Commands: clear ms through cz

COMMAND DESCRIPTION

Copyright

Disclaimer

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

Trademark List

SmartEdge	is a registered trademark of Telefonaktiebolaget LM Ericsson.
NetOp	is a trademark of Telefonaktiebolaget LM Ericsson.

Contents

1 Command Descriptions

Commands starting with “clear ms” through commands starting with “cz” 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 clear msdp peer

`clear msdp peer` [*`peer-addr`*]

1.1.1 Purpose

Clears the connection to Multicast Source Discovery Protocol (MSDP) peers.

1.1.2 Command Mode

Exec (10)

1.1.3 Syntax Description

`peer-addr`	Optional. IP address of the MSDP peer.

1.1.4 Default

None

1.1.5 Usage Guidelines

Use the **`clear msdp peer`** command to clear the connection to MSDP peers. If the ***`peer-addr`*** argument is specified, only the connection to the specified peer is cleared; otherwise, connections to all peers are cleared.

1.1.6 Examples

The following example shows how to clear the connection to the MSDP peer that has an IP address of **192.168.1.12:**

```
[local]Redback#clear msdp peer 192.168.1.12
```

1.2 clear msdp sa-cache

`clear msdp sa-cache` [*group-addr* [*src-addr*]] [**as** {*asn* | *nn*:*nn*}] [**peer** *peer-addr*]

1.2.1 Purpose

Clears the Multicast Source Discovery Protocol (MSDP) source active (SA) cache entries.

1.2.2 Command Mode

Exec (10)

1.2.3 Syntax Description

group-addr	Optional. IP address of the IGMP group.
src-addr	Optional. IP address of the multicast source that is transmitting to the group. A source does not need to be a member of the group.
as *asn*	Optional. Autonomous system number (ASN), in integer format, from which MSDP SA cache entries have been learned. The range of values is 1 to 65,535. The subrange 64,512 to 65,535 is reserved for private autonomous systems.
as *nn*:*nn*	Optional. ASN, in 4-byte integer format, from which MSDP SA cache entries have been learned. With the 4-byte integer format, the first *nn* indicates the two higher-order bytes, and the second *nn* denotes the two lower-order bytes.
peer *peer-addr*	Optional. Peer IP address from which MSDP SA cache entries have been learned.

1.2.4 Default

None

1.2.5 Usage Guidelines

Use the **`clear msdp sa-cache`** command to clear MSDP SA cache entries. If no options are specified, then all MSDP SA cache entries are cleared.

Use the ***`group-addr`*** argument to clear all MSDP SA cache entries for a specific group.

Use the ***`group-addr`*** and ***`src-addr`*** arguments together to clear MSDP SA cache entries for the specified (S, G) pair.

Use the **`as`** ***`asn`*** or **`as`** ***`nn`*****`:`*****`nn`*** construct to clear MSDP SA cache entries learned from the specified autonomous system.

Use the **`peer`** ***`peer-addr`*** construct to clear MSDP SA cache entries learned from the specified peer address.

1.2.6 Examples

The following example shows how to clear all MSDP SA cache entries for the **224.1.1.1**, **1.1.1.1** (S, G) pair, and all MSDP SA cache entries learned from autonomous system **12**, and the peer address, **10.10.1.37:**

```
[local]Redback#clear msdp sa-cache 224.1.1.1 1.1.1.1 as 12 peer 10.10.20.44
```

1.3 clear msdp statistics

`clear msdp statistics` [***`peer-addr`***]

1.3.1 Purpose

Clears Multicast Source Discovery Protocol (MSDP) peer statistics.

1.3.2 Command Mode

exec (10)

1.3.3 Syntax Description

`peer-addr`	Optional. IP address of the MSDP peer.

1.3.4 Default

None

1.3.5 Usage Guidelines

Use the **`clear msdp statistics`** command to clear MSDP peer statistics (counters).

Use the ***`peer-addr`*** argument to clear the statistics for only the specified MSDP peer.

1.3.6 Examples

The following example shows how to clear all MSDP statistics for the peer address, **192.168.1.6:**

```
[local]Redback#clear msdp statistics 192.168.1.6
```

1.4 clear ospf

`clear ospf` ***`instance-id`*** {**`neighbor`** {***`ip-addr`*** | **`all`** | **`interface`** {***`if-name`*** | ***`ip-addr`***}} | **`redistribution`** | **`routes`** | **`statistics`**} [**`neighbor`** {***`ip-addr`*** | **`interface`** {***`if-name`*** | ***`ip-addr`***}}]

1.4.1 Purpose

Clears Open Shortest Path First (OSPF) neighbor adjacencies, routes redistributed into OSPF, all routes, or statistics.

1.4.2 Command Mode

Exec (10)

1.4.3 Syntax Description

`instance-id`	OSPF instance ID. The range of values is 1 to 65,535. Required only if more than one instance is configured for the context.
`neighbor` ***`ip-addr`***	Neighbor IP address. Resets the connection with the OSPF neighbor at the specified IP address.
`all`	Resets all OSPF neighbor adjacencies.

`interface` ***`if-name`*** — Interface name. Resets the connection associated with the specified neighbor OSPF interface.

`interface` ***`ip-addr`*** — Interface IP address. Resets the connection associated with the specified neighbor OSPF interface. When used as an option, clears statistics associated with the specified OSPF interface.

`redistribution` — Clears routes that have been redistributed into OSPF.

`routes` — Clears all OSPF routes.

`statistics` — Clears OSPF statistics. If no optional keywords are used, clears all OSPF statistics.

1.4.4 Default

None

1.4.5 Usage Guidelines

Use the **`clear ospf`** command to clear neighbor adjacencies, redistributed routes, all routes, or statistics.

1.4.6 Examples

The following example shows how to clear all OSPF routes:

```
[local]Redback#clear ospf routes
```

1.5 clear pim rp

`clear pim rp` [*`rp-addr`*]

1.5.1 Purpose

Clears dynamically learned rendezvous point (RP) mappings in the local database.

1.5.2 Command Mode

Exec (10)

1.5.3 Syntax Description

rp-addr Optional. IP address of the RP.

1.5.4 Default

None

1.5.5 Usage Guidelines

Use the **clear pim rp** command to clear dynamically learned RP mappings in the local database.

Use the *rp-addr* argument to clear the RP mappings for only the specified RP.

Use the **show pim rp mapping** command to display the dynamically learned RP mappings in the local database.

1.5.6 Examples

The following example shows how to clear the RP mappings for the RP address, **192.168.1.32:**

```
[local]Redback#clear pim rp 192.168.1.32
```

1.6 clear pim traffic

clear pim traffic

1.6.1 Purpose

Clears all traffic statistics maintained by Protocol Independent Multicast (PIM).

1.6.2 Command Mode

Exec (10)

1.6.3 Syntax Description

This command has no keywords or arguments.

1.6.4 Default

None

1.6.5 Usage Guidelines

Use the **`clear pim traffic`** command to clear all traffic statistics maintained by PIM.

1.6.6 Examples

The following example shows how to clear all traffic statistics maintained by PIM:

```
[local]Redback#clear pim traffic
```

1.7 clear port counters

For all other traffic cards and all media interface cards (MICs), the syntax is:

`clear port counters` [*`slot/port`*]

1.7.1 Purpose

Clears the counters associated with ports, channels, and subchannels.

1.7.2 Command Mode

Exec (10)

1.7.3 Syntax Description

`slot` Optional. Chassis slot number for the traffic card for which counters are cleared. If omitted, clears port counters for all ports and channels on all cards.

`port` Required if you enter the *`slot`* argument. Port number for which counters are cleared.

1.7.4 Default

All counters associated with the specified port, channel, or subchannel are cleared.

1.7.5 Usage Guidelines

Use the **`clear port counters`** command to clear the counters associated with the specified port, channel, or subchannel.

Note: This command does not clear the corresponding Simple Network Management Protocol (SNMP) counters.

Note: The SmartEdge 100 router limits the value of the *`slot`* argument to 2.

Note:

The value for the *`port`* argument on the SmartEdge 100 router is either of the following:

- For a native port, it is 1 or 2.
- For a MIC port, it depends on the slot in which the ATM OC MIC is installed.

1.7.6 Examples

The following example shows how to clear the counters for Ethernet port **1** on the traffic card in slot **2:**

```
[local]Redback#clear port counters 2/1
```

1.8 clear port counters (ces)

`clear port counters` `[`*`slot/port:ds3-channel:ds1-channel:ds0-channel-group`*`]` **`ces`**

`clear port counters` `[`*`slot/port:ds3-channel:e1/ds1-channel`*`]` **`ces`**

1.8.1 Purpose

Clears the CES port counters on all or selected CESoPSN and SAToP circuits.

1.8.2 Command Mode

All modes.

1.8.3 Syntax Description

slot:port	Slot and port of the circuit.
ds3-channel	Channel of the circuit.
ds1-channel	Sub-channel of a CESoPSN circuit.
e1/ds1-channel	Sub-channel of a SAToP circuit.
ds0-channel-group	Sub-sub-channel group ID of a CESoPSN circuit.

1.8.4 Default

Clears all CES port counters.

1.8.5 Usage Guidelines

Circuit handle is optional which is used to clear port counters on a specific circuit. The clear scope can be slot, port, or channel (DS1 channel or DS0 group channel for CESoPSN; DS1/E1 channel for SAToP).

1.8.6 Examples

The following example shows how to clear port counters on a specific CESoPSN circuit.:

```
[local]Redback(config)#clear port counters  3/2:3:1:1 ces
```

1.9 clear port perf-monitor

For all other traffic cards and all media interface cards (MICs), the syntax is:

```
clear port perf-monitor [slot/port]
```

1.9.1 Purpose

Clears all performance-monitoring (PM) statistics for one or more ports, channels, or subchannels.

1.9.2 Command Mode

Exec (10)

1.9.3 Syntax Description

slot Optional. Chassis slot number of a traffic card for which PM statistics are cleared. If omitted, clears PM data for all ports and channels on all cards for which PM statistics are supported.

port Required if you enter the *slot* argument. Port number for which PM statistics are cleared.

1.9.4 Default

Clears PM statistics for all ports, channels, and subchannels that support PM statistics.

1.9.5 Usage Guidelines

Use the **clear port perf-monitor** command to clear PM statistics for one or more ports, channels, or subchannels. Use the optional arguments to clear PM statistics for a specific port, channel, or subchannel.

Note: The SmartEdge 100 router limits the value of the *slot* argument to 2.

Note: The value for the *port* argument on the SmartEdge 100 router depends on the MIC slot in which the ATM OC MIC is installed.

1.10 clear ppp counters

clear ppp counters [**all-contexts** | **context**]

1.10.1 Purpose

Clears counters for Point-to-Point Protocol (PPP) negotiation packet-in and packet-out and session-up and session-down counters.

1.10.2 Command Mode

Exec (10)

1.10.3 Syntax Description

all-contexts Optional. Clears context-specific PPP counters for all contexts. This keyword is available only for administrators authenticated to the local context.

context Optional. Clears context-specific PPP counters for the current context.

1.10.4 Default

None

1.10.5 Usage Guidelines

Use the **clear ppp counters** command to clear counters for PPP negotiation packet-in and packet-out and session-up and session-down counters.

1.10.6 Examples

The following example shows how to clear global PPP counters:

```
[local]Redback#clear ppp counters
```

The following example shows how to clear context-specific PPP counters for all contexts:

```
[local]Redback#clear ppp counters all-contexts
```

1.11 clear pppoe counters

clear pppoe counters

1.11.1 Purpose

Clears counters for Point-to-Point Protocol over Ethernet (PPPoE) negotiation packet-in and out and session-up and down counters.

1.11.2 Command Mode

Exec (10)

1.11.3 Syntax Description

This command has no keywords or arguments.

1.11.4 Default

None

1.11.5 Usage Guidelines

Use the **clear pppoe counters** command to clear counters for PPPoE negotiation packet-in and -out and session-up and -down counters.

1.11.6 Examples

The following example shows how to clear counters for PPPoE-encapsulated circuits:

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

1.12 clear radius counters

clear radius counters

clear radius counters route_download_server ***server-address server-port***

1.12.1 Purpose

Clears counters for Remote Authentication Dial-In User Service (RADIUS) access and accounting messages. It also clears counters for the route download server identified by the specified IP address and port.

1.12.2 Command Mode

Exec (10)

1.12.3 Syntax Description

server-address	The IP address or hostname of the route download server.
server-port	The UDP port being used by the server. The range is 1024 to 65535.

1.12.4 Default

None

1.12.5 Usage Guidelines

Use the **`clear radius counters`** command to clear counters for RADIUS access and accounting messages.

1.12.6 Examples

The following example shows how to clear RADIUS counters for RADIUS access and accounting messages:

```
[local]Redback>clear radius counters
```

1.13 clear route-map

`clear route-map` ***`map-name`*** **`counters`**

1.13.1 Purpose

Clears match and cache hit counts for a specified route map.

1.13.2 Command Mode

Exec (10)

1.13.3 Syntax Description

`map-name`	Route map name.
`counters`	Clears match and cache hit counts for a specified route map.

1.13.4 Default

None

1.13.5 Usage Guidelines

Use the **`clear route-map`** command to clear match and cache hit counts for a specified route map.

1.13.6 Examples

The following example shows how to clear match and cache hit counts for the **rmap1** route map:

```
[local]Redback#clear route-map rmap1
```

1.14 clear rsvp counters

clear rsvp counters [**all** | **general** | **packets**]

1.14.1 Purpose

Clears Resource Reservation Protocol (RSVP) counter information.

1.14.2 Command Mode

- Exec

1.14.3 Syntax Description

`all`	Optional. Clears all RSVP-related counters.
`general`	Optional. Clears only general RSVP-related counters.
`packets`	Optional. Clears only RSVP packet-related counters.

1.14.4 Default

Clears all RSVP counter information.

1.14.5 Usage Guidelines

Use the `clear rsvp counters` command to clear RSVP counter information.

1.14.6 Examples

The following example shows how to clear all RSVP-related counters:

```
[local]Redback>clear rsvp counters all
```

1.15 clear spanning-tree

clear spanning-tree ***bridge-name*** **counters**

1.15.1 Purpose

Clears the spanning-tree counters for the bridge instance.

1.15.2 Command Mode

Exec

1.15.3 Syntax Description

bridge-name **counters**	Specifies the name of the bridge.

1.15.4 Default

None

1.15.5 Usage Guidelines

Use the **clear spanning-tree** command to clear the spanning-tree counters for the bridge instance; that is, use the command to clear the spanning-tree counters that apply to the whole SmartEdge bridge.

1.15.6 Examples

The following example shows how to clear all spanning-tree counters in the **brdgrp1 bridge:**

```
[local]Redback#clear spanning-tree brdgrp1 counters
```

1.16 clear spanning-tree circuit

clear spanning-tree ***bridge-name*** **circuit** ***circuit-id*** **counters**

1.16.1 Purpose

Clears the spanning-tree counters for the specified circuits on the bridge.

1.16.2 Command Mode

Exec

1.16.3 Syntax Description

bridge-name Name of the bridge.

circuit *circuit-id* Specifies a circuit on the bridge. See Table 1 for the expanded syntax for the *circuit-id* argument.

