Commands: shoz through sz

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 “shoz” through commands starting with “sz” 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 shutdown (ATM)

`shutdown`

`no shutdown`

1.1.1 Purpose

Disables the specified Asynchronous Transfer Mode (ATM) OC, Ethernet, or Packet over SONET/SDH (POS) port.

1.1.2 Command Mode

- ATM OC configuration
- Port configuration

1.1.3 Syntax Description

This command has no keywords or arguments.

1.1.4 Default

All ports are disabled.

1.1.5 Usage Guidelines

Use the **shutdown** command to enable or disable the specified ATM, Ethernet, or POS port. No data is transmitted or received when the port is disabled (shut down).

Note: You must enable POS port before adding it to an Automatic Protection Switching (APS) group.

Note: By default, any ATM permanent virtual circuits (PVCs) that you configure on an ATM port are enabled, but you must enable the port for them to function.

Use the **no** form of this command to enable a port and have data transmitted or received on the port.

To display the port or channel state, enter the **show port detail** command (in any mode).

This command is also described in:

- *Configuring Circuits* for ATM, Frame Relay, and 802.1Q permanent virtual circuits (PVCs).
- *Configuring Cross-Connections* for cross-connected circuits.
- *Configuring GRE Tunnels* for Generic Routing Encapsulation (GRE) tunnel circuits.

1.1.6 Examples

The following example shows how to enable port `1` in for the Ethernet line card installed in slot `2`:

```
[local]Redback(config)#port ethernet 2/1

[local]Redback(config-port)#no shutdown
```

1.2 shutdown (BGP)

```
shutdown

no shutdown
```

1.2.1 Purpose

Administratively shuts down the Border Gateway Protocol (BGP) session with the specified neighbor or peer group.

1.2.2 Command Mode

- BGP neighbor configuration
- BGP peer group configuration

1.2.3 Syntax Description

This command has no keywords or arguments.

1.2.4 Default

None

1.2.5 Usage Guidelines

Use the **`shutdown`** command to administratively shut down the BGP session with the specified neighbor or peer group. This command is useful to temporarily shut down a session without removing the BGP neighbor from the SmartEdge router configuration.

Use the **`no`** form of this command to restore the BGP session between the SmartEdge router and the specified neighbor.

1.2.6 Examples

The following example shows how to administratively shut down the BGP session with the neighbor at IP address `10.100.3.2:`

```
[local]Redback(config-ctx)#router bgp 64001

[local]Redback(config-bgp)#neighbor 10.100.3.2 external

[local]Redback(config-bgp-neighbor)#shutdown
```

1.3 shutdown (Card)

`shutdown`

```
no shutdown
```

1.3.1 Purpose

Takes the I/O carrier card, services card, or line card out of service.

1.3.2 Command Mode

- Card configuration mode

1.3.3 Syntax Description

This command has no keywords or arguments.

1.3.4 Default

The I/O carrier card, services card, or line card is in service.

1.3.5 Usage Guidelines

Use the `shutdown` command to take the specified I/O carrier card, services card, or line card out of service in preparation for an on-demand diagnostic (ODD) session. No data is transmitted or received on any port when the line card is out of service.

In the current release, you can test the following SmartEdge router line cards:

- ATM OC-12c/STM-3c, and second-generation ATM OC line cards
- Fast Ethernet-Gigabit Ethernet line cards
- Gigabit Ethernet (any version)
- SONET/SDH OC-3c/STM-1c, OC-12c/STM-4c, OC-48c/STM-16c, OC-192c/STM-64c line cards
- Advanced Services Engine

You can test the following SmartEdge 100 cards:

- Controller carrier card (Ethernet management port)
- I/O carrier card and MICs (native ports, MIC ports)

Note: The state of each port on the carrier card or line card, including any cross-connected circuits, is saved to allow it to be restored after the line card is placed in service.

Note: The correspondence between the card name that appears in the CLI and the line card type is found in the *Card Types* section of the **`Configuring Cards`** document.

Use the **`no`** form of this command to put the card in service and restore the operational state of its ports.

To display the port state, enter the **`show port detail`** command (in any mode).

1.3.6 Examples

The following example shows how to take the Ethernet line card installed in slot `3` out of service:

```
[local]Redback#configure

[local]Redback(config)#card ge-5-port 3

[local]Redback(config-card)#shutdown
```

1.4 shutdown (Channel)

`shutdown`

`no shutdown`

1.4.1 Purpose

Disables the specified channel or channel group.

1.4.2 Command Mode

- DS-0 group configuration
- DS-1 configuration
- DS-3 configuration
- E1 configuration
- E3 configuration
- STM-1 configuration

1.4.3 Syntax Description

This command has no keywords or arguments.

1.4.4 Default

All channels are disabled.

1.4.5 Usage Guidelines

Use the **shutdown** command to enable or disable the specified channel or channel group.

No data is transmitted or received when the channel or channel group is shut down. You must use the **no** form of this command to enable any channel or channel group.

To display the channel state, enter the **show port detail** command (in any mode).

Use the **no** form of this command to enable a channel or channel group.

1.4.6 Examples

The following example shows how to enable DS-3 channel `1` on channelized OC-3 port `1` in slot `14`:

```
[local]Redback(config)#card ch-oc3oc12-8or2-port 14
[local]Redback(config-card)#exit
[local]Redback(config)#port channelized-oc3 14/1 pos
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#port ds3 14/1:1
[local]Redback(config-ds3)#no shutdown
```

1.5 shutdown (Mobile IP)

shutdown

no shutdown

1.5.1 Purpose

Disables or enables the foreign-agent (FA) instance, home-agent (HA) peer, or mobile node (MN) access to the SmartEdge router for an FA instance.

1.5.2 Command Mode

- FA configuration
- HA peer configuration
- Mobile IP interface configuration

1.5.3 Syntax Description

This command has no keywords or arguments.

1.5.4 Default

All FA instances, HA peers, and Mobile IP interfaces are enabled.

1.5.5 Usage Guidelines

Use the **shutdown** command to disable the FA instance, the HA peer, or the MN interface for an FA instance.

Use the **no** form of this command to enable the FA instance, the HA peer, or the MN interface for an FA instance.

1.5.6 Examples

The following example shows how to disable an FA instance:

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

[local]Redback(config-ctx)#router mobile-ip

[local]Redback(config-mip)#foreign-agent

[local]Redback(config-mip-fa)#shutdown
```

The following example shows how to disable an HA peer:

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

[local]Redback(config-ctx)#router mobile-ip

[local]Redback(config-mip)#foreign-agent

[local]Redback(config-mip-fa)#home-agent-peer 172.16.2.1

[local]Redback(config-mip-hapeer)#shutdown
```

The following example shows how to disable the MN interface for an FA instance:

```
[local]Redback(config-ctx)#router mobile-ip

[local]Redback(config-mip)#interface mn-access

[local]Redback(config-mip-if)#shutdown
```

1.6 shutdown (MSDP peers)

shutdown

no shutdown

1.6.1 Purpose

Disables a configured Multicast Source Discovery Protocol (MSDP) peer.

1.6.2 Command Mode

MSDP peer configuration

1.6.3 Syntax Description

This command has no keywords or arguments.

1.6.4 Default

The peer is up when configured.

1.6.5 Usage Guidelines

Use the **shutdown** command to disable a configured MSDP peer.

Use the **no** form of this command to bring up a configured MSDP peer.

1.6.6 Examples

The following example shows how to disable an MSDP peer:

```
[local]Redback(config-ctx)#router msdp
[local]Redback(config-msdp)#peer 10.200.1.2 local-tcp-source lo1
[local]Redback(config-msdp-peer)#shutdown
```

1.7 shutdown (Port)

shutdown

no shutdown

1.7.1 Purpose

Disables the specified port.

1.7.2 Command Mode

Port configuration

1.7.3 Syntax Description

This command has no keywords or arguments.

1.7.4 Default

All ports and channels are disabled.

1.7.5 Usage Guidelines

Use the **shutdown** command to enable or disable the specified port.

No data is transmitted or received when the port is shut down. You must use the **no** form of this command to enable any port.

To display the port state, enter the **show port detail** command (in any mode).

Use the **no** form of this command to enable a port.

1.7.6 Examples

The following example shows how to enable the first ATM port in slot 42:

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

[local]Redback(config-atm-oc)#no shutdown
```

The following example shows how to enable the Ethernet port 1 in slot 2.:

```
[local]Redback(config)#port ethernet 2/1

[local]Redback(config-port)#no shutdown
```

1.8 shutdown (PVC)

shutdown

no shutdown

1.8.1 Purpose

Disables the specified link group or Asynchronous Transfer Mode (ATM), Frame Relay, or 802.1Q permanent virtual circuit (PVC).

1.8.2 Command Mode

- ATM PVC configuration
- dot1q PVC configuration
- Frame Relay PVC configuration
- Link group configuration

- Link PVC configuration

1.8.3 Syntax Description

This command has no keywords or arguments.

1.8.4 Default

All PVCs are enabled.

1.8.5 Usage Guidelines

Use the **`shutdown`** command to disable the specified link group or ATM, Frame Relay, or 802.1Q PVC. No data is transmitted or received when a PVC or link group is shut down.

Note: The SmartEdge 100 router does not support Frame Relay or ATM PVCs.

Use the **`no`** form of this command to enable anATM PVC, Frame Relay PVC, 802.1Q PVC, or link group.

Note: You must also enable the port, channel, or both port and channel, on which circuits are configured for the circuits to function.

This command is also described in:

- *Configuring ATM, Ethernet, and POS Ports* for ATM OC, Ethernet, and Packet over SONET/SDH (POS) ports.
- *Configuring GRE Tunnels* for Generic Routing Encapsulation (GRE) tunnel circuits.

1.8.6 Examples

1.9 shutdown (RSVP LSP)

```
shutdown
```

```
no shutdown
```

1.9.1 Purpose

Disables a Resource Reservation Protocol (RSVP) label-switched path (LSP).

1.9.2 Command Mode

RSVP LSP configuration

1.9.3 Syntax Description

This command has no keywords or arguments.

1.9.4 Default

The RSVP LSP is enabled when configured.

1.9.5 Usage Guidelines

Use the **shutdown** command to disable an RSVP LSP.

Use the **no** form of this command to enable an existing RSVP LSP that has been disabled.

1.9.6 Examples

The following example shows how to disable the RSVP LSP, `test03`:

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

[local]Redback(config-rsvp)#lsp test03

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

1.10 shutdown (Spanning Tree)

shutdown

no shutdown

1.10.1 Purpose

Shuts down the Spanning Tree Protocol process on the bridge.

1.10.2 Command Mode

Spanning-tree configuration

1.10.3 Syntax Description

This command has no keywords or arguments.

1.10.4 Default

The Spanning Tree Protocol is running if enabled by the spanning-tree command (in bridge configuration mode).

1.10.5 Usage Guidelines

Use the shutdown command to shutdown the Spanning Tree Protocol process on the bridge.

1.10.6 Examples

The following examples shows how to shut down the Spanning Tree Protocol on a bridge.

```
[local]Redback(config-bridge-stp)#shutdown
```

1.11 shutdown (SSE)

shutdown [disk ***disk_num*****]**

no shutdown [disk ***disk_num*****]**

1.11.1 Command Mode

Card configuration

1.11.2 Syntax Description

disk ***disk_num***	Disk number on the SSE card. Shuts down an individual SSE disk. Shutting down both SSE disks does not shut down the SSE card. Values: 1 or 2.

1.11.3 Default

Both disks on the SSE card are enabled if inserted.

1.11.4 Usage Guidelines

Disables the SSE card or specified SSE disk. No data is transmitted or received when the card is shut down.

If the SSE card is configured for Network RAID 1 redundancy with RAID 0 disks, shutting down one of the disks stops the service of the entire card, because the other disk cannot be used by itself under RAID 0 configuration.

If you issue this command on the active SSE card during data synchronization on any partition, the following warning message appears:`Note: Executing the command during data synchronization on any of the partitions will cause data corruption. 30 Commit to continue; abort to exit without change.`

Use the **`no`** form of this command to enable the SSE card or SSE disk.

Before you decommission an SSE card that is not configured for redundancy, you must shut it down, using the **`shutdown`** command on the SSE card.

Caution!

Risk of data corruption and loss of charging records. Removing an SSE card from configuration without first shutting it down can cause file corruption. To avoid the risk, first enter the **`card sse`** ***`slot`***, **`shutdown`**, and **`commit`** commands. Wait at least 15 seconds for the card to completely shut down before entering the **`no card sse`** ***`slot`*** command.

1.11.5 Examples

The following example illustrates the shutdown of SSE `disk 2`.

```
[local]Redback(config)#card sse 2
[local]Redback(config-card)#shutdown disk 2
```

1.12 shutdown (Tunnel)

`shutdown`

`no shutdown`

1.12.1 Purpose

Disables a tunnel.

1.12.2 Command Mode

Tunnel configuration

1.12.3 Syntax Description

This command has no keywords or arguments.

1.12.4 Default

All tunnels are disabled.

1.12.5 Usage Guidelines

Use the **shutdown command** to disable a tunnel. Use this command in tunnel configuration mode to disable a tunnel that you created using the **peer-end-point** command (in tunnel configuration mode).

Use the **no** form of this command to enable a tunnel.

1.12.6 Examples

The following example shows how to enable an overlay tunnel:

```
[local]Redback(config)#tunnel ipv6-manual DenverTn1

[local]Redback(config-tunnel)#no shutdown
```

1.13 slowsync

slowsync

{**no** | **default**} **slowsync**

1.13.1 Purpose

Configures the SmartEdge router to slowly adjust its local clock rate to compensate for differences with a remote Network Time Protocol (NTP) clock source.

1.13.2 Command Mode

NTP server configuration

1.13.3 Syntax Description

This command has no keywords or arguments.

1.13.4 Default

Gradual adjustment of the local clock rate is disabled.

1.13.5 Usage Guidelines

Use the **`slowsync`** command to configure the SmartEdge router to slowly adjust its local clock rate to compensate for differences with a remote NTP clock source.

This command changes the rate of the SmartEdge router clock so that it gradually converges with the NTP server clock.

The NTP daemon adjusts the SmartEdge router clock within a few minutes if the difference between the SmartEdge router clock and the remote NTP server is greater than 5 seconds. This adjustment occurs within the first five minutes after the NTP daemon is started.

Use the **`no`** or **`default`** form of this command to disable gradual adjustment of the local clock rate.

1.13.6 Examples

The following example shows how to enable the gradual adjustment of the local clock rate:

```
[local]Redback(config-ntp-server)#slowsync
```

1.14 snmp alarm delete

`snmp alarm delete { active | clear } {` ***`entry-id`*** **`| all }`**

1.14.1 Purpose

Deletes active or clear alarm entries.

1.14.2 Command Mode

exec

1.14.3 Syntax Description

`active`	Delete an active alarm entry.
`clear`	Delete a cleared alarm entry.
`entry-id`	The alarmActiveIndex value that identifies the specific SNMP active or clear entry to delete.
`all`	All entries in alarmActive Table. Using this keyword with the **`active`** keyword will delete all active SNMP alarms. Using this keyword with the **`clear`** keyword will delete all cleared SNMP alarms.

1.14.4 Default

None.

1.14.5 Usage Guidelines

Use the **`snmp alarm delete`** command to delete entries in the alarmModelTable in ALARM-MIB.

If you use the **`active`** keyword you will delete active alarm entries. If you use the **`clear`** keyword, you will delete cleared alarm entries.

1.14.6 Example

```
[local]Redback(config)#snmp alarm delete
```

1.15 snmp alarm model

`snmp alarm model` ***`model-id`*** **`state`** ***`state`***

`no snmp alarm model` ***`model-id`*** **`state`** ***`state`***

1.15.1 Purpose

Creates an entry in the alarmModelTable and configures an alarm model in ALARM-MIB.

1.15.2 Command Mode

Global configuration

1.15.3 Syntax Description

`model`	Identifies that you want to configure an SNMP alarm model by entering the SNMP alarm model command mode in the CLI.
`model-id`	Uniquely identifies the SNMP alarm model you create using this command. Also sets the alarmActiveIndexValue for the alarm model.
`state` *`state`*	State to use for the notification event for the alarm model. All alarms are modeled as a series of states which are related using the alarmModelIndex. See Table 1 for the values for the *`state`* argument.

1.15.4 Default

None.

1.15.5 Usage Guidelines

Use the **`snmp alarm`** command to create an entry in the alarmModelTable in ALARM-MIB and create SNMP alarm models that allow you to configure how the system communicates certain notification events to allow for more detailed reporting between the SNMP manager and the reporting agent. Alarms are modeled as a series of states which are related using the alarmModelIndex in ALARM-MIB. Alarm states can be modeled using traditional notifications, generic alarm notifications (using the alarmActive State and the alarmClearState notifications defined in ALARM-MIB), or without the use of notifications.

Using the **`model`** keyword allows you to enter into the SNMP alarm model command mode in the CLI in order to access the following additional commands you can use to set up an alarm model:

- *description*
- *eventtype*
- *notify*
- *probablecause*
- *res-prefix*
- *sp-pointer*
- *vb-index*
- *vb-subtree*

Alarm states modeled using traditional notifications would specify a notification object identifier and optional one of the notification varbinds to identify the state. This alarm state is entered when the generated notification matches this information. The alarm would be added to the active alarm table.

Table 1 describes the values of the state argument. The alarm states are entered in the alarmModelTable in ALARM-MIB after being triggered by an event. The alarm is then added to the active alarm table based on the specified state (for example, if it is a clear event, it will be added to the alarm clear table).

Table 1 Values for the state Argument

Value	Description
`clear`	Clear state.
`indeterminate`	Indeterminate state.
`warning`	Warning state.
`minor`	Minor state.
`major`	Major state.
`critical`	Critical state.

Use the following show commands to display information about SNMP alarm models:

- **`show snmp alarm model`** command to display information about each alarm model.
- **`show snmp alarm active`** to display information about active alarms.
- **`show snmp alarm cleared`** to display information about cleared alarms.
- **`show snmp alarm stats`** to display general statistics about active alarms.

Enable debugging for snmp alarm models by using the **`debug snmp mib alarm`** command

Use the **`no`** form of this command to delete alarm entries.

1.15.6 Examples

The following example shows how to configure link up and link down notifications. The link up notification would be modeled as a clear event, the administrative link down as a warning and an operational link down as critical. The alarmModelTable has entries with the following values:

```
alarmModelListName  ""
alarmModelIndex  3
alarmModelState   1
alarmModelNotificationId linkUp
alarmModelVarbindIndex 1
alarmModelVarbindValue 1
alarmModelDescription  "link Up"
alarmModelSpecificPointer ituAlarmEntry.3.1
alarmModelVarbindSubtree  ifIndex (1.3.6.1.2.1.2.2.1.1)
alarmModelResourcePrefix 0.0
alarmModelRowStatus  active (1)
ituAlarmEventType  communicationsAlarm (2)
ituAlarmPerceivedSeverity cleared (1)
ituAlarmGenericModel  alarmModelEntry.0.3.1

alarmModelListName  ""
alarmModelIndex  3
alarmModelState   2
alarmModelNotificationId  linkDown
alarmModelVarbindIndex 2
alarmModelVarbindValue  down (2)
alarmModelDescription  "linkDown - administratively"
alarmModelSpecificPointer ituAlarmEntry.3.6
alarmModelVarbindSubtree ifIndex (1.3.6.1.2.1.2.2.1.1)
alarmModelResourcePrefix 0.0
alarmModelRowStatus  active (1)
ituAlarmEventType   communicationsAlarm (2)
ituAlarmPerceivedSeverity  warning (6)
ituAlarmGenericModel  alarmModelEntry.0.3.2

alarmModelListName  ""
alarmModelIndex  3
alarmModelState  3
alarmModelNotificationId linkDown
alarmModelVarbindIndex 2
alarmModelVarbindValue up (1)
alarmModelDescription  "linkDown - confirmed problem"
alarmModelSpecificPointer ituAlarmEntry.3.3
alarmModelVarbindSubtree ifIndex (1.3.6.1.2.1.2.2.1.1)
alarmModelResourcePrefix  0.0
alarmModelRowStatus  active (1)
ituAlarmEventType  communicationsAlarm (2)
ituAlarmPerceivedSeverity  critical (3)
ituAlarmGenericModel  alarmModelEntry.0.3.3
```

To configure the link up and link down notifications as described above, enter the following in the CLI:

```
[local]Redback(config)#snmp alarm model 3 state clear
[local]Redback(config-snmp-alarmmodel)#notify linkup
[local]Redback(config-snmp-alarmmodel)#vb-index 1 vb-value 1
[local]Redback(config-snmp-alarmmodel)#description "link Up"
[local]Redback(config-snmp-alarmmodel)#vb-subtree ifIndex
[local]Redback(config-snmp-alarmmodel)#sp-pointer ituAlarmEventType.0.3
[local]Redback(config-snmp-alarmmodel)#eventtype communicationsAlarm
[local]Redback(config-snmp-alarmmodel)#exit

[local]Redback(config)#snmp alarm model 3 state warning
[local]Redback(config-snmp-alarmmodel)#notify linkDown
[local]Redback(config-snmp-alarmmodel)#vb-index 4 vb-value 2
[local]Redback(config-snmp-alarmmodel)#sp-pointer ituAlarmEventType.0.3
[local]Redback(config-snmp-alarmmodel)#description "linkDown -
administratively"
[local]Redback(config-snmp-alarmmodel)#vb-subtree  ifindex
[local]Redback(config-snmp-alarmmodel)#eventtype communicationsalarm
[local]Redback(config-snmp-alarmmodel)#probablecause 14
[local]Redback(config-snmp-alarmmodel)#exit

[local]Redback(config)#snmp alarm model 3 state critical
[local]Redback(config-snmp-alarmmodel)#notify linkDown
[local]Redback(config-snmp-alarmmodel)#vb-index 4 vb-value 1
[local]Redback(config-snmp-alarmmodel)#sp-pointer ituAlarmEventType.0.3
[local]Redback(config-snmp-alarmmodel)#description "linkDown -
confirmed problem"
[local]Redback(config-snmp-alarmmodel)#vb-subtree  ifindex
[local]Redback(config-snmp-alarmmodel)#eventType communicationsalarm
[local]Redback(config-snmp-alarmmodel)#probableCause 8
```

1.16 snmp community

snmp community *string* [{**all-contexts** | **context** *ctx-name*}] [*access*] [**tag** *tag-name*] [**view** *view-name*]

no snmp community string

1.16.1 Purpose

Creates a community string that permits access to Management Information Base (MIB) objects. This command is used for Simple Network Management Protocol (SNMP) version 1 (SNMPv1) and SNMP version 2c (SNMPv2) only.

1.16.2 Command Mode

Global configuration

1.16.3 Syntax Description

string	Alphanumeric string to be used as the community string. The string can contain up to 64 characters; the first 28 characters must be unique.
all-contexts	Optional. Allows the community access to all contexts.
context ***ctx-name***	Optional. Name of the context that contains the specific instances of MIB objects available to the community. The default context is local.
access	Optional. Type of access, according to one of the following keywords: • **read-only**—Allows the community read-only access to MIB objects. • **read-write**—Allows the community read-write access to MIB objects.
tag ***tag-name***	Optional. Alphanumeric character string that matches one of the notification tag names defined by the **snmp notify-target** command in global configuration mode.
view ***view-name***	Optional. Name of the previously configured view.

1.16.4 Default

The default context is `local`. The default access is `read-only`. The default view name is `initial`.

1.16.5 Usage Guidelines

Use the **snmp community** command to create a community string that permits access to MIB objects.

Note: This command is used with SNMPv1 and SNMPv2 only. You do not need to enable SNMP server capabilities before creating communities.

When you create an SNMP community, it is accessible by both SNMPv1 and SNMPv2 agents. The community string can contain up to 63 characters; the first 28 characters in the string must be unique. You cannot include the **@** character in the community name because it is used in generating community names when you specify the **all-contexts** keyword.

Use the **all-contexts** keyword to trigger the automatic generation of community names for all managed contexts. This keyword allows you to create a community to support all contexts without having to enter the **snmp community** command for each context. For example, if a SmartEdge router has three configured contexts (local, aol, and uunet), the **snmp community** with the **Fred all-contexts** construct creates the structured community strings Fred@local, Fred@aol, and Fred@uunet.

Use the **tag** ***tag-name*** construct to link one or more SNMP communities to one or more IP addresses and thereby limit access to only the SNMP messages from those IP addresses.

The treatment of Border Gateway Protocol (BGP) peer up and peer down traps (bgpBackwardTransNotification and bgpEstablishedNotification) differs from the treatment of other context-specific traps:

- For BGP peer up and peer down traps:
  - If you specify the **all-contexts** keyword, the system reports traps from all contexts.
  - If you specify the **context** ***ctx-name*** construct, the system reports traps originating from the specified context.
  - If you specify neither the **all-contexts** keyword nor **context** ***ctx-name*** construct, the system reports only traps from the local context.
- For all other context-specific traps, the system reports traps from all contexts, regardless of whether the **all-contexts** keyword or **context** ***ctx-name*** construct is used.

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

1.16.6 Examples

The following command shows how to grant the `public` community read-only access to the MIB objects in the `generic` view, and trigger the automatic generation of community strings for the `local` context:

```
[local]Redback(config)#snmp community public view generic
```

1.17 snmp engine-id

snmp engine-id {**local** | **remote** ***name***} ***id-string***

no snmp engine-id remote ***name***

default fault snmp engine-id local

1.17.1 Purpose

Specifies a unique engine ID for the Simple Network Management Protocol (SNMP) Version 3 (SNMPv3) local or remote systems.

1.17.2 Command Mode

Global configuration

1.17.3 Syntax Description

`local`	Local engine ID.
`remote` ***`name`***	Remote engine ID.
`id-string`	String of 10 to 64 hexadecimal characters to be used for the engine ID. Use a colon as a separator after each two hexadecimal characters. For a detailed description and format of the SNMP engine ID, see RFC 2571, `An Architecture for Describing SNMP Management Frameworks`. The string can be arbitrary as long as its length conforms to the format described in RFC 2571. The default value is a variable-length octet string consisting of: • The Redback Networks Enterprise object identifier (OID), a defined type value, which defines the format of the remaining octets. • The management IP address, which is the IP address specified for the interface to which the Ethernet management port on the controller card is bound. • The receiving User Datagram Protocol (UDP) port number, which is either the default, 161, or the UDP port number specified by the `snmp server` command (in global configuration mode).

1.17.4 Default

The SNMP engine ID is a 24-character string consisting of the Redback Networks Enterprise Management Information Base (MIB) OID and the management port medium access control (MAC) address.

1.17.5 Usage Guidelines

Use the **`snmp engine-id`** command to specify a unique engine ID for SNMPv3.

Note: This command is used with SNMPv3 only. No equivalent exists for SNMP Version 1 (SNMPv1) or SNMP Version 2c (SNMPv2). You must enable the SNMP server using the **snmp server** command in global configuration mode before you can specify the engine ID.

Use the **no** form of this command to delete the remote engine ID. The local engine ID cannot be deleted.

Use the **default** form of this command to set the engine ID to the default value.

Caution!

Risk of data loss. Changing the engine ID invalidates security information for all SNMP users using authentication or privacy, and requires you to reenter the **snmp user** command (in global configuration mode). To reduce this risk, postpone entering the **snmp user** command until after you are satisfied with the definition of the engine ID.

Note: It is recommended that you enable the SNMP server using the **snmp server** command (in global configuration mode) before you configure the engine ID, although it is not required. The recommended sequence of configuration tasks is described in *Configure SNMPv3*.

1.17.6 Examples

The following example specifies an engine ID of `01:02:03:04:ab:cd`:

```
[local]Redback(config)#snmp engine-ID local 01:02:03:04:ab:cd
```

1.18 snmp group

snmp group *group-name* [{**context** *ctx-name* [**exact** | **prefix**]}] [**notify** *notify-view*] [**read** *read-view*] [**security-model** {**1** | **2c** | **usm** *level*}] [**write** *write-view*]

no snmp group *group-name* [{**context** *ctx-name* [**exact** | **prefix**]}] [**notify** *notify-view*]] [**read** *read-view*] [**security-model** {**1** | **2c** | **usm** *level*}] [**write** *write-view*]

1.18.1 Purpose

Creates a Simple Network Management Protocol (SNMP) Version 3 (SNMPv3) group.

1.18.2 Command Mode

Global configuration

1.18.3 Syntax Description

`group-name`	Name of the group. The string can be up to 32 characters in length.
`context` ctx-*`name`*	Optional. Name of the context. The default value is the local context.
`exact`	Optional. Matches only the context exactly as specified by the **`context`** *`name`* construct.
`prefix`	Optional. Matches any context that begins with the **`context`** *`name`* construct.
`notify` *`notify-view`*	Optional. Name of the view from which notifications are sent to the group.
`read` *`read-view`*	Optional. Name of the view to which this group has read access.
`security-model`	Optional. Specifies the security model to use for the group.
`1`	Specifies a security model based on SNMP Version 1 (SNMPv1) community strings.
`2c`	Specifies a security model based on SNMP Version 2c (SNMPv2) community strings.
`usm` *`level`*	Security model based on SNMP users (SNMPv3 only), according to one of the following keywords: • **`auth`**—Authorizes SNMP users. • **`no auth`**—Does not authorize SNMP users. • **`priv`**—Enforces authentication privilege level support in SNMPv3.
`write` *`write-view`*	Optional. Name of the view to this group has write access.

1.18.4 Default

A group, “initial”, is automatically created if needed (for instance, if the **`snmp user`** command is used in global configuration mode without specifying a group). This group uses the user security model with the **`noauth`** security level, and allows read access to the view, “restricted”. No *`write-view`* or *`notify-view`* is automatically defined. If the **`security-model`** keyword is not specified, the security model is **`usm`** and the security level is **`noauth`**.

1.18.5 Usage Guidelines

Use the **snmp group** command to create an SNMPv3 group.

Note: This command is used only with SNMPv3 to define access parameters for an SNMP group. You must enable the SNMP server using the **snmp server** command in global configuration mode before you can configure SNMP groups. For SNMP versions 1 and 2c, use the **snmp community** command (in global configuration mode).

Use the **no** form of this command to delete an SNMP group. If not specified in the **no** form of this command, optional parameters are set to their default values.

1.18.6 Examples

The following command shows how to create an SNMP group, `Admin`, that provides authorized read and modify access to the MIB objects defined in a view, `Admin-View`:

```
[local]Redback(config)#snmp group Admin security-model usm auth context
 local read Admin-View write Admin-View
```

1.19 snmp notify

snmp notify ***notify-name tag-name*** [{**inform** | **trap**}]

no snmp notify ***notify-name***

1.19.1 Purpose

Defines a Simple Network Management Protocol (SNMP) notification entry and associates a tag name with the entry.

1.19.2 Command Mode

Global configuration

1.19.3 Syntax Description

notify-name	Name of the notification. The string can be up to 32 characters in length.
tag-name	Tag name for the notification. The string can be up to 32 characters in length.

inform	Optional. Indicates that the notification requires a response from the SNMP target. If no response is sent within five seconds, the inform notification is sent again. The maximum number of retries is two.
trap	Optional. Indicates that the SNMP message is a trap, a nonconfirmed ***notification*** of certain events.

1.19.4 Default

The notification type is trap.

1.19.5 Usage Guidelines

Use the **snmp notify** command to define an SNMP notification entry and to associate a tag name with the entry.

You must enable the SNMP server using the **snmp server** command (in global configuration mode) before you use this command.

Use this command in conjunction with the **snmp notify-target** command (in global configuration mode), which references the ***tag-name*** argument.

Use the **no** form of this command to remove a notification entry and tag name from the configuration.

1.19.6 Examples

The following example defines a notify entry with the notify and tag names both set to V3Traps:

```
[local]Redback(config)#snmp notify V3Traps V3Traps trap
```

1.20 snmp notify-filter

snmp notify-filter ***filter-name oid-tree*** {**excluded** | **included**}

no snmp notify-filter ***filter-name oid-tree***

1.20.1 Purpose

Creates a Simple Network Management Protocol (SNMP) notify filter that includes or excludes specific notifications.

1.20.2 Command Mode

Global configuration

1.20.3 Syntax Description

filter-name	Name of the notify filter. The string can be up to 32 characters in length.
oid-tree	Object identifier (OID) of the Abstract Syntax Notation One (ASN.1) subtree for which the notifications are to be included or excluded. The format is a string of numbers (such as 1.3.6.2.4) or a word (such as system). Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example, 1.3.*.4.
excluded	Excludes the specified OID tree.
included	Includes the specified OID tree.

1.20.4 Default

None

1.20.5 Usage Guidelines

Use the **snmp notify-filter** command to create an SNMP notify filter that includes or excludes specific notifications.

Note: You must enable the SNMP server using the **snmp server** command (in global configuration mode) before configuring a notify filter.

Use this command in conjunction with the **snmp notify-target** command (in global configuration mode), which references the ***filter-name*** argument.

Use the **no** form of this command to remove the specified notify filter from the configuration.

1.20.6 Examples

The following example displays the notify filter, `F-NO-rpMau`, excluding the `rpMauNotifications` notifications:

```
[local]Redback(config)#snmp notify-filter F-NO-rpMau rpMauNotifications excluded
```

1.21 snmp notify-target

snmp notify-target *notify-target-name ip-addr* {[**address-context** *ctx-name*] [**port** *port*] **tag** *tag-list* **parameters** *target-parameters*} [**filter** *filter-name*] [**retry** *count*] [**timeout** *seconds*]

no snmp notify-target *notify-target-name ip-addr* {[**address-context** *ctx-name*] [**port** *port*] **tag** *tag-list* **parameters** *target-parameters*} [**filter** *filter-name*] [**retry** *count*] [**timeout** *seconds*]

1.21.1 Purpose

Configures the Simple Network Management Protocol (SNMP) target management station, which receives SNMP notifications.

1.21.2 Command Mode

Global configuration

1.21.3 Syntax Description

notify-target-name	Name of the notify target. The string can be up to 32 characters in length. Use the name specified using the **snmp notify** command (in global configuration mode).
ip-addr	IP address of the management station to receive the notifications.
address-context *ctx-name*	Optional. Name of the context from which the notifications are sent. The default context is local.
port *port*	Optional. User Datagram Protocol (UDP) port used to send the notifications to the target. The range of values is 1 to 65,535. The default port number is 162.
tag *tag-list*	List of notification tag names, separated by commas. No spaces are allowed in the list. Tag names are configured using the **snmp notify** command (in global configuration mode).
parameters *target-parameters*	Name of the target parameters for this target. Use the name specified using the **snmp target-parameters** command (in global configuration mode).
filter *filter-name*	Optional. Name of the filter to be applied to the target. Use the name specified using the **snmp notify-filter** command (in global configuration mode).

retry *count*	Optional. Number of times to retry when sending an inform notification. The range of values is 0 to 255; the default value is 2.
timeout *seconds*	Optional. Number of seconds to wait for a reply when an inform notification is sent. The range of values is 0 to 2,147,483,647; the default value is 5.

1.21.4 Default

The UDP port is 162. The context is local. The timeout value is five seconds. The number of retries is two.

1.21.5 Usage Guidelines

Use the **snmp notify-target** command to configure the SNMP target management station, which receives SNMP notifications.

Note: You must enable the SNMP server using the **snmp server** command (in global configuration mode) before you can configure the target management station.

The **snmp target** and the **snmp notify-target** commands are mutually exclusive. The **snmp target** command sets certain parameters to their default values; these parameters are notifyName, targParmName, tag, tagList, seconds, and count.

The **snmp target** command (in global configuration mode) is equivalent to the set of **snmp notify-target**, **snmp notify**, **snmp target-parameters**, and **snmp group** (only if the **notify** ***notify-view*** construct has not been set) commands.

Before specifying the ***notify-target-name*** argument, you must first create the name using the **snmp notify** command. You must enable the SNMP server using the **snmp server** command (in global configuration mode) before you can configure the target management station. Before specifying the **parameters** ***target-parameters*** construct, you must first create the name using the **snmp target-parameters** command (in global configuration mode). You must enable the SNMP server using the **snmp server** command (in global configuration mode) before you can configure the target management station. Before specifying the ***filter-name*** argument, you must first create the name using the **snmp notify-filter** command (in global configuration mode).

Use the **no** form of this command to remove a target from the configuration.

1.21.6 Examples

The following command configures the system to send notifications to a target, `Nm-Station1`, IP address `10.3.4.5`, using the tag `Inet-Informs`, parameters, `Param2`, and notify filter, `F-NO-rpMau`:

```
[local]Redback(config)#snmp notify-target Nm-Station1 10.3.4.5 tag
Inet-Informs parameters Param2 filter F-NO-rpMau
```

1.22 snmp ping

snmp ping *ping-test-name* **ip** {*hostname* | *ip-addr*} [**frequency** *seconds*] [**count** *count-num*] [**timeout** *seconds*] [**notify-complete**] [**notify-test-fail** *notify-test-num*] [**notify-probe-fail** *notify-probe-num*] [**df**] [**pattern** *hex-pattern*] [**size** *bytes*] [**source** *ip-addr*] [**tos** *tos*] [**ttl** *ttl-secs*]

no snmp ping *ping-test-name*

1.22.1 Purpose

Schedules an IPv4 ping test.

1.22.2 Command Mode

Context configuration

1.22.3 Syntax Description

ping-test-name	Indicates the name of the ping test you are creating.
ip	Identifies that you are going to schedule a ping for an IPv4 ping test.
hostname	Indicates the destination hostname on which you are scheduling a ping test.
ip-addr	Indicates the destination IP address on which you are scheduling a ping test.
frequency *seconds*	Optional. Sets the time interval between each ping test in seconds (1-86400). For example, if you set the number of seconds to 5, the ping test will run every 5 seconds.
count *count-num*	Optional. Sets the *count-num* number of ping probes per ping test. You can schedule up to 15 at once.

`timeout` *`seconds`*	Optional. Schedules an amount of time in seconds (1-60) that the system waits for a ping probe.
`notify-complete`	Optional. Indicates that the system will generate a pingTestCompleted notification when a ping test completes.
`notify-test-fail` *`notify-test-num`*	Optional. Indicates that the system will generate a pingTestFailed notification for this ping test. The *`notify-test-num`* argument identifies the number of ping probes (1-15) must fail in a ping test before the system generates this notification.
`notify-probe-fail` *`notify-probe-num`*	Optional. Indicates that pingProbeFailed notifications will be generated for this test, where *`notify-probe-num`* is the value of the MIB object, pingCtlTrapProbeFailureFilter.
`df`	Optional. Sets the Don't Fragment bit in the IP header to true. Do not use this keyword if you want to allow fragmenting in the IP packet.
`pattern` *`hex-pattern`*	Optional. Identifies the hexidecimal pattern to send in the ICMP packet as part of the ping test.
`size` *`bytes`*	Optional. Identifies the packet size, in bytes (32-18024), of the ICMP datagram to send for the ping test.
`source` *`ip-addr`*	Optional. Identifies the IP address of the interface where the ping probe will be sent.
`tos` *`tos`*	Optional. Sets the type of service (TOS) in the IP header in hexadecimal format.
`ttl` *`ttl-secs`*	Optional. Sets the time-to-live value in the IP header in seconds (1-255).

1.22.4 Default

Table 2 Optional Default Values

Option	Default Value
count	5 probes
df	false
frequency	600 seconds (10 minutes)
notify-probe-num	1 probe
notify-test-num	1
pattern	0x0
size	56 bytes

Option	Default Value
timeout	1 second
tos	0
ttl	255

1.22.5 Usage Guidelines

Use the **snmp ping** command to schedule an IPv4 ping test. This configuration is saved across system reloads and XCRP switchovers. Ping tests will not be scheduled if the SNMP server is not configured.

See the **ping** command and RFC 4560 for additional information on the options available with the ping command.

Use the **show snmp ping** command to view the scheduled test results.

1.22.6 Examples

The following command shows how to enable an snmp ping test with the name test on the server100 host. The test ping sends a packet size of 32 bytes to the server every 30 seconds and sends a notification to the SNMP server when it is complete:

```
[local]Redback(config)#snmp ping test ip server100 frequency 30
notify-complete size 32
```

The following command enables an snmp ping test with the name test on the server100 host. The test ping sends a packet size of 32 bytes to the server every 30 seconds and sends a notification to the SNMP server when it is complete:

```
[local]Redback#config

[local]Redback(config)#context local

[local]Redback(config-ctx)#snmp ping ping_name ip www.ericsson.com
```

1.23 snmp server

snmp server [**port** *port*] [**enhance ifmib**]

no snmp server

1.23.1 Purpose

Enables the Simple Network Management Protocol (SNMP) server for SNMP Version 1 (SNMPv1), SNMP Version 2c (SNMPv2), and SNMP Version 3 (SNMPv3), and enters SNMP server configuration mode.

1.23.2 Command Mode

Global configuration

1.23.3 Syntax Description

port *port*	Optional. Port number through which the SNMP server receives data. The range of values is 1 to 65,535; the default value is 161.
enhance ifmib	Optional. Enables enhancements to the Interfaces Management Information Base (IF-MIB) implementation.

1.23.4 Default

SNMP server capabilities are disabled. The default port is 161.

1.23.5 Usage Guidelines

Use the **snmp server** command to enable the SNMP server. This command enables the protocol engines for all supported versions of SNMP.

Use the **enhance ifmib** keyword to add the following functions to the IF-MIB:

- Supports Asynchronous Transfer Mode (ATM), Frame Relay, and 802.1Q permanent virtual circuits (PVCs)
- Supports ATM operations, administration, and management (OAM) trap notifications when the state of an ATM PVC transitions as a result of the OAM function
- Sets the IF-MIB object, ifDescr equal, to ifName
- Supports the IF-MIB objects, ifHCInOctets and ifHCOutOctets, wherever ifInOctets and ifOutoctets are supported
- Supports quality of service (QoS) transmit counters for each queue for each circuit and port for all line cards
- To display aggregate traffic counter and link group hierarchical structure information for circuits.

Use the **no** form of this command to disable the SNMP server.

Note: You must enter the **snmp server** and **no snmp server** commands in separate transactions for both to take effect. Within a single transaction, entering the **snmp server** command, followed by the **no snmp server** command, simply enables the server without then disabling it. Similarly, entering the **no snmp server** command, followed in the same transaction by the **snmp server** command, disables the server without then re-enabling it. To terminate the current transaction, enter the **commit** command (in global configuration mode) before you can configure the target management station. Then enter the form of the **snmp server** command as required. For more information on the **commit** command, see *Using the CLI*.

1.23.6 Examples

The following command shows how to enable the SNMP server on the default User Datagram Protocol (UDP) port (161):

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

1.24 snmp target

To send Simple Network Management Protocol (SNMP) version 1 notifications, use the following syntax:

snmp target *target-name ip-addr* [**port** *port*] **address-context** *ctx-name*] **security-name** *sec-name* [**trap**] [**version** *1*] [**view** *notify-view*]

no snmp target *target-name*

To send SNMP version 2 (SNMPv2) notifications, use the following syntax:

snmp target *target-name ip-addr* [[**port** *port*] **address-context** *ctx-name*] **security-name** *sec-name* [**inform** | **trap**] [**version 2**] [**view** *notify-view*]

no snmp target *target-name*

To send SNMP version 3 (SNMPv3) notifications, use the following syntax:

snmp target *target-name ip-addr* [[**port** *port*] **address-context** *ctx-name*] **security-name** *sec-name* [**group** *group-name*] [**inform** | **trap**] [**version** *3* [**security-level** *level*]] [**view** *notify-view*]

no snmp target *target-name*

1.24.1 Purpose

Configures the SNMP notifications sent to the SNMP target management station.

1.24.2 Command Mode

Global configuration

1.24.3 Syntax Description

target-name	Name of the target management station. The string can be up to 32 characters in length.
ip-addr	IP address of the target management station.
address-context *ctx-name*	Optional. Name of the context from which notifications are sent.
port *port*	Optional. User Datagram Protocol (UDP) port to receive notifications. The default port is 162.
security-name *sec-name*	Username or community string for the notifications. For SNMPv1 or SNMPv2, enter a community name you specified with the **snmp community** command (in global configuration mode). For SNMPv3, enter a username you specified with the **snmp user** command (in global configuration mode).
group *group-name*	Optional. String that specifies which group parameters apply to the notifications sent to the SNMP target management station. The group name is a name you specified with the **snmp group** command (in global configuration mode) for SNMPv3.
inform	Optional. Indicates that the type of notification is inform, a confirmed notification that requires a response from the SNMP target. If no response is sent within five seconds, the inform notification is sent again. The number of retries is two.
trap	Optional. Indicates that the type of notification is trap: a nonconfirmed notification.
version 1	Optional. Specifies that SNMPv1 is sent to the target.
version 2	Optional. Specifies that SNMPv2 is sent to the target.
version 3	Optional. Specifies that SNMPv3 is sent to the target.

security-level *level*	Optional. Applies only to SNMPv3. Security level to be applied to an SNMP target, according to one of the following keywords: • **auth**—Provides authorization. • **noauth**—Does not provide authorization. • **priv**—Privacy. Enforces authentication privilege level in SNMPv3.
view *notify-view*	Optional. SNMP notify view. The default view is restricted.

1.24.4 Default

The SNMP version is version 2c. The notification view created by the system is restricted. The notification type is trap. The port is 162.

1.24.5 Usage Guidelines

Use the **snmp target** command to configure the SNMP notifications sent to the SNMP target management station.

The **snmp target** and the **snmp notify-target** commands are mutually exclusive.

The **snmp target** command sets certain parameters to their default values; these parameters are notifyName, targParmName, tag, tagList, seconds, and count. It is equivalent to the set of **snmp notify-target**, **snmp notify**, **snmp target-parameters**, and **snmp group** commands (only if the **notify** *notify-view* construct has not been set).

Use the **no** form of this command to remove an SNMP target.

Note: SNMPv2 and SNMPv3 support both the **inform** and **trap** keywords, but SNMPv1 supports only the **trap** keyword.

1.24.6 Examples

The following example creates an SNMP target, `NM-Station1`, at IP address, `198.164.190.110`, to receive SNMPv2 and SNMPv3 traps from the view, `InetView`, using a community name of `Admin`:

```
[local]Redback(config)#snmp target NM-Station1 198.164.190.110
security-name Admin version 2c view InetView trap
```

1.25 snmp target-parameters

snmp target-parameters *parameter-name* **security-name** *sec-name* [**version** *version*] [**security-level** *level*]

no snmp target-parameters *parameter-name*

1.25.1 Purpose

Configures the security name and optionally the Simple Network Management Protocol (SNMP) version and security level used in notifications sent to the SNMP target management station.

1.25.2 Command Mode

Global configuration

1.25.3 Syntax Description

parameter-name	Name of the target parameter set.
security-name *sec-name*	Community name you specified using the **snmp community** command for SNMP Version 1 (SNMPv1) or SNMP Version 2c (SNMPv2), or username you specified using the **snmp user** command for SNMP Version 3 (SNMPv3).
version *version*	Optional. SNMP version to use to send the notifications, according to one of the following keywords: • **1**—Specifies SNMPv1. • **2c**—Specifies SNMPv2. • **3**—Specifies SNMPv3.
security-level *level*	Optional. Security level to be applied to an SNMP target, according to one of the following keywords: • **auth**—Provides authorization. • **noauth**—Does not provide authorization. • **priv**—Enforces authentication privilege level support in SNMPv3.

1.25.4 Default

None

1.25.5 Usage Guidelines

Use the **snmp target-parameters** command to configure the security name and optionally the SNMP version and security level used in notifications sent to the SNMP target management station.

Note: You must enable the SNMP server using the **snmp server** command (in global configuration mode) before you can configure target parameters.

Use this command in conjunction with the **snmp notify-target** command (in global configuration mode).

For the **auth**, **noauth**, and **priv** keywords, no authorization is provided in SNMPv1 and SNMPv2. You must specify the **noauth** keyword for SNMPv1 and SNMPv2. For SNMPv3, you can specify any of the three keywords. Enforcing either the optional **auth** or **priv** keyword applies authorization or privacy support to the designated SNMP target; use the optional **noauth** keyword to apply neither authorization nor privacy support.

Use the **no** form of this command to remove the specified target parameter information from the configuration.

1.25.6 Examples

The following command configures a set of parameters, `Param2`, that includes the security name, `ADMIN`, and specifies the SNMPv3 protocol using authorization:

```
[local]Redback(config)#snmp target-parameters Param2 security-name ADMIN
version 3 security-level auth
```

1.26 snmp traceroute

snmp traceroute *traceroute-test-name* {*hostname* | *ip-addr*} [**frequency** *seconds*] [**count** *count-num*] [**timeout** *seconds*] [**notify-path-change**] [**notify-test-complete**] [**notify-test-fail**] [**df**] [**initial-ttl** *ttl-seconds*] [**max-ttl** *ttl-seconds*] [**port** *number*] [**size** *bytes*] [**source** *ip-addr*] [**tos** *tos*]

no snmp traceroute *traceroute-test-name*

1.26.1 Purpose

Configures SNMP traceroute tests.

1.26.2 Command Mode

Context configuration

1.26.3 Syntax Description

`traceroute-test-name`	Indicates the name of the traceroute test you are creating.
`hostname`	Indicates the destination hostname on which you are scheduling a traceroute test.
`ip-addr`	Indicates the destination IP address on which you are scheduling a tracetroute test.
`frequency` *`seconds`*	Optional. Sets the time interval between each traceroute test in seconds (1-86400). For example, if you set the number of seconds to 5, the traceroute test will run every 5 seconds.
`count` *`count-num`*	Optional. Sets the *`count-num`* number of probes per test. You can schedule up to 15 at once.
`timeout` *`seconds`*	Optional. Schedules an amount of time in seconds (1-60) that the system waits for a traceroute probe.
`notify-path-change`	Optional. Indicates that the system will generate a traceRoutePathChange notification when a traceroute test has changed.
`notify-complete`	Optional. Indicates that the system will generate a traceRouteTestCompleted notification when a traceroute test completes.
`notify-test-fail`	Optional. Indicates that the system will generate a traceRouteTestFailed trap when the full path to a target cannot be determined.
`port` *`number`*	Optional. Sets the port number.
`df`	Optional. Sets the Don’t Fragment bit in the IP header to true. Do not use this keyword if you want to allow fragmenting in the IP packet.
`initial-ttl` *`initial-ttl-seconds`*	Optional. Sets the initial time-to-live (TTL) value in seconds (1-255).
`max-ttl` *`max-ttl-seconds`*	Optional. Sets the maximum time-to-live (TTL) value in seconds (1-255).
`size` *`bytes`*	Optional. Identifies the packet size, in bytes (40-32768), of the UDP datagram to send for the test.

source ***ip-addr***	Optional. Identifies the IP address of the interface where the probe will be sent.
tos ***tos***	Optional. Sets the type of service (TOS) in the IP header in hexadecimal format.

1.26.4 Default

Table 3 Optional Default Values

Option	Default Value
count	3 probes
df	false
frequency	600 seconds (10 minutes)
Initial-ttl	1
Max-ttl	30
port	33434
size	40 bytes
timeout	3 seconds
tos	0x0

1.26.5 Usage Guidelines

Users are able to configure SNMP traceroute notifications (RFC-4560) by enabling the notification control options. SNMP traceroute test configurations are persistent across node reload or switchover. When using the CLI to create traceroute tests, configurations are automatically saved in reliability data bases (RDB). When using SNMP set requests to create traceroute tests, users can set the storage type (volatile or non-volatile) that they would like to use.

1.26.6 Examples

The following command configures a basic SNMP traceroute test for ***traceroute-test-name*** sample-test on ***ip-addr*** 192.168.0.1 using all default values.

```
[local]Redback(config-ctx)#snmp traceroute sample-test ip 192.168.0.1
```

1.27 snmp trap

snmp trap

```
no snmp trap
```

1.27.1 Purpose

Enables SNMP trap notifications for cross-connect (pseudowire) state change events per Layer 2 virtual private network (L2VPN) profile or virtual private LAN services (VPLS) profile.

1.27.2 Command Mode

L2VPN cross-connect profile peer

VPLS profile neighbor

1.27.3 Syntax Description

This command has no keywords or arguments.

1.27.4 Default

SNMP trap notifications are not sent by default.

1.27.5 Usage Guidelines

Use the **snmp trap** command to enable SNMP trap notifications for cross-connect state change events per L2VPN or VPLS profile.

1.27.6 Examples

The following example shows how to enable SNMP trap notifications for cross-connect state change events associated with the L2VPN profile named **l2vpn-customerA-profile**:

```
[local]Redback(config)#l2vpn profile l2vpn-customerA-profile
[local]Redback(config-l2vpn-xc-profile)#peer 10.12.34.55
[local]Redback(config-l2vpn-xc-profile-peer)#snmp trap
```

The following example shows how to enable SNMP trap notifications for cross-connect state change events associated with the VPLS profile named **vpls-customerB-profile**:

```
[local]Redback(config)#vpls profile vpls-customerB-profile
[local]Redback(config-vpls-profile)#neighbor 10.12.34.55
[local]Redback(config-vpls-profile-neighbor)#snmp trap
```

1.28 snmp traps

`snmp traps`

`no snmp traps`

1.28.1 Purpose

Enables or disables SNMP trap notifications for NetOp™ EMS.

1.28.2 Command Mode

NetOp configuration

1.28.3 Syntax Description

This command has no keywords or arguments.

1.28.4 Default

The system forwards SNMP trap information to NetOp EMS by default.

1.28.5 Usage Guidelines

Use the **`snmp traps`** command to forward SNMP trap information to NetOp EMS. Use the **`no snmp traps`** command to suppress the forwarding of SNMP trap information to NetOp EMS. Use the **`show netop`** command to view this configuration information in the SmartEdge router CLI.

1.28.6 Examples

The following example shows how to stop forwarding SNMP trap information to NetOp EMS:

```
[local]Redback(config-netop)#no snmp traps

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

1.29 snmp traps [ospf-traps]

snmp traps ***ospf-traps***

{**no** | **default**} **snmp traps**

1.29.1 Purpose

Enables or disables one or more OSPF-TRAP-MIB notifications.

1.29.2 Command Mode

OSPF configuration

1.29.3 Syntax Description

ospf-traps	Specifies one or more OSPF traps listed in Table 4 to enable or disable.

1.29.4 Default

The system enables the OSPF-MIB IfStateChange, VirtIfStateChange, NbrStateChange, and VirtNbrStateChange notifications by default.

1.29.5 Usage Guidelines

Use this command to allow you to enable or disable each OSPF-TRAP-MIB notification in router ospf mode. The snmp traps command enables the OSPF-TRAP-MIB notification you specify from Table 4. Use the **default** keyword with this command to enable the IfStateChange, VirtIfStateChange, NbrStateChange, and VirtNbrStateChange notifications.

Use the **no snmp traps** form of this command to disable all OSPF-MIB notifications.

The following table describes the OSPF traps and the keywords that enable them in this command.

Table 4 Keywords for Supported Protocols and Servers

Keyword	Description
all	Enables all OSPF-TRAP-MIB notification.
ifstatechange	Enables the OSPF-TRAP-MIB IfStateChange notification.

Table 4 Keywords for Supported Protocols and Servers

Keyword	Description
`ifconfigerror`	Enables the OSPF-TRAP-MIB IfConfigError notification.
`ifauthfailure`	Enables the OSPF-TRAP-MIB IfAuthFailure notification.
`ifrxbadpacket`	Enables the OSPF-TRAP-MIB IfRxBadPacket notification.
`maxagelsa`	Enables the OSPF-TRAP-MIB Maxagelsa notification.
`nbrstatechange`	Enables the OSPF-TRAP-MIB NbrStateChange notification.
`originatelsa`	Enables the OSPF-TRAP-MIB OriginateLSA notification.
`txretransmit`	Enables the OSPF-TRAP-MIB TxReTransmit notification.
`virtifstatechange`	Enables the OSPF-TRAP-MIB VirtIfStateChange notification.
`virtnbrstatechange`	Enables the OSPF-TRAP-MIB VirtNBRStateChange notification.
`virtifconfigerror`	Enables the OSPF-TRAP-MIB VirtIfConfigError notification.
`virtifauthfailure`	Enables the OSPF-TRAP-MIB VirtIfAuthFailure notification.
`virtifrxbadpacket`	Enables the OSPF-TRAP-MIB VirtIfRxBadPacket notification.
`virtiftxretransmit`	Enables the OSPF-TRAP-MIB VirtIfTxReTransmit notification.

1.29.6 Examples

The following examples shows how to enable the TxReTransmit notification for OSPF-TRAP-MIB:

```
[local]jazz(config-ospf)#snmp traps txretransmit

[local]jazz(config-ospf)#
```

1.30 snmp user

snmp user *name* [**engine** *name*] [**group** *group-name*] [**security-model usm** {**noauth** | *authentication* {**key** { *auth-key* [**des56** *des-key*] | **encoded base64** [*auth-key* **des56** *des-key*] } | **password** *auth-pwd* [**des56** *priv-pwd*] } }]

no snmp user *name* [**engine** *name*] [**group** *group-name*] [**security-model usm** {**noauth** | *authentication* {**key** {*auth-key* [**des56** *des-key*] | **encoded base64** [*auth-key* **des56** *des-key*] } | **password** *auth-pwd* [**des56** *priv-pwd*] } }]

1.30.1 Purpose

Configures a Simple Management Network Protocol (SNMP) version 3 (SNMPv3) user.

1.30.2 Command Mode

Global configuration

1.30.3 Syntax Description

name	Name of the SNMP user, up to 32 characters.
engine *name*	Optional. Name of the remote engine previously configured using the **snmp engine-id** command.
group *group-name*	Optional. Name of the group to which the user belongs, up to 32 characters.
security-model usm	Optional. Specifies the User-Based Security Model (USM) for SNMPv3.
noauth	Specifies no authentication.
authentication	USM for SNMPv3, according to one of the following keywords: • **md5**—Specifies Message Digest 5 (MD5) authentication. • **sha**—Specifies Secure Hash Algorithm (SHA) authentication.
key *auth-key*	Authentication key value. Specified only for the user security model, with MD5 or SHA authentication.
encoded base64	Optional. Specifies that the key provided in the command is already in a base 64 encoded form. If you omit this keyword, the system encodes the *auth-key* argument prior to storing it in the configuration.

des56 ***des-key***	Optional. Data encryption standard 56 (DES56) encrypted key value. The minimum password length is eight characters.
password ***auth-pwd***	Authentication password. Specified only for the user security model, with MD5 or SHA authentication.
des56 ***priv-pwd***	Optional. DES56 encrypted privileged password in text string form. The minimum password length is eight characters.

1.30.4 Default

The default security model is USM with no authentication.

1.30.5 Usage Guidelines

Use the **snmp user** command to configure an SNMPv3 user. You must first enable the SNMP server using the **snmp server** command (in global configuration mode) before configuring a user.

Use the **no** form of this command to remove an SNMP user.

1.30.6 Examples

The following command creates an SNMP user, `Admin`, that is part of the group, `Group4`, and uses MD5 authentication with the password `xyzzy`, and an optional `des56` password, `loopy`:

```
[local]Redback(config)#snmp group Group4 all-contexts read all
write all security-model usm priv
[local]Redback(config)#snmp user Admin group Group4 security-model usm md5 passwor
```

Note: The command **snmp user security-model** needs to match the group security-model. In this example, the option **priv** in the user group, therefore; the SNMP user must specify the authentication type and password and the data encryption (**des56**) password.

1.31 snmp version

snmp version {**1** | **2c** | **3**}

no snmp version

1.31.1 Purpose

Specifies the version of the Simple Network Management Protocol (SNMP) traps that the NetOp Element Management System (EMS) server receives.

1.31.2 Command Mode

NetOp configuration

1.31.3 Syntax Description

`1`	Specifies that the SmartEdge router sends SNMP Version 1 (SNMPv1) traps to the NetOp EMS server.
`2c`	Specifies that the SmartEdge router sends SNMP Version 2c (SNMPv2c) traps to the NetOp EMS server.
`3`	Specifies that the SmartEdge router sends SNMP Version 3 (SNMPv3) traps to the NetOp EMS server.

