ERICSSON

Commands: e through f

COMMAND DESCRIPTION

8/190 82-CRA 119 1170/1-V1 Uen L

Contents

1 Command Descriptions

Commands starting with “e” through commands starting with “f” 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 ebgp-multihop

`ebgp-multihop` ***`max-hops`***

`no ebgp-multihop` ***`max-hops`***

1.1.1 Purpose

Configures the maximum number of hops used to reach the external Border Gateway Protocol (eBGP) neighbor when the neighbor or peer group is not directly connected.

1.1.2 Command Mode

- BGP neighbor configuration
- BGP peer group configuration

1.1.3 Syntax Description

`max-hops`	Maximum number of hops. The range of values is 1 to 255; the default value is 1.

1.1.4 Default

The maximum number of hops is set to 1.

1.1.5 Usage Guidelines

Use the **ebgp-multihop** command to configure the maximum number of hops used to reach the eBGP neighbor when the neighbor or peer group is not directly connected

Note: You must enable this command for BGP connections to be established with neighbors that are not directly connected.

Note: You cannot enable this command on a BGP neighbor that is part of a peer group, because this feature cannot be customized for individual members inside of a peer group.

Use the **no** form of this command to restore the maximum number of hops to the default value of 1.

1.1.6 Examples

The following example shows how to set the maximum number of hops to the neighbor at IP address, **12.10.10.1** to **3:**

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

[local]Redback(config-bgp)#neighbor 12.10.10.1 external

[local]Redback(config-bgp-neighbor)#egbp-multihop 3
```

1.2 ecmp-transit

ecmp-transit

no ecmp-transit

1.2.1 Purpose

Enables equal-cost multipath (ECMP) on label-switched path (LSP) transit nodes.

1.2.2 Command Mode

LDP router configuration

1.2.3 Syntax Description

This command has no keywords or arguments.

1.2.4 Default

ECMP is disabled on transit nodes and enabled on ingress nodes.

1.2.5 Usage Guidelines

Use the **ecmp-transit** command to enable ECMP on LSP transit nodes.

A constituent of an ECMP LSP can be protected against link failure at the label edge router (LER) using next-hop fast reroute (NFRR) for link protection when the LDP traffic is carried over a bypass RSVP LSP.

Note: Currently, ECMP over multiple bypass LSPs is not supported.

Use the **no** form of this command to disable ECMP on LSP transit nodes.

1.2.6 Examples

The following example shows how to enable ECMP on an LSP transit node:

```
[local]Redback#config
[local]Redback(config)#context local
[local]Redback(config-ctx)#router ldp
[local]Redback(config-ldp)#ecmp-transit
```

1.3 edit

edit ***url***

1.3.1 Purpose

Using the vi editor, creates or opens an existing file on the local file system for editing.

1.3.2 Command Mode

exec (10)

1.3.3 Syntax Description

url	URL of the file to be created or edited.

1.3.4 Default

None

1.3.5 Usage Guidelines

Use the **edit** command to create or open an existing file on the local file system for editing.

Use the **:q!** command to discard any edits and exit the editor; use the **:wq!** command to save any edits and exit the editor.

1.3.6 Examples

The following example shows how to open the **redback.cfg** file using the vi editor:

```
[local]Redback#edit redback.cfg
```

```
!
!  Configuration last changed by user 'pm' at Mon Jan  2 08:04:25 2006
!
service multiple-contexts
!
context local
!
  ip domain-lookup
!
 interface mgmt
  ip address 10.1.1.3/21
!
 enable encrypted 1 $1$........$kvQfdsjs0ACFMeDHQ7n/o.
!
 user test encrypted 1 $1$........$kvQfdsjs0ACFMeDHQ7n/o.
!
 ip route 10.1.0.0/16 10.12.208.1 cost 1 permanent
 ip route 155.53.0.0/16 10.12.208.1 cost 1 permanent
!
port ethernet 7/1
! XCRP management ports on slot 7 and 8 are configured through 7/1
 no shutdown
 bind interface mgmt local
!
system hostname supercomm7
!
service console-break
!
end
```

1.4 edge-port

edge-port

no edge-port

1.4.1 Purpose

Configures the associated port as a Rapid Spanning Tree Protocol (RSTP) edge port.

1.4.2 Command Mode

Spanning-tree profile configuration

1.4.3 Syntax Description

This command has no keywords or arguments.

1.4.4 Default

The associated port is not an edge port.

1.4.5 Usage Guidelines

Use the **edge-port** command to configure the associated port as an RSTP edge port.

1.4.6 Examples

The following example illustrates how the **spanning-tree profile** command creates the spanning-tree profile `womp` and configures it as an RSTP edge-port profile. In the second part of the example, an Ethernet port is assigned the spanning-tree profile `womp` and, therefore, is configured as an RSTP edge port:

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

1.5 egress

egress ***egress-addr***

1.5.1 Purpose

Specifies the IP address of the egress label-switched router (LSR) in a label-switched path (LSP).

1.5.2 Command Mode

- RSVP LSP configuration
- MPLS static LSP configuration

1.5.3 Syntax Description

egress-addr	IP address of the egress LSR.

1.5.4 Default

None

1.5.5 Usage Guidelines

Use the **egress** command to specify the IP address of the egress LSR in an LSP.

An egress LSR is the last LSR in the chain of LSRs that constitute an LSP. It forwards packets out of a network. The IP address of the egress LSR must be specified in both signaled and static LSPs.

1.5.6 Examples

The following example shows how to configure the egress IP address to 192.168.1.2 for the static LSP, lsp01:

```
[local]Redback(config-ctx)#router mpls-static
[local]Redback(config-mpls-static)#lsp lsp01
[local]Redback(config-mpls-static-lsp)#egress 192.168.1.2
```

1.6 egress prefer dscp-qos

egress prefer dscp-qos

no egress prefer dscp-qos

1.6.1 Purpose

Enables the use of only Differentiated Services Code Point (DSCP) bits for queuing at the Multiprotocol Label Switching (MPLS) egress router.

1.6.2 Command Mode

MPLS router configuration

1.6.3 Syntax Description

This command has no keywords or arguments.

1.6.4 Default

If penultimate hop popping is enabled, the tunnel label is removed at the penultimate hop, and the egress router uses the Virtual Private Network (VPN) label experimental (EXP) bits for queuing; however, if there is no VPN label, the egress router uses the DSCP bits for queuing. For more information, see *Configuring MPLS*.

1.6.5 Usage Guidelines

Use the **egress prefer dscp-qos** command to enable the use of only DSCP bits for queuing at the MPLS egress router.

Use the **no** form of this command to return the system to its default behavior.

1.6.6 Examples

The following example shows how to enable the use of only DSCP bits for queuing at the egress router:

```
[local]Redback(config-ctx)#router mpls
[local]Redback(config-mpls)#egress prefer dscp-qos
```

1.7 enable

enable [*level*]

no enable

1.7.1 Purpose

Modifies the privilege level for the current exec session.

1.7.2 Command Mode

exec

1.7.3 Syntax Description

level	Optional. Requested privilege level. The range of values is 0 to 15; if you do not enter a value, the system defaults to 15.

1.7.4 Default

When you enter this command without the *level* argument, the current exec session is held at level 15. For whatever value is set, the administrator's privilege level must be the same or higher.

1.7.5 Usage Guidelines

Use the **enable** command to modify the privilege level for the current exec session. Use the *level* argument to select the desired privilege level, up to the maximum privilege level configured for this administrator account. If this argument is omitted, the maximum privilege level (15) is enabled. This command is available for any privilege level.

If no passwords have been configured and if local authentication is enabled, you can enter the **enable** command in exec mode only on the console port; the system does not prompt for a password. By default, local authentication is enabled; see the **enable authentication** command in context configuration mode. If at least one password has been configured, you can enter the **enable** command from the console or a remote session; see the **enable password** and **enabled encrypted** commands in context configuration mode.

You can use the **enable** command to enter a privilege level password only if a password for the privilege level has been set. If you attempt to use this command for a privilege level that has no password, the system displays an error message and does not change the privilege level for the exec session.

For information on the privilege level passwords, see *Configuring Contexts and Interfaces*. Use the **show privilege** command to display the enabled privilege level.

Use the **no** form of this command to return to the initial privilege level configured for the administrator account. The **disable** command in exec mode performs the same function.

1.7.6 Examples

The following example shows the results of an attempt by an administrator to set the privilege level for the exec session to a privilege level for which no password is configured:

```
[local]Redback>enable 10

%No enable password configured for this level
```

The following example shows how to set the current exec session privilege level to **15**. The system prompts for the password, which is not displayed on the screen. After the administrator enters the correct password, the system enters privileged mode as indicated by the pound sign (#) in the prompt:

```
[local]Redback>enable 15

Password:
[local]Redback#
```

1.8 enable authentication

enable authentication {**none** | **local** | **radius** | **tacacs+**}

default enable authentication

1.8.1 Purpose

Specifies how the system performs privilege level authentication.

1.8.2 Command Mode

Context configuration

1.8.3 Syntax Description

none	Specifies no privilege level password authentication.
local	Specifies privilege level password authentication using the local configuration.
radius	Specifies privilege level password authentication using the RADIUS database.
tacacs+	Specifies privilege level password authentication using the Terminal Access Controller Access Control System Plus (TACACS+) database.

1.8.4 Default

The system authenticates privilege level passwords using the local configuration database.

1.8.5 Usage Guidelines

Use the **enable authentication** command to specify how the system performs privilege level authentication. If you select the **none** keyword, administrators are not prompted for a password when changing privilege levels.

If you enter the **radius** or **tacacs+** keyword, you must configure the enable passwords on the RADIUS or TACACS+ system, respectively. The format of the enable password is **enable** [***level***]**@***ctx-name*, where the ***level*** argument represents the privilege level of the password (and is not specified for level 15), and the ***ctx-name*** argument is the name of the context for which the password is configured.

Note: The separator character between the ***admin-name*** and the ***ctx-name*** argument is configurable and can be any of %, -, @, _, \\, #, and /. For information about configuring the separator character, see *Configuring Authentication, Authorization, and Accounting*. The default value is @, which is used throughout this document.

Use the **default** form of this command to configure the system to use the default authentication (local).

1.8.6 Examples

The following example shows how to configure the system to authenticate privilege level passwords using RADIUS:

```
[local]Redback(config-ctx)#enable authentication radius
```

The following example shows how the administrator names would be configured on the RADIUS server for privilege level **10** and privilege level **15** in the **local** context:

```
username = enable10@local

username = enable@local
```

1.9 enable encrypted

enable encrypted [**level** *level*] *encrypt-type password*

no enable encrypted [**level** *level encrypt-type*]

1.9.1 Purpose

Creates a password, in encrypted form, for the specified privilege level.

1.9.2 Command Mode

Context configuration

1.9.3 Syntax Description

level *level*	Optional. Privilege level for which to configure a password. The range of values is 0 to 15.
encrypt-type	Type of encryption used for a password; only type 1 is supported. Optional for the **no** form of this command.
password	Password to assign to the specified privilege level. This argument is not available when using the **no** form of this command.

1.9.4 Default

No passwords are assigned for any privilege level.

1.9.5 Usage Guidelines

Use the **enable encrypted** command to create a password, in encrypted form, for the specified privilege level.

The SmartEdge router supports up to 16 different privilege levels (0 through 15) for both administrators and commands. Privilege levels are enabled on a per-context basis.

If password authentication is enabled, the system prompts the administrator for a password when the administrator attempts to enter the privilege level using the **enable** command in exec mode. By default, local password authentication is enabled; see the **enable authentication** command in context configuration mode.

This command is similar to the **enable password** command in context configuration mode, except that this command requires you to enter the

password in encrypted form. Typically, you use the **enable password** command to configure a password in unencrypted form. However, to protect your passwords, the system always displays the **enable encrypted** command when displaying the configuration.

Use the **no** form of this command to delete the password for a specific privilege level.

1.9.6 Examples

The following example shows how to create an encrypted password for privilege level **15:**

