down
lg id 25 vlan-id 3769         Up       3.3.3.3         3769     131342   Down
---(more)---
```

The following table describes the fields in the **show xc down** command output.

Table 19 show xc down Command Output

Field	Description
L2 Circuit	Displays the circuit type and identifier for the physical (Layer 2) circuit hosting the local end of the XC, in the following format: • link group ID or physical circuit location. The physical circuit is defined in the following format: ***slot*** /***port***[:***chan-num***[:***sub-chan-num***]] • circuit type and virtual circuit ID. The circuit type can be a VLAN, VPI-VCI, or PPPoE session.
L2 State	Current state of the Layer 2 (physical) circuit. Can be Up (circuit is active) or Down (circuit is inactive).
Peer address	IP address of the peer router.
VC Id	Virtual circuit identifier for the local end of the XC.
L-Label	Local label. Inner label associated with the local end of an L2VPN cross-connection.
State	Current state of the VC. Can be Up (circuit is active) or Down (circuit is inactive).

1.57 show xc group

show xc group {***group-name*** | **default**} {**detail**}

1.57.1 Purpose

Displays information about a cross-connect (XC) group.

1.57.2 Command Mode

All modes

1.57.3 Syntax Description

group	Displays information about the XCs in a specific XC group.
group-name	Name of the XC group whose information to display. Displays information about the XCs in the specified XC group only.
default	Displays information about the XCs in the default XC group only.
detail	Optional. Displays detailed information about the L2VPN cross-connections in the specified group.

1.57.4 Default

None

1.57.5 Usage Guidelines

Use the **show xc group** command to display information about an XC group.

1.57.6 Examples

The following example displays output from the **show xc group** command. In this example, output is displayed for the **default** XC group:

```
[local]Redback>show xc group default
               LDP L2VPN Circuits

L2 Circuit                    L2 State Peer address    VC Id    L-Label  State
lg id 25 vlan-id 58           Up       3.3.3.3         102      131072   Up
lg id 25 vlan-id 54:1         Up       3.3.3.3         103      131073   Up
lg id 25 vlan-id 3501         Up       3.3.3.3         3501     131074   Up
lg id 25 vlan-id 3502         Up       3.3.3.3         3502     131075   Up
lg id 25 vlan-id 3503         Up       3.3.3.3         3503     131076   Up
lg id 25 vlan-id 3504         Up       3.3.3.3         3504     131077   Up
lg id 25 vlan-id 3505         Up       3.3.3.3         3505     131078   Up
lg id 25 vlan-id 3506         Up       3.3.3.3         3506     131079   Up
lg id 25 vlan-id 3507         Up       3.3.3.3         3507     131080   Up
lg id 25 vlan-id 3508         Up       3.3.3.3         3508     131081   Up
lg id 25 vlan-id 3509         Up       3.3.3.3         3509     131082   Up
lg id 25 vlan-id 3510         Up       3.3.3.3         3510     131083   Up
lg id 25 vlan-id 3511         Up       3.3.3.3         3511     131084   Up
lg id 25 vlan-id 3512         Up       3.3.3.3         3512     131085   Up
lg id 25 vlan-id 3513         Up       3.3.3.3         3513     131086   Up
lg id 25 vlan-id 3514         Up       3.3.3.3         3514     131087   Up
lg id 25 vlan-id 3515         Up       3.3.3.3         3515     131088   Up
lg id 25 vlan-id 3516         Up       3.3.3.3         3516     131089   Up
lg id 25 vlan-id 3517         Up       3.3.3.3         3517     131090   Up
lg id 25 vlan-id 3518         Up       3.3.3.3         3518     131091   Up
---(more)---
```

The following table describes the fields in the **show xc group** command output.

Table 20 show xc group Command Output

Field	Description
L2 Circuit	Displays the circuit type and identifier for the physical (Layer 2) circuit hosting the local end of the XC, in the following format: • link group ID or physical circuit location. The physical circuit is defined in the following format: ***slot*** /***port***[:***chan-num***[:***sub-chan-num***]] • circuit type and virtual circuit ID. The circuit type can be a VLAN, VPI-VCI, or PPPoE session.
L2 State	Current state of the Layer 2 (physical) circuit. Can be Up (circuit is active) or Down (circuit is inactive).
Peer address	IP address of the peer router.
VC Id	Virtual circuit identifier for the local end of the XC.
L-Label	Inner label associated with the local end of the XC.
State	Current state of the VC. Can be Up (circuit is active) or Down (circuit is inactive).

The following example displays detailed output from the **show xc group** command. In this example, detailed output is displayed for the **default** XC group:

```
[local]Redback>show xc group default detail


    LDP L2VPN Circuit lg id 25 vlan-id 58

L2 State         : Up               Peer             : 3.3.3.3
VC ID            : 102              XC state         : Up
Local Label      : 131072           Access Circuit   : 255/22:1:26/1/2/6
Remote Label     : 131126           L2VPN Circuit    : 255/12:103:63/0/1/1
EXP bits         : 0                Local Encap      : dot1q tsp
Remote Group ID  : 0                Remote Encap     :
Local VC Type    : VLAN             Remote VC Type   : VLAN
Local VC MTU     : 1500             Remote VC MTU    : 1500
Local VC Status  : forwarding       Remote VC Status : forwarding
XC group         : default          Negotiated cbit  : no
LSP Configured   :                  LSP Used         :
XC profile       :
Flags 0x800819e9: in-rib, in-lblmap, in-ldp, from-ldp, from-cfg
                : peer-up

    LDP L2VPN Circuit lg id 25 vlan-id 54:1

L2 State         : Up               Peer             : 3.3.3.3
VC ID            : 103              XC state         : Up
Local Label      : 131073           Access Circuit   : 255/22:1:26/1/2/15
Remote Label     : 131127           L2VPN Circuit    : 255/12:104:63/0/1/2
EXP bits         : 0                Local Encap      : dot1q-1q tu-tsp
Remote Group ID  : 0                Remote Encap     :
Local VC Type    : VLAN             Remote VC Type   : VLAN
Local VC MTU     : 1500             Remote VC MTU    : 1500
Local VC Status  : forwarding       Remote VC Status : forwarding
XC group         : default          Negotiated cbit  : no
LSP Configured   :                  LSP Used         :
XC profile       :
Flags 0x800819e9: in-rib, in-lblmap, in-ldp, from-ldp, from-cfg
                : peer-up