1.31.4 Default

SNMPv2c traps are sent to the NetOp EMS server.

1.31.5 Usage Guidelines

Use the **`snmp version`** command to specify the version of SNMP traps that the SmartEdge router sends to the NetOp EMS server.

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

Note: You must configure the SNMP community before you specify the version of the SNMP traps sent to the NetOp EMS server.

1.31.6 Examples

The following example configures the SmartEdge router to send SNMPv1 traps to the NetOp EMS server:

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

[local]Redback(config-netop)#snmp version 1
```

1.32 snmp view

snmp view *view-name* *oid-tree* {**excluded** | **included**}

no snmp view *view-name* [*oid-tree*]

1.32.1 Purpose

Defines a Simple Network Management Protocol (SNMP) Management Information Base (MIB) view.

1.32.2 Command Mode

Global configuration

1.32.3 Syntax Description

view-name	Alphanumeric string used as a label for the view record that you are updating or creating. The name is used to reference the record. The string can be up to 32 characters in length.
oid-tree	Object identifier (OID) of the ASN.1 subtree to be included, or excluded, from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4. Optional when used in the **no** form.
excluded	Excludes the specified OID tree.
included	Includes the specified OID tree.

1.32.4 Default

A default view, “restricted”, is enabled when it is referenced by a user creating a community without a specific view. This view provides access to the following MIB groups: system, snmp, snmpEngine, and snmpMPDStats.

1.32.5 Usage Guidelines

Use the **snmp view** command to define an SNMP MIB view. MIB views control which SNMP communities have access to specific MIB objects.

Use the **no** form of this command to remove the specified MIB view entry.

1.32.6 Examples

The following example shows how to create a view that includes all objects in the Internet subtree:

```
[local]Redback(config)#snmp view everything internet included
```

The following example shows how to create a view that includes only the system group and the interface MIB objects for the port with a value of 6:

```
[local]Redback(config)#snmp view port6 system include

[local]Redback(config)#snmp view port6 ifEntry.*.6 included
```

1.33 software license

software license

{no | default} software license

1.33.1 Purpose

Enables software licensing and accesses software license configuration mode.

1.33.2 Command Mode

Global configuration

1.33.3 Syntax Description

This command has no keywords or arguments.

1.33.4 Default

No software licensed features or functions are enabled.

1.33.5 Usage Guidelines

Use the **software license** command to enable software licensing and access software license configuration mode.

Use the **`no`** or **`default`** form to disable software licensing and remove any existing licenses.

1.33.6 Examples

The following example shows how to enable software licensing and accesses software license configuration mode:

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

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

1.34 source

`source` ***`ip-addr`*** **`port`** ***`port-number`***

`no source` ***`ip-addr`*** **`port`** ***`port-number`***

1.34.1 Purpose

Configures the source IP address and port number to put into the NetFlow packet for a NAT logging profile.

1.34.2 Command Mode

NAT Logging Profile

1.34.3 Syntax

`ip-addr`	Configures the source IP address of the export put into the NetFlow packet
`port-number`	Specifies the L4 port, the source port of the exporter

1.34.4 Usage Guidelines

Use the **`source`** command to configure the source IP address to put into the NetFlow packet and that the port number is the L4 port for a NAT logging profile.

Use the **`no`** form of this command to delete the source IP address value and port number.

For more information about how to configure NAT logging, see *nat logging-profile* and *Configure an Enhanced NAT Policy with Logging and Paired Mode*.

1.34.5 Example

```
[local]Redback#configuration     <-
Enter configuration commands, one per line, 'end' to exit
[local]Redback(config)#context nat-context
[local]Redback(config-ctx)#nat logging-profile nat-log-profile
[local]Redback(config-nat-profile)#source 10.10.10.1 port 4242
```

1.35 source-address

source-address ***src-addr***

{**no** | **default**} **source-address** ***src-addr***

1.35.1 Purpose

Configures the packet source IP address value for a dynamically verified static routing (DVSR) profile.

1.35.2 Command Mode

DVSR profile configuration

1.35.3 Syntax Description

src-addr	Source IP address of the verification packet. If the source IP address is not set, IP packets use the outbound interface primary IP address.

1.35.4 Default

Source IP address is not set.

1.35.5 Usage Guidelines

Use the **source-address** command to configure the packet source IP address value for a DVSR profile. Because some routers can only recognize the stable address of a router, such as the loopback address, you must configure the source IP address to ensure that the verified host has the route to reach the routers.

Use the **no** or **default** form of this command to delete the packet source IP address value from a DVSR profile.

1.35.6 Examples

The following example defines a DVSR profile source address of `10.1.1.1:`

```
[local]Redback(config-ctx)#dvsr-profile abc-webfarm

[local]Redback(config-dvsr)#source-address 10.1.1.1
```

1.36 source-path

`source-path` ***`er-name`***

`no source-path` ***`er-name`***

1.36.1 Purpose

Assigns a configured explicit route to a label-switched path (LSP).

1.36.2 Command Mode

RSVP LSP configuration

1.36.3 Syntax Description

`er-name`	Name of the explicit route to be used by the LSP.

1.36.4 Default

None

1.36.5 Usage Guidelines

Use the **`source-path`** command to assign a configured explicit route to an LSP.

Before you can assign a source path to an LSP, you must configure an explicit route to use as the source path. Use the **`explicit-route`** command in RSVP router configuration mode to indicate a list of specific hops through a network, and then use the **`source-path`** command to assign that explicit route to your LSP.

Use the **`no`** form of this command to remove an explicit route from an LSP.

1.36.6 Examples

The following example shows how to assign the explicit route `ER03` as the source path for the LSP, `Prod23:`

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

[local]Redback(config-rsvp)#lsp Prod23

[local]Redback(config-rsvp-lsp)#source-path ER03
```

1.37 spanning-tree (bridge)

`spanning-tree`

`no spanning-tree`

1.37.1 Purpose

Enables the Rapid Spanning Tree Protocol (RSTP) for the current bridge or bridged VPLS pseudowire and enters the spanning-tree configuration mode.

1.37.2 Command Mode

- Bridge configuration
- VPLS neighbor configuration

1.37.3 Syntax Description

This command has no keywords or arguments.

1.37.4 Default

RSTP is not enabled.

1.37.5 Usage Guidelines

Use this command to enable RSTP for the current bridge or VPLS pseudowire and enter spanning-tree configuration mode. RSTP is not supported on ATM.

Use the **`no`** form of this command to disable RSTP for the current bridge.

1.37.6 Examples

The following example illustrates the context-specific RSTP commands and the spanning-tree configuration mode:

```
[local]jeudi.lab(config)#context isp4
[local]jeudi.lab(config-ctx)#bridge grp1
[local]jeudi.lab(config-bridge)#spanning-tree
[local]jeudi.lab(config-bridge-stp)#?
```

1.38 spanning-tree profile

spanning-tree profile ***stp-name***

{**no** | **default**} **spanning-tree profile** ***stp-name***

1.38.1 Purpose

In global configuration mode, enables the configuration of Rapid Spanning Tree Protocol (RSTP) attributes. In other modes, assigns a spanning-tree profile to a circuit, port, or VPLS pseudowire.

1.38.2 Command Mode

- dot1q PVC configuration
- Global configuration
- Port configuration
- Link group configuration
- VPLS profile neighbor configuration

1.38.3 Syntax Description

stp-name	Name of the spanning-tree profile to be created, configured, or applied to a circuit.

1.38.4 Default

Spanning-tree profile attributes are set to their default values.

1.38.5 Usage Guidelines

Use the **spanning-tree profile** command to enable the configuration of RSTP attributes (global configuration mode). In other modes, use the command to assign a spanning-tree profile to a circuit, port, or VPLS pseudowire.

To configure the spanning-tree profile attributes or create a spanning-tree profile, enter the **spanning-tree profile** command in global configuration mode.

To assign the spanning-tree profile attributes to a 801.1Q permanent virtual circuit (PVC) or to a port, enter the **spanning-tree profile** command in 802.1Q PVC and port configuration modes, respectively.

Use the **no** form of this command (global configuration mode) to delete a spanning-tree profile.

1.38.6 Examples

The following example illustrates how the spanning-tree profile command creates the spanning-tree profile womp:

```
[local]Redback(config)#spanning-tree profile womp
```

1.39 speed (DS-1)

speed {56 | 64}

default speed

1.39.1 Purpose

Sets the speed for all DS-0 channels in a DS-1 channel on a channelized DS-3 channel or port.

1.39.2 Command Mode

DS-1 configuration

1.39.3 Syntax Description

56	Specifies that the DS-0 channel speed is 56 kbps.
64	Specifies that the DS-0 channel speed is 64 kbps; this is the default channel speed.

1.39.4 Default

The default value is 64 kbps.

1.39.5 Usage Guidelines

Use the **`speed`** command to set the speed for all DS-0 channels in a DS-1 channel on a channelized DS-3 channel or port.

Use the **`default`** form of this command to set the speed for all DS-0 channels in a DS-1 channel to the default speed.

1.39.6 Examples

The following example shows how to set the DS-0 channel speed to `56` kbps:

```
[local]Redback(config-ds1)#speed 56
```

1.40 speed (port)

`speed` *`speed`*

{**`no`** | **`default`**} **`speed`**

1.40.1 Purpose

Specifies the speed of the SmartEdge 100 native or Gigabit Ethernet (GE) copper-based port if auto-negotiation is disabled.

1.40.2 Command Mode

Port configuration

1.40.3 Syntax Description

`speed`	Ethernet port speed, according to one of the following keywords: • `10`—10 Mbps • `100`—100 Mbps • `1000`—1000 Mbps

1.40.4 Default

The speed of the port is 1000 Mbps.

1.40.5 Usage Guidelines

Use the **speed** command to specify the speed of the SmartEdge 100 native or GE copper-based port if auto-negotiation is disabled. If auto-negotiation is enabled, this command is ignored.

To specify the copper interface for this port, use the **medium-type** command (in port configuration mode). To set the mode for this port, use the **duplex** command (in port configuration mode).

This command does not apply to GE ports on any other SmartEdge router or to any Fast Ethernet (FE) port on any SmartEdge router. To set the speed of an FE port, use the **medium** command (in port configuration mode).

Use the **no** or **default** form of this command to set the port speed to the default condition.

1.40.6 Examples

The following example sets the speed of a SmartEdge 100 native port `1` to 100 Mbps:

```
[local]Redback(config)#port ethernet 2/1

[local]Redback(config)#speed 100
```

1.41 spf holddown

spf holddown ***interval*** [**level-1** | **level-2**]

no spf holddown

1.41.1 Purpose

Modifies the delay time between an event that triggers a Shortest Path First (SPF) calculation and the calculation itself.

1.41.2 Command Mode

IS-IS router configuration

1.41.3 Syntax Description

`interval`	Delay interval, in seconds, between the trigger event and the SPF computation. The range of values is 1 through 65535; the default value is 10.
`level-1`	Optional. Sets the holddown for level-1 routes independently.
`level-2`	Optional. Sets the holddown for level-2 routes independently.

1.41.4 Default

The SPF holddown is 5 seconds. When you enter this command without specifying level-1 or level-2 routing, SPF holddown value is the same for both level 1 and level 2.

1.41.5 Usage Guidelines

When fast convergence is not enabled, the **`spf holddown`** command modifies the delay time between an event that triggers an SPF calculation and the calculation itself. This delay capitalizes on the fact that computation triggers, such as new link-state protocol data units (LSPs), tend to occur in bursts. Starting the computation after the first event would cause another computation to be scheduled immediately after that due to further events.

When fast convergence is enabled, the holddown time acts as a window within which a specified number of SPFs are run. Because SPF calculations are performed when the topology changes, increasing this value reduces CPU usage, especially in large topologies, but slows the convergence of the network.

Use the **`no`** form of this command to restore the default delay value.

1.41.6 Examples

The following example shows how to set the delay between the event that triggers an SPF calculation and the calculation itself to `20` seconds for `level-1` routing:

```
[local]Redback(config-ctx)#router isis isis1

[local]Redback(config-isis)#spf holddown 20 level-1
```

1.42 spf interval

spf interval ***seconds*** [**level-1** | **level-2**]

no spf interval

1.42.1 Purpose

Configures the minimum interval between Shortest Path First (SPF) calculations.

1.42.2 Command Mode

IS-IS router configuration

1.42.3 Syntax Description

seconds	Minimum amount of time, in seconds, between SPF calculations. The range of values is 1 to 120; the default value is 5.
level-1	Optional. Sets the interval for level-1 routes independently.
level-2	Optional. Sets the interval for level-2 routes independently.

1.42.4 Default

The SPF interval is 10 seconds. When you enter this command without specifying level-1 or level-2 routing, the same SPF interval is used for both levels.

1.42.5 Usage Guidelines

Use the **spf interval** command to configure the minimum interval between SPF calculations.

Because SPF calculations are performed when the topology changes, increasing this value reduces CPU usage, especially in large topologies, but slows the convergence of the network.

Note: The **spf interval** command has no effect when fast convergence is enabled.

Use the **no** form of this command to restore the default SPF interval.

1.42.6 Examples

The following example shows how to set the minimum time between SPF calculations to `25` seconds:

```
[local]Redback(config-ctx)#router isis isis1

[local]Redback(config-isis)#spf interval 25
```

1.43 spf-timers

spf-timers ***delay holdtime***

{**no** | **default**} **spf-timers**

1.43.1 Purpose

Configures the delay time between the receipt of a topology change and the start of the SPF calculation, and as well as the hold time between two consecutive SPF calculations. For OSPFv3, also enables/disables fast convergence.

1.43.2 Command Mode

- OSPF router configuration
- OSPF3 router configuration

1.43.3 Syntax Description

delay	Delay time, in seconds, between the receipt of a topology change and the start of the SPF calculation. The range of values is 0 to 4,294,967,295. For OSPF, the default is 5. A value of 0 starts an SPF calculation immediately when a topology change occurs. For OSFPv3, the default is 0 to enable fast convergence.
holdtime	Minimum time, in seconds, between two consecutive SPF calculations. The range of values is 0 to 4,294,967,295. For OSPF, the default is 10. A value of 0 specifies that there is no minimum wait time between successive SPF calculations. For OSFPv3, the default is 0 to enable fast convergence.

1.43.4 Default

For OSPF, the delay is 5 seconds, and the hold time is 10 seconds.

For OSPFv3, the delay and hold time are both set to 0 to enable fast convergence.

1.43.5 Usage Guidelines

Use the **spf-timers** command to configure the delay time between the receipt of a topology change and the start of the SPF calculation, and as well as the hold time between two consecutive SPF calculations. Setting the delay and hold time to a low value enables faster switching to an alternate path in the event of failure. However, setting the delay and hold time to a low value also consumes more CPU processing time.

For OSPF, use the **spf-timers** command to set the timer values.

For OSPFv3, by default both timers are set to 0 to enable fast convergence. To disable fast convergence in OSPFv3, use the **spf-timers** command with non-zero timer values.

Use the **no** or **default** form of this command to return the delay and hold time to their default values.

1.43.6 Examples

The following examples set the SPF delay and hold time to `2` and `5` , respectively, for OSPF and OSPFv3.

```
[local]Redback#config

[local]Redback(config)#context local

[local]Redback(config-ctx)#router ospf 1

[local]Redback(config-ospf)#spf-timers 2 5

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

```
[local]Redback#config

[local]Redback(config)#context local

[local]Redback(config-ctx)#router ospf3 1

[local]Redback(config-ospf3)#spf-timers 2 5

[local]Redback(config-ospf3)#
```

1.44 spi

spi {*spi-num* | **in** *spi-num* | **out** *spi-num*}

no spi {*spi-num* | **in** *spi-num* | **out** *spi-num*}

1.44.1 Purpose

Specifies a security parameter index (SPI) for this key chain.

1.44.2 Command Mode

Key chain configuration

1.44.3 Syntax Description

spi-num	SPI index number. The range of values is 256 to 4294967295.
in	Assign this SPI number to a key chain for incoming traffic only.
out	Assign this SPI number to a key chain for outgoing traffic only.

1.44.4 Default

None

1.44.5 Usage Guidelines

Use the **spi** command to specify an SPI for this key chain. Use the **in** and **out** keywords to limit the SPI number to incoming or outgoing packets, respectively.

If you do not specify the direction, the SPI is assigned to both incoming and outgoing traffic.

Use the **no** form of this command to remove the SPI from the key chain.

1.44.6 Examples

The following example shows how to assign an SPI number of 256 to incoming traffic:

```
[local]Redback(config-ctx)#key-chain key-in key-id 101

[local]Redback(config-key-chain)#spi in 256
```

1.45 split-horizon

split-horizon [**poison** | **simple**]

{**no** | **default**} **split-horizon**

1.45.1 Purpose

Enables Routing Information Protocol (RIP) or RIP next generation (RIPng) split-horizon processing on the specified interface.

1.45.2 Command Mode

- RIP interface configuration
- RIPng interface configuration

1.45.3 Syntax Description

poison	Optional. Enables split-horizon processing with poison reverse.
simple	Optional. Enables simple split-horizon processing.

1.45.4 Default

Simple split-horizon processing is enabled.

1.45.5 Usage Guidelines

Use the **`split-horizon`** command to enable RIP or RIPng split-horizon processing on the specified interface.

Split-horizon processing prevents routing loops in distance-vector routing protocols. When simple split-horizon is enabled, it blocks route information from being advertised out any interface from which the information originated. The split-horizon mechanism is intended to speed up convergence after a link failure.

Split-horizon processing with poisonous reverse can break the loops more quickly by advertising routes with metric infinity (16) to the link from which they are learned.

Note: This command does not apply to loopback interfaces.

Use the **`no`** or **`default`** form of this command to disable split-horizon processing on the specified interface.

1.45.6 Examples

The following example shows how to disable split-horizon processing on the `fe01` interface:

```
[local]Redback(config-ctx)#router rip rip002

[local]Redback(config-rip)#interface fe01

[local]Redback(config-rip-if)#no split-horizon
```

1.46 sp-pointer

`sp-pointer` ***`sp-pointer`***

`no sp-pointer`

1.46.1 Purpose

Identifies the value of the OID of the first accessible object in the corresponding model-specific MIB definition.

1.46.2 Command Mode

SNMP alarm model configuration

1.46.3 Syntax Description

sp-pointer	Object identifier (OID) in words or numbers of the first accessible object in the corresponding model-specific MIB definition.

1.46.4 Default

None

1.46.5 Usage Guidelines

Use the **sp-pointer** command to identify value of the OID of the first accessible object in the corresponding model-specific MIB definition.

Use the **no** form of this command to remove the value of the OID of the first accessible object in the corresponding model-specific MIB definition.

1.46.6 Examples

The following example shows how to name the **ituAlarmEventType.0.3** OID as the value of the OID of the first accessible object in the corresponding model-specific MIB definition.

```
[local]jazz#config
[local]jazz(config)#snmp alarm model 1 state clear
[local]jazz(config-snmp-alarmmodel)#sp-pointer ituAlarmEventType.0.3
[local]jazz(config-snmp-alarmmodel)#
```

1.47 sse group

sse group ***group_name*** **[network-redundant [raid-0] | disk-redundant]**

no sse group ***group_name***

1.47.1 Command Mode

Global configuration

1.47.2 Syntax Description

group_name — Name of the SSE group. Alphanumeric characters and underscore (_) character.

network-redundant — Configures the group to support network redundancy using RAID 1 over two SSE cards on the same node. Each disk on the same SSE card operates independently unless you specify the **raid-0** keyword. The **network-redundant** or **disk-redundant** keyword is required during SSE group creation.

raid-0 — Optional. Specifies that both disks on an SSE card form a single RAID 0 hard disk.

disk-redundant — Configures the group to support disk redundancy using RAID 1 over two disks on one SSE card. The **network-redundant** or **disk-redundant** keyword is required during SSE group creation.

1.47.3 Default

No SSE group is configured.

1.47.4 Usage Guidelines

Creates an SSE group. Redundancy settings using the **network-redundant [raid-0]** or **disk-redundant** keywords must be configured when you first provision an SSE group.

If network redundancy is configured, up to two SSE cards can be assigned to a group. If disk redundancy is configured, only one SSE card can be assigned to a group. The **raid-0** keyword specifies that both disks on each SSE card are used to form a RAID 0 hard disk; if not specified, the SSE disks operate independently.

An SSE group can only be deprovisioned if no card is bound to it.

1.47.5 Examples

The following examples shows how to create an SSE group.