```
[local]Redback#(config-ctx)enable encrypted level 15 1 $1$..... $CMfiiltCkWPquxFs
```

The following example shows an administrator attempting to enter privilege level **15**. The administrator is prompted for the password (unencrypted, and not echoed):

```
[local]Redback>enable 15


password:


[local]Redback#
```

1.10 enable password

enable password [**level** *level*] *password*

no enable password [**level** *level*]

1.10.1 Purpose

Configures a password for the specified privilege level that the system will encrypt.

1.10.2 Command Mode

Context configuration

1.10.3 Syntax Description

level *level*	Optional. Privilege level for which to configure a password. The range of values is 0 to 15; the default value is 15.
password	Password to assign to the specified privilege level. This argument is not available when using the **no** form of this command.

1.10.4 Default

No passwords are assigned for any privilege level.

1.10.5 Usage Guidelines

Use the **enable password** command to configure a password for the specified privilege level that the system will encrypt.

The SmartEdge router supports up to 16 different privilege levels (0 through 15) for both administrators and commands. Privilege levels are enabled on a per-context basis.

If password authentication is enabled, the system prompts an administrator for the password when the administrator attempts to enter the privilege level using the **enable** command in exec mode. By default, local password authentication is enabled; see the **enable authentication** command in context configuration mode.

To protect your passwords, the system does not store or display this command. Instead, the system stores and displays the password in an encrypted form. When displaying the configuration, the system uses the **enable encrypted** command in context configuration mode.

Use the **no** form of this command to delete the password for a specific privilege level.

1.10.6 Examples

The following example shows an administrator attempting to enter privilege level 15. The administrator is prompted for the password to enter privilege level **15** (the password is not echoed):

```
[local]Redback>enable 15
password:
[local]Redback#
```

The following example shows how to create the **s00persecret** password for privilege level **15:**

```
[local]Redback(config-ctx)#enable password level 15 s00persecret
```

The following example shows how the previous command is stored and displayed by the system, in its encrypted form:

```
[local]Redback#show configuration
.
.
.
enable encrypted 1 $1$........$AGSXlr2Tk5AsG92NBXzqi0
.
.
.
```

1.11 enable vxworks-password

enable vxworks-password {***password*** | **encrypted** ***encypt-type password***}

no enable vxworks-password {***password*** | **encrypted** ***encypt-type password***}

1.11.1 Command Mode

Context configuration

1.11.2 Syntax Description

password	Assign an unencrypted password for the VxWorks shell.
encrypted	Assign an already encrypted password for the VxWorks shell.
encrypt-type	Type of encryption used for a password; only type 1 is supported.
password	Encrypted password.

1.11.3 Default

There is no password for the VxWorks shell.

1.11.4 Usage Guidelines

Use the **enable vxworks-password** command in the local context to assign a password to the VxWorks shell. You can assign a plain text password or an encrypted password.Use the **no** form of the command to disable the password (including the entire line that was previously configured after the **no**).

1.11.5 Example

The following example shows how to enable an encrypted password for the VxWorks shell:

```
[local]Redback(config-ctx)#enable vxworks-password
encrypted 1 $xttt7Hxlf.tty
```

1.12 encaps-access-line

encaps-access-line {**pppoa-llc** | **pppoa-null** | **ipoa-llc** | **ipoa-null** | **ether-aal5-llc-fcs** | **ether-aal5-llc** | **ether-aal5-null-fcs** | **ether-aal5-null** | **ethernet** | **value** *byte-range* **data-link** *data-type*}

no encaps-access-line

1.12.1 Purpose

Specifies the default encapsulation of an access line.

1.12.2 Command Mode

- Overhead profile configuration
- Overhead type configuration

1.12.3 Syntax Description

pppoa-llc	Specifies the Point-to-Point over Asynchronous Transfer Mode (PPPoA) Logical Link Control (LLC) encapsulation type.
pppoa-null	Specifies the PPPoA NULL encapsulation type.
ipoa-llc	Specifies the IP over ATM (IPoA) LLC encapsulation type.
ipoa-null	Specifies the IPoA NULL encapsulation type.
ether-aal5-llc-fcs	Specifies the Ethernet ATM adaptation layer type 5 (AAL5) Logical Link Control (LLC) with Frame Check Sequence (FCS) encapsulation type.
ether-aal5-llc	Specifies the Ethernet over AAL5 LLC without FCS encapsulation type.
ether-aal5-null-fcs	Specifies the Ethernet over AAL5 LLC NULL FCS encapsulation factor encapsulation type.
ether-aal5-null	Specifies the Ethernet over AAL5 NULL without FCS encapsulation type.
ethernet	Specifies the Ethernet encapsulation type.
value *byte-range*	Value of overhead in bytes. The range of values is 0 to 255; the default value is 0.
data-link *data-type*	Data link type; valid values for the *data-type* arguments are ATM or Ethernet.

1.12.4 Default

The size of the overhead is 0 bytes; the data-link type is ATM must be set.

1.12.5 Usage Guidelines

Use the **`encaps-access-line`** command to specify the encapsulation size, in bytes, for a specific access-line type. This command enables the system to take the encapsulation overhead of the access line into consideration so that the rate of traffic does not exceed the permitted traffic rate on the line. This downstream traffic shaping is controlled by QoS overhead profiles.

The Layer 2 overhead value is the number of bytes per packet of overhead for the access-line encapsulation types. Table 1 lists supported access-line encapsulation types and the number of bytes per packet of overhead for each. If the encapsulation type is not listed in Table 1, you can specify number of bytes of overhead, along with the data-link type (Ethernet or ATM).

Table 1 Supported Access-Line Encapsulation Types

Encapsulation Type	Bytes of Overhead	Overhead Components
pppoa-llc	12	8 bytes—AAL5 trailer 3 bytes—LLC 1 byte—NLPID
pppoa-null	8	8 bytes—AAL5 trailer
ipoa-llc	16	8 bytes—AAL5 trailer 8 bytes—LLC/snap
ipoa-null	8	8 bytes—AAL5 trailer
ether-aal5-llc-fcs	36	8 bytes—AAL5 trailer 8 bytes—LLC/snap 14 bytes—Ethernet header 4 bytes—FCS 2 bytes—padding
ether-aal5-llc	32	8 bytes—AAL5 trailer 8 bytes—LLC/snap 14 bytes—Ethernet header 2 bytes—padding

Table 1 Supported Access-Line Encapsulation Types

Encapsulation Type	Bytes of Overhead	Overhead Components
ether-aal5-null-fcs	28	8 bytes—AAL5 trailer 14 bytes—Ethernet header 4 bytes—FCS 2 bytes—padding
ether-aal5-null	24	8 bytes—AAL5 trailer 14 bytes—Ethernet header 2 bytes—padding
ethernet	18	14 bytes—Ethernet header 4 bytes—FCS

Note: RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*, defines the encapsulation types in more detail.

Use the **no** form of this command to specify the default access-line encapsulation type.

1.12.6 Examples

The following example shows how to configure an overhead profile for **example1**, and sets the default rate factor to **15**, a reserve value to **8**, and the encapsulation type to **ethernet**. After you set the overhead profile with default values, you configure **adsl1** and **vdsl1** with custom encapsulation and reserve values:

```
[local]Redback(config)#qos profile example1 overhead
[local]Redback(config-profile-overhead)#rate-factor 15
[local]Redback(config-profile-overhead)#encaps-access-line ethernet
[local]Redback(config-profile-overhead)#reserved 8
[local]Redback(config-profile-overhead)#type adsl1
```

1.13 encapsulation

encapsulation pppoe

no encapsulation pppoe

1.13.1 Purpose

Specifies the encapsulation type of the port pseudowire connection.

1.13.2 Command Mode

Port pseudowire configuration

1.13.3 Syntax Description

pppoe	Sets the encapsulation type of the port pseudowire connection to PPPoE.

1.13.4 Default

None

1.13.5 Usage Guidelines

Use the **encapsulation** command to set the encapsulation type of the port pseudowire connection to a specified protocol.

Use the **no** form of this command to remove the encapsulation type of the port pseudowire connection from the currently specified protocol.

1.13.6 Examples

The following example shows how to set the encapsulation type to **pppoe**:

```
[local]Redback(config-port)#encapsulation pppoe
```

1.14 encapsulation (channel)

encapsulation {ppp|cisco-hdlc}

1.14.1 Purpose

Specifies the encapsulation type of the current channel.

1.14.2 Command Mode

- ds3 configuration
- e1 configuration
- ds1 configuration
- ds0s configuration

1.14.3 Syntax Description

ppp	Sets the encapsulation type of the channel to PPP.
cisco-hdlc	Sets the encapsulation type of the channel to Cisco HDLC.

1.14.4 Default

PPP

1.14.5 Usage Guidelines

Use the **encapsulation** command to set the encapsulation type of the current channel.

MLPPP is supported by binding the channel to an MLPPP link-group.

1.14.6 Examples

```
[local]Redback(config-ds1)#encapsulation ppp
```

1.15 encapsulation (Ethernet Port)

encapsulation dot1q

no encapsulation

1.15.1 Purpose

Specifies the encapsulation for an Ethernet port to create 802.1Q permanent virtual circuits (PVCs).

1.15.2 Command Mode

Port configuration

1.15.3 Syntax Description

dot1q	Specifies 802.1Q encapsulation to support 802.1Q PVCs on the Ethernet port.

1.15.4 Default

The encapsulation is IP over Ethernet (IPoE).

1.15.5 Usage Guidelines

Use the **encapsulation (802.1Q)** command to specify the encapsulation for an Ethernet port to create 802.1Q PVCs.

Note: This command is also described for Ethernet ports without 802.1Q PVCs in *Configuring ATM, Ethernet, and POS Ports* .

Use the **no** form of this command to specify IP over Ethernet encapsulation.

Caution!

Risk of data loss. When you use the **no** form of this command to specify IPoE encapsulation, all 802.1Q PVCs defined on the port are deleted. To reduce the risk, ensure that the PVCs are not active before issuing the **no** form of this command.

1.15.6 Examples

The following example shows how to specify 802.1Q encapsulation for port **1** in slot **4:**