---(more)---
```

Table 21 describes the fields in the **`show xc group detail`** command.

Table 21 show xc group detail Command Output

Field	Description
L2 State	Current state of the layer 2 (physical) circuit. Can be Up (active), Standby, or Down (inactive).
VC ID	Identifies the virtual circuit on which this XC is configured.
Local Label	Inner label associated with the local end of a cross-connection.
Remote Label	Inner label associated with the remote end of a cross-connection.
EXP bits	EXP bits to be used for transport. Range is from 0 through 7.
Remote Group ID	Identifies the link group hosting this XC at the remote end (if the XC is configured under a link group).
Local VC Type	Type of circuit hosting the local end of the XC.
Local VC MTU	MTU on the local end of the XC.
Local VC Status	Current forwarding status of the VC hosting the local end of the XC. The status can be Forwarding, Forwarding Standby, Receive, or Transmit.
XC group	Identifies the group under which the local end of the XC is configured.

Table 21 show xc group detail Command Output

Field	Description
LSP Configured	Name of the LSP mapped to the XC (if the XC is configured on an LSP).
XC profile	Identifies any XC profile that is attached to this XC. The XC profile determines the configuration used by the XC.
Peer	IP address of the peer hosting the remote end of the XC.
XC state	Indicate whether the XC is active (Up) or inactive (Down).
Access Circuit	Circuit handle internally assigned to the local access circuit on the XC.
L2VPN Circuit	Circuit handle internally assigned to the L2VPN circuit.
Local Encap	Type of encapsulation on the local end of the XC. Can be: • Frame Relay over MPLS • Ethernet VLAN (dot1Q) • Ethernet • ATM AAL5 • ATM cell-mode • ATM RFC 1483 routed
Remote Encap	Type of encapsulation on the remote end of the XC. Can be: • Frame Relay over MPLS • Ethernet VLAN (dot1Q) • Ethernet • ATM AAL5 • ATM cell-mode • ATM RFC 1483 routed
Remote VC Type	Type of virtual circuit hosting the remote end of the XC. Can be VLAN, VPI-VCI, or PPPoE.
Remote VC MTU	MTU on the circuit hosting the remote end of the XC.
Remote VC Status	Current forwarding status of the VC hosting the remote end of the XC. The status can be Forwarding, Forwarding Standby, Receive, or Transmit.
Negotiated cbit	Indicates whether the control word is present in the pseudowire PDU. The presence of a sequence number indicates that the control word is present in the pseudowire PDU. If the negotiated value is set to yes, then only the control word is present in the PDU that is carried over the pseudowire.

Table 21 show xc group detail Command Output

Field	Description
LSP Used	Displays whether the primary or bypass (backup) LSP is currently active.
Flags	Identify the current running state of the XC.

1.58 show xc l2vpn

show xc l2vpn [[*slot/port*] *circuit-id* | **group** {*group-name* | **default**} | **lg id** *lg-name-in* | **ldp**} | **peer** *peer-addr*| **route** | **static**] [**detail**] | [**summary**]]

1.58.1 Purpose

Displays Layer 2 Virtual Private Network (L2VPN) cross-connect information.

1.58.2 Command Mode

All modes

1.58.3 Syntax Description

circuit-id Optional. Layer 2 (L2) circuit ID. Depending on the type of circuit being cross-connected, the L2 circuit ID takes one of the following constructs:

- **vpi-vci** ***vpi vci***—ATM permanent virtual circuit (PVC). Specifies the virtual path identifier (VPI) and virtual channel identifier (VCI). The range of values for the vpi and vci arguments are 0 to 255, and 1 to 65,535 respectively.
- **vpi-vci** ***vpi start-vci*** **through** ***end-vci***—Range of ATM PVCs. Specifies the VPI and the range of VCIs. The range of values for the vpi argument is 0 to 255; the range of values for the start-vci and end-vci arguments is 1 to 65,535.
- **vlan-id** ***pvc-vlan-id***—Virtual LAN (VLAN) 802.1Q PVC that is not within an 802.1Q tunnel. Specifies the PVC VLAN tag. The range of values for the pvc-vlan-id argument is 1 to 4,095.
- **vlan-id** ***start-pvc-vlan-id*** **through** ***end-pvc-vlan-id***—Range of VLAN 802.1Q PVCs that are not within an 802.1Q tunnel. Specifies the range of PVC VLAN tags. The range of values for the start-pvc-vlan-id and end-pvc-vlan-id arguments is 1 to 4,095.
- **vlan-id** ***tunl-vlan-id*****:*****pvc-vlan-id***—VLAN 802.1Q PVC that is within an 802.1Q tunnel. Specifies the VLAN tag for the tunnel followed by the PVC VLAN tag. The range of values for the tunl-vlan-id and pvc-vlan-id arguments is 1 to 4,095.
- **vlan-id** ***tunl-vlan-id*****:*****start-pvc-vlan-id*** **through** ***end-pvc-vlan-id*** —Range of VLAN 802.1Q PVCs that are within an 802.1Q tunnel. Specifies the VLAN tag for the tunnel followed by the range of PVC VLAN tags. The range of values for the tunl-vlan-id, start-pvc-vlan-id, and end-pvc-vlan-id arguments is 1 to 4,095.
- **dlci** ***dlci***—Data-link connection identifier (DLCI) for the Frame Relay PVC. The range of values for the dlci argument is 16 to 991.

For Ethernet ports with no 802.1Q PVCs, no circuit descriptor is specified.

group Optional. Displays cross-connection information only for a specific cross-connection group.

group-name Cross-connection group name.

default Displays cross-connection information only for the default cross-connection group.

lg id ***lg-name-in*** Specifies the name of an access link group to be cross-connected inbound

ldp Optional. Displays only Label Distribution Protocol (LDP) L2VPN cross-connection information.

peer ***peer-addr***	IP address of the remote peer provider edge (PE) router.
static	Optional. Displays only static L2VPN cross-connection information.
route	Displays L2VPN route information.
detail	Optional. Displays detailed L2VPN cross-connection information. When used with the xc-circuit argument, displays detailed L2VPN cross-connection information only for the specified cross-connected circuit.
summary	Displays summary L2VPN information.

1.58.4 Default

None.

1.58.5 Usage Guidelines

Use the **show xc l2vpn** command to display L2VPN-related information.

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

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in *Using the CLI*.

1.58.6 Examples

The following example displays information about all L2VPN cross-connections that are configured on the current router:

```
[local]Redback# show xc l2vpn

Static L2VPN Circuits
L2 Circuit                    L2 State Peer address    Label
10/1 vlan-id 1                Up       1.1.1.2         4097
10/1 vlan-id 2                Up       1.1.1.2         4098
10/1 vlan-id 3                Up       1.1.1.2         4099
10/1 vlan-id 4                Up       1.1.1.2         4100
10/1 vlan-id 5                Up       1.1.1.2         4101
LDP L2VPN Circuits
L2 Circuit                    L2 State Peer address    VC Id    L-Label
State

VPLS 0x4000002                Up       83.1.1.1        10       131073   Down
VPLS 0x4000003                Up       111.111.111.111 10       131074   Down
4/1 vpi-vci 1 100             Up       111.111.111.111 10000    131075   Down
```

The following table describes the fields in the **show xc l2vpn** command output.

Table 22 show xc l2vpn Command Output

Field	Description
L2 Circuit	Displays the circuit type and identifier for the physical (Layer 2) circuit hosting the local end of the XC, in the following format: • link group ID or physical circuit location. The physical circuit is defined in the following format: ***slot*** /***port***[:***chan-num***[:***sub-chan-num***]] • circuit type and virtual circuit ID. The circuit type can be a VLAN, VPI-VCI, or PPPoE session.
L2 State	Current state of the Layer 2 (physical) circuit. Can be Up (circuit is active) or Down (circuit is inactive).
Peer address	IP address of the peer router.
L-Label	Inner label associated with the local end of the L2VPN XC.

The following example shows how to display L2VPN route information:

```
[local]Redback>show xc l2vpn route
L2 Circuit               XC Circuit               Next-hop       Uptime
10/1:1023:63/1/2/4099    255/12:2:63/0/1/10       1.1.1.2        01:41:59
10/1:1023:63/1/2/4100    255/12:3:63/0/1/11       1.1.1.2        01:41:59
10/1:1023:63/1/2/4101    255/12:4:63/0/1/12       1.1.1.2        01:41:58
10/1:1023:63/1/2/4102    255/12:5:63/0/1/13       1.1.1.2        01:41:58
10/1:1023:63/1/2/4103    255/12:6:63/0/1/14       1.1.1.2        01:41:37
```

The following table describes the fields in the **show xc l2vpn route** command output.

Table 23 show xc l2vpn route Command Output

Field	Description
L2 Circuit	Displays the circuit type and identifier for the physical (Layer 2) circuit hosting the local end of the XC, in the following format: • link group ID or physical circuit location. The physical circuit is defined in the following format: ***slot*** /***port***[:***chan-num***[:***sub-chan-num***]] • circuit type and virtual circuit ID. The circuit type can be a VLAN, VPI-VCI, or PPPoE session.
XC Circuit	Circuit handle internally assigned to the XC (L2VPN) circuit.
Next-hop	IP address of the next-hop peer.
Uptime	Amount of time the XC (L2VPN) circuit has been in the Up state, displayed in the ***hours*:*minutes*:*seconds*** format.

The following example displays static L2VPN cross-connection information:

```
[local]Redback#show xc l2vpn static

Static L2VPN Circuits
L2 Circuit                    L2 State Peer address    Label
10/1 vlan-id 1                Up       1.1.1.2         4097
10/1 vlan-id 2                Up       1.1.1.2         4098
10/1 vlan-id 3                Up       1.1.1.2         4099
10/1 vlan-id 4                Up       1.1.1.2         4100
10/1 vlan-id 5                Up       1.1.1.2         4101
```

The following example displays detailed information about the L2VPN cross-connection configured on port `4` of the card installed in slot `1`:

```
[local]Redback>show xc l2vpn 4/1 vpi-vci 1 100 detail

LDP L2VPN Circuit 4/1 vpi-vci 1 100
L2 State         : Up            Peer            : 111.111.111.111
VC ID            : 10000         XC state        : Down
Local Label      : 131075        Access Circuit  : 4/1:1:63/1/2/4098
Remote Label     : 131072        L2VPN Circuit   : 255/12:785:63/0/1/8
EXP bits         : 0             Local Encap     : atm-cell
Remote Group ID  : 0             Remote Encap    :
Local VC Type    : ATM VCC Cell  Remote VC Type  : ATM VCC Cell
Local VC MTU     : 4470          Remote VC MTU   : 0
XC group         : foo           Negotiated cbit  : no
Flags 0x0008014a: delete-sig, in-lblmap, in-ldp, from-cfg :
```

The following table describes the fields in the **show xc l2vpn detail** command.

Table 24 show xc l2vpn detail Command Output

Field	Description
L2 State	Current state of the layer 2 (physical) circuit. Can be Up (active), Standby, or Down (inactive).
VC ID	Identifies the virtual circuit on which this XC is configured.
Local Label	Inner label associated with the local end of an L2VPN cross-connection.
Remote Label	Inner label associated with the remote end of an L2VPN cross-connection.
EXP bits	EXP bits to be used for transport. Range is from 0 through 7.
Remote Group ID	Identifies the link group hosting this XC at the remote end (if the XC is configured under a link group).
Local VC Type	Type of circuit hosting the local end of the XC.
Local VC MTU	MTU on the local end of the XC.
XC group	Identifies the group under which the local end of the XC is configured.
Peer	IP address of the peer hosting the remote end of the XC.
XC state	Indicate whether the XC is active (Up) or inactive (Down).
Access Circuit	Circuit handle internally assigned to the local access circuit on the XC.
L2VPN Circuit	Circuit handle internally assigned to the L2VPN circuit.

Table 24 show xc l2vpn detail Command Output

Field	Description
Local Encap	Type of encapsulation on the local end of the XC. Can be: • Frame Relay over MPLS • Ethernet VLAN (dot1Q) • Ethernet • ATM AAL5 • ATM cell-mode • ATM RFC 1483 routed
Remote Encap	Type of encapsulation on the remote end of the XC. Can be: • Frame Relay over MPLS • Ethernet VLAN (dot1Q) • Ethernet • ATM AAL5 • ATM cell-mode • ATM RFC 1483 routed
Remote VC Type	Type of virtual circuit hosting the remote end of the XC. Can be VLAN, VPI-VCI, or PPPoE.
Remote VC MTU	MTU on the circuit hosting the remote end of the XC.
Negotiated cbit	Indicates whether the control word is present in the pseudowire PDU. The presence of a sequence number indicates that the control word is present in the pseudowire PDU. If the negotiated value is set to yes, then only the control word is present in the PDU that is carried over the pseudowire.
Flags	For internal use: Identify the current running state of the XC.

1.59 show xc summary

```
show xc summary
```

1.59.1 Purpose

Displays summarized information about all XCs configured on the system.

1.59.2 Command Mode

All modes

1.59.3 Syntax Description

This command has no keywords or arguments.

1.59.4 Default

None

1.59.5 Usage Guidelines

Use the **show xc summary** command to display summarized information about all XCs configured on the system.

1.59.6 Examples

The following example displays output from the **show xc summary** command:

```
[local]Redback>show xc summary
    Total Static XCs: 0, Active Static XCs: 0
    Total LDP XCs: 2660, Active LDP XCs: 2660
    Total Bypass Endpoints: 9019, Active Bypass Endpoints: 9019
    Total Bypass XCs: 4505, Active Bypass XCs: 4505
```

The following table describes the fields in the **show xc summary** command output.

Table 25 show xc summary Command Output

Field	Description
Total Static XCs	Total number of static XCs currently configured on this router.
Active Static XCs	Number of static XCs that are currently active on this router.
Total LDP XCs	Total number of LDP XCs currently configured on this router.
Active LDP XCs	Number of LDP XCs that are currently active on this router.
Total Bypass Endpoints	Total number of bypass circuits currently configured on this router.
Active Bypass Endpoints	Number of bypass circuits that are currently active on this router.

Table 25 show xc summary Command Output

Field	Description
Total Bypass XCs	Total number of bypass XCs currently configured on this router.
Active Bypass XCs	Number of bypass XCs that are currently active on this router.

1.60 show xc up

`show xc up` [**`detail`**]

1.60.1 Purpose

Displays information about the active (up) bypass XCs configured on this system.

1.60.2 Command Mode

All modes

1.60.3 Syntax Description

`detail` Displays detailed information about the specified active bypass XC.

1.60.4 Default

None

1.60.5 Usage Guidelines

Use the **`show xc up`** command to display information about the active (up) bypass XCs configured on this system.

Note: The **`show xc up`** command displays information for bypass XCs only; the **`show xc up`** command output does not display information for L2VPN XCs.

1.60.6 Examples

The following example displays output from the **`show xc up`** command:

```
[local]Redback>show xc up

              LDP L2VPN Circuits

L2 Circuit                      L2 State Peer address    VC Id    L-Label  State
lg id 25 vlan-id 58             Up       3.3.3.3         102      131072   Up
lg id 25 vlan-id 54:1           Up       3.3.3.3         103      131073   Up
lg id 25 vlan-id 3501           Up       3.3.3.3         3501     131074   Up
lg id 25 vlan-id 3502           Up       3.3.3.3         3502     131075   Up
lg id 25 vlan-id 3503           Up       3.3.3.3         3503     131076   Up
lg id 25 vlan-id 3504           Up       3.3.3.3         3504     131077   Up
lg id 25 vlan-id 3505           Up       3.3.3.3         3505     131078   Up
lg id 25 vlan-id 3506           Up       3.3.3.3         3506     131079   Up
lg id 25 vlan-id 3507           Up       3.3.3.3         3507     131080   Up
lg id 25 vlan-id 3508           Up       3.3.3.3         3508     131081   Up
lg id 25 vlan-id 3509           Up       3.3.3.3         3509     131082   Up
lg id 25 vlan-id 3510           Up       3.3.3.3         3510     131083   Up
lg id 25 vlan-id 3511           Up       3.3.3.3         3511     131084   Up
lg id 25 vlan-id 3512           Up       3.3.3.3         3512     131085   Up
lg id 25 vlan-id 3513           Up       3.3.3.3         3513     131086   Up
lg id 25 vlan-id 3514           Up       3.3.3.3         3514     131087   Up
lg id 25 vlan-id 3515           Up       3.3.3.3         3515     131088   Up
lg id 25 vlan-id 3516           Up       3.3.3.3         3516     131089   Up
lg id 25 vlan-id 3517           Up       3.3.3.3         3517     131090   Up
lg id 25 vlan-id 3518           Up       3.3.3.3         3518     131091   Up
---(more)---
```

The following table describes the fields in the **show xc up** command output.

Table 26 show xc up Command Output

Field	Description
L2 Circuit	Displays the circuit type and identifier for the physical (Layer 2) circuit hosting the local end of the XC, in the following format: • Link group ID or physical circuit location. The physical circuit is defined in the following format: ***slot*** /***port***[:***chan-num***[:***sub-chan-num***]] • Circuit type and virtual circuit ID. The circuit type can be a VLAN, VPI-VCI, or PPPoE session.
L2 State	Current state of the Layer 2 (physical) circuit. Can be Up (circuit is active) or Down (circuit is inactive).
Peer address	IP address of the peer router.
VC Id	Virtual circuit identifier for the local end of the XC.
L-Label	Local label. Inner label associated with the local end of an L2VPN cross-connection.
State	Current state of the VC. Can be Up (circuit is active) or Down (circuit is inactive).

The following example displays output from the **show xc up detail** command:

```
[local]Redback>show xc up detail

    LDP L2VPN Circuit lg id 25 vlan-id 58

L2 State         : Up               Peer             : 3.3.3.3
VC ID            : 102              XC state         : Up
Local Label      : 131072           Access Circuit   : 255/22:1:26/1/2/6
Remote Label     : 131126           L2VPN Circuit    : 255/12:103:63/0/1/1
EXP bits         : 0                Local Encap      : dot1q tsp
Remote Group ID  : 0                Remote Encap     :
Local VC Type    : VLAN             Remote VC Type   : VLAN
Local VC MTU     : 1500             Remote VC MTU    : 1500
Local VC Status  : forwarding       Remote VC Status : forwarding
XC group         : default          Negotiated cbit  : no
LSP Configured   :                  LSP Used         :
XC profile       :
Flags 0x800819e9: in-rib, in-lblmap, in-ldp, from-ldp, from-cfg
                : peer-up

    LDP L2VPN Circuit lg id 25 vlan-id 54:1

L2 State         : Up               Peer             : 3.3.3.3
VC ID            : 103              XC state         : Up
Local Label      : 131073           Access Circuit   : 255/22:1:26/1/2/15
---(more)---
```

The following table describes the fields in the **`show xc up detail`** command.

Table 27 show xc up detail Command Output

Field	Description
L2 State	Current state of the layer 2 (physical) circuit. Can be Up (active) or Down (inactive).
VC ID	Identifies the virtual circuit on which this XC is configured.
Local Label	Inner label associated with the local end of an L2VPN cross-connection.
Remote Label	Inner label associated with the remote end of an L2VPN cross-connection.
EXP bits	EXP bits to be used for transport. Range is from 0 through 7.
Remote Group ID	Identifies the link group hosting this XC at the remote end (if the XC is configured under a link group).
Local VC Type	Type of circuit hosting the local end of the XC.
Local VC MTU	MTU on the local end of the XC.
Local VC Status	Indicates whether the VC hosting the local end of this XC is actively forwarding traffic or down.
LSP Configured	Name of the LSP mapped to the XC (if the XC is configured on an LSP).
XC profile	Identifies any XC profile that is attached to this XC. The XC profile determines the configuration used by the XC.
XC group	Identifies the group under which the local end of the XC is configured.
Peer	IP address of the peer hosting the remote end of the XC.
XC state	Current state of the XC. Can be Up (active) or Down (inactive).
Access Circuit	Circuit handle internally assigned to the local access circuit on the XC.

Table 27 show xc up detail Command Output

Field	Description
L2VPN Circuit	Circuit handle internally assigned to the L2VPN circuit.
Local Encap	Type of encapsulation on the local end of the XC. Can be: • Frame Relay over MPLS • Ethernet VLAN (dot1Q) • Ethernet • ATM AAL5 • ATM cell-mode • ATM RFC 1483 routed
Remote Encap	Type of encapsulation on the remote end of the XC. Can be: • Frame Relay over MPLS • Ethernet VLAN (dot1Q) • Ethernet • ATM AAL5 • ATM cell-mode • ATM RFC 1483 routed
Remote VC Type	Type of virtual circuit hosting the remote end of the XC. Can be VLAN, VPI-VCI, or PPPoE.
Remote VC MTU	MTU on the circuit hosting the remote end of the XC.
Remote VC Status	Current forwarding status of the VC hosting the remote end of the XC. Can be forwarding traffic (Up) or inactive (Down).
Negotiated cbit	Indicates whether the control word is present in the pseudowire PDU. The presence of a sequence number indicates that the control word is present in the pseudowire PDU. If the negotiated value is set to yes, then only the control word is present in the PDU that is carried over the pseudowire.
LSP Used	Indicates whether the control word is present in the pseudowire PDU. The presence of a sequence number indicates that the control word is present in the pseudowire PDU. If the negotiated value is set to yes, then only the control word is present in the PDU that is carried over the pseudowire.
Flags 0x800819e9:	Identifies the current running state of the XC.