```
[local]Redback(config)#sse group sse_group_1 network-redundant
```

1.48 sse group switch-over

```
sse group switch-over group_name
```

1.48.1 Command Mode

exec

1.48.2 Syntax Description

group_name	Name of the SSE group.

1.48.3 Default

The SSE group uses the active SSE card or SSE disk.

1.48.4 Usage Guidelines

Performs a manual switchover on an SSE group configured with redundancy to the standby SSE card or SSE disk. The standby SSE card or SSE disk must be available.

Use the **show sse group detail command** to view switchover status and notification of switchover failure.

1.48.5 Examples

```
[local]Redback#sse group switch-over sse_group_1
```

1.49 ssh

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

1.49.1 Purpose

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

1.49.2 Command Mode

exec

1.49.3 Syntax Description

ip-addr	IP address of the host with which to establish the Telnet session.
hostname	Hostname of the host with which to establish the Telnet session. The Domain Name System (DNS) must be enabled to use the *hostname* argument. The *hostname* argument can be specified in the format **name@***ctx-name*, where *ctx-name* is either the name of an existing context or the domain alias of an existing context name.
cipher *name*	Optional. Cipher to use for encrypting the session according to one of the keywords listed in Table 4-2.
admin-name	Optional. Name of administrator to log on to a remote system.
v2	Optional. Forces the use of SSH Version 2.

1.49.4 Default

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

1.49.5 Usage Guidelines

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

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

Table 5 Cipher Names

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

Table 5 Cipher Names

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

1.49.6 Examples

The following example shows how to establish an SSH session with a host at IP address, `192.168.190.32:`

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

1.50 ssh server full-drop

ssh server full-drop [*max-num*]

default ssh server full-drop [*max-num*]

1.50.1 Purpose

Specifies the maximum number of concurrent Secure Shell (SSH) sessions permitted on the system.

1.50.2 Command Mode

Global configuration

1.50.3 Syntax Description

max-num	Maximum number of concurrent SSH sessions permitted on the system. The range of values is 1 to 32; the default value is 16.

1.50.4 Default

A maximum of 16 concurrent SSH sessions is permitted on the system.

1.50.5 Usage Guidelines

Use the **`ssh server full-drop`** command to specify the maximum number of concurrent SSH sessions permitted on the system. The system drops all SSH connection requests after the maximum number of concurrent sessions is established.

The SmartEdge router supports up to 32 concurrent administrative sessions (Telnet and SSH) plus one connection to the console port. If the number of concurrent SSH sessions reaches the maximum set by this command, the remaining administrative sessions must be Telnet sessions.

While this command specifies a global system-wide limit to the number of SSH administrative sessions, you can also specify context-specific maximums for administrative sessions (Telnet and SSH) in one or more contexts, using the **`aaa authentication administrator`** command (in context configuration mode) with the **`maximum sessions`** ***num-sess*** construct. The number of concurrent Telnet and SSH sessions is governed by the configuration of context-specific limits as follows:

- Within a context, if the maximum number of permitted administrative sessions is larger than the maximum number of globally permitted SSH sessions, the remaining sessions (***num-sess–max-num***) for that context must be Telnet sessions.

- Within the system, the maximum number of concurrent sessions permitted is either 32 or the sum of all sessions permitted for each context, whichever is smaller. If the maximum number of concurrent sessions permitted on the system is greater than the maximum number of permitted SSH sessions, the remaining sessions must be Telnet sessions.

Use the **`default`** form of this command to return an attribute to the default value.

1.50.6 Examples

The following example shows how to limit the number of concurrent SSH sessions on the system to `10`. It limits the maximum number of concurrent administrative sessions in the `local` context to `10` and in the `isp1` context to `2`:

```
[local]Redback(config)#ssh server full-drop 10

[local]Redback(config)#context local

[local]Redback(config-ctx)#aaa authentication administrator maximum
sessions 10

[local]Redback(config)#context isp1

[local]Redback(config-ctx)#aaa authentication administrator maximum
sessions 2
```

As a result, there can be no more than 12 concurrent administrative sessions on the system and at least two of them must be Telnet sessions.

1.51 ssh server-keygen

`ssh server-keygen`

1.51.1 Purpose

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

1.51.2 Command Mode

exec

1.51.3 Syntax Description

This command has no keywords or arguments.

1.51.4 Default

None

1.51.5 Usage Guidelines

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

1.51.6 Examples

The following example enables SSH on the system:

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

1.52 ssh server rate-drop

ssh server rate-drop [*rate*]

default ssh server rate-drop [*rate*]

1.52.1 Purpose

Specifies the rate at which the system drops Secure Shell (SSH) connection requests when the start drop value has been reached.

1.52.2 Command Mode

Global configuration

1.52.3 Syntax Description

rate	Percentage of dropping unauthenticated connections after the start drop value has been exceeded. The range of values is 1 to 100; the default value is 100%.

1.52.4 Default

The drop value is 100%.

1.52.5 Usage Guidelines

Use the **ssh server rate-drop** command to specify the rate at which the system drops SSH connection requests when the start drop value has been reached.

This command is used in conjunction with the **ssh server full-drop** and **ssh server start-drop** commands (in global configuration mode) to instruct the system how to handle incoming SSH connection requests. After the number of sessions established on the system equals the number configured for the **ssh server start-drop** value, the system drops incoming SSH connection requests at the value specified by the **ssh server rate-drop** command.

Use the **default** form of this command to return an attribute to the default value.

1.52.6 Examples

The following example shows how to configure the maximum number of SSH sessions to the system to 10; the starting drop number to 5, and the drop value to 50. With this configuration, the system establishes the first five SSH sessions. The system then drops 50% (or one out of every two) subsequent connection requests until ten concurrent sessions are established. The system does not accept any additional SSH connections after ten concurrent SSH sessions are established:

```
[local]Redback(config)#ssh server start-drop 5
[local]Redback(config)#ssh server rate-drop 50
[local]Redback(config)#ssh server full-drop 10
```

1.53 ssh server start-drop

ssh server start-drop [*start-num*]

default ssh server start-drop [*start-num*]

1.53.1 Purpose

Configures the number of Secure Shell (SSH) connections after which the system can start to drop connection requests.

1.53.2 Command Mode

Global configuration

1.53.3 Syntax Description

start-num	Number of connections after which the system starts dropping connection requests. The range of values is 1 to 32; the default value is 16.

1.53.4 Default

The system drops connections after 16 concurrent sessions.

1.53.5 Usage Guidelines

Use the **`ssh server start-drop`** command to configure the number of SSH connections after which the system can start to drop connection requests.

This command is used in conjunction with the **`ssh server rate-drop`** and **`ssh server full-drop`** commands (in global configuration mode) to instruct the system how to handle incoming SSH connection requests. After this value has been exceeded, the system can drop subsequent SSH connection requests at the rate configured by the **`ssh server rate-drop`** command. After the number of connections specified by the **`ssh server full-drop`** command are established, the system drops all subsequent connection requests.

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

1.53.6 Examples

The following example shows how to configure the maximum number of SSH sessions to the system to `10`; the starting drop number to `5`, and the drop rate to `50`. The result is that five SSH connections to the system are allowed. After the fifth connection, subsequent connection requests have a 50% chance of being dropped. The system will not accept any SSH connections after ten concurrent SSH sessions are established:

```
[local]Redback(config)#ssh server start-drop 5
[local]Redback(config)#ssh server rate-drop 50
[local]Redback(config)#ssh server full-drop 10
```

1.54 ssh server v1

`ssh server v1`

{**`no`** | **`default`**} **`ssh server v1`**

1.54.1 Purpose

Enables and disables SSHv1.

1.54.2 Command Mode

exec

1.54.3 Syntax Description

This command has no keywords or arguments.

1.54.4 Default

SSHv1 is enabled by default

1.54.5 Usage Guidelines

Use the **`ssh server v1`** and **`default ssh server v1`** versions of this command to enable SSHv1 on the system. Use the **`no ssh server v1`** version of this command to disable SSHv1 on the system.

1.54.6 Examples

The following example shows how to disable SSHv1 on the system:

```
[local]Redback>no ssh server v1
```

1.55 ssm-map

ssm-map ***source-address acl-group***

1.55.1 Purpose

Enables the router to determine one or more multicast source addresses for group G. The mapping translates IGMPv1 or IGMPv2 membership reports to an IGMPv3 report, enabling the router to continue as if it had initially received an IGMPv3 report.

1.55.2 Command Mode

- igmp service profile configuration
- igmp snooping profile configuration

1.55.3 Syntax Description

source-address	Source IP address. If you specify the `ssm-map` to both IGMP snooping and an IGMP service profile, you must use the same ***source*** in both profiles and the same ***group-acl*** parameter values in both profiles.
group-acl	Multicast group access control list (ACL) filter. Specifies the multicast addresses mapped to the source IP address. If you specify the `ssm-map` to both IGMP snooping and an IGMP service profile, you must use the same ***source*** in both profiles and the same ***group-acl*** parameter values in both profiles.

1.55.4 Default

No SSM map exists. IGMPv1 and IGMPv2 membership reports are not translated to IGMPv3 reports.

1.55.5 Usage Guidelines

The source-specific multicast (SSM) mapping feature is an extension of multicast routing where traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. For multicast groups configured to use SSM, only source-specific multicast distribution trees are created, and not shared trees.

You can enable the router to determine one or more multicast source addresses for group reported in IGMPv1 or IGMPv2 membership reports. The SSM mapping translates IGMPv1 or IGMPv2 membership reports to an IGMPv3 report enable the router to continue as if it had initially received an IGMPv3 report.

When you configure SSM mapping, the SmartEdge router can discover source addresses from a statically configured table.

The following guidelines apply to the use of the **`ssm-map`** command:

- You must configure IGMPv3 on the interface.
- You usually have a map with IGMP. However, if you do not have a map or the map is broken because of a non-existent ACL, you will be running in the (*G) mode, which indicates no map has been established and the multicast is received. If the map is running correctly, you will be running in the (S,G) mode, which indicates a map has been established.
- When you enter the **`no ssm-map`** command, the router removes all SSM map (S,G) states and establishes a (*,G) state.
- SSM mapping does not require all hosts to support IGMPv3. SSM mapping translates IGMPv1 or IGMPv2 membership reports to an IGMPv3 report. This allows hosts running IGMPv1 or IGMPv2 to participate in SSM until the hosts transition to IGMPv3.
- Run the **`show igmp group detail`** and **`show igmp profile`** commands to verify SSM mapping status and operation.

For more information about the **`ssm-map`** command, see *Configuring IP Multicast*.

1.55.6 Examples

1.55.6.1 IGMPv3 Router with SSM Map Configuration and Verification

```
[core]Redback#show configuration
Building configuration...

Current configuration:
!
context core
!
 no ip domain-lookup
!
 interface routing_if
  ip address 10.1.1.1/24
  igmp version 3
  igmp service-profile cust_profile
  pim sparse-mode
 no logging console
!
 ip access-list group_acl
  seq 10 permit igmp 225.0.0.0 0.0.0.255
!
 igmp service-profile cust_profile
  ssm-map 1.1.1.1 group_acl
!
!
!
!
end
```

Check the status and operation of the IGMPv3 router with the `show igmp group detail` and `show igmp profile` commands

```
[core]Redback#show igmp group detail
Group                 : 225.0.0.0
  Interface           : routing_if
  Circuit             : 2/3:511:63:31/1/1/8
  Uptime              : 00:00:48
  Expires             : 00:03:44
  Last reporter       : 100.5.19.2
  Running version : v3
  Compatible mode : v2
  Host Count          : 0
  Filter mode         : Include
  Source list         :
    Source Address  Uptime     Expires    Forwarding  Reporter

   1.1.1.1         00:00:48   00:03:44   Yes         100.5.19.2
   SSM Mapping Source List:
   1.1.1.1

[core]Redback#show igmp profile cust_profile
Service Profile : cust_profile
 Circuit (Interface)  : 2/3:511:63:31/1/1/8 (routing_if)
  Bandwidth used (kbps)/port percent : 0/0%
  Groups (Max Allowed/Joined/Sticky) : 0/1/0
  Priority : 0
  Groups dropped
   Max count exceeded : 0
   Bandwidth exceeded : 0
   Priority drops : 0
   No bandwidth : 0
   Access denied : 0
 ssm-map (1.1.1.1,rtr_acl)
```

1.55.6.2 IGMP Snooper with SSM Map Configuration and Verification

```
! IGMP global configuration
igmp snooping profile snoop_profile
 ssm-map 1.1.1.1 group_acl
!
!
service multiple-contexts
!
!
!
! Bridge global configuration
bridge profile customer_profile
 igmp snooping profile snoop_profile
!


[customer]Redback#show configuration
Building configuration...

Current configuration:
!
context customer
!
 no ip domain-lookup
!
 interface to_ce bridge
  bridge name metro
 no logging console
!
 ip access-list group_acl
  seq 10 permit igmp 225.0.0.0 0.0.0.255
!
 bridge metro
  igmp snooping
   version 3
!
!
!
!
!
end
!
port ethernet 2/2
 no shutdown
 bind interface to_ce bridge
  bridge profile customer_profile
```

Check the status and operation of the IGMP snooper using the `show igmp group detail` command:

```
[customer]Redback#show igmp group detail
Group             : 225.0.0.0
  Interface       : metro
  Circuit         : 2/2:511:63:31/1/1/6
  Uptime          : 00:02:28
  Expires         : 00:02:01
  Last reporter   : 100.5.19.2
  Running version : v3
  Compatible mode : v2
  Host Count      : 0
  Filter mode     : Include
  Source list     :
    Source Address  Uptime     Expires    Forwarding  Reporter

   1.1.1.1         00:02:28   00:02:01   Yes          100.5.19.2
   SSM Mapping Source List:
   1.1.1.1
```

1.56 standby

`standby` {*`ip-addr`* | *`hostname`*}

`no standby` {*`ip-addr`* | *`hostname`*}

1.56.1 Purpose

Configures the IP address or hostname of a standby Dynamic Host Configuration Protocol (DHCP) server.

1.56.2 Command Mode

DHCP relay server configuration

1.56.3 Syntax Description

`ip-addr`	IP address of the standby DHCP server.
`hostname`	Hostname of the standby DHCP server.

1.56.4 Default

No standby DHCP server is assigned.

1.56.5 Usage Guidelines

Use the **`standby`** command to configure the IP address or hostname of a standby DHCP server.

Note: When a DHCP server is unreachable, you either forward packets to its standby DHCP server, or forward packets to all other DHCP servers in a DHCP server group, but not both; the **`standby`** and **`forward-all`** commands are mutually exclusive.

Use the **`no`** form of this command to remove the assignment of the standby DHCP server.

1.56.6 Examples

The following example shows how to configure `10.30.40.55` as the IP address for the standby DHCP server, where `192.168.1.10` is the IP address for the associated primary DHCP server:

```
[local]Redback(config-ctx)#dhcp relay server 192.168.1.10

[local]Redback(config-dhcp-relay)#standby 10.30.40.55

[local]Redback(config-dhcp-relay)#
```

1.57 standby-for

`standby-for` ***`ip-addr`***

{**`no`** | **`default`**} **`standby-for`**

1.57.1 Purpose

Enables a neighbor as a standby neighbor for a primary neighbor.

1.57.2 Command Mode

VPLS profile neighbor configuration

1.57.3 Syntax Description

`ip-addr`	IP address, in the form ***`A.B.C.D`***, of the primary neighbor for which the standby neighbor is being configured.

1.57.4 Default

No standby neighbor is configured.

1.57.5 Usage Guidelines

Use the **`standby-for`** command to enable a neighbor as a standby neighbor for a primary neighbor. A neighbor can serve as a standby for only one primary neighbor. This method of configuring a standby neighbor to reference a primary neighbor allows for establishing the primary and standby pseudowires using independent sets of attributes.

Before a standby neighbor can be enabled, the following conditions must be met:

- A primary neighbor must be configured in the same profile.
- A spoke connection type must be set for the neighbor.

- Local mode must be set to multitenant unit switch (MTU-s).

- No other standby neighbor in the Virtual Private LAN Services (VPLS) profile can reference the same primary neighbor IP address.

Use the **`no`** or **`default`** form of this command to disable a neighbor from being a standby neighbor for a primary neighbor.

1.57.6 Examples

The following example shows how to create a standby neighbor, `10.10.10.1`, for the primary neighbor, `20.20.5.5:`

```
[local]Redback#config

[local]Redback(config)#vpls profile foo

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

[local]Redback(config-vpls-profile-neighbor)#standby-for 20.20.5.5

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

1.58 startup-timer

`startup-timer` ***`seconds`***

1.58.1 Purpose

Specify the startup time used to bring up a Circuit Creation on Demand (CCOD).

1.58.2 Command Mode

dot1q-pvc configuration

1.58.3 Syntax Description

`seconds`	Specifies the number of seconds to bring up a Circuit Creation on Demand (CCOD). Supported range is 90 to 86,400 seconds.

1.58.4 Default

90 seconds

1.58.5 Usage Guidelines

The **`startup-timer`** command specifies the duration dot1q allows for the completion of initial circuit bring up. For example, if a user configures the startup-timer as 't' seconds and attempts to bring up PPPoE subscribers, then after PPA receives PADI and notifies dot1q, dot1q starts the timer and creates a CCOD circuit in the daemon. Dot1q limits the PPPoE negotiation with PPA to complete within the startup-timer setting of 't' seconds. If it does NOT complete within 't' seconds, dot1q tears down the CCOD circuit.

Once configured, this value can be changed but cannot be deleted. However, the default value of 90 seconds is equivalent to not configuring a startup-timer.

1.58.6 Examples

The following example shows how to set the CCOD startup timer:

```
[local]bt21c(config-dot1q-pvc)#startup-timer 95
```

1.59 static

`static` ***`ip-addr`*** [**`source`** ***`source-address`***]

`no static` ***`ip-addr`*** [**`source`** ***`source-address`***]

1.59.1 Purpose

Configures static membership in a multicast group for all circuits associated with an IGMP snooping profile. All circuits attached to the specified IGMP snooping profile will have a static membership in the specified multicast group.

1.59.2 Command Mode

IGMP snooping profile configuration

1.59.3 Syntax Description

ip-addr	IP address of a multicast group.
source*source-address*	Specifies a particular router as a source for the multicast group.

1.59.4 Default

No static memberships are added to the IGMP snooping profile.

1.59.5 Usage Guidelines

Use the **static** command to configure the static membership for multicast groups setting in an IGMP snooping profile. All circuits attached to the specified IGMP snooping profile will have a static membership with the specified multicast group.

Use the **no** form of this command to delete a static membership for a multicast group.

1.59.6 Examples

The following example shows how to configure an IGMP snooping profile called `sanjose1` with a static membership for a multicast group with the `233.1.1.1` IP address:

```
[local]Router#configure

[local]Router(config)#igmp snooping profile sanjose1

[local]Router(config-igmp-snooping-profile)#static 233.1.1.1
```

1.60 static encapsulation

static encapsulation l2tpv3 {session-id in *rx-session-id* out *tx-session-id*} | {cookie {*inbound* | *outbound*}}

no static encapsulation l2tpv3 {cookie {in | out} | session-id

1.60.1 Purpose

Configures fixed values for the L2TPv3 tunnel cookie and session-id parameters. The L2TPv3 tunnel is running in a VPLS pseudowire.