```
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#encapsulation dot1q
```

1.16 encapsulation (link group mode)

encapsulation {**dot1q** | **pppoe**}

{**no** | **default**} **encapsulation**

1.16.1 Purpose

Specifies the encapsulation type for the access link group.

1.16.2 Command Mode

Link-group configuration

1.16.3 Syntax Description

dot1q	Specifies 802.1Q encapsulation for the ports to be added to the link group.
pppoe	Specifies Point-to-Point Protocol over Ethernet (PPPoE) encapsulation for the ports to be added to the link group.
no | **default**	Use the **no** or **default** keyword to reset the encapsulation of the link group to it default IP over Ethernet (IPoE) encapsulation type; that is, no encapsulation.

1.16.4 Default

An access link group is created with IPoE encapsulation.

1.16.5 Usage Guidelines

Use the **encapsulation (access lg)** command to specify the encapsulation for the access link group.

If you specify the **dot1q** keyword, you can use the **bind authentication** or the **bind auto-subscriber** command in link-group configuration mode to bind the link group to its interface. For 802.1Q encapsulation, the value for the ***max-ses*** argument in the **bind authentication** command is 1.

If you specify the **pppoe** keyword, you can use the **bind authentication** or **bind subscriber** command to bind the link group to its interface. For PPPoE encapsulation, the value of ***max-ses*** in the **bind authentication** command must be greater than 1.

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

Note: For a description of the application of this command to ports that are not to be added to an access link group, see *Configuring ATM, Ethernet, and POS Ports* .

1.16.6 Examples

The following example shows how to create an 802.1Q-encapsulated access link group, named `grp24`:

```
[local]Redback(config)#link-group grp24 access
[local]Redback(config-link-group)#encapsulation dot1q
[local]Redback(config-link-group)#bind authentication pap chap maximum 3
```

1.17 encapsulation (POS)

encapsulation {**cisco-hdlc** | **frame-relay** | **ppp**}

no encapsulation

1.17.1 Purpose

Specifies the encapsulation type for a Packet over SONET/SDH (POS) port.

1.17.2 Command Mode

Port configuration

1.17.3 Syntax Description

cisco-hdlc	Specifies Cisco High-Level Data Link Control (HDLC) or other higher layer protocol as the encapsulation type; this is the default.
frame-relay(1)	Specifies Frame Relay as the encapsulation type as described in RFC 1490, `Multiprotocol Interconnect over Frame Relay`.
ppp	Specifies Point-to-Point Protocol (PPP) encapsulation, as described in RFC 2615, `PPP over SONET/SDH` and RFC 1662, `PPP in HDLC-like Framing` as the encapsulation type.

(1) Frame Relay is not supported on the Channelized OC-3/STM-1 (8/4-port) or OC-12/STM-4 (2/1-port) line card.

1.17.4 Default

The encapsulation type for POS ports is Cisco HDLC.

1.17.5 Usage Guidelines

Use the **encapsulation (POS)** command to specify the encapsulation type for a POS or Ethernet port.

Note: To use this POS port as a working or protect port in an APS group, specify Cisco HDLC encapsulation.

The commands that are available depend on the encapsulation type specified by this command. For example, if you specify Cisco HDLC, none of the Frame Relay commands are available.

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

1.17.6 Examples

The following example shows how to specify Frame Relay encapsulation for a POS port:

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

[local]Redback(config-port)#encapsulation frame-relay
```

1.18 encapsulation (PPPoE)

encapsulation pppoe

no encapsulation

1.18.1 Purpose

Specifies the encapsulation type for an Ethernet port without 802.1Q permanent virtual circuits (PVCs).

1.18.2 Command Mode

Port configuration

1.18.3 Syntax Description

pppoe	Specifies Point-to-Point over Ethernet (PPPoE) encapsulation.

1.18.4 Default

The default encapsulation type for Ethernet ports is IP over Ethernet (IPoE).

1.18.5 Usage Guidelines

Use the **encapsulation (PPPoE)** command to specify the encapsulation type for an Ethernet port without 802.1Q PVCs.

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

1.18.6 Examples

The following example shows how to specify PPPoE encapsulation for an Ethernet port:

```
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#encapsulation pppoe
```

1.19 encrypt

encrypt ***sharedkey*** delimiter ***character***

no encrypt

1.19.1 Purpose

Encrypts the identity attributes associated with the redirected subscriber HTTP session.

1.19.2 Command Mode

HTTP redirect profile configuration

1.19.3 Syntax Description

sharedkey	Shared key used to encrypt the identity attributes associated with the redirected subscriber HTTP session.
delimiter ***character***	Character that marks when the encrypted data starts and ends. The delimiter character is not displayed as part of the redirected subscriber HTTP session.

1.19.4 Default

The identity attributes associated with the redirected subscriber HTTP session are redirected in plain text.

1.19.5 Usage Guidelines

Use the **encrypt** command to encrypt the identity attributes associated with the redirected subscriber HTTP session. The encryption ensures the confidentiality of the identity attributes.

Use the **no** form of this command to remove the **encrypt** command from the HTTP redirect profile.

To encrypt the identity attributes associated with a redirected subscriber HTTP session, the SmartEdge router performs an Exclusive Or (XOR) operation. The router takes the variable representing each identity attribute and then applies the XOR operator to each character using a shared key. The identity attributes and sharedkey are all in ASCII text. The XOR operation on the ASCII text produces binary text. Because it is required that the URL be transmitted in ASCII text, the binary text is encoded to a two-character hexadecimal value. To decrypt the string of hexadecimal values, map each two-character hexadecimal

value to its ASCII value and apply the XOR operation to it using the same shared key.

If the shared key is shorter than the combined string of identity attributes, the shared key is repeated within the XOR equation so that each ASCII value that represents a value for the identity attribute is paired with a value from the shared key. For instance, here are sample identity attributes and a shared key to encrypt:

- Username portion of the subscriber name. For example, joe.
- Domain portion of the subscriber name. For example, example.com.
- IP address of the subscriber session. For example, 10.1.11.22.
- Shared key. For example, abcd.

Here is how the XOR equation appears using this data:

```
joe@example.com10.1.11.22

abcdabcdabcdabcdabcdabcda
```

Here is an example of a redirected HTTP session that is encrypted:

```
http://example.com/061413144a57515658514a50514f504f/index.html
```

where 061413144a57515658514a50514f504f is the encrypted data.

1.19.6 Examples

The following example, encrypts the identity attributes associated with the redirected subscriber HTTP session.

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#http-redirect profile Redirect
[local]Redback(config-hr-profile)#message
“Please wait while you are redirected to the customer portal server. Thank you.”
[local]Redback(config-hr-profile)#encrypt secret29$%*() delimiter :
```

1.20 end

end

1.20.1 Purpose

Exits the current configuration mode and returns to exec mode.

1.20.2 Command Mode

All configuration modes

1.20.3 Syntax Description

This command has no keywords or arguments.

1.20.4 Default

None

1.20.5 Usage Guidelines

Use the **end** command to exit the current configuration mode and return to exec mode. When you enter this command, all commands that you have entered since the beginning of the configuration session, or since the last **abort** or **commit** command in configuration mode, are committed to the database.

1.20.6 Examples

The following example displays an administrator exiting interface configuration mode and returning to exec mode:

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

[local]Redback#
```

1.21 end-to-end-delay

end-to-end-delay latency *packet-latency* jitter *buffer-depth* outage-criteria *entry-value exit-value*

default end-to-end-delay

1.21.1 Purpose

Configures the end-to-end delay settings of a CESoPSN or SAToP interworking function (IWF).

1.21.2 Command Mode

CESoPSN or SAToP Config Mode.

1.21.3 Syntax Description

packet-latency	Packet latency in milliseconds. For CESoPSN: The range of values is 1 to 8; the default value is 1. Granularity is 0.125 milliseconds For SAToP: On an e1, the range of values is 1 to 8. On a t1, the value must be .9948 milliseconds. Granularity is 1 milliseconds
buffer-depth	Depth of the jitter buffer in milliseconds. The range of values is 3 to 320; the default value is 5. Granularity is 1 millisecond.
entry-value	Number of consecutive packets with sequential numbers that is required to enter loss-of-packet state (LOPS). The range of values is 1 to 15; the default value is 1.
exit-value	Number of consecutive packets with sequential numbers that is required to exit loss-of-packet state (LOPS). The range of values is 1 to 10; the default value is 10.

1.21.4 Default

CESoPSN and SAToP E1: Packet latency 1; jitter buffer depth 5; entry criteria 1; exit criteria 10.

SAToP DS1: Packet latency .9948; jitter buffer depth 5; entry criteria 1; exit criteria 10.

1.21.5 Usage Guidelines

CESoPSN: Packet latency specifies how many frames are in each packet, where each frame is 125 microseconds.

SAToP: Packet latency of 125 microseconds corresponds to 193 Bits for a DS1 channel and 256 bits for an E1 channel. RFC 4553 requires support for a DS1-channel payload size of 192 bytes and of 256 bytes for E1 channels. This corresponds to 0.9948 milliseconds of packet latency on a DS1, since there are 193 bits per DS1 frame (125 microseconds per frame). On an E1 channel, 193 bytes corresponds to 1 millisecond of packet latency, thus this restriction does not apply.

Packet Latency value of .9948 is rejected if configured on E1 channels.

CES jitter buffer is common for both UDP and MPLS pseudowires. Include a jitter buffer where the payload of received CESoPSN packets is stored prior to play-out to the local TDM trunk. The size of this buffer allows accommodation to the PSN-specific packet delay variation [RFC5086] and should be set to two times the expected packet jitter through the network. Note that an additional latency of, nominally, one-half of this value will be incurred.

Buffer-depth / *packet-latency* must be ≤ 64.

Buffer-depth can be from minimum 3 × *packet-latency* to maximum 64 × *packet-latency*, *or* 320 milliseconds, whichever is smaller, in increments of 125 microseconds.

The minimum ratio between *buffer-depth* and *packet-latency* shall be no smaller than 3.

The maximum value for the LOPS ***entry-value*** is ceiling (ceiling (*buffer-depth* / *packet-latency*) / 2) − 1)

1.21.6 Examples

The following example shows how to configure end-to-end latency on a CESoPSN IWF:

```
[local]Redback(config)#port ds0s 1/1:1:1:1
[local]Redback(config-ds0-ces)#timeslot 16
[local]Redback(config-ds0-ces)#l2vpn local
[local]Redback(config-ds0-ces)#cesopsn
[local]Redback(config-ds0-cesopsn)#end-to-end-delay latency 4 jitter 160 outage-criteria 2 10
```

This example shows how to configure end-to-end latency on a SAToP E1 IWF:

```
[local]Redback(config)#port e1 1/1:1:1
[local]Redback(config-e1-ces)#l2vpn local
[local]Redback(config-e1-ces)#satop
[local]Redback(config-e1-satop)#end-to-end-delay latency 4 jitter 160 outage-criteria 2 10
```

This example shows how to configure end-to-end latency on a SAToP DS1 IWF:

```
[local]Redback(config)#port ds1 1/1:1:1
[local]Redback(config-ds1-ces)#l2vpn local
[local]Redback(config-ds1-ces)#satop
[local]Redback(config-ds1-satop)#end-to-end-delay latency .9948 jitter 160 outage-criteria 2 10
[local]Redback(config-ds1-satop)#loss-of-packet-state-criteria 1 10
```

1.22 endpoint-independent filtering

endpoint-independent filtering {**udp** | **tcp**}

{**no**} **endpoint-independent filtering** {**udp** | **tcp**}

1.22.1 Command Mode

- NAT policy configuration
- NAT policy class configuration

1.22.2 Syntax Description

tcp	TCP traffic is filtered.
udp	UDP traffic is filtered.