1.16.4 Default

None

1.16.5 Usage Guidelines

Use the **clear spanning-tree** command to clear the spanning-tree counters for the specified 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 1 describes the components of the **circuit-id** argument:

Table 1 Building Blocks of the circuit-id Argument

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

1.16.6 Examples

The following example shows how to clear all counters specific to the circuits in the Ethernet port `2/1` in the `brdgrp1` bridge:

```
[local]Redback#clear spanning-tree brdgrp1 circuit 2/1 ethernet counters
```

1.17 clear sse group counters

`clear sse group counters` ***`group_name`***

1.17.1 Command Mode

Exec

1.17.2 Syntax Description

`group_name`	Name of the SSE group.

1.17.3 Default

None

1.17.4 Usage Guidelines

Clears counters on the specified SSE group. Any subsequent execution of the **`show sse {group | partition} counters [`*`group_name`*` [`*`partition_name`*`]]`** command shows only the statistics since the counters were last cleared with the **`clear sse group counters`** ***`group_name`***command.

The command does not persist for the following events:

- SSE group switchover
- XCRP switchover
- Card reload
- System reload
- Disk removal or insertion

1.17.5 Examples

```
[local]Redback#clear sse group counters sse_group_1
```

1.18 clear subscriber

To clear one or more subscriber sessions:

```
clear subscriber {agent-remote-id id | encapsulation sessions
| {session slot/port[:chan-num[:sub-chan-num]] [circuit-id]} |
{session l2tp lns id} | username subscriber}
```

To reauthenticate one or more subscriber clientless IP service selection (CLIPS) sessions:

```
clear subscriber {{session slot/port[:chan-num[:sub-chan-num]]
[circuit-id]} | username subscriber}} clips-bounce
```

1.18.1 Purpose

Clears or reauthenticates one or more subscriber sessions.

1.18.2 Command Mode

Exec

1.18.3 Syntax Description

`agent-remote-id` *`id`*
The subscriber session to be cleared, where the *`id`* argument is the value of the agent remote ID in a subscriber record. Enter the *`id`* argument as a structured subscriber username in the form subscriber@context

`encapsulation` *`sessions`*
The Point-to-Point Protocol (PPP) or PPP over Ethernet (PPPoE) subscriber sessions to be cleared. This construct is available only for 802.1Q and Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs). For the possible values of the *`sessions`* argument, see Table 2.

`session`
Limits the output to the specified session or circuit.

`slot`
Chassis slot number for a traffic card. This keyword is required to clear subscriber information in this slot.

`port`
Port number on the specified traffic card. This keyword is required to clear subscriber information in this slot.

`circuit-id`
Optional. A subscriber session identifier, or a subscriber username that filters which subscriber information this command displays. See Table 3 for information about the *`circuit-id`* argument.

`l2tp lns id`
Limits the output to the Layer 2 Tunneling Protocol (L2TP) network server (LNS) circuit specified by the *`id`* argument.

username ***subscriber*** Optional. Limits the output to the subscriber specified by name. Enter the ***subscriber*** argument as a structured subscriber username in the form subscriber@context.

clips-bounce Optional. Reauthenticates CLIPS sessions.

1.18.4 Default

None

1.18.5 Usage Guidelines

Use the **clear subscriber** command to clear or reauthenticate one or more subscriber sessions. When restarted, terminated subscriber sessions restart with new parameters.

The **encapsulation** ***sessions*** construct specifies the PPP or PPPoE subscriber sessions to be cleared; see Table 2. This construct is available only for 802.1Q and ATM PVCs.

Table 2 Values for the sessions Argument

Construct	Description
ppp all	Clears all PPP subscriber sessions in the current context.
ppp all-context	Clears all PPP subscriber sessions in all contexts. This option is available only in the local context.
pppoe all	Clears all PPPoE subscriber sessions in the current context.
pppoe all-context	Clears all PPPoE subscriber sessions in all contexts. This option is available only in the local context.
ppp pppoe all	Clears all PPP and PPPoE subscriber sessions in the current context.
ppp pppoe all-context	Clears all PPP and PPPoE subscriber sessions in all contexts. This option is available only in the local context.

The ***circuit-id*** argument represents the following keywords and arguments identified in Table 3. All circuit-IDs relevant to the subscriber session must be included to effectively clear the subscriber:

{**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 3 Building Blocks of the circuit-id Argument

Construct	Description
clips ***clips-session***	A filter that limits the output 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 output 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 output 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 output 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.

When the command clears a PPP or PPPoE session, the session terminates and logs off the subscriber. It then attempts to renegotiate and reauthenticate a new session with the remote peer on that circuit. For a session on a RFC 1483 bridge-encapsulated circuit, the command brings down and brings back up the circuit, and attempts to reauthenticate the subscriber.

For information about the format of a structured username, see *Configuring Authentication, Authorization, and Accounting*.

1.18.6 Examples

The following example shows how to clear the subscriber, `dave@isp1:`

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

The following example shows how to clear a subscriber on slot 1 and port 1 with a VLAN tag value of 2 on PPPoE session 7:

```
[[local]Redback>clear subscriber session 1/1 vlan-id 2 pppoe 7
```

1.19 clear subscriber encapsulation mobile-ip

clear subscriber encapsulation mobile-ip {**all** | **all-context**}

1.19.1 Purpose

Clears all Mobile IP subscribers in the current context or all contexts.

1.19.2 Command Mode

Exec (10)

1.19.3 Syntax Description

`all`	Clears all Mobile IP subscribers in the current context.
`all-context`	Clears all Mobile IP subscribers in all contexts.

1.19.4 Default

None

1.19.5 Usage Guidelines

Use the **clear subscriber encapsulation mobile-ip** command to clear all Mobile IP subscribers in the current context or all contexts.

1.19.6 Examples

The following example shows how to clear all Mobile IP subscribers in all contexts:

```
[local]Redback#clear subscriber encapsulation mobile-ip all-context
```

1.20 clear system nvlog

clear system nvlog

1.20.1 Purpose

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

1.20.2 Command Mode

Exec (10)

1.20.3 Syntax Description

This command has no keywords or arguments.

1.20.4 Default

None

1.20.5 Usage Guidelines

Use the **clear system nvlog** to clear the contents of NVRAM on the controller card to which you are connected. The NVRAM stores logs of trap- and panic-related messages from the operating system and can be used to help debug system crashes in the absence of a local console (connected to the Craft 2 port).

1.20.6 Examples

The following example shows how to clear the contents of the NVRAM on the active controller card:

```
[local]Redback#clear system nvlog
```

The following example shows how to clear the contents of the NVRAM on the standby controller card; in this example, the administrator is connected to the Craft 2 port on the standby controller card:

```
[local]standby>clear system nvlog
```

1.21 clear vpls

clear vpls {*bridge-name* {**all** | **peer** *ip-addr* [**pw-id** *pw-num* | **pw-name** *pw-name*]} | **profile** *prof-name* {**all** | **peer** *ip-addr*}}

1.21.1 Purpose

Resets Virtual Private LAN Services (VPLS) peer connections on a specified VPLS bridge or profile.

1.21.2 Command Mode

Exec (10)

1.21.3 Syntax Description

bridge-name	VPLS-enabled bridge name. Resets connections for all VPLS peers on the specified bridge instance.
all	Resets all VPLS peer connections.
peer *ip-addr*	Neighbor IP address, in the form *A.B.C.D*, for the VPLS peer. Resets the connection for the specified VPLS peer.
pw-id *pw-num*	Optional. Pseudowire number. Resets connections for the VPLS peers that use the specified pseudowire number.
pw-name *pw-name*	Optional. Pseudowire name. Resets connections for the VPLS peers that use the specified pseudowire name.
profile *prof-name*	Name of the VPLS profile. Resets connections for all VPLS peers in the specified profile.

1.21.4 Default

None

1.21.5 Usage Guidelines

Use the **clear vpls** command to reset VPLS peer connections on a specified VPLS bridge or profile. When a peer connection is reset, the peer instance is brought to the `admin down` state before it is re-enabled. This operation tears down the pseudowires, the circuits are marked down, Label Forwarding

Information Base (LFIB) entries are removed, and the medium access control (MAC) addresses learned over the pseudowires are discarded.

1.21.6 Examples

The following example shows how to reset the connection to the VPLS peer with the IP address, **192.168.1.37**, on the VPLS bridge, **bridge-12:**

```
[local]Redback#clear vpls bridge-12 peer 192.168.1.37
```

The following example shows how to resets the connections to all VPLS peers in the VPLS profile, **prof12:**

```
[local]Redback#clear vpls profile prof12 all
```

1.22 clear vpls counters

clear vpls {*bridge-name* {**all** | **peer** *ip-addr* [**pw-id** *pw-num* | **pw-name** *pw-name*]} | **profile** *prof-name* {**all** | **peer** *ip-addr*}} **counters**

1.22.1 Purpose

Resets the counters for the Virtual Private LAN Services (VPLS) peers on a specified VPLS bridge or profile.

1.22.2 Command Mode

Exec (10)

1.22.3 Syntax Description

bridge-name	VPLS-enabled bridge instance name. Resets the counters for all VPLS peers on the specified bridge instance.
all	Resets all VPLS peer counters.
peer *ip-addr*	Neighbor IP address, in the form *A.B.C.D*, for the VPLS peer. Resets the counters for the specified VPLS peer.
pw-id *pw-num*	Optional. Pseudowire number. Resets the counters for the VPLS peers that use the specified pseudowire number.

pw-name *pw-name* Optional. Pseudowire name. Resets counters for the VPLS peers that use the specified pseudowire name.

profile *prof-name* Name of the VPLS profile. Resets the counters for all VPLS peers in the specified profile.

1.22.4 Default

None

1.22.5 Usage Guidelines

Use the **clear vpls counters** command to reset the counters for the VPLS peers on a specified VPLS bridge or profile.

Note: This command does not reset the VPLS circuit counters associated with the peer. To clear the VPLS circuit counters, use the **clear circuit counters vpls** (in any mode).

1.22.6 Examples

The following example shows how to reset the VPLS counters for the VPLS peer with the neighbor IP address, **192.168.1.37**, on the VPLS bridge, **bridge-12:**

```
[local]Redback#clear vpls bridge-12 peer 192.168.1.37 counters
```

The following example shows how to reset all VPLS counters for all VPLS peers in the VPLS profile, **prof12:**

```
[local]Redback#clear vpls profile prof12 all counters
```

1.23 clear vpls disable

clear vpls {*bridge-name* {**all** | **peer** *ip-addr* [**pw-id** *pw-num* | **pw-name** *pw-name*]} | **profile** *prof-name* {**all** | **peer** *ip-addr*}} **disable**

1.23.1 Purpose

Sets the administrative state to `admin down` for Virtual Private LAN Services (VPLS) peer connections on a specified VPLS bridge or profile, instead of resetting the peer connections.

1.23.2 Command Mode

Exec (10)

1.23.3 Syntax Description

bridge-name — VPLS-enabled bridge instance name. Sets the administrative state to `admin down` for all VPLS peers on the specified bridge instance.

all — Sets the administrative state to `admin down` for all VPLS peers.

peer ***ip-addr*** — Neighbor IP address, in the form ***A.B.C.D***, for the VPLS peer. Sets the administrative state to `admin down` for the specified VPLS peer.

pw-id ***pw-num*** — Optional. Pseudowire number. Sets the administrative state to `admin down` for the VPLS peers that use the specified pseudowire number.

pw-name ***pw-name*** — Optional. Pseudowire name. Sets the administrative state to `admin down` for the VPLS peers that use the specified pseudowire name.

profile ***prof-name*** — Name of the VPLS profile. Sets the administrative state to `admin down` for all VPLS peers on the specified profile.

1.23.4 Default

None

1.23.5 Usage Guidelines

Use the **clear vpls disable** command to set the administrative state to `admin down` for VPLS peer connections on a specified VPLS bridge or profile, instead of resetting the peer connections.

Use the **clear vpls** command to re-enable the peer connections.

1.23.6 Examples

The following example shows how to set the administrative state to `admin down` for the VPLS peer with the IP address, **192.168.1.37**, on the VPLS bridge, **bridge-12:**

```
[local]Redback#clear vpls bridge-12 peer 192.168.1.37 disable
```

The following example shows how to set the administrative state to `admin down` for all VPLS peers in the VPLS profile, **prof12:**

```
[local]Redback#clear vpls profile prof12 all disable
```

1.24 clear vpls mac-flush

clear vpls {*bridge-name* {**all** | **peer** *ip-addr* [**pw-id** *pw-num* | **pw-name** *pw-name*]} | **profile** *prof-name* {**all** | **peer** *ip-addr*}} **mac-flush**

1.24.1 Purpose

Resets Virtual Private LAN Services (VPLS) peers by sending a medium access control (MAC) flush type-length-value (TLV) over the pseudowires of VPLS peers on the specified VPLS bridge or profile to remove the MAC entries.

1.24.2 Command Mode

Exec (10)

1.24.3 Syntax Description

bridge-name	VPLS-enabled bridge instance name. Sends a MAC flush TLV over the pseudowires of all VPLS peers on the specified bridge instance.
all	Sends a MAC flush TLV over the pseudowires of all VPLS peer connections.
peer *ip-addr*	Neighbor IP address, in the form *A.B.C.D*, for the VPLS peer. Sends a MAC flush TLV over the pseudowire of the specified VPLS peer.
pw-id *pw-num*	Optional. Pseudowire number. Sends a MAC flush TLV over the pseudowires of the VPLS peers that use the specified pseudowire number.
pw-name *pw-name*	Optional. Pseudowire name. Sends a MAC flush TLV over the pseudowires of the VPLS peers that use the specified pseudowire name.
profile *prof-name*	Name of the VPLS profile. Sends a MAC flush TLV over the pseudowires of all VPLS peers in the specified profile.

1.24.4 Default

None

1.24.5 Usage Guidelines

Use the **clear vpls mac-flush** command to reset VPLS peers by sending a MAC flush TLV over the pseudowires of VPLS peers on the specified VPLS bridge or profile to remove the MAC entries. When the MAC flush TLV is received, the receiving device deletes the MAC entries identified within the MAC flush TLV.

1.24.6 Examples

The following example shows how to send a MAC flush TLV over the pseudowire of the VPLS peer with the IP address, **192.168.1.37**, on the VPLS bridge, **bridge-12:**

```
[local]Redback#clear vpls bridge-12 peer 192.168.1.37 mac-flush
```

The following example shows how to send a MAC flush TLV over the pseudowires of all VPLS peers in the VPLS profile, **prof12:**

```
[local]Redback#clear vpls profile prof12 all mac-flush
```

1.25 clear vpls restart

clear vpls {*bridge-name* {**all** | **peer** *ip-addr* [**pw-id** *pw-num* | **pw-name** *pw-name*]} | **profile** *prof-name* {**all** | **peer** *ip-addr*}} **restart**

1.25.1 Purpose

Restarts Virtual Private LAN Services (VPLS) peer connections for the specified VPLS bridge or profile.

1.25.2 Command Mode

Exec (10)

1.25.3 Syntax Description

bridge-name VPLS-enabled bridge instance name. Restarts the connections for all VPLS peers in the specified bridge instance.

all Restarts all VPLS peer connections.

peer *ip-addr* — Neighbor IP address, in the form *A.B.C.D*, for the VPLS peer. Restarts the connection for the specified VPLS peer.

pw-id *pw-num* — Optional. Pseudowire number. Restarts the connections for the VPLS peers that use the specified pseudowire number.

pw-name *pw-name* — Optional. Pseudowire name. Restarts the connections for the VPLS peers that use the specified pseudowire name.

profile *prof-name* — Name of the VPLS profile. Restarts the connections for all VPLS peers in the specified profile.