1.60.2 Command Mode

VPLS profile neighbor configuration

1.60.3 Syntax Description

`cookie` *`inbound`*	Sets the parameters of inbound L2TPv3 cookies. The syntax of *`inbound`* argument follows: `in` *`rx-size rx-4-byte-high-value rx-4-byte-low-value`*
`cookie` *`outbound`*	Sets the parameters of outbound L2TPv3 cookies. The syntax of *`outbound`* argument follows: `out` *`tx-size tx-4-byte-high-value tx-4-byte-low-value`*
`session-id in` *`rx-session-id`* `out` *`rx-session-id`*	Sets the session-ids of inbound and outbound L2TPv3 encapsulated packets.
`l2tpv3`	Specifies that this command apples to static L2TPv3 sessions.
`rx-size`	Inbound (rx) cookie size (32 or 64 bits).
`rx-4-byte-high-value`	Inbound (rx) cookie 4-byte high-value (0 to 4294967295)
`rx-4-byte-low-value`	Inbound (rx) cookie 4-byte low-value (0 to 4294967295).
`tx-size`	Outbound (tx) cookie size (32 or 64 bits).
`tx-4-byte-high-value`	Outbound (tx) cookie 4-byte high-value (0 to 4294967295).
`tx-4-byte-low-value`	Outbound (tx) cookie 4-byte low-value (0 to 4294967295).

1.60.4 Default

The session-ID and cookie parameters are dynamically configured (not static) when the L2TPv3 sessions begins.

1.60.5 Usage Guidelines

Use this command to configure fixed values for the L2TPv3 tunnel cookie and session-id parameters. The L2TPv3 tunnel is running in a VPLS pseudowire.

Note: You must configure the source address of L2TPv3 encapsulated packets by entering it using the `ip soft-gre` command as shown in the example below.

Use the **no** form of this command to delete the fixed values set for the L2TPv3 session-ID and cookie parameters.

1.60.6 Examples

The following example shows the fixed configuration of the L2TPv3 cookie and session-ID parameters for the VPLS pseudowire bound to the interface targeted to the neighbor with IP address `67.1.1.2`. The L2TPv3 tunnel is configured only for outbound cookies:

```
[local]Router#configure
[local]Router(config)#context local
[local]Router(config-ctx)#ip soft-gre 10.10.10.1                          //source address
[local]Router(config-ctx)#exit
[local]Router(config)#vpls profile P11
[local]Router(config-vpls-profile)#neighbor 67.1.1.2                      //destination address
[local]Router(config-vpls-profile-neighbor)#pw-label in 5001 out 5001
[local]Router(config-vpls-profile-neighbor)#static encapsulation l2tpv3 session-id in 30 out 30
[local]Router(config-vpls-profile-neighbor)#static encapsulation l2tpv3 cookie out 32 0 15
[local]Router(config-vpls-profile-neighbor)#end
```

1.61 static-group

static-group ***group-addr source-addr***

no static-group ***group-addr source-addr***

1.61.1 Purpose

Creates a static multicast route, (*,G) or (S,G), with a subscriber circuit as the outgoing interface (OIF).

1.61.2 Command Mode

IGMP service profile configuration

1.61.3 Syntax Description

group-addr	Multicast group IP address.
source-addr	Multicast source IP address.

1.61.4 Default

None

1.61.5 Usage Guidelines

Use the **static-group** command in create a static multicast route, (*,G) or (S,G), with a subscriber circuit as the OIF.

Note: Protocol Independent Multicast (PIM) normally creates dynamic multicast routes; the **static-group** command allows you to create static multicast routes.

An OIF is an outgoing circuit that receives traffic destined for a given multicast group. When the static multicast route is configured in IGMP service profile configuration mode, the OIF is a subscriber circuit.

To configure all subscriber circuits on a multibind interface to receive multicast traffic for a specified multicast group, configure the **static-group** command in an Internet Group Management Protocol (IGMP) service profile that is bound to a subscriber (default) profile.

Use the **no** form of this command to delete the static multicast route.

1.61.6 Examples

The following example shows how to create a static multicast route, `10.10.10.1 20.20.20.0`, for IGMP service profile, `pro78`, and then applies the service profile to the default subscriber profile:

```
[local]Redback(config-context)#igmp service-profile pro78

[local]Redback(config-igmp-service-profile)#static-group 10.10.10.1
20.20.20.2

[local]Redback(config-igmp-service-profile)#exit

[local]Redback(config-context)#subscriber default

[local]Redback(config-sub)#ip igmp service-profile pro78
```

1.62 stats-collection

stats-collection

1.62.1 Purpose

Accesses stats collection configuration mode.

1.62.2 Command Mode

Global configuration

1.62.3 Syntax Description

This command has no keywords or arguments.

1.62.4 Default

None

1.62.5 Usage Guidelines

Use the **`stats-collection`** command to access stats collection configuration mode.

1.62.6 Examples

The following example shows how to access stats collection configuration mode:

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

[local]Redback(config-stats-collect)#
```

1.63 std-interval

`std-interval` ***`interval`***

{**`no`** | **`default`**} **`std-interval`**

1.63.1 Purpose

Configures the interval between transmission of continuity check message (CCM) PDUs from each maintenance association endpoint (MEP) in the current maintenance association (MA).

1.63.2 Command Mode

CCM configuration

1.63.3 Syntax Description

`std-interval` ***`interval`***	Sets the time interval between transmitting CCM PDUs. The transmission interval can be no less than 3 milliseconds and no more than 10 minutes. The default transmission rate is 100 milliseconds.

1.63.4 Default

100 milliseconds

1.63.5 Usage Guidelines

Use the **`std-interval`** command to configure the interval between transmission of CCM PDUs from each MEP in the current MA. The following list shows the allowed values for the ***`interval`*** argument:

- 10m: (10 minutes)
- 1m: (1 minute)
- 10s: (10 seconds)
- 1s: (1 second)
- 100ms: (100 milliseconds)
- 10ms: (10 milliseconds)
- 3ms: (3-1/3 milliseconds)

When you configure a MEP on a link group, the CFM process transmits CCM PDUs over a single active circuit in the bundle. If the active circuit goes down, a fault might not be reported if the no CCM PDUs are lost during the time it takes to redirect traffic to other links in the bundle. Setting the ***`interval`*** argument to a shorter time period reduces the likelihood of not reporting a fault.

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

1.63.6 Examples

In the following example, the **`std-interval`** command sets the interval between transmission of CCM PDUs to 10 milliseconds:

```
[local]Redback(config)#ethernet-cfm instance-1
[local]Redback(config-ether-cfm)#level 4
[local]Redback(config-ether-cfm)#domain-name sbc.com
[local]Redback(config-ether-cfm)#disable-linktrace
[local]Redback(config-ether-cfm)#group-mac 01:01:01:01:01:01
[local]Redback(config-ether-cfm)#maintenance-association bayarea
[local]Redback(config-ether-cfm-ma)#ccm
[local]Redback(config-ether-cfm-ma-ccm)#frame-loss 10
[local]Redback(config-ether-cfm-ma-ccm)#std-interval 10ms
```

1.64 sticky-groups

```
sticky-groups acl-name
no sticky-groups
```

1.64.1 Purpose

Enables Internet Group Management Protocol (IGMP) groups to be sticky.

1.64.2 Command Mode

IGMP service profile configuration

1.64.3 Syntax Description

acl-name	Access control list (ACL) of groups to be sticky.

1.64.4 Default

Sticky groups are disabled.

1.64.5 Usage Guidelines

Use the **sticky-groups** command to enable IGMP groups to be sticky.

Groups defined by the ACL will never be dropped, unless an explicit leave for that group is received.

Use the **no** form of this command to disable sticky groups.

1.64.6 Examples

The following example enables IGMP groups, as specified by the ACL, `foo3`, to be sticky:

```
[local]Redback(config-ctx)#igmp service-profile bar

[local]Redback(config-igmp-service-profile)#sticky-groups foo3
```

1.65 stub-router

stub-router [**on-startup** [*interval*] | **bgp-converge-delay** [*interval*] | **strict-bgp-tracking**]

no stub-router

1.65.1 Purpose

Configures the router as an Open Shortest Path First (OSPF) or OSPF Version 3 (OSPFv3) stub router.

1.65.2 Command Mode

- OSPF router configuration
- OSPF3 router configuration

1.65.3 Syntax Description

on-startup	Optional. Sets router as a stub router on startup, and continues until timer expires.
interval	Optional. Timer interval in seconds. The range of values is 10 to 3,600 seconds; the default value is 210 seconds.

`bgp-converge-delay`	Optional. Sets router as a stub router on startup, and continues until timer expires or the Border Gateway Protocol (BGP) converges.
`strict-bgp-tracking`	Optional. Sets router as a stub router whenever BGP has not converged. If BGP is not converged or not running, stub router operation remains active. There is no time out for the stub router as long as BGP is not converged.

1.65.4 Default

The router is not configured as a stub router.

1.65.5 Usage Guidelines

Use the **`stub router`** command to configure the router as an OSPF or OSPFv3 stub router. To avoid transit traffic, a stub router advertises all of its links using the maximum cost of 65,535.

Use the **`set-overload-bit`** command in IS-IS router configuration mode without any option to indefinitely set the stub router configuration.

Use the **`on-startup`** keyword if BGP is not configured on the router, or if BGP convergence is not an issue. When the router starts, OSPF or OSPFv3 temporarily sets the stub router configuration to allow the router to reach full functionality, with complete routing information on the router.

Use the **`bgp-converge-delay`** keyword if BGP is not fully converged, and you want to use the stub router configuration to delay other routers from sending transit traffic through the router until BGP converges. If the BGP converge delay time expires, the stub router configuration is removed, even if BGP has not converged; therefore, you should adjust the BGP converge delay time so that it is appropriate to your network size and the amount information in the BGP routing table.

Use the **`strict-bgp-tracking`** keyword if BGP is not fully converged, and you want to use the stub router configuration to stop other routers from sending transit traffic through the router to until BGP converges. The stub router configuration is removed only when full BGP convergence is reached.

Use the **`no`** form of this command to remove the stub router configuration.

1.65.6 Examples

The following example shows how to configure the SmartEdge router as an OSPF stub router:

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

[local]Redback(config-ospf)#stub-router
```

1.66 subnet (DHCP Server Policy)

subnet ***ip-addr/subnet-mask*** [**name** ***subnet-name***]

no subnet ***ip-addr/subnet-mask*** [**name** ***subnet-name***]

1.66.1 Purpose

Creates a subnet for this internal Dynamic Host Configuration Protocol (DHCP) server and accesses DHCP subnet configuration mode.

1.66.2 Command Mode

DHCP server configuration

1.66.3 Syntax Description

ip-addr/subnet-mask	IP address and subnet mask for this subnet.
name ***subnet-name***	Optional. Name of the subnet; it must be unique.

1.66.4 Default

No subnets are created for any DHCP server.

1.66.5 Usage Guidelines

Use the **subnet** command to create a subnet for this internal DHCP server and access DHCP subnet configuration mode.

The value of the ***ip-addr*** and ***subnet-mask*** arguments must match the value of one of the ***ip-addr*** and ***subnet-mask*** arguments that you specified, using the **ip address** command (in interface configuration mode), for the interface that you enabled for this DHCP server, using the **dhcp server** command (in interface configuration mode). For more information about the **ip address** command, see the *Command List*

Use the **name** ***subnet-name*** construct to assign a unique name to this subnet.

Use the **no** form of this command to delete the subnet from the DHCP server configuration.

1.66.6 Examples

The following example shows how to create the `sub2` subnet:

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

[local]Redback(config-ctx)#dhcp-if multibind

[local]Redback(config-if)#ip address 12.1.1.0/24

[local]Redback(config-if)#ip address 13.1.1.1/24 secondary

[local]Redback(config-if)#dhcp server 13.1.1.1

[local]Redback(config-if)#exit

[local]Redback(config-ctx)#dhcp server policy

[local]Redback(config-dhcp-server)#subnet 12.1.1.0/24 name sub2

[local]Redback(config-dhcp-subnet)#
```

1.67 subnet (DHCPv6 Server Policy)

subnet ***ipv6-prefix/subnet-mask*** [**name** ***subnet-name***]

no subnet ***ipv6-prefix/subnet-mask*** [**name** ***subnet-name***]

1.67.1 Purpose

Accesses DHCPv6 server policy subnet configuration mode, where you can configure DHCPv6 server attributes that are applicable only to subscribers in the specified subnet.

1.67.2 Command Mode

DHCPv6 server policy configuration

1.67.3 Syntax Description

ipv6-prefix	Specifies the IPv6 subnet to which you want apply a specific set of DHCPv6 server attributes. The IPv6 subnet must not overlap with any other interface prefix.
name *subnet-name*	Optional. Name of the subnet; it must be unique.

1.67.4 Default

None.

1.67.5 Usage Guidelines

Use the **subnet** command to access DHCPv6 server policy subnet configuration mode, where you can configure DHCPv6 server attributes that are applicable only to subscribers in the specified subnet.

Options configured for the subnet (in DHCPv6 server policy subnet configuration mode) take precedence over options specified in the top-level DHCPv6 server policy (DHCPv6 server policy configuration mode).

Only those options that are administratively configured for a subnet differ from the options configured in the top-level DHCPv6 server policy (in DHCPv6 server policy configuration mode). If you do not specify a particular DHCPv6 policy option for the subnet (in DHCPv6 server policy subnet configuration mode), the subnet takes its configuration from the top-level DHCPv6 server policy configuration (as specified in DHCPv6 server policy configuration mode).

Use the **no** version of this command to remove an IPv6 subnet configuration from a DHCPv6 server policy.

1.67.6 Examples

The following example shows how to access DHCPv6 server policy subnet configuration mode:

```
[local]Redback(config-ctx)#dhcpv6 server
[local]Redback(config-dhcp-server)#subnet 2001:a:b:3f::/64
[local]Redback(config-dhcpv6-subnet)#
```

The following example shows a sample DHCPv6 server policy configuration where the administrator specifies a different set of DHCPv6 attributes for subscribers in the subnet 2001:a:db8:3f::/6. In this example, subscribers in the specified subnet (2001:a:b:3f::/6) use a domain for DNS resolution (NY1.com) that is different from the domain used by all other clients:

```
[local]Redback(config-ctx)#dhcpv6 server
[local]Redback(config-dhcpv6-server)#option domain-name-server 2005:db8:b:3f::2
[local]Redback(config-dhcpv6-server)#option domain-search SJ1.com
[local]Redback(config-dhcp-server)#subnet 2001:a:db8:3f::/64
[local]Redback(config-dhcpv6-subnet)#option domain-search NY1.com
```

1.68 subscriber (context configuration)

subscriber {**default** | **name** ***sub-name*** | **profile** ***prof-name***}

no subscriber {**default** | **name** ***sub-name*** | **profile** ***prof-name***}

1.68.1 Purpose

Creates a default subscriber profile, a named subscriber profile, or an individual named subscriber record, and enters subscriber configuration mode.

1.68.2 Command Mode

Context configuration

1.68.3 Syntax Description

default	Specifies the creation of the default subscriber profile.
name ***sub-name***	Named subscriber record.
profile ***prof-name***	Named subscriber profile.

1.68.4 Default

No default profile, named subscriber profile, or subscriber record exists.

1.68.5 Usage Guidelines

Use the **subscriber** command to configure a default subscriber profile, a named subscriber profile, or an individual named subscriber record, and enter subscriber configuration mode. When created, a default or named subscriber profile is empty; there are no default values associated with it.

Use the **default** keyword to create a default subscriber profile. Each configured attribute in the default profile is appended to all subscriber records in the context. However, if you configure a named subscriber profile or a subscriber record, attribute values in the named subscriber profile or subscriber record override the values set in the default profile record.

Use the **name** ***sub-name*** construct to create a named subscriber record. Attribute values in the subscriber record override the values set in the named and default subscriber profiles. This is true whether the named subscriber record is created through the local configuration or is accessed through a Remote Authentication Dial-In User Service (RADIUS) server.

Use the **profile** ***prof-name*** construct to create a named subscriber profile. Each configured attribute in the named profile is appended to any subscriber record to which the profile is assigned. However, if you configure a subscriber record, attribute values in the subscriber record override the values set in the named subscriber profile.

The maximum length for the ***sub-name*** argument together with a separator character and the domain name for the subscriber, is 253 characters. The domain name is the name of the context in which the subscriber is configured, or a domain alias for the context.

For information about configuring domain aliases, see *Configuring Contexts* For information about configuring the format, ***sub-name@domain-name***, see *Configuring Authentication, Authorization, and Accounting*.

If this subscriber will be a user of clientless IP service selection (CLIPS), or if this named or default subscriber profile is intended for such subscribers, you must adhere to the following restrictions:

- For static CLIPS circuits, a subscriber record or its assigned profile must have one and only one IP address. Use the **ip address** command (in subscriber configuration mode) to assign the IP address.

- For dynamic CLIPS circuits, a subscriber record or profile must have no IP addresses; instead, use the **dhcp max-addrs** command (in subscriber configuration mode) and specify `1` as the value for the ***max-num*** argument. For more information about the **dhcp max-addr** command, see *Configuring DHCP*.

Use the **no** form of this command to delete a default or named profile or named subscriber record.

Note: If you modify a subscriber record for a subscriber that is already bound, you must use the **clear subscriber** command (in exec mode) for the changes to take effect. For more information on the **clear subscriber** command, see *Configuring Contexts and Interfaces*. The subscriber session is ended and restarted with the new parameters. This is true regardless of whether subscriber records are configured locally or in RADIUS.

1.68.6 Examples

The following example creates the subscriber record, `dave:`

```
[local]Redback(config)#context isp2
[local]Redback(config-ctx)#subscriber name dave
[local]Redback(config-sub)#
```

The following example configures primary and secondary Domain Name System (DNS) servers for the default subscriber profile:

```
[local]Redback(config-ctx)#subscriber default
[local]Redback(config-sub)#dns primary 10.1.1.1
[local]Redback(config-sub)#dns secondary 10.1.1.2
```

The following example creates the named profile, `isp2`:

```
[local]Redback(config)#context isp2
[local]Redback(config-ctx)#subscriber profile isp2
[local]Redback(config-sub)#
```

An RFlow profile can be applied to a static subscriber record through the **`subscriber name`** or **`subscriber profile`** context command either in the ingress direction, egress direction, or bi-directionally to profile`p1` for a user **`dave`**:

```
[local]Redback(config)# context p1
[local]Redback(config-ctx)# subscriber name dave
[local]Redback(config-sub)# flow apply ip profile p1 in
```

1.69 subscriber dhcp-lease idle-timeout

`subscriber dhcp-lease idle-timeout`

`no subscriber dhcp-lease idle-timeout`

1.69.1 Purpose

Enables setting subscriber-specific DHCP lease times with internal DHCP server and DHCP proxy server.

1.69.2 Command Mode

Context configuration

1.69.3 Syntax Description

This command has no keywords or arguments.

1.69.4 Default

No default profile, named subscriber profile, or subscriber record exists.

1.69.5 Usage Guidelines

Use the **`subscriber dhcp-lease idle-timeout`** command in context configuration mode to enable setting subscriber-specific DHCP lease times with internal DHCP server and DHCP proxy server.

Normally, the **`idle`** ***`minutes`*** option provides a session idle timeout value to the subscriber currently being configured, that is, the subscriber-specific idle timeout value. However, when the **`subscriber dhcp-lease idle-timeout`** command is entered for the context, the **`idle`** ***`minutes`*** option instead sets the subscriber-specific DHCP lease times.

Alternatively, you can configure the subscriber lease time using your RADIUS database and providing a value for RADIUS Attribute #28-Idle Timeout. If you use your RADIUS database, you must also configure the SmartEdge router with the **`subscriber dhcp-lease idle-timeout`** command.

After you enter the **`subscriber dhcp-lease idle-timeout`** command to enable setting subscriber-specific DHCP lease times, you can set the idle timeout value for each subscriber with the **`timeout idle`** command, However, when subscriber-specific DHCP lease times have been enabled, the **`direction`** and **`threshold`** keyword in the **`timeout idle`** command have no meaning and are ignored.

DHCP split lease times apply when the SmartEdge router is configured as a DHCP proxy and the subscriber-specific DHCP lease times are set separately from the external DHCP server's setting for DHCP lease times.

The value entered for the subscriber lease time should be less than 50% of the external DHCP server lease time for split lease to be effective.

When you configure shorter subscriber-specific lease times, DHCP clients have a shorter failover time (to the backup ICR SmartEdge chassis) and allow the DHCP server to reclaim inactive clients' IP address leases more quickly.

Caution: Setting a too low lease time can adversely affect the session bring up rate as well as the recovery rate of DHCP and CLIPS sessions. A too low lease time might cause the SmartEdge router to lose subscribers IP leases.

See the following example.

Use the **`no`** form of this command to disable subscriber-specific DHCP lease times.

1.69.6 Examples

The following example shows how to configure the DHCP lease time specifically for the subscriber named `dhcpuser`:

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

[local]Redback(config-ctx)#subscriber dhcp-lease idle-timeout

[local]Redback(config-ctx)#subscriber name dhcpuser

[local]Redback(config-sub)#timeout idle 20
```

1.70 subscriber dhcp-server-lease absolute-timeout

`subscriber dhcp-server-lease absolute-timeout`

`no subscriber dhcp-server-lease absolute-timeout`

1.70.1 Purpose

Uses either the subscriber absolute timeout or the RADIUS session-timeout as the DHCP lease time for DHCP and CLIPS subscriber sessions. This command is enabled by default. Use the no form of the command (**`no subscriber dhcp-server-lease absolute-timeout`**) to override this default behavior and to use the absolute-timeout (session-timeout) value as the session duration rather than as the DHCP lease time.