1.22.3 Default

NAT operates in point-to-point (P2P) mode using Address-Dependent Filtering with firewall enabled for all UDP traffic in the current class.

1.22.4 Usage Guidelines

Use the **endpoint-independent filtering** command with the **tcp** or **udp** keyword to enable Endpoint-Independent filtering of UDP or TCP traffic. Specify either an existing address pool (by using the **pool** command) or the `ignore` action (using the **ignore** command). Enabling endpoint-independent filtering allows point to multi-point traffic and disables firewalls for the specific transport protocol in the current class.

For more information about Endpoint-Independent filtering, see *Configuring NAT Policies*.

You can apply endpoint-independent filtering:

- At the class level within a NAT policy, so that P2MP traffic can be enabled for selected UDP or TCP traffic streams.
- To the default class at the policy level.

Note: You must first configure an enhanced NAT policy before you can configure the **endpoint-independent filtering** command.

Use the **no** form of this command to disable P2MP mode for the current class, restoring P2P mode.

1.22.5 Examples

The following example shows how to enable P2MP mode for all TCP and UDP traffic in the class **yes_p2mp**:

```
[local]Redback(config)#context nat_context
[local]Redback(config-ctx)#nat policy basic_nat
[local]Redback(config-policy-nat)#drop
[local]Redback(config-policy-nat)#access group basic_nat_rules
[local]Redback(config-policy-group)#class yes_p2mp
[local]Redback(config-policy-group-class)#pool NAPT_POOL local
[local]Redback(config-policy-group-class)#endpoint-independent filtering udp
[local]Redback(config-policy-group-class)#endpoint-independent filtering tcp
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#class firewall
[local]Redback(config-policy-group-class)#pool NAPT_POOL local
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#class no_NAT
[local]Redback(config-policy-group-class)#ignore
```

1.23 enforce first-as

enforce first-as

no enforce first-as

1.23.1 Purpose

Enables verification of the first AS number in a received AS path from an eBGP peer.

1.23.2 Command Mode

BGP neighbor configuration

1.23.3 Syntax Description

This command has no keywords or arguments.

1.23.4 Default

This command is enabled.

1.23.5 Usage Guidelines

Use the **enforce first-as** command to enable verification of the first AS number in a received AS path from an eBGP peer.

By default, a BGP router compares the remote AS number of an eBGP peer with the AS number of the first segment in the paths received from that peer. If those AS numbers do not match, the BGP router:

- Sends a NOTIFICATION message to eBGP peer that contains error code 3 (UPDATE Message Error) and error subcode 11 (Malformed AS_PATH). For more information on these error codes, see RFC 4271, *A Border Gateway Protocol 4 (BGP-4)*.
- Drops the session with the eBGP peer.

Note: When an eBGP neighbor is first added to a peer group, first-AS-path verification is enforced for that neighbor regardless of whether first-AS-path verification is enabled or disabled.

Note: This command is not supported for BGP peer groups.

Use the **show configuration bgp** command to see whether first-AS-path verification is enabled or disabled for a BGP neighbor.

Use the **no** form for this command to disable first-AS-path verification for a BGP neighbor.

1.23.6 Examples

The following example shows how to disable the verification of the first AS number in a received AS path from eBGP peer**10.10.10.20**:

```
[local]Redback(config-bgp)#neighbor 10.10.10.20 external
[local]Redback(config-bgp-neighbor)#no enforce first-as
```

The following example shows how to enable the verification of the first AS number in a received AS path from the eBGP peer**10.10.10.20:**:

```
[local]Redback(config-bgp)#neighbor 10.10.10.20 external
[local]Redback(config-bgp-neighbor)#enforce first-as
```

1.24 enforce ttl

```
enforce ttl

no enforce ttl
```

1.24.1 Purpose

Enables Border Gateway Protocol (BGP) time-to-live (TTL) security check in the kernel for the specified BGP neighbor or BGP peer group.

1.24.2 Command Mode

- BGP neighbor configuration
- BGP peer group configuration

1.24.3 Syntax Description

This command has no keywords or arguments.

1.24.4 Default

BGP TTL security check is not enabled in kernel.

1.24.5 Usage Guidelines

Use the **`enforce ttl`** command to enable BGP TTL security check in the kernel for the specified BGP neighbor or BGP peer group.

The BGP TTL security check feature can be used instead of, or in conjunction with, the BGP Session Protection via TCP Message Digest 5 (MD5) signature option for external BGP (eBGP); however, the TTL-based security check mechanism is more simple to operate because it does not require the coordination for managing the MD5 keys.

Caution!

Risk of data loss. Enabling the BGP TTL security check on only one end of an eBGP session causes the session to drop. To reduce the risk, verify that the BGP TLL security check feature is enabled on both ends of the eBGP session.

The BGP TTL security check is designed to protect the BGP infrastructure from CPU-utilization based attacks caused by sending control traffic that appears to be valid control traffic to a BGP session. It protects the BGP infrastructure by setting the value of the TTL field to 255 in outgoing BGP packets, and dropping incoming BGP packets that have TTL values less than the maximum TTL value (255) minus the maximum number of eBGP hops allowed.

For example, if you use the **ebgp-multihop** command to set the maximum number of hops used to reach an eBGP neighbor to two, then you should receive eBGP packets with TTL values of no less than 253 (255 - 2). When the BGP TTL security check is enabled using the **enforce ttl** command, all incoming BGP packets that have a TTL value less than 253 are dropped.

If the **ebgp-multihop** command is not used to set the maximum number of hops, then the default maximum hop value of 1 is used, and the BGP TTL security check drops all incoming BGP packets with TTL values less than 254.

1.24.6 Examples

The following example shows how to enable the BGP TTL security check to drop all BGP packets with a TTL value lower than **254** received from BGP neighbor, **10.10.10.20:**

```
[local]Redback(config-bgp)#neighbor 10.10.10.20 external

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

1.25 equipment-loopback (DS-1 and DS-3)

equipment-loopback {**customer** | **network**}

default equipment-loopback

1.25.1 Purpose

Configures a DS-3 channel or port, either clear-channel or channelized, or a DS-1 channel, to respond to or ignore remote loopback requests.

1.25.2 Command Mode

- DS-1 configuration
- DS-3 configuration

1.25.3 Syntax Description

customer	Configures the channel or port to respond to remote loopback requests; this is the default.
network	Configures the channel or port to ignore remote loopback requests.

1.25.4 Default

The channel or port responds to remote loopback requests.

1.25.5 Usage Guidelines

Use the **equipment-loopback** command to configure a DS-3 channel or port, either clear-channel or channelized, or a DS-1 channel, to respond to or ignore remote loopback requests.

Note: This command is not available for a fractional DS-1 channel, using the **timeslot** command (in DS-1 configuration mode) with any assignment of DS-0 time slots other than the default range (1 to 24).

Use the **default** form of this command to configure the channel or port to respond to remote loopback requests.

Note: This command is also documented in *Configuring ATM, Ethernet, and POS Ports* for Asynchronous Transfer Mode (ATM) DS-3 ports.

1.25.6 Examples

The following example shows how to configure DS-3 channel **1** on port **1** on the channelized OC-12 traffic card in slot **3** to ignore remote loopback requests:

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

[local]Redback(config-ds3)#equipment-loopback network
```

1.26 ethernet-cfm

ethernet-cfm ***instance-name***

{**no** | **default**} **ethernet-cfm** ***instance-name***

1.26.1 Purpose

Creates a CFM instance and enters CFM configuration mode where the parameters of the maintenance points in the instance can be specified.

1.26.2 Command Mode

Global configuration

1.26.3 Syntax Description

instance-name	The name used to identify the CFM service instance on the SmartEdge router.

1.26.4 Default

No CFM service instances exist.

1.26.5 Usage Guidelines

Use the **cfm** command to create a CFM instance and enter the CFM configuration mode where the parameters of the maintenance points in the instance can be specified. You can create multiple CFM instances.

Table 2 CFM Instances Restrictions

Restriction Synopsis	Restriction Description
Each service instance is limited to a single maintenance domain (MD) and a single MD level.	Effectively, each service instance is equivalent to a MD.
Each MD name must be unique within the SmartEdge router.	The MD names created in the CFM instances of the SmartEdge router must be unique even if they occur in different CFM instances.

The default MD name is the same as the CFM instance name set by the **ethernet-cfm** command.

1.26.6 Examples

The following example shows how to use this command to create the maintenance instance `instance-1 at MD level 4:`

```
[local]Redback(config)#ethernet-cfm instance-1

[local]Redback(config-ether-cfm)#level 4
```

1.27 ethernet-cfm linktrace

ethernet-cfm linktrace from {***local-map*** | {***circuit*** | ***link-group***} [***transport*** |***vlan***]} **to** {***dest-mac*** | ***rmep***} ***level***

1.27.1 Purpose and Usage Guidelines

Initiates a CFM link-trace from a specified circuit, transport circuit, Ethernet link group, port, or local maintenance association endpoint (MEP) to a specified remote MEP (RMEP) or MAC address.

1.27.2 Command Mode

Exec (10)

1.27.3 Syntax Description

local-map	**md** ***md-id*** **ma** ***ma-id*** **mep** ***mep-id*** Specifies the maintenance domain (MD), maintenance association (MA), and ID of a local MEP where the link-trace starts. The value specified for this argument must correspond to a valid 802.1Q PVC.
circuit	***slot/port*** [***:ch:sub***] Specifies the Ethernet circuit or port where the link-trace starts.
link-group	**lg** {***link-group-name*** | **id** ***link-group-id***} Specifies the link group where the link-trace starts. Range for ***link-group-id*** is from 1 through 784.

transport	**transport** {***transport-vlans*** | **any**} Optional. Specifies the transport circuits initiating the link-trace. The **transport** keyword specifies a transport circuit is to used to initiate the linktrace. This keyword is followed by how the transport circuit is defined under the port. The VLAN ID is required and specifies which VLAN tag(s) are used by the linktrace. The ***transport-vlans*** argument is either a range or single VLAN. It must be one of the following constructs: • ***pvc-vlan-id-first - pvc-vlan-id-last***—A range of PVCs (outer VLAN tags). • ***pvc-vlan-id***—The outer VLAN tags). • ***tunl-vlan-id:pvc-vlan-id-first - pvc-vlan-id-last***—A range of PVCs (inner VLAN tags) in an 802.1Q tunnel (outer VLAN tag). • ***tunl-vlan-id:pvc-vlan-id***—A PVC (inner VLAN tag) in an 802.1Q tunnel (outer VLAN tag). If you enter **any**, the ***vlan-id*** that follows specifies the link-trace initiator. In the following example, `33:68` would be the link-trace initiator: `...transport any vlan-id 33:68...`
vlan	**vlan-id** ***vlan-id*** Optional. Specifies the parent circuit of link-trace. If no transport circuits are specified in the command, this parameter also specifies the VLAN tag of the loopback initiator. The ***vlan-id*** argument is one of the following constructs: • ***pvc-vlan-id*** — VLAN tag value of a PVC (outer VLAN tag). • ***tunl-vlan-id:pvc-vlan-id*** — VLAN tag value for an 802.1Q tunnel followed by the VLAN tag value for the PVC within the tunnel. The ***vlan-id*** argument must also specify a PVC configured in the link group or port specified by the ***link-group*** or ***circuit*** arguments.
to ***dest-mac***	**to** ***nn:nn:nn:nn:nn:nn*** Specifies the MAC address of the device where the link-trace ends.

to ***rmep***	**to rmep** ***rmep-id*** Specifies the ID of the remote maintenance association endpoint (RMEP) where the link-trace ends. The value specified for this argument must correspond to a valid 802.1Q PVC.
level	**level** ***level*** Specifies the MD level of the device initiating the link-trace. Enter an integer from 0 to 7.