1.25.4 Default

None

1.25.5 Usage Guidelines

Use the **clear vpls restart** command to restart VPLS peer connections for the specified VPLS bridge or profile. When a peer connection is restarted, the peer is shut down and reinitialized. The VPLS circuit assigned to the peer may change when the peer connection is restarted.

1.25.6 Examples

The following example shows how to restart the peer connection for the VPLS peer with the IP address, **192.168.1.37**, on the VPLS bridge, **bridge-12:**

```
[local]Redback#clear vpls bridge-12 peer 192.168.1.37 restart
```

The following example shows how to restart the peer connections for all VPLS peers in the VPLS profile, **prof12:**

```
[local]Redback#clear vpls profile prof12 restart
```

1.26 clear vrrp statistics

clear vrrp statistics {**all** | **global** | **interface** [*if-name* [*vrrp-id*]]}

1.26.1 Purpose

Clears Virtual Router Redundancy Protocol (VRRP) statistics.

1.26.2 Command Mode

Exec (10)

1.26.3 Syntax Description

`all`	Clears all VRRP statistics.
`global`	Clears global VRRP statistics.
`interface`	Clears VRRP statistics for all interfaces.
`if-name`	Optional. Interface name. Clears VRRP statistics for the specified interface.
`vrrp-id`	Optional. virtual router ID. Used only with the optional ***`if-name`*** argument. The range of values is 1 to 255.

1.26.4 Default

None

1.26.5 Usage Guidelines

Use the **`clear vrrp statistics`** command to clear VRRP statistics.

1.26.6 Examples

The following example shows how to clear all VRRP statistics from the routing table:

```
[local]Redback#clear vrrp statistics all
```

1.27 client-to-client reflection

`client-to-client reflection`

`no client-to-client reflection`

1.27.1 Purpose

Enables route reflection between clients of a Border Gateway Protocol (BGP) route reflector.

1.27.2 Command Mode

BGP router configuration

1.27.3 Syntax Description

This command has no keywords or arguments.

1.27.4 Default

Routes are reflected from one client to other clients.

1.27.5 Usage Guidelines

Use the **`client-to-client reflection`** command to enable route reflection between clients of a BGP route reflector.

By default, routes are reflected between clients of a route reflector. Under certain circumstances, a network administrator may not want routes that have been learned from one client to be reflected to other clients. One example is the case where clients are fully meshed. In this case, use the **`no client-to-client reflection`** command to disable route reflection.

Use the **`no`** form of this command to disable client-to-client reflection.

1.27.6 Examples

The following example shows how to configure the router as a unicast route reflector for neighbors, **102.210.210.1** and **122.101.12.145**, and disable client-to-client reflection:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#no client-to-client reflection
[local]Redback(config-bgp)#neighbor 102.210.210.1 internal
[local]Redback(config-bgp-neighbor)#address-family ipv4 unicast
[local]Redback(config-bgp-peer-af)#route-reflector-client
[local]Redback(config-bgp-peer-af)#exit
[local]Redback(config-bgp-neighbor)#exit
[local]Redback(config-bgp)#neighbor 122.101.12.145 internal
[local]Redback(config-bgp-neighbor)#address-family ipv4 unicast
[local]Redback(config-bgp-peer-af)#route-reflector-client
```

1.28 clips-group

`clips-group` ***`group-name`*** **`dhcp`** [**`maximum`** ***`max-num`***] [**`context`** ***`ctx-name`***]

`no clips-group` ***`group-name`***

1.28.1 Purpose

Creates an empty group to which you can assign redundant ports and permanent virtual circuits (PVCs) on which will be created dynamic clientless IP service selection (CLIPS) circuits.

1.28.2 Command Mode

Global configuration

1.28.3 Syntax Description

`group-name`	Name for a group of ports and PVCs on which dynamic CLIPS circuits will be created.
`dhcp`	Specifies that the Dynamic Host Configuration Protocol (DHCP) will be used for a group of ports and PVCs on which dynamic CLIPS circuits will be created.
`maximum` ***`max-num`***	Optional. Maximum number of CLIPS sessions allowed on this group. The range of values is 1 to 16,000; the default value is 16,000.
`context` ***`ctx-name`***	Optional. Name of the context in which the subscriber is authenticated.

1.28.4 Default

No CLIPS groups are created.

1.28.5 Usage Guidelines

Use the **`clips-group`** command to create an empty group to which you can assign redundant ports and PVCs on which will be created dynamic CLIPS circuits. CLIPS groups are available only for Ethernet and Gigabit Ethernet ports and the 802.1Q PVCs configured on them.

Note: The SmartEdge router associates the CLIPS group with the slot of the first port or PVC that you assign to the group. To change the slot, you must delete the group, recreate it, and then assign to it as the first member, a port or PVC that you have configured on the card in the new slot.

Use the **no** form of this command to delete the CLIPS group.

1.28.6 Examples

The following example shows how to create the **dynamic-clips** group for the **dhcp** context:

```
[local]Redback(config)#clips-group dynamic-clips dhcp context dhcp
```

1.29 clips pvc

clips pvc ***start-ses-num*** [**through** ***end-ses-num***]

no clips pvc ***start-ses-num*** [**through** ***end-ses-num***]

1.29.1 Purpose

Creates a static circuit or a range of clientless IP service selection (CLIPS) static circuits on an Ethernet port, a static 802.1Q permanent virtual circuit (PVC) on an Ethernet port, or an Asynchronous Transfer Mode (ATM) PVC, and enters CLIPS PVC configuration mode.

1.29.2 Command Mode

- ATM PVC configuration
- dot1q PVC configuration
- link group configuration
- link PVC configuration
- port configuration

1.29.3 Syntax Description

start-ses-num	Numeric session ID or first numeric session ID in a range of IDs for the static circuits being created; the range of values is 1 to 131,072.
through ***end-ses-num***	Optional. Final numeric session ID in a range of IDs for the static circuits being created; the range of values is 2 to 131,072.

1.29.4 Default

No static circuits are created.

1.29.5 Usage Guidelines

Use the **clips pvc** command to create a static circuit or a range of static circuits on an Ethernet port, an 802.1Q PVC on an Ethernet port, or an ATM PVC, and enter CLIPS PVC configuration mode.

You must first enter the **service clips** command in ATM PVC, dot1q PVC, link group, link PVC, or port configuration mode for this command to be available.

You must have encapsulated the ATM PVC with RFC 1483 bridged encapsulation (**bridge1483** keyword) for this command to be available in ATM PVC configuration mode.

You cannot create static CLIPS PVCs on on-demand ATM or 802.1Q PVCs.

You can specify any type of encapsulation for an 802.1Q PVC or Ethernet port, but if you encapsulate the PVC using the **multi** keyword, you cannot create a CLIPS PVC on a child circuit on the PVC.

If you create a range of static circuits, the session ID for each circuit is appended to the ***prefix1*** argument in the **bind auto-subscriber** command (in CLIPS PVC configuration mode).

You can create up to 8,000 static circuits on an Ethernet port, an 802.1Q PVC on an Ethernet port, or an ATM PVC.

Use the **no** form of this command to delete an existing static circuit or range of static circuits.

1.29.6 Examples

The following example shows how to create 10 circuits with session numbers **1** to **10** on port **1** of an Ethernet traffic card in slot **4:**

```
[local]Redback(config)#port ether 4/1

[local]Redback(config-port)#service clips

[local]Redback(config-port)#clips pvc 1 through 10

[local]Redback(config-clips-pvc)#
```

1.30 clock set

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

1.30.1 Purpose

Sets the time of day and calendar date of both the system clock and the real-time clock.

1.30.2 Command Mode

Exec (10)

1.30.3 Syntax Description

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

1.30.4 Default

None

1.30.5 Usage Guidelines

Use the **clock set** command in exec mode to set the time of day and calendar date of the time-of-day clock and, if present on the installed controller cards, the real-time clock (RTC). The time-of-day clock for a SmartEdge router is implemented in software. When a system with an XCRP4 ControllerSMRP2 Controller card is powered on, the RTC sets the time-of-day clock; otherwise, the time-of-day clock is undefined until it is configured and set using the operating system. The time-of-day clock can be maintained by synchronization with a Network Time Protocol (NTP) server. Periodically, the operating system updates the RTC based on the current value of the time-of-day clock.

To configure the system clock, which is different from the time-of-day clock and RTC, enter the **system clock-source**, **system clock-source external**, or **system clock-source timing-type** command in global configuration mode. To configure the time-of-day clock, enter the **clock set**, **system clock summer-time**, or **system clock timezone** command (in global configuration mode). The system clock performs system hardware timing functions.

Note: The setting of the time-of-day clock is not preserved across system reloads unless the controller card has an RTC. On system reload, the time-of-day clock is initialized with the current setting of the RTC.

1.30.6 Examples

The following example shows how to set the clock to **12:01** p.m. on **Jun 28, 2005:**

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

1.31 clock-source (ces)

clock-source {loop | card-reference | ces-domain *domain-group-id.domain-id*

1.31.1 Purpose

Configures the clock source settings of a CESoPSN or SAToP circuit.

1.31.2 Command Mode

Global Config Mode.

1.31.3 Syntax Description

loop	Use loop timing.
card-reference	Use the reference clock on the card
ces-domain	Use one of the card's CES timing domains. The channel's RX recovered clock is conditioned by the card timing domain.
domain-group-id	Timing domain group for **ces-domain**, "1" for ports 1-4; "2" for ports 5-8.
domain-id	ID of the timing domain within the group. The range is from 1 to 8.

1.31.4 Default

None.

1.31.5 Usage Guidelines

CESoPSN: The **ces-domain** option configures the DS1 / E1 and all DS0 groups within the DS1 / E1 for adaptive clock recovery.

SAToP: The **ces-domain** option configures the DS1 / E1 for adaptive clock recovery.

If the configured ***domain-group-id*** does not apply to the DS1/E1 channel's SONET port, then the action is rejected, and the following message is displayed: "`Port / ces timing domain mismatch`"

The timing domain for SAToP and CESoPSN are independent of each other. The user should make sure the timing domains configured for each are independent. The system will reject a clock-source if a timing domain already configured for CESoPSN is entered by the user for SAToP (or vice versa).

CESoPSN: Do not mix E1 and T1 channels within the same clock domain

1.31.6 Examples

The following example shows how to configure the clock source on a CESoPSN circuit:

```
[local]Redback(config)#port channelized-ds1 2/1:1:3
[local]Redback(config-ces-chan-dsl)#clock-source ces-domain 1.3
```

The following example shows how to configure the clock source on a SAToP E1 circuit:

```
[local]Redback(config)#port channelized-e1 2/1:3
[local]Redback(config-ces-chan-el)#clock-source ces-domain 1.4
```

1.32 clock-source (E/T-carrier)

`clock-source {global-reference | loop}`

1.32.1 Purpose

Specifies the source for the transmit clock for a clear-channel DS-3 channel or port, clear-channel E3 port, DS-1 channel, or for an E1 channel or port.

1.32.2 Command Mode

- DS-1 configuration
- DS-3 configuration
- E1 configuration
- E3 configuration

1.32.3 Syntax Description

`global-reference` Specifies the system clock on the active controller card as the clock source.

`loop` Specifies the receive clock derived from the incoming signal on the channel as the clock source.

1.32.4 Default

The source for the transmit clock is the source of the system clock on the active controller card.

1.32.5 Usage Guidelines

Use the **clock-source** (E/T-carrier) command to specify the source for the transmit clock for a clear-channel DS-3 channel or port, clear-channel E3 port, DS-1 channel, or E1 channel or port.

Use the **global-reference** keyword to specify the system clock on the active controller card. Use the **loop** keyword to select the receive clock from the incoming signal on the channel as the source.

You can specify a different clock source for each clear-channel DS-3 channel and each DS-1 channel on a channelized OC-12 port.

You can specify a different clock source for each clear-channel E1 channel on a channelized STM-1 port.

You can specify a different clock source for each E3 port on a clear-channel E3 traffic card.

Use the **show port detail** command (in any mode) to display the status of the clock source.

Note: The clock source for the channelized OC-12 port is always derived from the system clock on the active controller card, the source you specify by entering the **system clock-source** command (in global configuration mode).

Note: If you specify a range of DS-0 time slots other than the default range (1–24) with the **timeslot** command (in DS-1 configuration mode), you cannot specify the **loop** keyword as the clock source for a DS-1 channel. If you attempt to specify the **loop** keyword with fewer time slots than the full range defined, an error message displays.

Use the **default** form of this command to set the clock source to the default.

1.32.6 Examples

The following example shows how to select the derived receive clock for the DS-3 port as the source for the transmit clock:

```
[local]Redback(config)#port ds3 3/1

[local]Redback(config-ds3)#clock-source loop
```

1.33 clock-source (port)

`clock-source` {`card-reference` | `local` | `loop`}

1.33.1 Purpose

Specifies the transmit clock source for the port.

1.33.2 Command Mode

- ATM OC configuration
- port configuration

1.33.3 Syntax Description

`card-reference`
Specifies the clock source for the port is the reference clock configured for the card in the **`clock-source (card configuration mode)`** command. This clock source is the default for third-generation ATM OC ports.

This keyword is not supported by ATM OC MIC ports.

`local`
Specifies the onboard clock as the clock source. This clock source is the default for 10GE and OC-192c/STM-64c ports in port configuration mode and for ATM OC MIC and second-generation ATM OC-3c/STM1c ports in ATM OC configuration mode.

The `local` option does not apply to the *Channelized OC-3/STM-1 or OC-12/STM-4* line card.

`loop`
Specifies the receive clock derived from the incoming signal on the port as the transmit clock source.

1.33.4 Default

For ATM OC ports, the transmit clock source is the clock source specified for the SmartEdge 400 or SmartEdge 800 traffic card. For 10GE and OC-192c/STM-64c ports and ATM OC MIC ports, the transmit clock source is the onboard clock.

1.33.5 Usage Guidelines

Use the **`clock-source`** (port) command to specify the transmit clock source for second- or third-generation ATM OC, or 10GE, or OC-192c/STM-64c port.

Note: Changes to the clock source setting will not cause LOF on the 8-port ATM OC-3c/STM-1c (atm-oc3e-8-port) and 2-port ATM OC-12c/STM-4c cards.

Caution!

Risk of data loss. If you specify the onboard clock on the SmartEdge 400 or SmartEdge 800 active controller card as the clock source for the ATM traffic card by using the **`clock-source`** command with the **`global-reference`** keyword (in card configuration mode), there might be a brief traffic interruption might occur on all ports on the card if the active controller card is removed from the system. To reduce the risk, specify the derived received clock on the ATM traffic card as the clock source (by using the **`clock-source`** command with the **`local`** keyword) for a second- or third-generation ATM OC traffic card. This warning does not apply to the 8-port ATM OC-3c/STM-1c (atm-oc3e-8-port) and 2-port ATM OC-12c/STM-4c cards.

The clock source choice for second- or third-generation ATM OC traffic cards allows its ports to function without packet loss during a switchover to the standby controller card when the active controller card is removed from the SmartEdge chassis. If the clock source for the traffic card is the system clock on the active controller card, packets can be lost during the brief interval of the switchover. For this reason, we highly recommend that you specify the local clock on the second- or third-generation ATM OC traffic card as the clock source for its ports.

Table 4 shows the possible clock source configurations for the second- or third-generation ATM OC traffic card and its ports and the impact during switchover.

Table 4 ATM Port Configurations and Potential Packet Loss

ATM Traffic Card Clock Source	Port Clock Source	Impact During Switchover
`global-reference`	**`loop`**	Potential loss of packets
	`card-reference`	Potential loss of packets
`local` (the default source)	**`loop`**	No loss of packets
	`card-reference` (the default source)	No loss of packets

Use the **`default`** form of this command to set the clock source to the default.

1.33.6 Examples

The following example shows how to specify the derived receive clock for the ATM OC-3 port as the transmit clock source. In this configuration, packet loss can occur should the active controller card be removed from the chassis:

```
[local]Redback(config)#card atm-oc3e-8-port 3

[local]Redback(config-card)#clock-source global reference

[local]Redback(config)#port atm 3/1

[local]Redback(config-atm-ds3)#clock-source loop
```

The following example shows how to specify the **local** clock as the source for the transmit clock for a 8-port ATM OC-3c/STM-1c traffic card and its port **1**. This configuration prevents packet loss should the active controller card be removed from the chassis:

```
[local]Redback(config)#card atm-oc3e-8-port 4

[local]Redback(config-card)#clock-source local

[local]Redback(config)#port atm 4/1

[local]Redback(config-atm-oc)#clock-source card-reference
```

1.34 clock-source (card configuration mode)

```
clock-source {local | global-reference}

default clock-source
```

1.34.1 Purpose

Configures the clock source for either of the following:

- Channelized OC-3/STM-1 or OC-12/STM-4 line card.
- A second- or third-generation OC line card.

1.34.2 Command Mode

- card configuration (Channelized OC-3/STM-1 or OC-12/STM-4 line card)

- card configuration (second- or third-generation OC line card)

1.34.3 Syntax Description

`local` Specifies the clock source used by the line card is supplied by the line card itself; that is, its on-board clock.

`global-reference` Specifies the clock source used by the line card is whatever option the system clock on the XCRP controller card has been set to; default value.

1.34.4 Default

`global-reference`

1.34.5 Usage Guidelines

If you choose **`global-reference`**, see the *system clock-source* command for the source of the system clock.

1.34.6 Example

```
[local]rock1200(config)#card ch-oc3oc12-8or2-port-sm 11
[local]rock1200(config-card)#clock-source global-reference
```

1.35 clpbit

`clpbit` [**`propagate qos to atm`**]

{**`no`** | **`default`**} **`clpbit`** [**`propagate qos to atm`**]

1.35.1 Purpose

Sets the cell loss priority (CLP) bit in all cells transmitted over Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs) and that reference this ATM profile.

1.35.2 Command Mode

ATM profile configuration

1.35.3 Syntax Description

`propagate qos to atm`	Optional. Specifies that the CLP bit is set based on the IP precedence and Differentiated Services Code Point (DSCP) bits as assigned by the quality of service (QoS) policy attached to an ATM PVC that references this profile.

1.35.4 Default

The CLP bit is set to zero.

1.35.5 Usage Guidelines

Use the **`clpbit`** command to set the CLP bit in all cells transmitted over ATM PVCs that reference this ATM profile. If you do not specify the optional **`propagate qos to atm`** construct, the CLP bit is set to one; if you do specify this, the CLP bit is set based on the IP precedence and DSCP bits.

Note: For more information about the use of this command for QoS propagation, see *Configuring Circuits for QoS*.

Use the **`no`** or **`default`** form of this command to set the CLP bit to zero in all circuits referencing that ATM profile.

1.35.6 Examples

The following example shows how to set the CLP bit to one in an ATM profile, **low_rate**. All cells transmitted over PVCs that reference this profile have the CLP bit set to one:

```
[local]Redback(config)#atm profile low_rate

[local]Redback(config-atmpro)clpbit
```

1.36 clpbit propagate qos from atm

clpbit propagate qos from atm [**class-map** ***map-name***]

no clpbit propagate qos from atm [**class-map** ***map-name***]

1.36.1 Purpose

Propagates the cell loss priority (CLP) bit to packet descriptor (PD) values in cells transmitted over Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs) that reference the ATM profile for incoming packets.

1.36.2 Command Mode

ATM profile configuration

1.36.3 Syntax Description

class-map ***map-name***	Optional. Name of an ingress ATM classification map, an alphanumeric string of up to 39 characters, for defining a custom mapping of CLP values to quality of service (QoS) PD values.

1.36.4 Default

CLP bit values are not propagated to PD values.

1.36.5 Usage Guidelines

Use the **clpbit propagate qos from atm** command to propagate the CLP bit to PD values in cells transmitted over ATM PVCs that reference the ATM profile for incoming packets.

Note: CLP bit priority settings cannot be directly propagated to IP header DSCP bits.

Note: For more information about the CLP bit and its use in ATM profiles, see *Configuring Circuits*.

If you use the optional `class-map` ***map-name*** construct to specify a custom mapping schema for packets transmitted on ATM PVCs that reference the ATM profile, the operating system sets the initial QoS PD value according to the CLP values in the packet's received ATM cell headers. If a packet is composed of multiple ATM cells, the SmartEdge router assigns a CLP value of 1 if any ATM cell that makes up the adaptation layer type 5 (AAL5) packet has the CLP bit set to 1 (for second-generation ATM traffic cards).

If no classification map is specified, the SmartEdge router uses the default mapping described in Table 5.

Table 5 ATM CLP Bits Mapped to the QoS PD Value

ATM CLP Bit	PD Priority Value	PD Drop-Precedence Value	AF Label	QoS PD Value
0	1	2	AF11	10
1	0	0	DF	0

Use the **no** form of this command to disable propagation from the ATM CLP bit to internal QoS classification values.

1.36.6 Examples

The following example shows how to propagate ATM CLP bits to the DSCP bit values in cells transmitted over ATM PVCs that reference the ATM profile, **low_rate:**

```
[local]Redback(config)#atm profile low_rate

[local]Redback(config-atm-profile)#clpbit propagate qos from atm
```

1.37 clpbit propagate qos to atm

clpbit propagate qos to atm [**class-map** ***map-name***]

no clpbit propagate qos to atm [**class-map** ***map-name***]

1.37.1 Purpose

Propagates the quality of service (QoS) classification values from the internal packet descriptor (PD) to the cell loss priority (CLP) bit in cells transmitted over Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs) that reference the ATM profile for outgoing packets.

1.37.2 Command Mode

ATM profile configuration

1.37.3 Syntax Description

`class-map` *`map-name`*	Optional. Name of an egress ATM classification map, an alphanumeric string of up to 39 characters, for mapping Differentiated Services Code Point (DSCP) bits to CLP bits.

1.37.4 Default

QoS PD values are not propagated to the ATM CLP bit.

1.37.5 Usage Guidelines

Use the `clpbit propagate qos to atm` command to propagate the QoS classification values from the internal PD to the CLP bit in cells transmitted over ATM PVCs that reference the ATM profile for outgoing packets.

Note: For more information about the CLP bit and its use in ATM profiles, see *Configuring Circuits*.

QoS PD values are mapped to the ATM CLP bit as described in Table 6.

Table 6 QoS PD Value to ATM CLP Bit Mapping

PD Priority Value	PD Drop-Precedence Value	AF Label	ATM CLP Bit
7	N/A	Network Control	0
6	N/A	Reserved	0
5	N/A	EF	0
4	0-2	AF41	0
4	3-7	AF42, AF43	1
3	0-2	AF31	0
3	3-7	AF32, AF33	1

Table 6 QoS PD Value to ATM CLP Bit Mapping

PD Priority Value	PD Drop-Precedence Value	AF Label	ATM CLP Bit
2	0-2	AF21	0
2	3-7	AF22, AF23	1
1	0-2	AF11	0
1	3-7	AF12, AF13	1
0	N/A	DF	1

If you specify a custom mapping schema for the optional **`class-map`** ***`map-name`*** construct, packets received on ATM PVCs that reference the ATM profile have the CLP values of the cells in the AAL5 packet set according to internal QoS classification values. If you do not specify a classification map, the SmartEdge router uses the default mapping described in Table 6.

Use the **`no`** or **`default`** form of this command to restore the default behavior.

1.37.6 Examples

The following example shows how to .propagate DSCP bits from IP packets to the CLP bit in cells transmitted over ATM PVCs that reference the ATM profile, **low_rate:**

```
[local]Redback(config)#atm profile low_rate

[local]Redback(config-atm-profile)#clpbit propagate qos to atm
```

1.38 cluster-id

`cluster-id` ***`ip-addr`***

`no cluster-id` ***`ip-addr`***

1.38.1 Purpose

Assigns a cluster ID if the Border Gateway Protocol (BGP) cluster has more than one route reflector.

1.38.2 Command Mode

BGP router configuration

1.38.3 Syntax Description

ip-addr IP address of the route reflector.

1.38.4 Default

The router ID is used as the cluster ID.

1.38.5 Usage Guidelines

Use the **cluster-id** command to assign a cluster ID if the BGP cluster has more than one route reflector. If this command is not enabled, the router ID is used as the cluster ID.

Together, a route reflector and its clients form a cluster. If there is more than one route reflector in a cluster, all route reflectors in that cluster should be configured with the same ID. A common cluster ID allows a route reflector to recognize updates from other route reflectors in the same cluster, prevents the possibility of a routing loop, and prevents the sending of duplicate updates.

Note: Do not configure a cluster ID if the device is not a route reflector.

Use the **no** form of this command to remove a cluster ID.

1.38.6 Examples

The following example shows how to configure a cluster ID of **100.25.34.5:**

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

[local]Redback(config-ctx)#router bgp 100

[local]Redback(config-bgp)#cluster-id 100.25.34.5
```

1.39 collection

```
collection

no collection
```

1.39.1 Purpose

Enables the collection of bulk statistics (bulkstats) for all the entities to which this bulkstats policy has been applied.

1.39.2 Command Mode

Bulkstats configuration

1.39.3 Syntax Description

This command has no keywords or arguments.

1.39.4 Default

Bulk statistics are not collected for any policy.

1.39.5 Usage Guidelines

Use the **`collection`** command to enable the collection of bulkstats for all the entities to which this bulkstats policy has been applied.

Before you enable bulkstats collection for a bulkstats policy, you must perform the following tasks for it:

- Specify the primary bulkstats file server using the **`receiver`** command in bulkstats configuration mode.
- Specify the directory on the local SmartEdge router where collected data is stored using the **`localdir`** command in bulkstats configuration mode.
- Specify the name and location of the collection files on the bulkstats file server using the **`remotefile`** command in bulkstats configuration mode.

You must also perform these tasks:

- Create one or more schema profiles using the **`bulkstats schema profile`** command in global configuration mode.
- Apply one or more schema profiles using the **`schema`** command (in bulkstats configuration mode) for system-wide statistics or the **`bulkstats schema`** command for applying an existing schema profile and bulk statistics policy.

You can enable collection for a bulkstats policy at any time after you have performed these tasks. It is not necessary to disable collection before you apply the policy to an entity, such as a port, channel, or circuit.

Use the **`no`** form of this command to disable collection for this bulkstats policy.

1.39.6 Examples

The following command shows how to enable the collection of bulk statistics:

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

[local]Redback(config-ctx)#bulkstats policy bulk

[local]Redback(config-bulkstats)#collection
```

1.40 comment

comment *text*

1.40.1 Purpose

Assigns a comment to the current configuration database transaction.

1.40.2 Command Mode

All configuration modes

1.40.3 Syntax Description

text	Text string of up to 25 characters describing the current configuration database transaction.

1.40.4 Default

None

1.40.5 Usage Guidelines

Use the **comment** command to assign a textual description to the current configuration database transaction. This string displays in the output of the **show transaction** command (in any mode).

You can modify the comment at any point during a configuration session.

Note: When you enter the **comment** command, any existing comment is overwritten.

1.40.6 Examples

The following example shows how to assign a comment for the current configuration database transaction:

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

1.41 commit

commit [{**at** ***yyyy*:*mm*:*dd*:*hh*:*mm***[**:*ss***]} | {**in** ***minutes***}] [***text***]

1.41.1 Purpose

Commits an outstanding configuration database transaction.

1.41.2 Command Mode

All configuration modes

1.41.3 Syntax Description

at ***yyyy*:*mm*:*dd*:*hh*:*mm***[**:*ss***]

Optional. Time at which to commit the configuration database transaction, specified as year, month, day, hour, minutes, and optionally, seconds. The hour is in a 24-hour format; for example, 6:00 p.m. is 18:00. This construct is not allowed in exec mode.

in ***minutes***

Optional. Number of minutes to wait before committing current database transaction. This construct is not allowed in exec mode.

text

Optional. Text string of up to 25 characters describing the transaction.

1.41.4 Default

In any configuration mode, commits the current configuration database transaction.

1.41.5 Usage Guidelines

Use the **commit** command to commit an outstanding configuration database transaction. You can use the **at** or **in** keywords to schedule the transaction to be committed at a later time. You can also associate a comment with the transaction.

Commands entered in any configuration mode do not immediately change the working configuration of the SmartEdge router. Outstanding configuration commands are maintained in a transaction. To commit the transaction so that the commands take effect, you must enter the `commit` command.

Caution!

Risk of incorrect operation. You can cause problems in your system if you commit configuration changes to the database before you validate them. To reduce the risk, always save your configuration before and after you enter the transaction commands in separate files, and validate the configuration changes in the transaction before you commit it.

When any database transaction is committed, a new database transaction is started for the configuration session, and subsequent commands entered in the session are part of the new transaction.

Note:

The configuration database is locked whenever the system is not ready to incorporate your configuration commands with the `commit` command. During a database locked situation, you can enter global configuration mode, and can test out modifications, but you cannot commit these changes. If you attempt to commit a configuration change when the database is locked, you are notified with a prompt to either wait for the lock to be freed, or to return to the configuration mode prompt:

- Waiting causes the system to wait until the lock is freed or up to 20 seconds before prompting you again.

- Returning to the configuration mode prompt leaves your configuration changes as they are, so that you can make more configuration changes or commit your changes at a later time.

1.41.6 Examples

The following example examines commits the current database transaction in **60** minutes, with the comment **Cfg BGP in local ctx:**

```
[local]Redback(config)#commit in 60 Cfg BGP in local ctx
```

The following example displays information on the transaction:

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

```
 TID       State                  Sequence       State Information
           User                   Comment

-------------------------------------------------------------------
 3491      Waiting to Commit      3634           Committing in 60 min

           admin1                 Cfg BGP in local ctx
```

1.42 community-list

`community-list` ***`cl-name`***

`no community-list` ***`cl-name`***

1.42.1 Purpose

Creates a Border Gateway Protocol (BGP) community list and enters community list configuration mode.

1.42.2 Command Mode

Context configuration

1.42.3 Syntax Description

`cl-name` Name of the community list.

1.42.4 Default

There are no preconfigured community lists.

1.42.5 Usage Guidelines

Use the **`community-list`** command to create a BGP community list and enter community list configuration mode where you can define conditions using the **`permit`** and **`deny`** commands.

A community is an attribute shared among a group of prefixes; for example, 10.1.1.0/24, 20.1.1.0/24, and 30.1.1.0/24. A single prefix can be associated with multiple comminutes. You can specify multiple communities in a single community list entry using a regular expression. Like access control lists, community lists can have multiple entries that are examined in order of ascending sequence number.

To set the communities attribute and match clauses based on communities, use the **`set community`** and **`match community-list`** commands in route map configuration mode.

Note: A reference to a community list that does not exist, or does not contain any configured entries, implicitly matches and permits all community lists.

Use the **`no`** form of this command to remove a community list.

1.42.6 Examples

The following example shows how to configure the community list, **permit_local**, and enter community list configuration mode:

```
[local]Redback(config-ctx)#community-list permit_local

[local]Redback(config-community-list)#
```

1.43 condition

`condition` ***`cond-id`*** **`time-range`**

`no condition` ***`cond-id`***

1.43.1 Purpose

Creates an access control list (ACL) condition and enters ACL condition configuration mode.

1.43.2 Command Mode

Access control list configuration

1.43.3 Syntax Description

`cond-id`	Condition ID in integer or IP address format. The ID range of values is 1 to 4294967295.
`time-range`	Specifies a time range condition type.

1.43.4 Default

None

1.43.5 Usage Guidelines

Use the **condition** command to create an ACL condition, and to enter ACL condition configuration mode.

An ACL condition is comprised of up to seven ACL condition statements (using any combination of the **absolute** and **periodic** commands in ACL condition configuration mode). When an ACL statement references an ACL condition, the ACL condition statements apply those time-dependent rules to the referencing IP ACL or policy ACL statement.

Use the **no** form of this command to delete an ACL condition.

1.43.6 Examples

The following example shows how to create the time range condition identified as **342** for the IP ACL, **protect**, and enter ACL condition configuration mode:

```
[local]Redback(config-ctx)#ip access-list protect

[local]Redback(config-access-list)#condition 342 time-range

[local]Redback(config-acl-condition)#
```

The following example shows how to create the time range condition identified as **10.1.2.3** for the policy ACL, **control**, and enter ACL condition configuration mode:

```
[local]Redback(config-ctx)#policy access-list control

[local]Redback(config-access-list)#condition 10.1.2.3 time-range

[local]Redback(config-acl-condition)#
```

1.44 confederation identifier

confederation identifier {*asn* | *as*:*nn*}

no confederation identifier {*asn* | *as*:*nn*}

1.44.1 Purpose

Configures a Border Gateway Protocol (BGP) confederation identifier.

1.44.2 Command Mode

BGP router configuration

1.44.3 Syntax Description

asn	Autonomous system number (ASN). The range of values is 1 to 65,535. The subrange of 64,512 to 65,535 is reserved for private autonomous systems.
as:nn	ASN and a 2-byte number.

1.44.4 Default

No confederation identifier is configured.

1.44.5 Usage Guidelines

Use the **`confederation identifier`** command to configure a BGP confederation identifier. Use this command in conjunction with the **`confederation peers`** command in BGP router configuration mode to reduce internal BGP (iBGP) mesh by dividing an autonomous system into subautonomous systems and grouping them into a single confederation.

In the confederation, the subautonomous systems have external BGP (eBGP) connections to each other, but they exchange information as though they were iBGP peers. This means that they preserve next-hop, Multi-Exit Discriminator (MED), and local preference information. Externally, the confederation appears as a single autonomous system, and the confederation identifier is viewed as the ASN.

Use the **`no`** form of this command to remove a confederation identifier.

1.44.6 Examples

In the following example, the confederation consists of subautonomous systems, **65501**, **65502**, **65503**, and **65504**. Externally, there appears to be a single autonomous system with ASN **100:**

```
[local]Redback(config-ctx)#router bgp 65501

[local]Redback(config-bgp)#confederation identifier 100

[local]Redback(config-bgp)#confederation peers 65502 65503 65504
```

1.45 confederation peers

```
confederation peers {asn... | as:nn...}
```

```
no confederation peers {asn... | as:nn...}
```

1.45.1 Purpose

Configures the subautonomous systems that belong to a Border Gateway Protocol (BGP) confederation.

1.45.2 Command Mode

BGP router configuration

1.45.3 Syntax Description

asn...	One or more autonomous system numbers (ASNs). The range of values is 1 to 65,535. The subrange of 64,512 to 65,535 is reserved for private autonomous systems.
as:nn...	One or more ASNs and a 2-byte number.

1.45.4 Default

No subautonomous systems are configured.

1.45.5 Usage Guidelines

Use the **confederation peers** command to configure the subautonomous systems that belong to a BGP confederation. Use this command in conjunction with the **confederation identifier** command in BGP router configuration mode to reduce internal BGP (iBGP) mesh. Subautonomous systems are visible within the confederation, but externally.

In the confederation, the subautonomous systems have external BGP (eBGP) connections to each other, but they exchange information as though they were IBGP peers. This means that they preserve next-hop, Multi-Exit Discriminator (MED), and local preference information. Externally, the confederation appears as a single autonomous system, and the confederation identifier is viewed as the ASN.

Use the **no** form of this command to remove an autonomous system from a BGP confederation.

1.45.6 Examples

The following example shows how to specifiy that autonomous systems, `65501`, `65502`, `65503`, and `65504` belong to a single confederation that is known externally as ASN `100:`

```
[local]Redback(config-ctx)#router bgp 65501

[local]Redback(config-bgp)#confederation identifier 100

[local]Redback(config-bgp)#confederation peers 65502 65503 65504
```

1.46 configure (URL)

configure ***url*** [**besteffort** [**implicit**]] [**verbose** [***lines***]]

1.46.1 Purpose

Configures the system from a preexisting configuration file on the local or a remote file system.

1.46.2 Command Mode

Exec (10)

1.46.3 Syntax Description

url
URL of an existing configuration file. For the format of this argument, see the Usage Guidelines section.

besteffort
Optional. Ignores errors in the configuration file, and continues executing the command file.

implicit
Optional. Commits the changes to the configuration database as the file is processed.

verbose
Optional. Displays each line and its line number when configuring from a preexisting configuration file.

lines
Optional. Number of configuration file lines to process. The range of values is 1 to 4,294,967,295; the default value is to process all lines.

1.46.4 Default

None

1.46.5 Usage Guidelines

Use the **configure** ***url*** command to configure the system from a configuration file on the local or a remote file system. Configuration commands are read from the file associated with the URL that you specify with the ***url*** argument. The system does not restart when loading a configuration file.

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

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

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

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

Table 7 describes the syntax for the ***url*** argument when accessing a file on a remote server.

Table 7 url Syntax for Accessing a File on a Remote Server

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

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

The ***filename*** argument can be up to 256 characters in length. The ***hostname*** argument can only be used if Domain Name System (DNS) is enabled with the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands (in context configuration mode). For more information, see *Configuring DNS*.

Note: If you enter this command without specifying a URL, the system begins an interactive configuration session and enters global configuration mode. For information about using the **`configure`** command for this purpose, see *Load Balancing*.

By default, if an error is encountered, the system displays a message and stops processing the configuration file. Use the **`besteffort`** keyword to configure the system to continue processing a file, even if an error is encountered; in this case, all commands in the configuration file that do not fail are applied to the database.

Use the **`implicit`** keyword to commit the configuration changes to the database as the file is processed unless the database or a database record is locked.

If the system stops a commit because of a database lock, the system displays the following message:

```
Database lock contention detected

   globally locked for:
```

and then displays the reason for the database lock with the following prompt:

```
Would you like to wait (w) or abort (a)?
```

If the system stops a commit because of a record lock, the system displays the following message:

```
Database lock contention detected

   locked by process nn with transaction id nnnn

   locking transaction was started on transaction-date-time

Would you like to wait (w) or abort (a)?
```

Enter **`w`** to wait until the database is unlocked; enter **`a`** to cancel the current transaction and roll back the database to the previous commit.

Possible reasons for a database lock include:

- Standby synchronization—The online database in the memory of the standby controller card is being synchronized with the online database in the memory of the active controller card.

- Binary configuration—The binary configuration file on the local file system is being updated from the online database.
- Switchover—The system is in the process of switching over from the currently active controller card to the standby controller card.
- Backend bulk download—The online database is being accessed by another process on the system.

1.46.6 Examples

The following example shows how to configure the system from a configuration file on the local file system:

```
[local]Redback#configure /flash/old_config.cfg
```

1.47 configure

`configure`

1.47.1 Purpose

Enters global configuration mode.

1.47.2 Command Mode

Exec (10)

1.47.3 Syntax Description

This command has no keywords or arguments.

1.47.4 Default

None

1.47.5 Usage Guidelines

Use the **`configure`** command to enter global configuration mode. This mode provides commands that allow you to make changes that are universal to the system, such as configuring the system clock or creating login banners. It also provides commands that allow you to enter other configuration modes.

To show information on the changes you are implementing, use the **show configuration** command.

Note: To load a configuration file, enter the **configure** ***url*** command (in exec mode).

1.47.6 Examples

The following example shows how to enter global configuration mode:

```
[local]Redback#configure


Enter configuration commands, one per line, 'end' to exit

[local]Redback(config)#
```

1.48 conform mark dscp

conform mark dscp ***dscp-class***

{**no** | **default**} **conform mark dscp**

1.48.1 Purpose

Assigns a quality of service (QoS) Differentiated Services Code Point (DSCP) priority to IP packets that conform to the configured QoS rate. For IPv4 packets, the DSCP marking is the upper six bits of the IPv4 header Type of Service (ToS) field. For IPv6 packets, the DSCP marking is the upper six bits of the IPv6 header Traffic Class field.

1.48.2 Command Mode

- Policy class rate configuration
- Policy rate configuration

1.48.3 Syntax Description

dscp-class Priority with which packets conforming to the rate are marked. Values can be:

- An integer from 0 to 63.
- One of the keywords listed in Table 8.

1.48.4 Default

No action is taken on packets that conform to the configured rate.

1.48.5 Usage Guidelines

Use the **`conform mark dscp`** command to mark inbound packets that conform to the configured rate with a DSCP value.

You can configure the rate using the **`rate`** command (in policy ACL class, metering policy, or policing policy configuration mode). Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **`conform mark dscp`** command, specifying a new value for the *`dscp-class`* argument, which supersedes the one previously configured.

Table 8 lists the keywords for the *`dscp-class`* argument.

Table 8 DSCP Class Keywords

DSCP Class	Keyword	DSCP Class	Keyword
Assured Forwarding (AF) Class 1/ Drop precedence 1	`af11`	Class Selector 0 (same as default forwarding)	`cs0` (same as `df`)
AF Class 1/Drop precedence 2	`af12`	Class Selector 1	`cs1`
AF Class 1/Drop precedence 3	`af13`	Class Selector 2	`cs2`
AF Class 2/Drop precedence 1	`af21`	Class Selector 3	`cs3`
AF Class 2/Drop precedence 2	`af22`	Class Selector 4	`cs4`
AF Class 3/Drop precedence 3	`af23`	Class Selector 5	`cs5`
AF Class 3/Drop precedence 1	`af31`	Class Selector 6	`cs6`
AF Class 3/Drop precedence 2	`af32`	Class Selector 7	`cs7`
AF Class 3/Drop precedence 3	`af33`	Default Forwarding (same as Class Selector 0)	`df` (same as `cs0`)
AF Class 4/Drop precedence 1	`af41`	Expedited Forwarding	`ef`
AF Class 4/Drop precedence 2	`af42`		
AF Class 4/Drop precedence 3	`af43`	Assured Forwarding—Class 4/Drop precedence 3	

For more information about DSCP values, see RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.

Caution!

Risk of packet reordering. Packets can be reordered into a different major DSCP class. To reduce the risk, ensure that the marking of conforming packets and exceeding packets differ only within a major DSCP class. Major DSCP classes are identified by the Class Selector code, and include CS0=DF, CS1=AF11, AF12, AF13, CS2=AF21, AF22, AF23, CS3=AF31, AF32, AF33, CS4=AF41, AF42, AF43, and CS5=EF. For example, if you mark conforming packets with AF11 and you want to avoid reordering, mark exceeding packets with AF11, AF12, or AF13 only.

Caution!

Risk of overriding configurations. The SmartEdge router checks for and applies marking in a specific order. To reduce the risk, remember the following guidelines: Circuit-based marking overrides class-based marking and Border Gateway Protocol (BGP) destination-based marking, through route maps, overrides both circuit-based and class-based marking.

Use the **no** or **default** form of this command to return to the default behavior of not taking any action on packets that conform to the configured rate.

1.48.6 Examples

The following example shows how to configure the policing policy, `protection1`, to mark all packets that conform to the configured rate with a DSCP value representing a high priority of expedited forwarding (`ef`) and, by default using the `conform mark` command, to drop all packets that exceed the rate configured for the policing policy:

```
[local]Redback(config)#qos policy protection1 policing

[local]Redback(config-policy-policing)#rate 10000 burst 100000

[local]Redback(config-policy-rate)#conform mark dscp ef
```

1.49 conform mark precedence

conform mark precedence ***prec-value***

```
{no | default} conform mark precedence
```

1.49.1 Purpose

Assigns a quality of service (QoS) Differentiated Services Code Point (DSCP) drop-precedence value to IP packets that conform to the configured QoS drop precedence value. For IPv4 packets, the DSCP marking is applied to the IPv4 header Type of Service (ToS) field. For IPv6 packets, the DSCP marking is applied to the IPv6 header Traffic Class field. In either case, the specific bits affected are those denoted by *dd* in the octet field with the format *pppddxxx*.

1.49.2 Command Mode

- Policy class rate configuration
- Policy rate configuration

1.49.3 Syntax Description

prec-value	Drop precedence value. See Table 9.

1.49.4 Default

No action is taken on packets that conform to the configured rate.

1.49.5 Usage Guidelines

Use the **conform mark precedence** command to mark inbound packets that conform to the configured rate with a drop precedence value corresponding to the AF class of the packet.

You can configure rate using the **rate** command (in policy ACL class, metering policy, or policing policy configuration mode).

In general, the level of forwarding assurance of an IP packet is based on: (1) the resources allocated to the AF class to which the packet belongs, (2) the current load of the AF class, and, in case of congestion within the class, (3) the drop precedence of the packet. In case of congestion, the drop precedence of a packet determines the relative importance of the packet within the AF Differentiated Services Code Point (DSCP) class. Packets with a lower drop precedence value are preferred and protected from being lost, while packets with a higher drop precedence value are discarded.

With AF classes AF1 (AF11, AF12, AF13), AF2 (AF21, AF22, AF23), AF3 (AF31, AF32, AF33), and AF4 (AF41, AF42, AF43), the second integer represents a drop precedence value. Table 9 shows how the AF drop precedence value of an incoming packet is changed when it exits the SmartEdge router after being tagged with a new drop precedence. (See also RFC 2597, ***Assured Forwarding PHB Group***.)

Table 9 Drop Precedence Values

DSCP Value of an Incoming Packet	Packet is Tagged with a Drop Precedence Value	DSCP Value of the Outgoing Packet
AF11, AF12, AF13	1	AF11
AF21, AF22, AF23		AF21
AF31, AF32, AF33		AF31
AF41, AF42, AF43		AF41
AF11, AF12, AF13	2	AF12
AF21, AF22, AF23		AF22
AF31, AF32, AF33		AF32
AF41, AF42, AF43		AF42
AF11, AF12, AF13	3	AF13
AF21, AF22, AF23		AF23
AF31, AF32, AF33		AF33
AF41, AF42, AF43		AF43

Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **conform mark precedence** command, specifying a new value for the ***prec-value*** argument, which supersedes the one previously configured.

Caution!

Risk of overriding configurations. The SmartEdge router checks for and applies marking in a specific order. To reduce the risk, remember the following guidelines: Circuit-based marking overrides class-based marking and Border Gateway Protocol (BGP) destination-based marking, through route maps, overrides both circuit-based and class-based marking.

Use the **no** or **default** form of this command to return to the default behavior of not taking any action on packets that conform to the configured rate.

1.49.6 Examples

The following example shows how to configure the policing policy, `protection1`, to mark all packets that conform to the configured rate with a drop precedence value of **1** and drop all packets that exceed the rate:

```
[local]Redback(config)#qos policy protection1 policing

[local]Redback(config-policy-policing)#rate 10000 burst 100000

[local]Redback(config-policy-rate)#conform mark precedence 1
```

1.50 conform mark priority

conform mark priority {*group-num* | **ignore**} [{**drop-precedence** {*group-num* | **ignore**} | **af-drop** *drop-value*}

{**no** | **default**} **conform mark priority**

1.50.1 Purpose

Marks packets that conform to the configured quality of service (QoS) rate with a priority group number, a drop-precedence value, or both, while leaving the packet's IP header Differentiated Services Code Point (DSCP) value unmodified.

1.50.2 Command Mode

- Policy class rate configuration
- Policy rate configuration

1.50.3 Syntax Description

group-num

Priority group number. The range of values is 0 to 7.

The scale used by this command for packet priority, from 0 (highest priority) to 7 (lowest priority), is the relative inverse of the scale used by QoS classification map and classification definition commands.

ignore

Specifies that the internal packet descriptor (PD) priority or drop-precedence value is not modified.

`drop-precedence`	Optional. Enables you to specify a setting for either the drop-precedence portion of the PD QoS field or the priority group, or both.
`af-drop` ***`drop-value`***	Optional. Target internal drop-precedence value in two-bit format; leaves the least significant bit unmodified. The range of values is 1 to 3.

1.50.4 Default

No action is taken on packets that conform to the configured rate. Default mapping of priority groups to queues is listed in Table 10.

1.50.5 Usage Guidelines

Use the **`conform mark priority`** command to mark packets that conform to the configured QoS rate with a priority group number, a drop-precedence value, or both, while leaving the packet's IP header DSCP value unmodified.

To configure the rate, enter the **`rate`** command (in policy ACL class, metering policy, or policing policy configuration mode).

A priority group is an internal value used by the SmartEdge router to determine into which egress queue the inbound packet is placed. The type of service (ToS) value, DSCP value, and Multiprotocol Label Switching (MPLS) experimental (EXP) bits are unchanged by this command. The actual queue number depends on the number of queues configured on the circuit. For more information, see the **`num-queues`** command in the *Command List*.

The SmartEdge router uses the factory preset, or default, mapping of a priority group to queue, according to the number of queues configured on a circuit; see Table 10.

Table 10 Default Mapping of Priority Groups to Queues

Prio rity Group	8 Queues	4 Queue s	2 Queues	1 Queue
0	queue 0	queue 0	queue 0	queue 0
1	queue 1	queue 1	queue 1	queue 0
2	queue 2	queue 1	queue 1	queue 0
3	queue 3	queue 2	queue 1	queue 0
4	queue 4	queue 2	queue 1	queue 0
5	queue 5	queue 2	queue 1	queue 0
6	queue 6	queue 2	queue 1	queue 0
7	queue 7	queue 3	queue 1	queue 0

Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **conform mark priority** command, specifying a new value for the ***group-num*** argument. This supersedes the value previously configured.

Caution!

Risk of overriding configurations. The SmartEdge router checks for and applies marking in a specific order. To reduce the risk, remember the following guidelines: Circuit-based marking overrides class-based marking and Border Gateway Protocol (BGP) destination-based marking, through route maps, overrides both circuit-based and class-based marking.

Use the **no** or **default** form of this command to specify the default behavior.

1.50.6 Examples

The following example shows how to configure the policy to mark all packets that conform to the configured rate with priority group number **3** and drop all packets that exceed the rate:

```
[local]Redback(config)#qos policy protection1 policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#conform mark priority 3
```

1.51 conform no-action

conform no-action

{**no** | **default**} **conform no-action**

1.51.1 Purpose

Specifies that no marking is made on packets that conform to the configured quality of service (QoS) rate.

1.51.2 Command Mode

- Policy class rate configuration
- Policy rate configuration

1.51.3 Syntax Description

This command has no keywords or arguments.

1.51.4 Default

No marking is taken on packets that conform to the configured rate.

1.51.5 Usage Guidelines

Use the **conform no-action** command to specify that no marking is made on packets that conform to the configured QoS rate.

To configure the rate, enter the **rate** command (in policy ACL class, metering policy, or policing policy configuration mode).

Use the **no** or **default** form of this command to specify that no marking is made.

1.51.6 Examples

The following example shows how to configure the policy to mark all packets that conform to the configured rate with no action:

```
[local]Redback(config)#qos policy protection1 policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#conform no-action
```

1.52 congestion

congestion {**red** **min_threshold** *min* **max_threshold** *max* **probability** *prob* **weight** *weight-exp* | **epd** [[**min_threshold** *min*] **max_threshold** *max*]}

{**no** | **default**} **congestion** {**red** | **epd**}

1.52.1 Purpose

Specifies the congestion avoidance algorithm, either weighted random early detection (RED) or early packet discard (EPD), and its parameters for the specified Asynchronous Transfer Mode (ATM) profile.

1.52.2 Command Mode

ATM profile configuration

1.52.3 Syntax Description

`red`	Specifies the weighted RED algorithm.
`epd`	Specifies the EPD algorithm.
`min-threshold` ***`min`***	For the weighted RED algorithm, the average buffer or queue occupancy in packets below which no packets are dropped. For the EPD algorithm, the number of packets below which no packets are dropped. Optional only when specifying the EPD algorithm. The range of values is 1 to 9,999; the default value is 8 packets.
`max-threshold` ***`max`***	For the weighted RED algorithm, the average buffer or queue occupancy in packets above which all packets are dropped. For the EPD algorithm, the number of packets above which all packets are dropped. The range of values is 2 to 10,000; the default value is 26 packets.
`probability` ***`prob`***	Inverse of the probability of dropping a packet as the average queue occupancy approaches the maximum threshold. The resulting probability (1/***prob***) is the fraction of packets dropped when the average queue depth is at the maximum threshold. The range of values is 8 to 32,768; the default value is 16.
`weight` ***`weight-exp`***	Exponent representing the inverse of the exponentially weighted moving average. The range of values is 7 to 10; the default value is 9.

1.52.4 Default

The default congestion avoidance algorithm is weighted RED with the default parameters.

1.52.5 Usage Guidelines

Use the **`congestion`** command to set the weighted RED or EPD parameters for the specified ATM profile. These parameters specify how buffer utilization is to be managed under congestion by signaling to the sources of traffic that the network is on the verge of entering a congested state.

This signaling is accomplished by dropping packets according to the type of congestion algorithm and the type of port on which the ATM VP or PVC is configured:

- For the weighted RED algorithm, which is supported for second-generation ATM OC traffic cards only, packets are dropped with a probability that varies as a function of how many packets are waiting in a queue at any particular time, and of the values of the ***max***, ***min***, ***prob***, and ***weight-exp*** arguments.

- For ports on second-generation ATM OC traffic cards, when the congestion exceeds the value of the ***max*** argument, packets are dropped until the buffers are below the value of the ***max*** argument.

Use the **`min-threshold`** ***min*** construct as follows:

- For the weighted RED algorithm, use this construct to set the average buffer or queue occupancy in packets at or below which no packets are dropped.
- For the EPD algorithm, use this construct to specify the minimum value below which no packets are dropped. This construct is ignored if the profile is assigned to a shaped VP or PVC on a second-generation ATM OC traffic card.

Use the **`max-threshold`** ***max*** construct as follows:

- For the weighted RED algorithm, use this construct to set the average buffer or queue occupancy in packets above which packets are dropped; as the average occupancy approaches the maximum threshold value, packets are dropped with increasing probability, as a function of the value of the ***prob*** argument.
- For the EPD algorithm, use this construct to set the value above which all packets are dropped.

Use the **`probability`** ***prob*** construct to establish the probability of a packet being dropped as the average queue occupancy approaches the maximum threshold value. The value of the ***prob*** argument is the inverse of the probability of a packet being dropped. The higher the value of the ***prob*** argument, the lower the probability of a packet being dropped.

The average queue occupancy is computed as a moving average of the instantaneous queue occupancy. Use the **`weight`** ***weight-exp*** construct to set the inverse of the exponential moving average. The larger the value of the ***weight-exp*** argument, the longer term the average.

If this command is not entered, any PVC that is created on a port on a second-generation ATM OC traffic card and that references this profile uses weighted RED for the congestion avoidance algorithm with the default values for the parameters.

Note: For more configuration guidelines for ATM profiles, VPs, and PVCs with regard to congestion avoidance, see the *Configuring ATM Ports* section of *Configuring ATM, Ethernet, and POS Ports*.

Use the **`no`** and **`default`** forms of this command to perform the functions listed in Table 11.

Table 11 Functions of default and no Forms of the congestion Command

Command	Function
`no congestion red`	Enables RED default parameters if RED is configured; generates an error message if EPD is configured.
`default congestion red`	Enables RED default parameters if RED is configured; generates an error message if EPD is configured.
`no congestion epd`	Enables RED default parameters if EPD is configured; generates an error message if RED is configured.
`default congestion epd`	Enables EPD default parameters if EPD is configured; generates an error message if RED is configured.

1.52.6 Examples

The following example shows how to specify the RED parameters for an existing profile, **atm-pro:**

```
[local]Redback(config)#atm profile atm-pro

[local]Redback(config-atm-profile)#congestion red min-threshold 1 max-threshold 255
probability 15 weight 10
```

1.53 congestion-map

`congestion-map` ***`map-name`***

`no congestion-map` ***`map-name`***

1.53.1 Purpose

Assigns a congestion avoidance map to an Asynchronous Transfer Mode (ATM) weighted fair queuing (ATMWFQ), a modified deficit round-robin (MDRR), or priority weighted fair queuing (PWFQ) policy.

1.53.2 Command Mode

- ATMWFQ policy configuration

- MDRR policy configuration

- PWFQ policy configuration

1.53.3 Syntax Description

map-name Congestion avoidance map name.

1.53.4 Default

No congestion avoidance map is assigned to any ATMWFQ, MDRR, or PWFQ policy; without a congestion avoidance map assigned, an MDRR or PWFQ policy drops packets from the end of a queue only when the maximum queue depth is exceeded, the queue depth being that of the circuit to which the policy is attached. For an ATMWFQ policy, packets are dropped from the end of a queue according the congestion avoidance specified by the ATM profile assigned to the circuit.

1.53.5 Usage Guidelines

Use the **congestion-map** command to assign a congestion avoidance map to any ATMWFQ, MDRR, or PWFQ policy.

To create a congestion avoidance map, enter the **qos congestion-avoidance-map** command (in global configuration mode).

Use the **no** form of this command to delete the congestion avoidance map from the policy.

1.53.6 Examples

The following example shows how to assign the congestion avoidance map, **map-red4p**, to the PWFQ policy, **pwfq4:**

```
[local]Redback(config)#qos policy pwfq4 pwfq

[local]Redback(config-policy-pwfq)#congestion-map map-red4p

[local]Redback(config-policy-pwfq)#
```

1.54 connected-route

connected-route:

no connected-route

1.54.1 Purpose

Installs a single route that is connected to a specifiable virtual IP address which is contained in the routing table of the current VRRP routing context.

1.54.2 Command Mode

VRRP configuration

1.54.3 Syntax Description

This command has no keywords or arguments.

1.54.4 Default

The **connected-route** command is not enabled.

1.54.5 Usage Guidelines

Use the **connected-route** command to install a single route connected to a specifiable virtual IP address which is contained in the routing table of the current VRRP routing context.

Use the **no** form of this command to remove the virtual IP address connected routes.

1.54.6 Examples

The following example shows that the route connected to virtual IP address `10.1.1.100` has been installed by running the **connected-route** command:

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

[local]Redback(config-if)#ip address 10.1.1.1/24

[local]Redback(config-if)#vrrp 1 backup

[local]Redback(config-vrrp)#connected-route

[local]Redback(config-vrrp_#virtual-address 10.1.1.100

[local]Redback(config-vrrp)#exit

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

1.55 connection-mode

connection-mode {**unencrypted** | **tls** | **tls unencrypted**}

no connection-mode

1.55.1 Purpose

Configures the type of encryption, if any, that the SmartEdge router allows on the connection to the NetOp™ Element Management System (EMS) server.

1.55.2 Command Mode

NetOp configuration

1.55.3 Syntax Description

`tls`	Allows Transport Level Security (TLS) connections, also known as Secure Sockets Layer (SSL) communication, between the SmartEdge router and the NetOp EMS server.
`unencrypted`	Allows unencrypted connections between the SmartEdge router and the NetOp EMS server.

1.55.4 Default

Allow both TLS and unencrypted connections.

1.55.5 Usage Guidelines

Use the **connection mode** command to configure the type of encryption, if any, that the SmartEdge router allows on the connection to the NetOp EMS server.

To allow both TLS and unencrypted communication, include both the **tls** and **unencrypted** keywords in the command or use the **no** form of this command.

The SmartEdge router negotiates the connection mode with the NetOp EMS server immediately after a raw connection is established between the two. In this negotiation, the NetOp EMS server acts as a client and the SmartEdge router acts as the server.

Use the **no** form of this command to return to the default condition.

1.55.6 Examples

The following example shows how to enable communication with the NetOp EMS server and allow either a TLS or unencrypted connection to it:

```
[local]Redback#config

[local]Redback(config)#netop

[local]Redback(config-netop)#connection-mode tls unencrypted
```

1.56 connections

connections {**icmp** | **tcp** | **udp**} **maximum** ***max-sess***

no connections {**icmp** | **tcp** | **udp**}

1.56.1 Purpose

Specifies the maximum number of sessions allowed for the specified protocol for each circuit.

1.56.2 Command Mode

NAT policy configuration

1.56.3 Syntax Description

icmp Specifies the Internet Control Message Protocol (ICMP) as the protocol for which session limit control is to be enabled.

tcp Specifies the Transmission Control Protocol (TCP) as the protocol for which session limit control is to be enabled.

udp Specifies the User Datagram Protocol (UDP) as the protocol for which session limit control is to be enabled.

maximum ***max-sess*** Maximum number of sessions allowed for this protocol for each circuit to which you have applied this Network Address Translation (NAT) policy. The range of values is 1 to 65,535.

1.56.4 Default

The maximum number of sessions is not specified.

1.56.5 Usage Guidelines

Use the **connections** command to specify the maximum number of sessions allowed for the specified protocol for each circuit.

The maximum number that you specify applies to all access control list (ACL) classes, including the default class, for which you have specified admission control using the **admission-control** command (in NAT policy configuration mode).

If the maximum number of sessions for a specific protocol is not specified using this command, the admission control for that protocol, if specified using the **admission-control** command (in NAT policy or policy group class configuration mode), is ignored.

Use the **no** form of this command to specify the default condition.

1.56.6 Examples

The following example shows how to specify **100** as the maximum number of sessions for each TCP circuit:

```
[local]Redback(config-policy-nat)#connections tcp maximum 100
```

1.57 constraint

constraint *name*

no constraint *name*

1.57.1 Purpose

Creates a constraint or specifies a constraint that is applied to the traffic engineering (TE) tunnel during Constrained Shortest Path First (CSPF) calculation.

1.57.2 Command Mode

- RVSP LSP configuration
- RSVP constraint configuration

1.57.3 Syntax Description

name	Name of the CSPF constraint.

1.57.4 Default

No constraint is created or applied.

1.57.5 Usage Guidelines

Use the **constraint** command to create a constraint or specify a constraint that is applied to the TE tunnel during CSPF calculation. Use the commands in RSVP constraint configuration mode to define the constraint. You can define the following constraints:

- Administrative group
- Exclude links
- Hop limit
- Minimum bandwidth
- Priority

Use the **no** form of this command to remove the constraint.

1.57.6 Examples

The following example shows how to create a constraint, `RED_PATH`, for CSPF calculation:

```
[local]Redback#configure

[local]Redback(config)#context local

[local]Redback(config-ctx)#router rsvp

[local]Redback(config-rsvp)#constraint RED_PATH

[local]Redback(config-rsvp-constr)#admin-group include red

[local]Redback(config-rsvp-constr)#exclude node 10.1.1.1

[local]Redback(config-rsvp-constr)#hop-limit 25

[local]Redback(config-rsvp-constr)#minimum-bandwidth 3 mps

[local]Redback(config-rsvp-constr)#priority 5 5
```

The following example shows how to apply the constraint `RED_PATH` to the TE label-switched path (LSP) during CSPF calculation:

```
[local]Redback#config

[local]Redback(config)#context local

[local]Redback(config-ctx)#router rsvp

[local]Redback(config-rsvp)#lsp lsp1

[local]Redback(config-rsvp-lsp)#constraint RED_PATH
```

1.58 context

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

no context ***ctx-name***

1.58.1 Purpose

When entered in exec mode, changes from the existing context to the specified context or displays the specified information for the specified context.

When entered in global configuration mode, creates a new context, or selects an existing one for modification, and enters context configuration mode.

1.58.2 Command Mode

- Exec
- Global configuration

1.58.3 Syntax Description

`ctx-name`	Name of a new or existing context; an alphanumeric string with up to 63 characters.
`show show-param`	Optional. Type of information to be displayed for the specified context.

1.58.4 Default

The local context is defined on the system.

1.58.5 Usage Guidelines

The action of the `context` command depends on the mode in which it is executed:

- In exec mode, use the `context` command to change to a different context and enter context configuration mode. Include the `show show-param` construct to display information for the specified context without entering that context.

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

- In global configuration mode, use the `context` command to create a new context or specify an existing context or the domain alias of an existing context and enter context configuration mode.

  You cannot create new contexts on the system unless you have enabled the multiple context feature using the `service multiple-contexts` command (in global configuration mode).

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

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

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

1.58.6 Examples

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

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

The following example displays IP route information for the **local** context:

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

Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP,
I B - IBGP, O - OSPF, IA - OSPF inter area,
N1 - OSPF NSSA external type 1

N2 - OSPF NSSA external type 2, E1 - OSPF external type 1

E2 - OSPF external type 2

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2

> - Active Route

Type Network Next Hop Dist Metric UpTime Interface
> C 10.3.0.0/16 0 0 01:01:50 three
> C 10.13.49.0/24 0 0 01:01:50 mgmt
> S 155.0.0.0/8 10.13.49.254 1 0 01:01:39 mgmt
> C 193.4.0.0/16 0 0 01:01:50 one
> C 193.10.25.7/32 0 0 01:01:50 lo1
```

The following example shows how to use the domain alias `subs1234` to enter the context configuration mode for the context named **blanch**. For more information on the domain alias, see the description of the **domain** command:

```
[local]Redback(config)#context subs1234
[local]Redback(config-ctx)#show context

Context Name          Context ID        VPN-RD    Description

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

blanch 0x40080005
```

1.59 context-filter ifmib

`context-filter ifmib`

`no context-filter ifmib`

1.59.1 Purpose

Restricts Simple Network Management Protocol (SNMP) responses to circuits bound to the context assigned to the community or group that sends the query.

1.59.2 Command Mode

SNMP server configuration

1.59.3 Syntax Description

This command has no keywords or arguments.

1.59.4 Default

Context filtering is not applied to SNMP responses.

1.59.5 Usage Guidelines

Use the **`context-filter ifmib`** command to restrict SNMP responses to circuits bound to the context assigned to the community or group that sends the query. Information about circuits bound to other contexts is not reported.

The **`context-filter ifmib`** command applies only to the following types of circuits:

- 802.1Q permanent virtual circuits (PVCs)
- Asynchronous Transfer Mode (ATM) PVCs
- Frame Relay data-link connection identifier (DLCI) PVCs

If the SNMP community or group that sends the SNMP query is local or the context assigned to the SNMP community is local, the SNMP agent sends back information about circuits regardless of their binding.

1.59.6 Examples

The following example shows how to enable the SmartEdge router to send context-specific IF-MIB responses to SNMP queries:

```
[local]Redback(config)#snmp server
[local]Redback(config-snmp-server)#context-filter ifmib
```

1.60 context vpn-rd

`context` ***`ctx-name`*** **`vpn-rd`** ***`route-distinguisher`***

1.60.1 Purpose

Creates a new Virtual Private Network (VPN) context, or selects an existing one for modification, and enters context configuration mode.

1.60.2 Command Mode

Global configuration

1.60.3 Syntax Description

`ctx-name`

Name of a new or existing context; an alphanumeric string with up to 63 characters.

`route-distinguisher`

VPN route-distinguisher, which can be expressed in either of the following formats:

- ***`asn`*****`:`*****`nnnn`***, where ***`asn`*** is the autonomous system number and ***`nnnn`*** is a 32-bit integer.
- ***`ip-addr`*****`:`*****`nn`***, where ***`ip-addr`*** is the IP address in the form ***`A.B.C.D`*** and ***`nn`*** is a 16-bit integer.

1.60.4 Default

None. A route distinguisher must be configured for a VPN context to be functional.

1.60.5 Usage Guidelines

Use the **`context vpn-rd`** command to create a new VPN context, or select an existing one for modification, and enter context configuration mode. You cannot create new contexts on the system unless you have enabled the multiple context feature using the **`service multiple-contexts`** command (in global configuration mode).

Entering the full **`context vpn-rd`** command is required to create a VPN context. Entering the command without the **`vpn-rd`** ***`route-distinguisher`*** construct creates a context that will not be recognized as VPN-enabled.

Each VPN context supports only one route distinguisher, and the ***`route distinguisher`*** argument must conform to the format specified in Internet Draft, `BGP/MPLS VPNs`, draft-ietf-ppvpn-rfc2547bis-01.txt.

An existing non-VPN context cannot be configured as a VPN context. You must delete the existing non-VPN context, and recreate it as a VPN context. Likewise, a VPN context cannot be configured as a non-VPN context. You must delete the existing VPN context, and recreate it as a non-VPN context.

Note: Each VPN context only supports one route distinguisher, and the route distinguisher must conform to the format specified in Internet Draft, `BGP/MPLS VPNs`, draft-ietf-ppvpn-rfc2547bis-01.txt.

1.60.6 Examples

The following example shows how to create a VPN context **vpncontext** with the route distinguisher **701:3**:

```
[local]Redback(config)#context vpncontext vpn-rd 701:3

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

The following example shows how to create a multicast VPN context **mvpn** with the route distinguisher **1:1**. In this example, a point-to-point intercontext interface **test-if** is defined for interfacing to the default multicast distribution tree (MDT) group. This interface is assigned intercontext group number **1** and IP address **10.10.10.1/32**. The MDT default group is then specified with IP address **232.1.1.1**:

```
[local]Redback(config)#context test-mvpn vpn-rd 1:1

[local]Redback(config-ctx)#interface test-if intercontext p2p 1

[local]Redback(config-if)#ip address 10.10.10.1/32

[local]Redback(config-if)#mdt default-group 232.1.1.1
```

1.61 continue

`continue` [***`seq-num`***]

1.61.1 Purpose

Passes execution control to a different entry in the route map and continuing execution at that entry.

1.61.2 Command Mode

Route map configuration

1.61.3 Syntax Description

seq-num	Optional. Sequence number of the route map entry to pass control to if **`continue`** is executed. This value must be greater than the sequence number of the current route map entry. The range is 1 to 4294967295.

1.61.4 Default

If **`continue`** is executed and no ***`seq-num`*** is specified, control is passed to the route map entry with the next highest sequence number.

1.61.5 Usage Guidelines

Use **`continue`** within a route map entry to allow execution to continue if the match conditions in the entry succeed (or no match conditions are specified).

If **`continue`** is not included, execution stops when all match conditions in the route map entry are satisfied and any **`set`** clauses in the entry have been applied. If any match conditions within the entry fail, control flows to the route map entry with the next highest sequence number; no **`set`** operations are applied in this case.

If the **`continue`** clause is present but no match conditions are specified, any **`set`** operations within the entry are applied and then control flows to the route map entry specified by the ***`seq-num`*** argument. If the ***`seq-num`*** is not specified, control flows to the route map entry with the next highest sequence number.

If the **`continue`** clause is present and at least one match condition has been specified, the specified **`set`** operations are applied if all match conditions are satisfied. Control then flows to the route map entry specified by the ***`seq-num`*** argument. If not specified, control flows to the route map entry with the next highest sequence number. If any match condition in the entry fails, the **`set`** operations and the **`continue`** clause are ignored. Control is passed to the route map entry with the next highest sequence number.

If a **`set`** operation is applied and a **`continue`** clause passes control to another route map entry, the modified route attribute is used in the new route map entry for any match conditions or **`set`** operations. For **`set`** operations that affect attributes with absolute values (for example, **`set metric`**), the existing attribute value is overwritten. For **`set`** operations that affect attributes with cumulative values (for example, **`set community additive`**), the value is appended to the existing attribute value.

If all match conditions succeed and a **`continue`** clause passes control to subsequent route map entries where matches are unsuccessful, the default **`deny`** action is taken, even if one of the route map entries successfully matched, and the decision taken to **`permit`** a route is reset after a **`continue`** occurs.

If all match conditions in a route map entry with a **`deny`** action are successful, the route is denied and all **`set`** operations are ignored.

1.61.6 Examples

The following example uses the **`continue`** clause to affect execution flow within a route map.

If a successful match occurs in route map entry 10, the AS path is prepended with 10 and execution continues at route map entry 30. In route map entry 30, the AS path is prepended with 12 (so that the new AS path is 12 10), and the metric is set to 10.

If the match in route map entry 10 is not successful, control is passed to route map entry 20. If a successful match occurs in route map entry 20, the AS path is prepended with 11 and execution flows to route map entry 30, where the AS path is then prepended with 12 (so that the new AS path is 12 11), and the metric is set to 10.

If the match in route entry 10 is unsuccessful and the match in route map entry 20 is unsuccessful, the AS path is set to 12, and the metric is set to 10.

```
[local]Redback(config-ctx)#route-map MAP1 permit 10
[local]Redback(config-route-map)#match ip address prefix-list p1
[local]Redback(config-route-map)#set as-path prepend 10
[local]Redback(config-route-map)#continue 30
[local]Redback(config-croute-map)#exit
[local]Redback(config-ctx)#route-map MAP1 permit 20
[local]Redback(config-route-map)#match ip address prefix-list p2
[local]Redback(config-route-map)#set as-path prepend 11
[local]Redback(config-route-map)#continue
[local]Redback(config-croute-map)#exit
[local]Redback(config-ctx)#route-map MAP1 permit 30
[local]Redback(config-route-map)#set as-path prepend 12
[local]Redback(config-route-map)#set metric 10
[local]Redback(config-croute-map)#exit
```

1.62 control-word

control-word [**sequence-number** [**zero**]]

no control-word [**sequence-number** [**zero**]]

1.62.1 Purpose

Enables the inclusion of a control word in the packet header.

1.62.2 Command Mode

- L2VPN XC group configuration
- L2VPN profile peer configuration mode
- VPLS profile neighbor configuration

1.62.3 Syntax Description

`sequence-number` Optional. Enables sequence number support on packets on AAL2 PWs.(1)

`zero` Optional. Disables sequence number support on AAL2 packets.(2)

*(1) The **sequence-number** keyword is supported for AAL2 PWs only.*

*(2) The **zero** keyword is supported for AAL2 PWs only. For all other (non-AAL2) PW types, the sequence number is not supported and is disabled by default.*

1.62.4 Default

For AAL5 PWs, the control word is always included in the packet header.

1.62.5 Usage Guidelines

The `control-word` command enables the inclusion of a control word in the packet header. For AAL2 PWs, this command can also be used to enable or disable the inclusion of incremental sequence numbers that ensure disassembled packets are reassembled properly.

Note: The `control word` command in L2VPN XC group configuration mode is supported for AAL2 pseudowires (PWs) only. The `control word` command in L2VPN profile peer configuration mode is supported for all PW types (including AAL2 PWs) that have an L2VPN profile attached.

You can enable the inclusion of a control word in the packet header of a PW. The 4-byte control word is inserted after the PW label. The control word contains the following fields:

- For AAL2 PWs that have a sequence number enabled, a 16-bit packet sequence number that is used to detect packet reordering and packet loss (if the sequence number is enabled). Note that for all other non-AAL2 PWs, sequence number support is disabled.
- Payload length

The sequence number contains 16 bits and ranges from 1 through 65535. Sequence numbers are added to the control word in an incremental fashion, and the number wraps to 1 after reaching the maximum value. The inclusion of a sequence number ensures that any disassembled packets are reordered properly.

To disable the inclusion of a sequence number on an AAL2 PW, enter the `control-word sequence-number zero` command.

After you enable the inclusion of the control word in the packet header, a single control word is included for each cross-connection group. The control word is applied to all pseudowires that are configured under the particular group. Do not apply the `control word` command to any PWs that have Frame Relay or

AAL5 encapsulation enabled because those PWs always have the control word included in the packet header by default.

1.62.6 Examples

The following example shows how to enable the inclusion of a control word in the ATM packet header for an L2VPN cross-connection group called `atmgroup1`:

```
[local]Redback(config-ctx)#l2vpn

[local]Redback(config-l2vpn)#xc-group atmgroup1

[local]Redback(config-l2vpn-xc-group)#control-word
```

The following example shows how to enable the inclusion of a control word and a sequence number in the ATM packet header for an L2VPN cross-connection group called `atmgroup1`:

```
[local]Redback(config-ctx)#l2vpn

[local]Redback(config-l2vpn)#xc-group atmgroup1

[local]Redback(config-l2vpn-xc-group)#control-word sequence-number
```

The following example shows how to disable the inclusion of a sequence number in the ATM packet header for an L2VPN cross-connection group called `atmgroup1`:

```
[local]Redback(config-ctx)#l2vpn

[local]Redback(config-l2vpn)#xc-group atmgroup1

[local]Redback(config-l2vpn-xc-group)#control-word sequence-number zero
```

The following example shows how to disable the inclusion of a control word in the ATM packet header for an L2VPN cross-connection group called `atmgroup1`:

```
[local]Redback(config-ctx)#l2vpn

[local]Redback(config-l2vpn)#xc-group atmgroup1

[local]Redback(config-l2vpn-xc-group)#no control-word
```

1.63 copy

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

1.63.1 Purpose

Copies a file from a remote file server to the SmartEdge router from the SmartEdge router to a file server, or from one location to another on the local SmartEdge router file system on either the active or standby controller card.

1.63.2 Command Mode

Exec (10)

1.63.3 Syntax Description

mate	Optional. Specifies that the source file is on the other controller card.
src-url	URL of the file to be copied.
dest-url	URL of the destination of the copy operation.
passive	Optional. Specifies passive mode for the File Transfer Protocol (FTP).
-noconfirm	Optional. Avoids a confirmation prompt when overwriting an existing file on the local file system.
clear	If ***src-url*** is the ISP log file, clears the contents of the local ISP log file after the file is copied successfully. If the system stops logging ISP entries because the ISP file reaches the size limit, this keyword causes the system to resume ISP logging. This keyword is only available in exec (15) mode.

1.63.4 Default

None

1.63.5 Usage Guidelines

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

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

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

Note: The SmartEdge 100 router does not support standby controller cards; therefore, the mate keyword is not applicable.

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

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

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

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

Note: This procedure assumes that a system exists that is reachable by the SmartEdge router to service these requests.

Table 12 describes the syntax for the *url* argument when copying the file to a remote server.

Table 12 Syntax for the url Argument in the copy Command

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

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

The *filename* argument can be up to 256 characters in length. You can only use the *hostname* argument if Domain Name System (DNS) is enabled with the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands (in context configuration mode); see *Configuring DNS*.

Use the **clear** keyword to extract the ISP log file from the system. You cannot use FTP or RCP to extract the ISP log file from the system. If ***src-url*** is the ISP log file, this keyword clears the contents of the local ISP log file, after the file is copied out successfully. The ISP log file is available at /flash/.isp.log. If the system stopped logging ISP entries because the file reached the size limit set using the **isp-log size** command, this keyword causes the system to resume ISP logging.

1.63.6 Examples

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

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

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

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

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

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

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

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

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

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

The following example copies the ISP log file to a remote server and subsequently clears the contents of the local ISP file:

```
[local]Redback#copy /flash/.isp.log ftp://john:test@192.168.145.99/.isp.log clear
```

1.64 cost (OSPF)

`cost` *`cost`*

{**`no`** | **`default`**} **`cost`**

1.64.1 Purpose

Configures the cost used in Shortest Path First (SPF) computations for the specified interface, or sham link.

1.64.2 Command Mode

- OSPF interface configuration
- OSPF sham link configuration
- OSPF3 interface configuration

1.64.3 Syntax Description

`cost`	Interface or sham link cost. The range of values is 1 to 65,535. By default, the value set by the **`auto-cost`** command (in OSPF or OSPF3 router configuration mode) is used. If the auto cost is not configured, the default cost is 1.

1.64.4 Default

If this command is not enabled, the value specified through the **`auto-cost`** command is used. If the auto cost is not configured, the cost value is 1.

1.64.5 Usage Guidelines

Use the **`cost`** command to configure the cost used in SPF computation for the specified interface, or sham link.

The lower the cost, the more likely the interface, or sham link, is to be used to forward data traffic. You can assign only one cost per interface.

Use the **`no`** or **`default`** form of this command to return the cost to its default value.

1.64.6 Examples

The following example shows how to configure the cost of **3** for the **ospf1** interface:

```
[local]Redback(config-ospf)#interface ospf1

[local]Redback(config-ospf-if)#cost 3
```

1.65 cost (spanning-tree)

`cost` ***`cost-value`***

{**`no`** | **`default`**} **`cost`**

1.65.1 Purpose

Sets the Rapid Spanning Tree Protocol (RSTP) cost of the associated port.

1.65.2 Command Mode

Spanning-tree profile configuration

1.65.3 Syntax Description

`cost-value`	The RSTP cost of the associated port. The range of values is 1 to 200,000,000.

1.65.4 Default

The system automatically assigns a cost to the port, depending on its speed.

1.65.5 Usage Guidelines

Use the **`cost`** command to set the RSTP cost of the associated port.

1.65.6 Examples

The following example illustrates how the **`spanning-tree profile`** command creates the spanning-tree profile **prof1** and sets its cost to the value `5000`. In the second part of the example, an Ethernet port is assigned the spanning-tree profile **prof1** and therefore the spanning-tree cost of bridging to the port is set at `5000`:

```
[local]Redback(config)#spanning-tree profile prof1
[local]Redback(config-stp-prof)#cost 5000
[local]Redback(config-stp-prof)#exit
[local]Redback(config)#port ethernet 1/1
[local]Redback(config-port)#spanning-tree profile prof1
```

1.66 count exclude subscriber

count exclude subscriber layer-2 [**ppp-pppoe-control**]

{**no** | **default**} **count exclude subscriber layer-2** [**ppp-pppoe-control**]

1.66.1 Purpose

Excludes Layer 2 header data only, or Layer 2 header data, Point-to-Point Protocol (PPP) control data, and PPP over Ethernet (PPPoE) control data from subscriber statistics collection.

1.66.2 Command Mode

Stats collection configuration

1.66.3 Syntax Description

layer-2	Excludes Layer 2 header data only.
ppp-pppoe-control	Optional. Excludes Layer 2 header and PPP and PPPoE control data.

1.66.4 Default

All data in the subscriber packet is included in statistics collection.

1.66.5 Usage Guidelines

Use the **count exclude subscriber** command to exclude Layer 2 header data only, or Layer 2 header data, PPP control data, and PPPoE control data from subscriber statistics collection.

Use the **layer-2** keyword to exclude Layer 2 header data only. Use the **ppp-pppoe-control** keyword to exclude Layer 2 header data and PPP and PPPoE control data.

Use the **no** or **default** form of this command to include Layer 2 header data and PPP and PPPoE control data in the statistics collection.

1.66.6 Examples

The following example shows how to exclude both Layer 2 header data and PPP and PPPoE control data from statistics collection:

```
[local]Redback(config)#stats-collection
[local]Redback(config-stats-collect)#count exclude subscriber layer-2  ppp-pppoe-control
```

1.67 counters (ATM)

`counters l2`

{**`no`** | **`default`**} **`counters`**

1.67.1 Purpose

Enables statistics to be collected for Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs) that reference the ATM profile.

1.67.2 Command Mode

ATM profile configuration

1.67.3 Syntax Description

`l2`	Enables statistics collection for Layer 2 traffic, both at the cell and segmentation and reassembly (SAR) packet level.

1.67.4 Default

ATM counters are enabled.

1.67.5 Usage Guidelines

Use the **`counters`** command to enable or disable the collection of statistics for ATM PVCs that reference the ATM profile.

This command is useful if the profile is referenced by ATM PVCs that are used for OAM traffic (VCIs 1 to 31).

Use the **`no`** or **`default`** form of this command to disable statistics collection for PVCs that reference the profile.

1.67.6 Examples

The following example shows how to configure an ATM profile, `low_rate`, to enable statistics collection for Layer 2 traffic (**l2**) on all ATM PVCs that reference the profile:

```
[local]Redback(config)#atm profile low_rate

[local]Redback(config-atm-profile)#counters l2
```

1.68 counters (malicious traffic)

`counters`

`no counters`

1.68.1 Purpose

Enables the generation of malicious-traffic counters.

1.68.2 Command Mode

Malicious-traffic context configuration mode

1.68.3 Syntax Description

This command has no keywords or arguments.

1.68.4 Default

Malicious-traffic counters is disabled by default.

1.68.5 Usage Guidelines

Use the **`counters`** command to enable the generation of malicious-traffic counters.

Use the **`no`** form of this command to disable malicious-traffic counters.

For more information about malicious traffic counters, see *Configuring Malicious Traffic Detection and Monitoring*.

1.68.6 Examples

The following example shows how to enable the collection of malicious traffic statistics:

```
[local]Redback(config-ctx-malicious-traffic)#counters
```

1.69 counters (VPLS)

counters

no counters

1.69.1 Purpose

Enables circuit statistics for Virtual Private LAN Services (VPLS) circuits.

1.69.2 Command Mode

VPLS profile neighbor configuration

1.69.3 Syntax Description

This command has no keywords or arguments.

1.69.4 Default

VPLS pseudowire circuit counters are disabled.

1.69.5 Usage Guidelines

Use the **counters** command to enable circuit statistics for VPLS circuits.

When enabled, packet receive and transmit statistics are collected for each pseudowire circuit associated with this neighbor.

Use the **show circuit counters vpls** command (in any mode) to display packet counter information for VPLS circuits.

Use the **no** form of this command to disable circuit statistics for VPLS circuits.

1.69.6 Examples

The following example shows how to enable circuit statistics for VPLS circuits:

```
[local]Redback#config

[local]Redback(config)#vpls profile prof1

[local]Redback(config-vpls-profile)#neighbor 10.10.10.1

[local]Redback(config-vpls-profile-neighbor)#counters

[local]Redback(config-vpls-profile-neighbor)#
```

1.70 crc16

```
crc16

no crc16
```

1.70.1 Purpose

Specifies a 16-bit cyclic redundancy check (CRC) on a Packet over SONET/SDH (POS) port.

1.70.2 Command Mode

Port configuration

1.70.3 Syntax Description

This command has no keywords or arguments.

1.70.4 Default

A 32-bit CRC is used.

1.70.5 Usage Guidelines

Use the `crc16` command to specify a 16-bit CRC on a POS port configured with either Synchronous Optical Network (SONET) or Synchronous Digital Hierarchy (SDH) framing. We recommend a 32-bit CRC.

This command applies only to a POS port on an OC-48c/STM-16c traffic card, OC-12c/STM-4c traffic card, or OC-3c/STM-1c traffic card.

Note: The SmartEdge 100 router does not support POS ports.

Use the **no** form of this command to specify a 32-bit CRC.

1.70.6 Examples

The following example shows how to specify a 16-bit CRC for a POS port in slot 9:

```
[local]Redback(config)#port pos 9/1

[local]Redback(config-port)#crc16
```

1.71 crc32

crc32

no crc32

1.71.1 Purpose

Sets the cyclic redundancy check (CRC) length to 32 bits for the High-Level Data Link Control (HDLC) frame for a clear-channel DS-3 channel or port, E3 port, DS-1 channel, E1 channel or port, or DS-0 channel group.

1.71.2 Command Mode

- DS-0 group configuration
- DS-1 configuration
- DS-3 configuration
- E1 configuration
- E3 configuration

1.71.3 Syntax Description

This command has no keywords or arguments.

1.71.4 Default

The default CRC length is 16 bits.

1.71.5 Usage Guidelines

Use the **crc32** command to set the CRC length to 32 bits for the HDLC frames for a clear-channel DS-3 channel or port, E3 port, DS-1 channel, E1 channel or port, or DS-0 channel group. The CRC determines if there have been any errors in data transmission, reading, or writing.

Use the **no** form of this command to set the CRC length to 16 bits.

1.71.6 Examples

The following example shows how to set the CRC length to 32 bits:

```
[local]Redback(config)#port ds3 3/1

[local]Redback(config-ds3)#crc32
```

1.72 create-lsp-circuit

create-lsp-circuit

no create-lsp-circuit

1.72.1 Purpose

Enables the creation of pseudocircuits for Label Distribution Protocol (LDP) label-switched paths (LSPs).

1.72.2 Command Mode

LDP router configuration

1.72.3 Syntax Description

This command has no keywords or arguments.

1.72.4 Default

Pseudocircuits are not created for LDP LSPs.

1.72.5 Usage Guidelines

Use the **create-lsp-circuit** command to enable the creation of pseudocircuits for LDP LSPs. Before packet statistics for LDP LSPs can be collected, pseudocircuits for the LDP LSPs must first be created.

Note: Resource Reservation Protocol (RSVP) LSP circuit creation is always enabled.

Use the **no** form of this command to disable the creation of pseudocircuits for LDP LSPs.

1.72.6 Examples

The following example shows how to enable the creation of pseudocircuits for LDP LSPs:

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

[local]Redback(config-ctx)#router ldp

[local]Redback(config-ldp)#create-lsp-circuit

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

1.73 csnp interval

csnp interval *seconds* [**level-1** | **level-2**]

no csnp interval

1.73.1 Purpose

Configures the interval at which complete sequence number protocol data units (CSNPs) are sent over the interface.

1.73.2 Command Mode

IS-IS interface configuration

1.73.3 Syntax Description

seconds	Interval of time, in seconds, between transmission of CSNPs on multiaccess networks. The range of values is 1 to 65535; the default value is 10 seconds.
`level-1`	Optional. Configures the CSNP interval for level 1 independently.
`level-2`	Optional. Configures the CSNP interval for level 2 independently.

1.73.4 Default

CSNP packets are sent over LAN interfaces every 10 seconds. CSNPs are not sent over point-to-point (P2P) interfaces. When you enter this command without specifying either IS-IS level 1 or level 2 routing, CSNPs are sent at the same interval for both IS-IS levels.

1.73.5 Usage Guidelines

Use the **`csnp interval`** command to configure the interval at which CSNPs are sent over the interface. By default, CSNP packets are sent over LAN interfaces every 10 seconds. To enable the sending of CSNP packets on P2P interfaces, use the **`csnp periodic-on-ptp`** command in IS-IS interface configuration mode.

CSNPs contain a list of all link-state protocol data unit (LSP) packets in the database. An IS-IS system receiving CSNPs can compare this information with its own LSP database to determine whether it and the CSNP transmitter have synchronized LSP databases.

A shorter interval allows faster convergence; however, it increases bandwidth and CPU usage, and can add to instability in the network. In addition to saving bandwidth and CPU usage, a longer interval can increase overall network stability.

Use the **`no`** form of this command to restore the default interval at which CSNPs are sent over the interface.

1.73.6 Examples

The following example shows how to configure the CSNP interval on the **fa4/1** interface at **15** seconds for IS-IS **level-1** routing only:

```
[local]Redback(config-ctx)#router isis ip-backbone

[local]Redback(config-isis)#interface fa4/1

[local]Redback(config-isis-if)#csnp interval 15 level-1
```

1.74 csnp periodic-on-ptp

```
csnp periodic-on-ptp
```

```
no csnp periodic-on-ptp
```

1.74.1 Purpose

Enables periodic complete sequence number protocol data units (CSNPs) to be sent on the point-to-point (P2P) interface.

1.74.2 Command Mode

IS-IS interface configuration

1.74.3 Syntax Description

This command has no keywords or arguments.

1.74.4 Default

The command is disabled.

1.74.5 Usage Guidelines

Use the `csnp periodic-on-ptp` command to enable periodic CSNPs to be sent on a P2P interface. Sending periodic CSNPs on P2P interfaces can increase the stability of the network, especially when flooding topology has been heavily pruned.

Use the `csnp interval` command in IS-IS interface configuration mode to modify the interval at which CSNPs are sent over the interface.

Use the `no` form of this command to disable the sending of CSNPs on a P2P interface.

1.74.6 Examples

The following example shows how to enable sending periodic CSNPs for IS-IS **level-1** only on the **fa4/1** interface:

```
[local]Redback(config-ctx)#router isis ip-backbone
[local]Redback(config-isis)#interface fa4/1
[local]Redback(config-isis-if)#csnp periodic-on-ptp level-1
```

1.75 cspf

cspf

no cspf

1.75.1 Purpose

Specifies that the Constrained Shortest Path First (CSPF) algorithm calculates the traffic engineering (TE) label-switched path (LSP).

1.75.2 Command Mode

RSVP LSP configuration

1.75.3 Syntax Description

This command has no keywords or arguments.

1.75.4 Default

CSPF calculation is disabled.

1.75.5 Usage Guidelines

Use the **cspf** command to enable CSPF calculation on the TE LSP.

Use the **no** form of this command to disable CSPF calculation.

1.75.6 Examples

The following example shows how to enable CSPF calculation:

```
[local]Redback#config

[local]Redback(config)#context local

[local]Redback(config-ctx)#router rsvp

[local]Redback(config-rsvp)#lsp lsp1

[local]Redback(config-rsvp-lsp)#cspf
```