1.70.2 Command Mode

Context configuration

1.70.3 Syntax Description

This command has no keywords or arguments.

1.70.4 Default

By default, the **`subscriber dhcp-server-lease absolute-timeout`** command is in effect, and the absolute-timeout (session-timeout) value is used as the DHCP lease.

1.70.5 Usage Guidelines

This command applies only to the internal DHCP server. Use the **`no subscriber dhcp-server-lease absolute-timeout`** command in context mode to override the default behavior and apply the absolute-timeout (session-timeout) value as the duration of the session. When the **`no subscriber dhcp-server-lease absolute-timeout`** command is configured, AAA does not propagate the absolute-timeout value to DHCP. Instead, AAA uses the absolute-timeout value as the session timeout to terminate the session after the timer expires. To restore the default behavior of using the absolute-timeout value as the DHCP lease, use the **`subscriber dhcp-server-lease absolute-timeout`** command. Note that this command is not shown in the configuration list, even if it is explicitly entered; however, the no form does appear. .

1.71 subscriber (IPv6 software license configuration)

`subscriber active ipv6` ***`sub-num`*** **`password`** ***`password`***

`no subscriber active ipv6` ***`sub-num`*** **`password`** ***`password`***

1.71.1 Purpose

Configures the system-level features of IPv6 subscriber sessions.

1.71.2 Command Mode

Software license configuration

1.71.3 Syntax Description

`active ipv6` ***`sub-num`***	Number of active subscriber sessions licensed, according to one of the following keywords: • `500`—Licenses 500 active subscriber sessions. • `64000`—Licenses 64,000 active IPv6 subscriber sessions.
`password`	Specifies that the password that follows is not encrypted. For IPv6 subscriber sessions, the SmartEdge router supports only unencrypted passwords.
`password`	Paid license password that is required to enable the IPv6 subscriber function.

1.71.4 Default

No subscriber sessions are licensed.

1.71.5 Usage Guidelines

Use the **subscriber** command to configure the system-level features of IPv6 subscriber sessions. This command configures the number of concurrent active subscriber sessions allowed.

Note: An individual dual-stack subscriber session requires one IPv4 license and one IPv6 license. Those IPv4 and IPv6 licenses are consumed at the time of authentication, whether subscribers are authenticated locally or through RADIUS. The licenses are not returned to the license pool until the entire subscriber session for both stacks (IPv4and IPv6) is down. For example, if the IPv4 session for a dual-stack subscriber goes down while the IPv6 session remains active, the IPv4 license is not returned to the license pool until the IPv6 session goes down, at which time both licenses (IPv4 and IPv6) are returned to the pool.

Note: Subscriber sessions remain active during PPA traffic card software upgrades.

Note: IPv6 subscriber licenses are supported on the SmartEdge 100, 400, 800, and 1200 routers only.

Use the **no** form of this command to disable support for IPv6 subscriber sessions.

1.71.6 Examples

The following example show how to license `500` active subscriber sessions:

```
[local]Redback(config-license)#subscriber active ipv6 500 password sub-active-ipv6-password
sub-active16-password
```

1.72 subscriber (software license configuration)

```
subscriber {active sub-num | bandwidth kbits | dynamic-service |
high-availability} {encrypted 1 | password} password

no subscriber {active sub-num {encrypted 1 | password} password |
bandwidth kbits | dynamic-service | high-availability}

default subscriber bandwidth 60
```

1.72.1 Purpose

Configures the system-level features of subscriber sessions.

1.72.2 Command Mode

Software license configuration

1.72.3 Syntax Description

`active` *`sub-num`*	Number of active subscriber sessions licensed, according to one of the following keywords: • `2000`—Licenses 2,000 active subscriber sessions. • `4000`—Licenses 4,000 active subscriber sessions. • `8000`—Licenses 8,000 active subscriber sessions. • `16000`—Licenses 16,000 active subscriber sessions. • `24000`—Licenses 24,000 active subscriber sessions. • `32000`—Licenses 32,000 active subscriber sessions. • `48000`—Licenses 48,000 active subscriber sessions. The number of active subscriber sessions that you can enter depends on your licenses and the SmartEdge router model.
`bandwidth` *`kbits`*	Average bandwidth, in kilobits per second (kbps) for each active subscriber session to be licensed, according to one of the following keywords: • `60`—Specifies 60,000 bps. • `100`—Specifies 100,000 bps. • `250`—Specifies 250,000 bps. • `1000`—Specifies 1,000,000 bps.

`dynamic-service`	Enables dynamic services features and functions for subscribers. See the Usage Guidelines section for more information.
`high-availability`	Enables subscriber sessions to be preserved during a controller card switchover.
`encrypted 1`	Specifies that the password that follows is encrypted.
`password`	Specifies that the password that follows is not encrypted.
`password`	Paid license password that is required to enable the subscriber function. The ***`password`*** argument is unique for each value of the ***`sub-num`*** and ***`kbits`*** arguments and for each function; it is provided at the time the license is paid.

1.72.4 Default

No subscriber sessions are licensed, the average bandwidth is 60 kbps for each licensed subscriber session, and the dynamic service and high-availability options for licensed subscriber sessions are disabled.

1.72.5 Usage Guidelines

Use the **`subscriber`** command to configure the system-level features of subscriber sessions. This command configures the number of concurrent active subscriber sessions allowed and the average bandwidth for each subscriber session. You can also use it to enable subscriber dynamic services and specify whether subscriber sessions are to be preserved during a controller card switchover.

You can specify a password in either encrypted or unencrypted form. The **`show configuration`** command (in any mode) does not display either form of the password.

Note: Subscriber sessions remain active while the line card PPA software is upgraded with the new patch release.

Use the **`active`** ***`sub-num`*** construct to specify the number of active licensed subscriber sessions. You can enter the **`subscriber`** command multiple times with this construct. The number of licensed active sessions allowed on the system is the sum of the individual licensed values entered. This construct also enables clientless IP service selection (CLIPS) circuits. You must use this construct to enable any of the other subscriber functions.

Use the **`bandwidth`** ***`kbits`*** construct to specify a larger bandwidth for the licensed subscriber sessions.

Use the **dynamic-service** keyword to enable dynamic services features and functions. These features and functions include:

- Asynchronous Transfer Mode (ATM) nonstatic profiles and the dynamic assignment of ATM profiles to on-demand permanent virtual circuits (PVCs)
- CLIPS dynamic circuits
- Remote Authentication Dial-In User Service (RADIUS) refresh

Use the **high-availability** keyword to ensure that subscribers sessions are not dropped during a controller card switchover. This option requires that your SmartEdge router has two controller cards installed.

Note: The SmartEdge 100 router does not have a standby controller card.

Use the **no** form of this command to enable the default value for the specified keyword. A password is required for this form only if you are disabling the license for the number of active subscribers.

Use the **default** form of this command to revert the subscriber attributes to their default values without any additional licensed software features. The default is 60 kbps bandwidth for each licensed subscriber session and dynamic service and high-availability options for licensed subscriber sessions are disabled.

1.72.6 Examples

The following example shows how to license `40000` active subscriber sessions, specify the average bandwidth for them, enable dynamic services, and enable sessions to be preserved during a switchover. (The system has two controller cards installed):

```
[local]Redback(config-license)#subscriber active 16000 password
sub-active16-password

[local]Redback(config-license)#subscriber active 8000 password
sub-active8-password

[local]Redback(config-license)#subscriber active 2000 password
sub-active2-password

[local]Redback(config-license)#subscriber bandwidth 250 password
sub-band250-password

[local]Redback(config-license)#subscriber dynamic-service password
sub-dynamic-password

[local]Redback(config-license)#subscriber high-availability password
sub-high-password
```

1.73 summary-address (IS-IS)

summary-address *ip-addr* {*netmask* | */prefix-length*} [**level-1** | **level-2**]

no summary-address *ip-addr* {*netmask* | */prefix-length*} [**level-1** | **level-2**]

1.73.1 Purpose

Provides IP route aggregation during the processes of route leaking and route redistribution.

1.73.2 Command Mode

IS-IS address family configuration

1.73.3 Syntax Description

ip-addr	IP address of the route.
netmask	Network mask in the form *A.B.C.D*.
prefix-length	Prefix length. The range of values is 0 to 32.
level-1	Optional. Sets IP route aggregation for level 1 routes independently.
level-2	Optional. Sets IP route aggregation for level 2 routes independently.

1.73.4 Default

No route aggregation is applied. When you enter this command without specifying the Intermediate System-to-Intermediate System (IS-IS) level, a summary address is only applied to an IS-IS level 2 domain.

1.73.5 Usage Guidelines

Use the **summary-address** command to provide IP route aggregation during the processes of route leaking and route redistribution.

Note: Currently, the **interarea-distribute** command is available only for IPv4 and IPv6 unicast address families.

A summary address is active if one or multiple more-specific routes are found during route leaking, redistribution, or both. Otherwise, the summary address is nonactive, and all IP addresses are included in the local link-state protocol (LSP) data units. If the summary address is active, all more-specific addresses in the summary range are suppressed during the local LSP generation. The metric of the summary address is equal to the lowest metric of all more-specific routes. A black hole is installed for an active summary address.

Use the **no** form of this command to remove the route aggregation from the configuration.

1.73.6 Examples

The following example shows how to suppress all more-specific level 2 routes that match the `10.0.0.0 255.0.0.0` constraint:

```
[local]Redback(config-ctx)#router isis isis1

[local]Redback(config-isis)#address-family ipv4 unicast

[local]Redback(config-isis)#summary-address 10.0.0.0 255.0.0.0
```

1.74 summary-address (OSPF)

summary-address {*ip-addr/prefix-length* | *ipv6-addr/prefix-length*} [**not-advertise** | **tag** *tag*]

no summary-address {*ip-addr/prefix-length* | *ipv6-addr/prefix-length*} [**not-advertise** | **tag** *tag*]

1.74.1 Purpose

Summarizes external routes that are redistributed into the Open Shortest Path First (OSPF) or OSPF Version 3 (OSPFv3) routing domain.

1.74.2 Command Mode

- OSPF router configuration
- OSPF3 router configuration

1.74.3 Syntax Description

ip-addr/prefix-length	Specifies the IP address, in the form *A.B.C.D*, and the prefix length, separated by the slash (/) character. The range of values for the *prefix-length* argument is 0 to 32.
ipv6-addr/prefix-length	Specifies the IP Version 6 (IPv6) address, in the form *A:B:C:D:E:F:G:H*, and the prefix length, separated by the slash (/) character. The range of values for the *prefix-length* argument is 0 to 128.
not-advertise	Optional. Suppresses the advertisement of Type 5 link-state advertisements (LSAs) for routes contained in the specified IP address range.
tag *tag*	Optional. Route tag included in translated external route summarization Type 5 link-state advertisements (LSAs). An unsigned 32-bit integer, the range of values is 1 to 4,294,967,295; the default value is 0.

1.74.4 Default

No external redistributed routes are summarized.

1.74.5 Usage Guidelines

Use the **summary-address** command to summarize external routes that are redistributed into the OSPF or OSPFv3 routing instance.

Use the **no** form of this command to disable route summarization of an IP address block and allow all individual routes to be redistributed into the OSPF or OSPFv3 routing instance.

1.74.6 Examples

The following example shows how to advertise a summary of the routes that fall into the `10.0.0.0 255.0.0.0` range:

```
[local]Redback(config-ospf)#summary-address 10.0.0.0 255.0.0.0
```

1.75 summary-address (RIP)

summary-address {*ip-addr/prefix-length* | *ipv6-addr/prefix-length*} [**metric** *metric*]

{**no** | **default**} **summary-address** {*ip-addr/prefix-length* | *ipv6-addr/prefix-length*} [**metric** *metric*]

1.75.1 Purpose

Summarizes information about Routing Information Protocol (RIP) or RIP next generation (RIPng) routes sent over the specified interface in RIP or RIPng update packets.

1.75.2 Command Mode

- RIP interface configuration
- RIPng interface configuration

1.75.3 Syntax Description

ip-addr/prefix-length	Specifies the IP address, in the form *A.B.C.D*, and the prefix length, separated by the slash (/) character. The range of values for the *prefix-length* argument is 0 to 32.
ipv6-addr/prefix-length	Specifies the IP Version 6 (IPv6) address, in the form *A:B:C:D:E:F:G:H*, and the prefix length, separated by the slash (/) character. The range of values for the *prefix-length* argument is 0 to 128.
metric *metric*	Optional. Metric used for the route. The range of values is 1 to 16. If this construct is not used, the value set through the **default-metric** command (in RIP or RIPng router configuration mode) is used for the route.

1.75.4 Default

Route address ranges are not summarized.

1.75.5 Usage Guidelines

Use the **summary-address** command to summarize information about RIP or RIPng routes sent over the specified interface, thereby reducing the size of the RIP or RIPng update packets.

Use the **no** or **default** form of this command to disable RIP or RIPng route summarization.

1.75.6 Examples

The following example summarizes routes in the `10.0.0.0 255.0.0.0` range:

```
[local]Redback(config-ctx)#router rip rip002

[local]Redback(config-rip)#interface fe01

[local]Redback(config-rip-if)#summary-address 10.0.0.0 255.0.0.0
```

1.76 supply

supply

{**no** | **default**} **supply**

1.76.1 Purpose

Enables the sending of Routing Information Protocol (RIP) or RIP next generation (RIPng) packets on the specified interface.

1.76.2 Command Mode

- RIP interface configuration
- RIPng interface configuration

1.76.3 Syntax Description

This command has no keywords or arguments.

1.76.4 Default

If the interface has been enabled through the **interface** command (in RIP or RIPng router configuration mode), it can transmit RIP or RIPng packets; otherwise, it cannot.

1.76.5 Usage Guidelines

Use the **supply** command to enable the sending of RIP or RIPng packets on the specified interface.

If more than one circuit is bound to the interface, RIP or RIPng updates are not sent.

Note: This command does not apply to loopback interfaces.

Use the **no** or **default** form of this command to disable the sending of RIP or RIPng packets on an interface.

1.76.6 Examples

The following example show how to enable the sending of RIP packets on the fe01 interface:

```
[local]Redback(config-ctx)#router rip rip002

[local]Redback(config-rip)#interface fe01

[local]Redback(config-rip-if)#supply
```

1.77 sustained-creation-rate

sustained-creation-rate ***value***

default sustained-creation-rate

1.77.1 Purpose

Sets the number of flows the system can apply to a circuit in each second after the first second elapses.

1.77.2 Command Mode

Flow configuration

1.77.3 Syntax Description

value	Rate, for each second after the first second, at which the system can create flows over a sustained period of time. The range of values is 1 to 2,097,152.

1.77.4 Default

None

1.77.5 Usage Guidelines

Use the **sustained-creation-rate** command to establish the number of flows the system can apply to a circuit in each second after the first second elapses.

Use the **default** form of this command to set the rate at the previously set value.

1.77.6 Examples

The following example shows how to set the number of flows applied to a circuit to `1000` in each second after the first second elapses:

```
[local]Redback(config-ac-profile)#sustained-creation-rate 1000
```

1.78 switchover pseudowire

```
switchover pseudowire vc-id vc-id peer peer-address
[context local]
```

1.78.1 Purpose

In a redundant Layer 2 VPN (L2VPN) cross-connect (XC), this command forces a switch over from the active XC to the standby XC.

1.78.2 Command Mode

exec

1.78.3 Syntax Description

`vc-id` *`vc-id`*	LDP virtual circuit ID of the standby pseudowire. The range of values is 0 through 4,294,967,295.
`peer` *`peer-address`*	IP address of the remote end of a backup peer in a redundant pair of L2VPN XCs.
`context local`	Optional. The context in which the L2 VPN XC is configured. If specified, the context must be **`local`**.

1.78.4 Usage Guidelines

Use the **`switchover pseudowire`** command to force a switch over from the active XC to the standby XC in a redundant L2VPN XC.

1.78.5 Examples

The following example shows how to force a switch over from the active XC to the standby XC `100` on the Provider Edge (PE) peer at IP address **`10.22.31.42`**:

```
[local]Redback#switchover pseudowire 100 peer 10.22.31.42
```

1.79 system alarm

`system alarm` {**`air-filter`** *`months`* | **`redundancy suppress`** | **`transceiver suppress`**}

{**`no`** | **`default`**} **`system alarm`** {**`air-filter`** | **`redundancy suppress`** | **`transceiver suppress`**}

1.79.1 Purpose

Enables the alarm for the air filter or suppresses redundancy or transceiver alarms for the SmartEdge 400, 600, 800, 1200 or 1200H chassis.

1.79.2 Command Mode

Global configuration

1.79.3 Syntax Description

air-filter *months*	Number of months in the service interval. The range of values is 1 to 12; the default value is 6.
redundancy suppress	Disables the alarms related to redundant controller cards.
transceiver suppress	Disables the alarms related to transceivers.

1.79.4 Default

The alarm for the air filter is disabled. The alarm controller card redundancy is enabled. The transceiver alarms is disabled.

1.79.5 Usage Guidelines

Use the **system alarm** command to enable the alarm for the air filter or suppress redundancy or transceiver alarms (including corresponding SNMP traps) for a SmartEdge 400, 600, 800, 1200 or 1200H chassis.

Note: The SmartEdge 100 router does not support this command.

The air filter alarm is generated at the end of the service interval based on the service date stored in the EEPROM of the fan tray unit. Use the **air-filter** ***months*** construct to update the EEPROM with the service interval.

To display the current service date, enter the **show hardware fantray detail** command in any mode. To update the current service date after the air filter or fan tray unit has been replaced, enter the **service air-filter** command (in exec mode).

Use the **redundancy suppress** construct to suppress alarms related to redundant controller cards for SmartEdge routers that are configured with a single controller card. The following bulleted list displays the suppressed alarms:

- Backup fail: peer dead
- Controller missing
- Controller manual switch requested
- Controller auto switch completed
- Controller forced switch requested
- Controller switch completed
- Controller exerciser switch failed

- Controller switch failed
- Peer inventory fail
- Peer shared format mismatch
- Peer controller card type incompatible
- Peer SONET/SDH mode incompatible

Use the **no** form of the **system alarm air-filter** command to disable alarms for the air filter. Use the **default** form of the **system alarm air-filter** command to set the service interval to 6 months.

Use the **no** or **default** form of the **system alarm redundancy suppress** command to enable alarms related to redundant controller cards for SmartEdge routers that are configured with a single controller card.

Additionally, you can use the **no** form of this command to enable alarms for redundant controller cards and to enable transceiver alarms (including corresponding SNMP traps).

1.79.6 Examples

The following example shows how to enable the air filter alarm and specify a three-month service interval:

```
[local]Redback(config)#system alarm air-filter 3
```

1.80 system clock-source

system clock-source {**internal** | **line** {**primary** | **secondary**} *slot/port*}

{**no** | **default**} **system clock-source** {**internal** | **line** {**primary** | **secondary**} *slot/port*}

1.80.1 Purpose

Specifies whether the SmartEdge router gets its system clock from an internal source or the receive line of a line card.