1.27.4 Default

There is no default behavior.

1.27.5 Examples

1.27.5.1 Basic Linktrace Example

The following example illustrates the **ethernet-cfm linktrace** command:

```
[local]Redback#ethernet-cfm linktrace from 5/1 to 00:01:02:03:ab:12 level 3
```

1.27.5.2 CFM Linktrace Initiated by a Transport circuit

In the following example, port 1/1 is configured with two transport circuits:

```
port ethernet 1/1
 encapsulation dot1q
  dot1q pvc transport any
  dot1q pvc transport 10-20
```

The following command uses the transport circuit `any` to initiate a CFM linktrace assuming that a MEP is configured on it.

```
[local]Redback#ethernet-cfm loopback 1/1 transport any vlan-id 100 to 00:01:02:01:01:02 level 4
```

The following command uses the transport circuit `10-20` to initiate a CFM linktrace assuming that a MEP is configured on it.

```
[local]Redback#ethernet-cfm loopback 1/1 transport 10-20 vlan-id 10 to 00:01:02:01:01:02 level 4
```

1.28 ethernet-cfm loopback

ethernet-cfm loopback from {***local-map*** | {***circuit*** | ***link-group***} [[***transport***] ***vlan***]} **to** {***dest-mac*** | ***rmep***} ***level*** [***data***] [***size***]

1.28.1 Purpose and Usage Guidelines

Initiates a CFM loopback message (LBM) from a specified circuit, transport circuit, Ethernet link group, port, or local maintenance association endpoint (MEP) to a specified remote MEP (RMEP) or MAC address.

1.28.2 Command Mode

Exec (10)

1.28.3 Syntax Description

local-map	**md** ***md-id*** **ma** ***ma-id*** **mep** ***mep-id*** Specifies the maintenance domain (MD), maintenance association (MA), and ID of a local MEP where the link-trace starts. The value specified for this argument must correspond to a valid 802.1Q PVC.
circuit	***slot/port*** [***:ch:sub***] Specifies the Ethernet circuit or port where the link-trace starts.
link-group	**lg** [***link-group-name*** | **id** ***link-group-id***] Specifies the link group from which the LBR is sent. Link group ID. Range for the ***link-group-id*** is from 1 through 784.

transport	**transport** {***transport-vlans*** | **any**} Optional. Specifies the transport circuits initiating the loopback. This keyword is followed by how the transport circuit is defined under the port. The VLAN ID is required and specifies which VLAN tag(s) are used by the loopback. Specifies a range or single VLAN. It must be one of the following constructs: • ***pvc-vlan-id-first - pvc-vlan-id-last***—A range of PVCs (outer VLAN tags). • ***pvc-vlan-id***—The outer VLAN tags). • ***tunl-vlan-id:pvc-vlan-id-first - pvc-vlan-id-last***—A range of PVCs (inner VLAN tags) in an 802.1Q tunnel (outer VLAN tag). • ***tunl-vlan-id:pvc-vlan-id***—A PVC (inner VLAN tag) in an 802.1Q tunnel (outer VLAN tag). If you enter **any**, the ***vlan-id*** that follows specifies the loopback initiator. In the following example, `33:68` would be the loopback initiator: `...transport any vlan-id 33:68...`
vlan	**vlan-id** ***vlan-id*** Specifies the parent circuit of loopback. If no transport range is specified in the command, this parameter also specifies the VLAN tag sent in the LBR as the loopback initiator. The ***vlan-id*** argument is one of the following constructs: • ***pvc-vlan-id*** — VLAN tag value of a PVC (outer VLAN tag). • ***tunl-vlan-id:pvc-vlan-id*** — VLAN tag value for an 802.1Q tunnel followed by the VLAN tag value for the PVC within the tunnel. The ***vlan-id*** argument must also specify a PVC configured in the link group or port specified by the ***link-group*** or ***circuit*** arguments.
to ***dest-mac***	**to** ***nn:nn:nn:nn:nn:nn*** Specifies the MAC address of the device to which the LBR is sent and which returns the LBR.
to ***rmep***	**to rmep** ***rmep-id*** Specifies the ID of the remote maintenance association endpoint (RMEP) to which the LBR is sent and which returns the LBR. The value specified for this argument must correspond to a valid 802.1Q PVC.

level	**level** ***level*** Specifies the MD level of the device initiating the loopback. Enter an integer from 0 to 7.
data	**data** ***data*** Optional. Specifies the data carried by the LBR PDU. Up to 127 ASCII characters can be specified. If **data** ***data*** is not specified, CFM loopbacks are sent without any data.
size	**size** ***size*** Optional. Specifies the loopback message (LBM) size. The (LBM) contains the number of bytes specified by this parameter in which the data pattern specified by **data** ***data*** is repeated as many times as it takes to reach the specified size. You can specify up to 1500 bytes for the LBM size.

1.28.4 Default

There is no default behavior.

1.28.5 Examples

1.28.5.1 Specifying the Data Carried by the CFM Loopback

The following example illustrates the **ethernet-cfm loopback** command in which the LBM carries the data string, `324cuai:`

```
[local]Redback#ethernet-cfm loopback from 5/1 to 00:01:02:03:ab:12 level 5 data 324cuai
```

1.28.5.2 CFM Loopback Initiated by a Transport circuit

In the following example, port 1/1 is configured with two transport circuits:

```
port ethernet 1/1
 encapsulation dot1q
  dot1q pvc transport any
  dot1q pvc transport 10-20
```

The following command uses the transport circuit `any` to initiate a CFM loopback assuming that a MEP is configured on it.

```
[local]Redback#ethernet-cfm loopback 1/1 transport any vlan-id 100 to 00:01:02:01:01:02 level 4
```

The following command uses the transport circuit `10-20` to initiate a CFM loopback assuming that a MEP is configured on it.

```
[local]Redback#ethernet-cfm loopback 1/1 transport 10-20 vlan-id 10 to 00:01:02:01:01:02 level 4
```

1.29 ethernet-cfm measure-delay

ethernet-cfm measure-delay {two-way} from {*circuit*|*local-mep*} to {*dest-mac*|*rmep*} *level* [*priority*] [*interval*] [*count*]

1.29.1 Purpose and Usage Guidelines

Initiates monitoring of Ethernet frame delay from a specified circuit or local maintenance association endpoint (MEP) to a specified remote MEP (RMEP) or MAC address.

Only one Ethernet delay measurement (ETH-DM) can be initiated at a time for a single MEP, and while the transaction is active, a new ETH-DM cannot be initiated for the same MEP.

Delay and delay variation are rounded to the floor value. Delay variation is calculated as the difference in two consecutive delays for (count-1) frames.

1.29.2 Command Mode

Exec

1.29.3 Syntax Description

two-way	**two-way** Initiates a two-way delay measurement (2DM).
local-mep	**domain** ***md-id*** **ma** ***ma-id*** **mep** ***mep-id*** Specifies the maintenance domain (domain), maintenance association (MA), and ID of a local MEP where the measurement starts.
circuit	***slot/port*** Specifies the Ethernet circuit where the measurement starts.
to ***dest-mac***	**to** ***nn:nn:nn:nn:nn:nn*** Specifies the MAC address of the destination device.
to ***rmep***	**to** ***rmep-id*** Specifies the ID of the RMEP.
level	**level** ***level*** Specifies the ME group level of the device initiating the measurement; required when ***circuit*** is specified. Enter an integer from 0 to 7.

priority	**priority** ***priority*** Specifies the 802.1p priority associated with the operation, administration and maintenance (OAM) service frames, which must be the same priority as the data traffic. For 2DMs, the frames are sent with the priority that was specified when the command was issued. The received 2DM frames are looped at the card level without any change to the priority. The default priority for outgoing 2DM frames is 7.
interval	**interval** ***interval*** Specifies, in seconds, the time period to wait between sending each DM message. Enter a value from 1s to 3600s. The default is 1s.
count	**count** ***count*** Specifies the total number of DM messages to send. Enter an integer from 1 to 100. The default is 10.

1.29.4 Default

None.

1.29.5 Examples

The following example shows the results of a 2DM with a total of 10 messages and a one second interval between each message.

```
[local]Redback#ethernet-cfm measure-delay two-way from 1/1 vlan-id 10 to rmep 5
level 1 priority 5 interval 1s count 10
circuit: 1/1 vlan-id 10, handle: 1/1:1023:63/1/2/17, vlan id: 10, inner vlan id: 0
2-way ETH-DM from 1/1 vlan-id 10 to 00:07:01:01:01:01 level 1 count 10
2-way ETH-DM in progress...
 1  00:07:01:01:01:01 delay  58 usec delay variation 0 usec
 2  00:07:01:01:01:01 delay  67 usec delay variation 9 usec
 3  00:07:01:01:01:01 delay  74 usec delay variation 7 usec
 4  00:07:01:01:01:01 delay  76 usec delay variation 2 usec
 5  00:07:01:01:01:01 delay  80 usec delay variation 4 usec
 6  00:07:01:01:01:01 delay  75 usec delay variation 5 usec
 7  00:07:01:01:01:01 delay  81 usec delay variation 6 usec
 8  00:07:01:01:01:01 delay  85 usec delay variation 4 usec
 9  00:07:01:01:01:01 delay  72 usec delay variation 13 usec
 10 00:07:01:01:01:01 delay  69 usec delay variation 3 usec
2-way ETH-DM completed.
----- Delay measurement statistics -----
10 packets sent, 10 packets received
delay min/avg/max = 58/73/85 usec
avg delay variation = 5 usec
```

1.30 ethernet to qos

ethernet {***802.1p-value*** | **all**} **to qos** ***pd-value***

default ethernet {***802.1p-value*** | **all**}

1.30.1 Purpose

Translates Ethernet 802.1p values to packet descriptor (PD) quality of service (QoS) values on ingress.

1.30.2 Command Mode

Class map configuration

1.30.3 Syntax Description

802.1p-value	An integer from 0 (lowest priority) to 7 (highest priority) representing the contents of the three user priority bits in the 802.1p virtual LAN (VLAN) Tag Control Information (TCI) field.
all	Maps all valid values for the source value to the specified target value. Any existing configuration for the classification map is overridden.
pd-value	An integer from 0 to 63 (six bits), with the packet priority encoded in three higher-order bits and the packet drop precedence in the three lower-order bits. You can enter the value in decimal or hexadecimal format, for example **16** or **0x10**. You can also enter a standard Differentiated Services Code Point (DSCP) marking label as defined in *DSCP Class Keywords*. The scale used by this command for packet priority, from 0 (lowest priority) to 7 (highest priority), is the relative inverse of the scale used by the **mark priority** command. For details on this command, see *Configuring Rate-Limiting and Class-Limiting*.

1.30.4 Default

None

1.30.5 Usage Guidelines

Use the **ethernet to qos** command to define ingress mappings from Ethernet 802.1p values to PD QoS values.

If you specify the **all** keyword, all valid 802.1p values are mapped to the specified PD value. Any existing configuration for the classification map is overridden. You can use the **all** keyword to specify a single default value for all the mapping entries, then override that value for a subset of entries by entering subsequent mapping commands without this keyword.

Use the **default** form of this command to revert one or all map entries to either the default 8P0D or mapping schema values, if a mapping schema has been specified.

1.30.6 Examples

The following example shows how to define the classification map **8021p-to-pd** for PD bits on ingress, then map the Ethernet 802.1p values **1** and **7** to PD user priority values **af33** and **af21**, respectively:

```
[local]Redback(config)#qos class-map 8021p-to-pd ethernet in

[local]Redback(config-class-map)#ethernet 1 to qos af33

[local]Redback(config-class-map)#ethernet 7 to qos af21
```

1.31 ethernet use-ip

ethernet {*802.1p-value* | **all**} **use-ip** [*class-map-name*]

default ethernet {*802.1p-value* | **all**}

1.31.1 Purpose

For IP packets, determines packet descriptor (PD) values by mapping IP Differentiated Services Code Point (DSCP) values instead of Ethernet 802.1p values on ingress. For IPv4 packets, the DSCP marking is the upper six bits of the IPv4 header Type of Service (ToS) field. For IPv6 packets, the DSCP marking is the upper six bits of the IPv6 header Traffic Class field.

1.31.2 Command Mode

Class map configuration

1.31.3 Syntax Description

802.1p-value	An integer from 0 (lowest priority) to 7 (highest priority) representing the contents of the three user priority bits in the 802.1p virtual LAN (VLAN) Tag Control Information (TCI) field.
all	Maps all valid values for the source value to the specified target value. Any existing configuration for the classification map is overridden.
use-ip	Enables a secondary mapping lookup using the packet's DSCP bits as input. If no classification map is specified for the secondary lookup, the default DSCP-to-target mapping is used.
class-map-name	Optional. Name of the secondary classification map.

1.31.4 Default

None

1.31.5 Usage Guidelines

Use the **ethernet use-ip** command to set initial PD values based on IP header DSCP bits instead of Ethernet 802.1p values on ingress.

If you specify the **all** keyword, all valid 802.1p values are configured to use DSCP-to-PD mapping. Any existing configuration for the classification map is overridden. You can use the **all** keyword to specify a single default value for all the mapping entries, then override that value for a subset of entries by entering subsequent mapping commands without this keyword.

If you specify the optional ***class-map-name*** argument, the resulting DSCP-to-PD mapping uses the specified DSCP-to-PD classification map. The secondary classification map must have a value of **ip** for the ***marking-type*** argument, and a value of **in** for the mapping direction. If no secondary classification map is specified, the default DSCP-to-target mapping is used.

Use the **default** form of this command to revert one or all map entries to either the default 8P0D or mapping schema values, if a mapping schema has been specified.

1.31.6 Examples

The following example shows how to define the classification map **8021p-to-pd** to determine initial QoS PD values on ingress, and specifies **7P1D** encoding as a default mapping schema. It then overrides the default **7P1D** values for Ethernet 802.1p value **1** with PD value **0x24**, and specifies that the IP header DSCP value determines the initial QoS PD value for packets received with Ethernet 802.1p value **3**:

```
[local]Redback(config)#qos class-map 8021p-to-pd ethernet in
[local]Redback(config-class-map)#mapping-schema 7P1D
[local]Redback(config-class-map)#ethernet 1 to qos 0x24
[local]Redback(config-class-map)#ethernet 3 use-ip
```

1.32 eventtype

```
eventtype {communicationsAlarm | envirnomentalAlarm |
equipmentAlarm | integrityViolation | operationalViolation
| other | physicalViolation | processingErrorAlarm | quali
tyOfServiceAlarm | securityServideOrMechanismViolation |
timeDomainViolation}

no eventtype
```

1.32.1 Purpose

Describes the alarm communication event type.

1.32.2 Command Mode

SNMP alarm model configuration

1.32.3 Syntax Description

communicationsAlarm	The alarm is related to the communication between systems.
envirnomentalAlarm	The alarm is related to the functions of the network environment.
equipmentAlarm	The alarm is caused by a problem with the equipment or hardware in your network.
integrityViolation	The alarm is a result of a breach in system integrity.
operationalViolation	The alarm is a result of a problem with the operation of the system.
other	The alarm is related to some other problem that is not a communication, environmental, equipment, integrity, operational, physical, processing error, quality of service, security service or mechanism, or time problem.
physicalViolation	The alarm is related to a physical violation of the system.
processingErrorAlarm	The alarm is a result of a processing error
qualityOfServiceAlarm	The alarm is a result of a problem with QoS.
securityServiceOrMechanismViolation	The alarm is a result of problem with security service or a security mechanism.
timeDomainViolation	The alarm is a result of a time domain violation.

1.32.4 Default

None

1.32.5 Usage Guidelines

Use the **eventtype** command to describe the notification event that the alarm model identifies. These values are a subset to those defined by IANAItuEventType. Running this command results in an entry in the ituAlarmTable.

Use the **no** form of this command to remove the alarm description.

1.32.6 Examples

The following example shows how to configure the alarm description as **qualityofservice**.

```
[local]jazz#config
[local]jazz(config)#snmp alarm model 1 state clear
[local]jazz(config-snmp-alarmmodel)#eventtype qualityofservice
[local]jazz(config-snmp-alarmmodel)#exit
```

1.33 exceed drop

exceed drop [**qos-priority** *group-num*]

{**no** | **default**} **exceed drop** [**qos-priority** *group-num*]

1.33.1 Purpose

Specifies how packets are dropped when the traffic rate exceeds the quality of service (QoS) rate and burst tolerance.

1.33.2 Command Mode

- Policy class rate configuration
- Policy rate configuration

1.33.3 Syntax Description

qos-priority *group-num*	Optional. Packet descriptor (PD) QoS priority group number. This option is available only if the QoS rate is configured with an excess burst tolerance. The range of values for the *group-num* argument is 0 to 7.

1.33.4 Default

If the excess burst tolerance is not configured, all packets exceeding the QoS burst tolerance are dropped. If the excess burst tolerance is configured, packets exceeding the QoS burst tolerance are dropped randomly.

1.33.5 Usage Guidelines

Use the **exceed drop** command to specify how packets are dropped when the traffic rate exceeds the QoS rate and burst tolerance. Use this command as part of a policing policy for incoming packets and as part of a metering policy for outgoing packets.

You can configure the traffic rate, burst tolerance, and excess burst tolerance with the **rate** command in policy ACL class, metering policy, or policing policy configuration mode. The following conditions determine how packets are dropped:

- If the excess burst tolerance is not configured, all packets exceeding the configured burst tolerance are dropped.
- If the excess burst tolerance is configured, and the traffic rate does not exceed the excess burst tolerance, packets are dropped according to one of the following conditions:

- If the **qos-priority** ***group-num*** construct is not configured, packets are dropped randomly.
- If the **qos-priority** ***group-num*** construct is configured, only packets with a QoS priority less than the specified ***group-num*** argument are dropped. All other packets are not dropped.

  Note: Use the **violate drop** commands in policy class rate and policy rate configuration modes to specify how packets are dropped when the traffic rate exceeds the configured excess burst tolerance.

Caution!

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

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

1.33.6 Examples

The following example shows how to drop packets that exceed the traffic rate and burst tolerance:

```
[local]Redback(config)#qos policy protection1 policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#exceed drop
```

1.34 exceed mark dscp

exceed mark dscp ***dscp-class***

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

1.34.1 Purpose

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

1.34.2 Command Mode

- Policy class rate configuration
- Policy rate configuration

1.34.3 Syntax Description

dscp-class	Priority with which packets exceeding the rate are marked. Values can be: • An integer from 0 to 63. • One of the keywords listed in Table 3.

1.34.4 Default

Packets exceeding the policing rate are dropped.

1.34.5 Usage Guidelines

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

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

Table 3 lists the keywords for the ***dscp-class*** argument.

Table 3 DSCP Class Keywords

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

Note: RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*, defines the Class Selector code points.

Caution!

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

Caution!

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

Use the **no** or **default** form of this command to return to the default behavior of dropping packets that exceed the rate.

1.34.6 Examples

The following example shows how to configure the policy to mark all packets that conform to the configured rate with a DSCP value representing a high priority and drop all packets that exceed the rate:

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

1.35 exceed mark precedence

exceed mark precedence *prec-value*

{**no** | **default**} **exceed mark precedence**

1.35.1 Purpose

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

1.35.2 Command Mode

- Policy class rate configuration
- Policy rate configuration

1.35.3 Syntax Description

prec-value	Drop precedence bits value. See Table 4.

1.35.4 Default

Packets exceeding the policy rate are dropped.

1.35.5 Usage Guidelines

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

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

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

With AF classes AF1 (AF11, AF12, AF13), AF2 (AF21, AF22, AF23), AF3 (AF31, AF32, AF33), and AF4 (AF41, AF42, AF43), the second integer represents a drop precedence value. Table 4 shows how the AF drop precedence value of an incoming packet is changed when it exits the SmartEdge router after being tagged with a new drop precedence. (See also RFC 2597, ***Assured Forwarding PHB Group***.)

Table 4 Drop Precedence Values

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

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

Caution!

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

Use the **no** or **default** form of this command to return to the default behavior of dropping packets that exceed the rate.

1.35.6 Examples

The following example shows how to configure the policy to mark all packets that conform to the configured rate with an IP precedence value of **3** and use the **conform mark** command, which by default, drops all packets that exceed the rate:

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

1.36 exceed mark priority

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

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

1.36.1 Purpose

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

1.36.2 Command Mode

- Policy class rate configuration
- Policy rate configuration

1.36.3 Syntax Description

group-num	PD QoS priority group number. The range of values is 0 to 7. The scale used by this command for packet priority, from 0 (highest priority) to 7 (lowest priority), is the relative inverse of the scale used by QoS classification map and classification definition commands.
ignore	Specifies that the internal PD priority or drop-precedence value is not modified.
drop-precedence	Optional. Enables you to specify a setting for either the drop-precedence portion of the PD QoS field or the PD QoS group, or both.
af-drop *drop-value*	Optional. Specifies the target internal drop-precedence value in two-bit format, leaving the least significant bit unmodified. The range of values is 1 to 3.

1.36.4 Default

Packets exceeding the rate are dropped.

1.36.5 Usage Guidelines

Use the **exceed mark priority** command to mark packets that exceed the QoS rate and burst tolerance with a PD QoS group number, a drop-precedence value, or both, while preserving the packet's IP header. To configure the rate,

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

A PD QoS group is an internal value used by the SmartEdge router to determine into which egress queue the inbound packet should be placed. The type of service (ToS) value, Differentiated Services Code Point (DSCP) value, and Multiprotocol Label Switching (MPLS) experimental (EXP) bits are unchanged by this command. The actual queue number depends on the number of queues configured on the circuit. For more information, see the **num-queues** command in *Configuring Queuing and Scheduling*.