1.80.2 Command Mode

Global configuration

1.80.3 Syntax Description

`internal`	Specifies the internal clock on the active controller card; this is the default.
`line`	Specifies a line card receive line as the clock source.
`primary`	Specifies a primary port from which the transmit clock is derived.
`secondary`	Specifies a secondary port from which the transmit clock is derived.
`slot`	Chassis slot number of the port from which the transmit clock is derived.
`port`	Number of the port from which the transmit clock is derived.

1.80.4 Default

The transmit clock is generated from the internal clock on the active controller card.

1.80.5 Usage Guidelines

Use the **`system clock-source`** command to specify whether the SmartEdge router gets its system clock from an internal source or the receive line of a line card.

If you specify the **`line`** keyword, you can select both a primary and secondary clock source, but not in the same command. Appropriate line cards include any Asynchronous Transfer Mode (ATM) OC-3, ATM OC-12, OC-3c/STM-1c, OC-12c/STM-4c, or OC-48c/STM-16c card.

Note: To set the system clock, enter the **`clock set`** command (in exec mode); see the **`clock set`** command in the *Command List*.

Note: The SmartEdge 100 router does not support this command.

Note: Changes to the clock source setting will not cause LOF on the 8-port ATM OC-3c/STM-1c.

Use the **`no`** or **`default`** form of this command to select the default value for the clock source.

1.80.6 Examples

The following example selects the secondary transmit clock source to be derived from the received clock on port `1` in slot `3`:

```
[local]Redback(config)#system clock-source timing-type sdh
[local]Redback(config)#system clock-source line secondary 3/1
```

Note: The `system clock-source timing-type sdh` and `system clock-source line primary 3/1` commands are dependent on the framing type that is configured on the POS port.

1.81 system clock-source external

system clock-source external { **primary** | **secondary**}[**framing** ***type***]

{**no** | **default**} **system clock-source external** {**primary** | **secondary**} [**framing** ***framing-type***]

1.81.1 Purpose

Specifies external equipment as the source of the transmit data clock for all ports in the system.

1.81.2 Command Mode

Global configuration

1.81.3 Syntax Description

primary	Specifies a primary external clock source.
secondary	Specifies a secondary external clock source.
framing ***type***	Optional. Framing for the external interface, according to one of the following keywords: • **crc4**—Specifies cyclic redundancy check (CRC)-4 framing for an E1 interface. • **esf**—Specifies Extended Super Frame (ESF) formatting for a DS-1 interface. • **no-crc4**—Specifies non-CRC-4 framing for an E1 interface. • **sf**—Specifies Super Frame (SF) formatting for a DS-1 interface. The default framing type is **sf**.

1.81.4 Default

The transmit clock is generated from the internal clock on the active controller card.

1.81.5 Usage Guidelines

Use the **system clock-source external** command to specify external equipment as the source of the transmit data clock for all ports in the system. The type of equipment can be building integrated timing supply (BITS) or synchronization supply unit (SSU).

The type of framing you specify must be compatible with the version of the active controller card:

- For a Cross-Connect Route Processor (XCRP) Version 4 (XCRP4) Controller card, it must be compatible with the timing interface that you have specified using the **system clock-source timing-type** command (in global configuration mode).

- For an XCRP Controller card, it must be compatible with the hardware version of the card, either XCRP-T1 BITS (DS-1 interface) or XCRP-E1 SSU (E1 interface).

If the framing type that you specify is incompatible, the system displays a warning message and rejects this command.

To specify an internal source, use the **system clock-source** command (in global configuration mode).

Note: To set the system clock, enter the **clock set** command (in exec mode); see the **clock set** command in the *Command List*.

Note: The SmartEdge 100 router does not support this command.

Use the **no** or **default** form of this command to select the default value for the clock source.

1.81.6 Examples

The following example shows how to select an external source with the CRC-4 framing to be the primary source for the transmit clock:

```
[local]Redback(config)#system clock-source external primary framing  crc4
```

1.82 system clock-source timing-type

system clock-source timing-type {**sonet** | **sdh**}

```
{no | default} system clock-source timing-type
```

1.82.1 Purpose

Specifies the type of timing interface for the Cross-Connect Route Processor (XCRP) Version 4 (XCRP4) Controller card.

1.82.2 Command Mode

Global configuration

1.82.3 Syntax Description

`sonet`	Specifies Synchronous Optical Network (SONET) timing for the clock interface.
`sdh`	Specifies Synchronous Digital Hierarchy (SDH) timing for the clock interface.

1.82.4 Default

The timing type is SONET.

1.82.5 Usage Guidelines

Use the `system clock-source timing-type` command to specify the type of timing interface for the XCRP4 Controller card.

To disable external timing, enter the `no system clock-source external` command (in global configuration mode). To disable line timing, enter the `no system clock-source` command (in global configuration mode).

This command applies only to the XCRP4 Controller card.

Note: To set the system clock, enter the `clock set` command (in exec mode); see the `clock set` command in the *Command List*.

Note: The SmartEdge 100 router does not support this command.

Use the `no` or `default` form of this command to specify the default timing type as SONET.

1.82.6 Examples

The following example shows how to specify SDH timing for external timing mode:

```
[local]Redback(config)#system clock-source timing-type sdh
[local]Redback(config)#system clock-source external
primary framing crc4
```

If using line timing mode:

```
[local]Redback(config)#system clock-source timing-type sdh
[local]Redback(config)#system clock-source line primary 3/1
```

Note: The `system clock-source timing-type sdh` and `system clock-source line primary 3/1` commands are dependent on the framing type that is configured on the POS port.

1.83 system clock summer-time

system clock summer-time *zone1 zone2* {**date** *yyyy:mm:dd:hh:mm* [*:ss*] *yyyy:mm:dd:hh:mm*[*:ss*] | **recurring** *start-date end-date*}

{**no** | **default**} **system clock summer-time** *zone1 zone2* {**date** *yyyy:mm:dd:hh:mm*[*:ss*] *yyyy:mm:dd:hh:mm*[*:ss*] | **recurring** *start-date end-date*}

1.83.1 Purpose

Enables the system to automatically switch to daylight saving time or standard time.

1.83.2 Command Mode

Global configuration

1.83.3 Syntax Description

zone1	Previously defined name of the time zone to which this adjustment applies; for example, Pacific Standard Time (PST).
zone2	Name of the time zone to be displayed when summer time is in effect; for example, Pacific Daylight Time (PDT).
date	Specifies start and end dates for summer time.
yyyy:*mm*:*dd*:*hh*:*mm*[:*ss*]	Year, month, day, hour, minutes, and optionally seconds expressed in a 24-hour format; for example, 6:30 p.m. is expressed as 18:30.

`recurring`	Indicates if the rules for switching to summer time are the same each year. If the `recurring` keyword is not followed by date information, the rules for the United States are applied. The offset applied is 60 minutes.
`start-date end-date`	Dates for the beginning and end of summer time. Each argument includes the following components separated by a space: • *`week`*—Week of the month (`first`, 1 to 4, or `last`). • *`day`*—Day of the week; for example, Sunday, Monday, and so on. • *`month`*—Month of the year; for example, January, February, and so on. • *`hh`*—Hour of the day, expressed in a 24-hour format; for example, 6:00 p.m. is expressed as 18:00.

1.83.4 Default

Automatic switch to daylight saving time is disabled.

1.83.5 Usage Guidelines

Use the **`system clock summer-time`** command to enable the system to automatically switch to daylight saving time or standard time.

The start time is relative to standard time and the end time is relative to summer time. If the starting month is after the ending month, the system assumes that you are in the Southern Hemisphere.

The value for the *`zone1`* argument must be a previously defined time zone using the **`system clock timezone`** command (in global configuration mode).

The value for the *`zone2`* argument is name of the time zone specified by the *`zone1`* argument when summer time is in effect.

Use the **`recurring`** keyword if the rules for switching to summer time are applied in precisely the same way each year. The first set of variables (*`week`*, *`day`*, *`month`*, *`hh`*) refers to the start day; the second set refers to the end day.

Note: Use the **recurring** keyword in this command with a specified date, because the system default (U.S. summer time) cannot be deleted.

However, this recurring time summer time zone information will be deleted if you enter the **no system clock timezone** command. In addition, entire the **system clock summer-time** configuration data will be removed.

Alternatively, you can use the **date** keyword to specify a start and end date for summer time. In the **date** format, you can specify start and end dates for multiple years at the same time, as long as the time zones to which the dates apply are unique and there is no overlap of dates.

Use the **no** form of this command to disable the automatic switch to daylight saving time or standard time and delete the information for the specified time zone and for the specified year.

Use the **default** form of this command to perform the same function as the **system clock summer-time** command.

To set the system clock, enter the **clock set** command (in exec mode); the **clock set** command is in the *Command List*.

1.83.6 Examples

The following example shows how to enable the system to switch to daylight saving time (`summer-time`), which will start on the `first Sunday` in `April` at 7:00 a.m. and end on the `last Sunday` in `October` at 3:00 a.m. for the `PST` and Mountain Standard Time (`MST`) time zones, (`PDT` and `MDT`, respectively), that were previously defined using the **system clock timezone** command:

```
[local]Redback(config)#system clock summer-time PST PDT recurring first
Sunday April 6 last Sunday October 2
[local]Redback(config)#system clock summer-time MST MDT recurring first
Sunday April 6 last Sunday October 2
```

The next example shows how to enable the system to switch to daylight saving time in a Southern Hemisphere location:

```
[local]Redback(config)#system clock summer-time AST ADT date
2005:10:26:02:00 2005:04:06:02:00
```

The final example shows how to disable the automatic switch and delete the summer time information for the Atlantic Standard Time (`AST`) time zone:

```
[local]Redback(config)#no system clock summer-time AST ADT date
2005:10:26:02:00 2005:04:06:02:00
```

1.84 system clock timezone

system clock timezone ***zone hours*** [***minutes***] [**local**]

```
no system clock timezone [zone]
```

1.84.1 Purpose

Defines one or more time zones and their distances from Greenwich Meridian Time (GMC) for display purposes.

1.84.2 Command Mode

Global configuration

1.84.3 Syntax Description

`zone`	User-defined name of the time zone to be displayed when standard time is in effect; for example, Pacific Standard Time (PST).
`hours`	Number of hours that the time zone is offset from GMC. The range of values is –23 to 23; the default value is 0.
`minutes`	Optional. Number of minutes that the time zone is offset from GMC. The range of values is 0 to 59; the default value is 0.
`local`	Optional. Specifies that the time zone being defined is the local time zone.

1.84.4 Default

The default time zone is GMC. If no time zone is defined with the `local` keyword, the system uses GMC when displaying time.

1.84.5 Usage Guidelines

Use the **`system clock timezone`** command to define one or more time zones and their distances from GMC. The system keeps time in GMC and the specified local time zone displays. The specified local time zone is also used when you enter the **`clock set`** command (in exec mode). See the **`clock set`** command in the *Command List*.

You can specify multiple time zones; the only time zone assumed to be local is the one with the optional `local` keyword.

Use the **`no`** form of this command with the time zone specified to delete previously configured information for that time zone. If the specified time zone was configured as the local time zone, the system reverts to GMC time. Use the **`no`** form of this command with no time zone specified to remove all previously configured time zone and corresponding daylight saving information.

1.84.6 Examples

The following example shows how to define Atlantic Standard Time (AST), Eastern Standard Time (EST), Central Standard Time (CST), Mountain Standard Time (MST), PST, and Hawaii Standard Time (HST) time zones. PST is also specified as the local time zone:

```
[local]Redback(config)#system clock timezone AST -4

[local]Redback(config)#system clock timezone EST -5

[local]Redback(config)#system clock timezone CST -6

[local]Redback(config)#system clock timezone MST -7

[local]Redback(config)#system clock timezone PST -8 local

[local]Redback(config)#system clock timezone HST -10
```

The following example shows how to deletes the EST time zone information:

```
[local]Redback(config)#no system clock timezone EST
```

1.85 system confirmations context

system confirmations context

{no | default} system confirmations context

1.85.1 Purpose

Enables the system to query the user when attempting to create a context.

1.85.2 Command Mode

Global configuration

1.85.3 Syntax Description

This command has no keywords or arguments.

1.85.4 Default

System confirmation query is disabled.

1.85.5 Usage Guidelines

Use the **system confirmations context** command to enable the system to query a user when attempting to create a context.

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

1.85.6 Examples

The following example shows how to display the **system confirmations context** command when it is enabled:

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

[local]Redback(config)#context account

Are you sure you want to create context account?
```

1.86 system confirmations removal warn

system confirmations removal-warn ***text***

{no | default} system confirmations removal-warn

1.86.1 Purpose

Sets a warning message that appears when a user enters the no form of a configuration command.

1.86.2 Command Mode

Global configuration

1.86.3 Syntax Description

text	Warning message to appear when a user deletes a configuration setting.

1.86.4 Default

No warning message appears when a user deletes a configuration setting.

1.86.5 Usage Guidelines

Use this command to set a warning message that appears when a user deletes a configuration setting.

The warning message you set can contain up to 255 characters. The system displays the error message when a user enters a CLI command proceeded by the no keyword. The warning message is only displayed; it does not allow a response from the user.

The system can display warning messages for other commands. This ability may result in two warnings appearing at once in some cases. For example, you can use the **system confirmation context** command to display the following error when a user uses the **no context** command:

```
Are you sure you want to delete context xyz?
```

If this feature is turned on or you want to avoid duplicate messages, use the **no** form of this command to turn off the error message that appears when a user deletes a configuration setting.

Use the **no** or **default** form of this command to display no warning message when a user deletes a configuration setting.

1.86.6 Examples

The following example shows how to set the system to display the warning message, “`Warning! Using this command may undo an important setting. If you are uncertain about the function of this command, type ‘abort’ now and check with your system administrator`” when a user enters a command proceeded by the **no** keyword:

```
[local]Redback(config)#system confirmations removal-warn Warning! Using
this command may undo an important setting. If you are uncertain about the
function of his command, type ‘abort’ now and check with your system
administrator.
```

1.87 system contact

system contact ***text***

no system contact

1.87.1 Purpose

Identifies the system contact.

1.87.2 Command Mode

Global configuration

1.87.3 Syntax Description

`text`	Text that explains the department or person to contact, and how, for information regarding the system.

1.87.4 Default

No system contact information is configured.

1.87.5 Usage Guidelines

Use the **`system contact`** command to configure the system to identify the person or department to contact regarding system information. The system contact information is available using the sysContact Management Information Base-II (MIB-II) object. The *`text`* argument can be any alphanumeric string, including spaces. The *`text`* cannot be longer than one line.

Use the **`no`** form of this command to remove system contact information.

1.87.6 Examples

The following example shows how to set a contact string:

```
[local]Redback(config)#system contact IS Hotline 1-800-555-1567
```

1.88 system hostname

`system hostname` *`hostname`*

`default system hostname`

1.88.1 Purpose

Specifies the system hostname.

1.88.2 Command Mode

Global configuration

1.88.3 Syntax Description

`hostname`	Alphanumeric string to be used as the hostname for the system.

1.88.4 Default

The factory-assigned hostname is Redback.

1.88.5 Usage Guidelines

Use the **`system hostname`** command to specify the system hostname. This hostname is available using the sysName Management Information Base-II (MIB-II) object. Do not expect the case to be preserved. Uppercase and lowercase characters appear the same to many Internet software applications. It might seem appropriate to capitalize a name, the same way you do in conventional text, but Internet conventions dictate that computer names appear as all lowercase. For more information, see RFC 1178, `Choosing a Name for Your Computer.`

The name must also follow the rules for Advanced Research Projects Agency Network (ARPANET) hostnames. Names must start with a letter, end with a letter or digit, and have (as interior characters only) letters, digits, hyphens (-), periods (.), and underscores (_). Names must be 63 characters or fewer. For more information, see RFC 1035, `Domain Names—Implementation and Specification`.

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

1.88.6 Examples

The following example shows how to change the hostname to `freebird:`

```
[local]Redback(config)#system hostname freebird

[local]freebird(config)#
```

1.89 system-id

`system-id` ***`name`***

```
{no | default} system-id
```

1.89.1 Purpose

Assign an ID to identify the SmartEdge router in Access Node Control Protocol (ANCP) sessions transmitted to an ANCP neighbor peer.

1.89.2 Command Mode

ANCP configuration

1.89.3 Syntax Description

name	ID used for the ANCP sessions. The format is a 6-byte hexadecimal string in the form ***hh:hh:hh:hh:hh:hh***.

1.89.4 Default

The ID is set to the medium access control (MAC) address of the Ethernet management port or to CA:FE:18:07:29:09 if the system cannot read the MAC address of the Ethernet management port.

1.89.5 Usage Guidelines

Use the **system-id** command to assign an ID to identify the ANCP sessions transmitted by the SmartEdge router. If you configure the system ID, it is included as the sender name in adjacency packets sent by the SmartEdge router. If you do not configure it, the system uses one of the following alternatives:

- If the SmartEdge router has received the MAC address of the port on which the ANCP neighbor is connected, it uses that MAC address.
- Otherwise, the SmartEdge router uses either the MAC address of the Ethernet management port or CA:FE:18:07:29:09, depending on whether the MAC address of the Ethernet management port is readable.

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

1.89.6 Examples

The following example shows how to specify `12:34:56:78:9a:bc` as the SmartEdge router ID for ANCP sessions:

```
[local]Redback(config-ancp)#system-id 12:34:56:78:9a:bc
```

1.90 system lacp mac-addr

system lacp mac-addr ***mac-addr***

{**no** | **default**} **lacp mac-addr** ***mac-addr***

1.90.1 Purpose

Configures the medium access control (MAC) address that will be used in the Link Aggregation Control Protocol (LACP) packet negotiation with peers.

1.90.2 Command Mode

Global configuration

1.90.3 Syntax Description

mac-addr	MAC address to be used for the link group in the form ***hh*:*hh*:*hh*:*hh*:*hh*:*hh***.

1.90.4 Default

The MAC address of the system backplane is used.

1.90.5 Usage Guidelines

Use the **system lacp mac-addr** command to configure the MAC address to be used in the system link aggregation group ID (LAG ID) in LACP packets that are exchanged with the peer.

Use the **no** or **default** form of this command to revert back to the original MAC address on the system backplane.

1.90.6 Examples

The following example shows how to change the MAC address to **11:22:33:44:55:66:**

```
[local]Redback(config)#system lacp mac-addr 11:22:33:44:55:66

[local]Redback(config)#commit Transaction committed
```

The following example shows how to set set the MAC address back to the default MAC address:

```
[local]Redback(config)#no system lacp mac-addr

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

1.91 system lacp priority

`system lacp priority` [*`priority`*]

`default system lacp priority`

1.91.1 Purpose

Configures the system Link Aggregation Control Protocol (LACP) priority to be used in the system link aggregation group ID (LAG ID) in LACP packets that are exchanged with the peer.

1.91.2 Command Mode

Global configuration

1.91.3 Syntax Description

`priority`	Optional. Numeric value that sets the number of LACP packets exchanged between peers; the default value is 2.

1.91.4 Default

The default value is 2.

1.91.5 Usage Guidelines

Use the **`system lacp priority`** command to configure the system LACP priority to be used in the system link aggregation group ID (LAG ID) in LACP packets that are exchanged with the peer.

Use the **default** form of this command to set the LACP priority to 2.

1.91.6 Examples

The following example shows how to set the LACP packets to priority 4:

```
[local]Redback(config)#system lacp priority 4

[local]Redback(config)#commit Transaction committed
```

The following example shows how to set the LACP packets back to the default value:

```
[local]Redback(config)#no system lacp priority 4
```

1.92 system location

system location *text*

no system location

1.92.1 Purpose

Configures the system location information.

1.92.2 Command Mode

Global configuration

1.92.3 Syntax Description

text	Text that explains the physical location of the system.

1.92.4 Default

No system location is specified.

1.92.5 Usage Guidelines

Use the **`system location`** command to configure the system location information available using the sysLocation Management Information Base-II (MIB-II) object. The ***`text`*** argument can be any alphanumeric string, including spaces. The text cannot be longer than one line.

Use the **`no`** form of this command to remove system location information.

1.92.6 Examples

The following example shows how to set a location string:

```
[local]Redback(config)#system location Building 3, 2nd Floor, Lab 3
```