The SmartEdge router uses the factory preset, or default, mapping of a PD QoS group to queue, according to the number of queues configured on a circuit; see Table 5.

Table 5 Default Mapping of Priority Groups

PD QoS group	8 Queues	4 Queues	2 Queues	1 Queue
0	Queue 0	Queue 0	Queue 0	Queue 0
1	Queue 1	Queue 1	Queue 1	Queue 0
2	Queue 2	Queue 1	Queue 1	Queue 0
3	Queue 3	Queue 2	Queue 1	Queue 0
4	Queue 4	Queue 2	Queue 1	Queue 0
5	Queue 5	Queue 2	Queue 1	Queue 0
6	Queue 6	Queue 2	Queue 1	Queue 0
7	Queue 7	Queue 3	Queue 1	Queue 0

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

Caution!

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

Note: By default, the SmartEdge router assigns a PD QoS group to each egress queue, according to the number of queues configured on a circuit. You can override the default mapping of packets into egress queues by creating a customized queue priority map using the **qos queue-map** command in global configuration mode.

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

1.36.6 Examples

The following example shows how to configure the policy to mark all packets that exceed the configured rate with a PD QoS group of **3** and use the **exceed mark** command, which by default, drops all packets that exceed the rate:

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

1.37 exceed no-action

exceed no-action

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

1.37.1 Purpose

Specifies that no action is taken on packets that exceed the configured quality of service (QoS) rate and burst tolerance.

1.37.2 Command Mode

- Policy class rate configuration
- Policy rate configuration

1.37.3 Syntax Description

This command has no keywords or arguments.

1.37.4 Default

Packets exceeding the rate are dropped.

1.37.5 Usage Guidelines

Use the **exceed no-action** command to specify that no action is taken on packets that exceed the rate.

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

Caution!

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

Use the **no** or **default** form of this command to return to the default behavior of dropping packets that exceed the rate.

1.37.6 Examples

The following example shows how to configure the policy to take no action on packets that exceed the rate:

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

1.38 exclude

exclude {***node-ip-addr*** | ***link-ip-addr***}

no exclude

1.38.1 Purpose

Specifies nodes or links to exclude from the Constrained Shortest Path First (CSPF) calculation.

1.38.2 Command Mode

RSVP constraint configuration

1.38.3 Syntax Description

node-ip-addr	IP address of a node to exclude from the label-switched path (LSP).
link-ip-addr	IP address of a link to exclude from the LSP.

1.38.4 Default

No nodes or links are excluded from the CSPF calculation.

1.38.5 Usage Guidelines

Use the **exclude** command to exclude nodes or links from the CSPF path calculation.

Use the **no** form of this command to remove nodes or links excluded from the CSPF calculation.

1.38.6 Examples

The following example shows how to exclude node `10.2.3.4` from an LSP that traverses the network:

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#constraint constraint1
[local]Redback(config-rsvp-constr)#exclude node 10.2.3.4
```

1.39 exclude (NAT)

exclude [*port-start* to *port_end* | exclude well-known]

no exclude [*port-start* to *port_end* | exclude well-known]

1.39.1 Purpose

Excludes the port range from a specific address or an address range of a pool or excludes well-known port ranges for the entire pool, 0 to 1023.

1.39.2 Command Mode

NAT pool record configuration.

1.39.3 Syntax Description

to	Indicates the limit of the port range. Use the **to** keyword to exclude an address range of a pool.
port-start	Starting port number or a specific port number address. The range of values is 0 through 65535. When you configure the ***port-start***and ***port-end*** parameters, the system rounds the range down or up, respectively, to the nearest multiple of 32. For example, configuring the exclude from 12 to 61 excludes ports from 0 to 63.
port-end	Ending port number.
well-known	Excludes TCP and UDP port ranges from 0 to 1023 from a specific address or an address range of a pool. This is an alias of "exclude 0 to 1023".

1.39.4 Default

None.

1.39.5 Usage Guidelines

Use the **exclude** command to exclude following:

- the port range from a specific address
- an address range of a pool
- well known port ranges for the entire pool, 0 to 1023

You cannot configure more than 4 excludes per IP or address range. Specifying a 5th exclude option displays an error message.

Use the **no** version of this command to delete the port range from a specific address or an address range of a pool.

1.39.6 Example

The following example shows you how the exclude ports 5000 through 1000 for both TCP and UDP and well known ports 0 through 1023.

```
[local]rock1200(config-ctx)#context na-context
[local]rock1200(config-ctx)#ip nat pool nat-pool napt multibind
[local]rock1200(config-nat-pool)#address 85.62.163.1 to 85.62.163.14 port-block 0 to 15
[[local]rock1200(config-nat-pool-record)#exclude ?
  0..65536    Define port range start
  well-known  Exclude port range from 0 to 1023

[local]rock1200(config-nat-pool-record)#exclude 5000 to 10000 <-Excludes ports 5000-10000 for both TCP and UDP
[local]rock1200(config-nat-pool-record)#exclude well-known <- Remove TCP and UDP ports 0-1023 for the entire p
```

1.40 exclusive

exclusive

1.40.1 Purpose

Configures a primary LSP to support pseudowire (PW) traffic only.

1.40.2 Command Mode

RSVP LSP configuration

1.40.3 Syntax Description

This command has no keywords or arguments.

1.40.4 Default

None

1.40.5 Usage Guidelines

Use the **exclusive** command to configure a primary LSP to support PW traffic only.

Note: Only primary LSPs can be configured to be exclusive. Mapped bypass and backup LSPs inherit exclusivity from the primary LSP.

For more information about mapped RSVP LSPs, see one of the following sections, as appropriate:

Use the **no** version of this command to return the LSP to non-exclusive configuration.

1.40.6 Examples

The following example shows how to configure the LSP called **RBAK1_RC1_BLACK** to support PW traffic only.

```
[local]Redback(config-rsvp)#lsp RBAK1_RC1_BLACK
[local]Redback(config-rsvp-lsp)#exclusive
```

1.41 exit

exit

1.41.1 Purpose

Exits the current configuration mode and returns to the next highest-level configuration mode. At the exec prompt, closes an active terminal or console session, and terminates the session.

1.41.2 Command Mode

All modes

1.41.3 Syntax Description

This command has no keywords or arguments.

1.41.4 Default

None

1.41.5 Usage Guidelines

Use the **exit** command to exit the current configuration mode, return to exec mode, or close an active terminal or console session.

Entering this command in any configuration mode exits the current configuration mode and returns to the next highest level configuration mode. When you enter this command in global configuration mode and return to exec mode, all commands that you have entered since the beginning of the configuration session, or since the last **abort** or **commit** command in any configuration mode, are committed to the database.

1.41.6 Examples

The following example displays an administrator exiting global configuration mode and returning to exec mode:

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

The following example displays how to exit an active Telnet session:

```
[local]Redback>exit
```

1.42 exp-bits

exp-bits ***bits-num***

no exp-bits ***bits-num***

1.42.1 Purpose

Specifies the EXP bits configuration in an L2VPN profile.

1.42.2 Command Mode

L2VPN profile peer configuration

1.42.3 Syntax Description

bits-num	Number of EXP bits to be used for transport over an XC. Range of bits is from 0 to 7.

1.42.4 Default

None.

1.42.5 Usage Guidelines

Use the **exp-bits** command to specify the EXP bits to be used for transport on an XC in an L2VPN profile. Any XCs that have the profile attached inherit this configuration for the EXP bits.

Use the **no** form of this command to remove the EXP bits configuration from an L2VPN profile.

1.42.6 Examples

The following example shows how to configure an L2VPN profile to specify that 5 EXP bits are used for transport over an XC:

```
[local]Redback(config)#exp-bits 5
```

1.43 explicit-null (LDP)

[**neighbor** *ip-addr*] **explicit-null** [**prefix-list** *pl-name*]

no [**neighbor** *ip-addr*] **explicit-null** [**prefix-list** *pl-name*]

1.43.1 Purpose

Enables an egress router to advertise an explicit null label (value 0), in place of an implicit null label (value 3), to the penultimate hop router.

1.43.2 Command Mode

LDP router configuration

1.43.3 Syntax Description

neighbor *ip-addr*	Optional. Neighbor IP address. Enables the advertisement of explicit null labels to the neighbor specified by the *ip-addr* argument. When a neighbor is not specified, explicit null advertisement is enabled for all neighbors in the context.
prefix-list *pl-name*	Optional. Prefix list name. Applies the filters in the specified prefix list to label advertisements and enables advertisement of explicit null labels only for directly connected prefixes that are permitted by the prefix list. When the prefix list is not specified, explicit null label advertisement is enabled for all directly connected prefixes.

1.43.4 Default

The implicit null label (value 3) is advertised.

1.43.5 Usage Guidelines

Use the **explicit-null** command to enable an egress router to advertise an explicit null label (value 0), in place of an implicit null label (value 3), to the penultimate hop router.

By default, Label Distribution Protocol (LDP) advertises an implicit null label for directly connected prefixes. An implicit null label causes the upstream router to perform penultimate hop popping (PHP), and the implicit null label is not transmitted on the egress router. In some cases, such as quality of service (QoS) enforcement, PHP may not be desirable. In those cases, using the **explicit-null** command causes the egress router to advertise an explicit null label in place of an implicit null label for directly connected prefixes, which forces the upstream router to transmit packets with an explicit null label on the last hop.

If a neighbor IP address is specified, then the **explicit-null** command is neighbor-specific, and applies only to the LDP neighbor whose transport address matches the IP address specified in the command. If a neighbor address is not specified, then the **explicit-null** command is non neighbor-specific, and applies to all LDP neighbors in the context.

When both a neighbor-specific **explicit-nul**l command and a non neighbor-specific **explicit-null** command exist, only the neighbor-specific command applies to the neighbor whose transport address matches the IP address given in the neighbor-specific explicit-null command.

Use the **no** form of this command to disable explicit null label advertisement.

1.43.6 Examples

The following example shows how to enable advertising explicit-null label to neighbor **10.1.1.1** for directly connected prefixes that match the prefix-list, **net01:**

```
[local]Redback(config-ctx)#ip prefix-list net01 permit 155.0.0.0/8 ge 8
[local]Redback(config-ctx)#router ldp
[local]Redback(config-ldp)#neighbor 10.1.1.1 explicit-null prefix-list net01
```

1.44 explicit-null (RSVP)

explicit-null

no explicit-null

1.44.1 Purpose

Enables an egress router to advertise an explicit null label (value 0), in place of an implicit null label (value 3), to the penultimate hop router.

1.44.2 Command Mode

RSVP router configuration

1.44.3 Syntax Description

This command has no keywords or arguments.

1.44.4 Default

The implicit null label (value 3) is advertised.

1.44.5 Usage Guidelines

Use the **explicit-null** command to enable an egress router to advertise an explicit null label (value 0), in place of an implicit null label (value 3), to the penultimate hop router.

By default, Resource Reservation Protocol (RSVP) advertises an implicit null label for directly connected prefixes. An implicit null label causes the upstream router to perform penultimate hop popping (PHP), and the implicit null label is not transmitted on the egress router. In some cases, such as quality of service (QoS) enforcement, PHP may not be desirable. In those cases, using the **explicit-null** command causes the egress router to advertise an explicit null label in place of an implicit null label for directly connected prefixes, which forces the upstream router to transmit packets with an explicit null label on the last hop.

Use the **no** form of this command to use the implicit null label.

1.44.6 Examples

The following example shows how to enable the explicit null value:

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

1.45 explicit-route

explicit-route *er-name*

no explicit-route *er-name*

1.45.1 Purpose

Creates an explicit route (ERO) and enters RSVP explicit route configuration mode.

1.45.2 Command Mode

RSVP router configuration

1.45.3 Syntax Description

er-name	Name of the explicit route; an alphanumeric string.

1.45.4 Default

None

1.45.5 Usage Guidelines

Use the **explicit-route** command to create an explicit route and to enter RSVP explicit route configuration mode.

When an label-switched path (LSP) is configured to use an explicit route, it uses the path determined by the specified explicit route. If the path defined by the explicit route is not topologically possible, either because the network is partitioned, or because of insufficient resources, the LSP fails. No alternate paths can be used. If the LSP does not fail, it continues to use the explicit route.

When you reference a source path in RSVP LSP configuration mode with an ERO, the router does not use Constrained Shortest Path First (CSPF). If you specify the **strict** option in the **next-hop** command in RSVP explicit route configuration mode, the router uses the strict way to traverse the path. If you specify the **loose** option in RSVP explicit route configuration mode, the router uses the Gateway Protocol (IGP) to traverse the path.

When you reference an explicit route using the **dynamic-path** command in RSVP LSP configuration mode, the ingress router uses CSPF to traverse the path. The ERO becomes one of the constraints used in CSPF computation. The path traverses the next hops that are in the ERO in a strict or loose way.

Use the **no** form of this command to delete an explicit route.

1.45.6 Examples

The following example shows how to create a Resource Reservation Protocol (RSVP) explicit route, **ex-route02**,using a constraint, **constaint1**, which consists of two next hops:

```
[local]Redback#config
[local]Redback(config)#context local
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#explicit-route ex-route02
[local]Redback(config-rsvp-explicit-route)#next-hop 13.1.1.2
[local]Redback(config-rsvp-explicit-route)#next-hop 14.1.1.2
```

1.46 export-version

export-version v5

1.46.1 Purpose

Specifies the export format used to send flow records to the external collector.

1.46.2 Command Mode

Flow collector configuration

1.46.3 Syntax Description

v5	Configures the external collector to use version 5 formatting when exporting flow records.

1.46.4 Default

None.

1.46.5 Usage Guidelines

Use the **export-version** command to specify the export format used to send flow records to the external collector.

Note: In this release, only v5 formatting is supported.

1.46.6 Examples

The following example shows how to configure an external collector to use v5 formatting for exporting flow records:

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#flow collector c1
[local]Redback(config-flow-collector)#export-version v5
```

1.47 export-version (NAT)

export-version v9

no export-version v9

1.47.1 Purpose

Specifies the export format used to send flow records to the external collector.

1.47.2 Command Mode

NAT Logging configuration

1.47.3 Syntax Description

v9	Configures the external collector to use version 9 formatting when exporting flow records.

1.47.4 Default

None.

1.47.5 Usage Guidelines

Use the **export-version** command to specify the export version 9 format used to send flow records to the external collector.

Use the **no** form of this command to disable the export version 9 format for exporting flow records.

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

1.47.6 Examples

The following example shows how to configure an external collector to use export v9 format for exporting flow records:

```
[local]Redback(config)#context nat-context
[local]rock1200(config-ctx)#nat ?
  logging-profile  Configure NAT logging profile
  policy           Configure NAT policy
[local]Redback(config-ctx)#nat logging-profile logging1
[local]Redback(config-nat-profile)#export-version v9
```

1.48 export route-target

export route-target {**ext-com** | **route-map** *route-map* [*ctx-name*]}

no export route-target {**ext-com** | **route-map** *route-map* [*ctx-name*]}

1.48.1 Purpose

Creates a list of export route targets for a specified Virtual Private Network (VPN) context.

1.48.2 Command Mode

BGP address family configuration

1.48.3 Syntax Description

ext-com	Route target extended community value that is added to the export target list. The route target extended community value can be expressed in either of the following formats: • ***asn*:*nnnn***, where ***asn*** is the autonomous system number, ***nnnn*** is either a 32-bit integer or a 16-bit integer, depending on the size of the ASN. You can specify the ASN as either a two-byte (two-octet) or four-byte (four-octet) integer. A value of 65535 or lower is interpreted as a two-byte integer, unless you add an **L** suffix (for example, **125L**), in which case it is interpreted as a four-byte integer. A value larger than 65535 is always interpreted as a four-byte integer, and the **L** suffix is optional. If the ASN is two-bytes, then ***nnnn*** is a 32-bit integer. If the ASN is four-bytes, then ***nnnn*** is a 16-bit integer. • ***ip-addr*:*nn***, where ***ip-addr*** is the IP address in the form ***A.B.C.D*** and ***nn*** is a 16-bit integer.
route-map *route-map*	Name of the route map used for this VPN context.
ctx-name	Optional. Name of the context in which the route map is defined.

1.48.4 Default

None. A VPN context has no export route targets unless this command is used.

1.48.5 Usage Guidelines

Use the **export route-target** command to create a list of export route targets for a specified VPN context.

Use the ***ext-com*** argument to configure a single route target extended community, or use the **route-map** ***route-map*** construct to configure an export route map for finer control over exported Border Gateway Protocol (BGP) routes. You can configure a single route target extended community, an export route map, or both. You can add multiple export route targets on the same line, or you can issue the command multiple times with individual route targets. Export route targets are sent as extended community attributes to other provider edge (PE) routers.

A route map allows you to filter routes or change attributes such as the export route target based on policy requirements. A route map may only be used when a target community value has not yet been configured. Use the optional ***ctx-name*** argument to reference a route-map in another context. If the optional ***ctx-name*** argument is not specified, then the route maps in the current context are referenced.

Note: The **export route-target** command can only be used in VPN contexts.

Use the **no** form of this command to remove a list of export route targets for a specified VPN context.

1.48.6 Examples

The following example shows how to configure the export route targets, **701:3** and **192.168.1.2:5:**

```
[local]Redback(config)#context vpncontext vpn-rd 701:3
[local]Redback(config-ctx)#router bgp vpn
[local]Redback(config-bgp)#address-family ipv4 unicast
[local]Redback(config-bgp-af)#export route-target 701:3 192.168.1.2:5
```

The following example shows how to configure an export route map, **customer-export-map:**

```
[local]Redback(config)#context vpncontext vpn-rd 701:3
[local]Redback(config-ctx)#route map customer-export-map permit 10
[local]Redback(config-route-map)#match as-path foo
[local]Redback(config-route-map)#set ext-community RT:701:3
[local]Redback(config-route-map)#exit
[local]Redback(config-ctx)#route map customer-export-map permit 20
[local]Redback(config-route-map)#set ext-community RT:701:3
[local]Redback(config-route-map)#exit
[local]Redback(config-ctx)#router bgp vpn
[local]Redback(config-bgp)#address-family ipv4 unicast
[local]Redback(config-bgp-af)#export route-target route-map customer-export-map
```

1.49 ext-community-list

ext-community-list *ecl-name*

no ext-community-list *ecl-name*

1.49.1 Purpose

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

1.49.2 Command Mode

Context configuration

1.49.3 Syntax Description

ecl-name	Name of the extended community list.

1.49.4 Default

There are no pre-configured extended community lists.

1.49.5 Usage Guidelines

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

The extended communities attribute consists of a set of extended communities. Each extended community is coded as an eight octet extended community number. An extended communities attribute is specified by configuring an extended communities list. You can specify multiple extended communities in a single extended community list entry. Like access control lists, extended community lists can have multiple entries that are examined in order of ascending sequence number.

All routes with the extended communities attribute belong to the communities listed in the attribute.

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

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

Use the **no** form of this command to remove an extended community list.

1.49.6 Examples

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

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

1.50 fast-convergence (IS-IS)

fast-convergence [*spf-delay-interval* | *max-spf-count*]

no fast-convergence

default fast-convergence

1.50.1 Purpose

Enables fast convergence for an Intermediate System-to-Intermediate System (IS-IS) instance.

1.50.2 Command Mode

IS-IS router configuration

1.50.3 Syntax Description

spf-delay-interval	Optional. Delay time, in milliseconds, between the receipt of a topology change and the start of the Shortest Path First (SPF) calculation. Valid values are 0 to 999; the default value is 100.
max-spf-count	Optional. Maximum number of additional SPF calculations allowed per level during the SPF hold time. Valid values are 0 to 15; the default value is 3.

1.50.4 Default

Fast convergence is enabled for all instances of IS-IS routers.

1.50.5 Usage Guidelines

Use the **fast-convergence** command to enable fast convergence for an IS-IS instance.

IS-IS fast convergence enables network operators to offer high availability IP services by:

- Responding to important network events, such as topology changes.
- Quickly propagating the information to the entire domain, minimizing the possibility of packet loss in the network.

This fast response affects not only the local router that has the link status change, but also the entire IS-IS routing domain.

IS-IS fast convergence response is adaptive to the frequency of network events. It reacts quickly when there is a sudden network change, but it slows down when there are persistent topology changes, to offer IS-IS routing stability.

Note: We recommend that you not configure the SPF to run continuously. For example, in large networks where a single SPF calculation can take 200 milliseconds or more, do not set the SPF delay value to 50 milliseconds, the *max-spf-count* to 3 calculations, and the SPF holddown (using the **spf holddown** command) to 1 second. This configuration can result in excessive CPU utilization when other applications try to run between SPF calculations.

Using the **fast-convergence** command to configure a maximum SPF count greater than zero enables additional SPF calculations in the SPF holddown interval. Configuring the maximum SPF count to zero prevents additional SPF calculations, which imposes a delay (holddown) interval between a second event and it's SPF calculation. In other words, a maximum SPF count of zero enforces delay between an event that triggers an SPF calculation and the calculation itself.

Note: The SPF delay interval configured with the **fast convergence** command overrides the SPF delay interval set with the **spf interval** command.

Use the **debug isis spf-events** command to turn on error messages related to IS-IS fast convergence.

Use the **no** form of this command to disable fast convergence for an IS-IS instance. This command reverts the system to normal operation, in which the holddown time is in seconds (instead of milliseconds), and there is always a delay between successive SPF calculations.

Use the **default** form of this command to enable fast-convergence with the default settings, or to return the current fast-convergence SPF configuration to the default settings.

1.50.6 Examples

The following example shows how to enable fast convergence on the IS-IS instance, **ip-backbone**, using the default configuration.

```
[local]Redback(config-ctx)#router isis ip-backbone
[local]Redback(config-isis)#fast-convergence
```

The following example shows how to use this command to do the following:

- Enable fast convergence on an IS-IS instance
- Set the delay between the receipt of a topology change and the start of the SPF calculation to 10 milliseconds.
- Allow a maximum of 5 additional SPF calculations to be performed during the SPF hold time.

```
[local]Redback(config-ctx)#router isis ip1

[local]Redback(config-isis)#fast-convergence 10 5
```

1.51 fast-convergence (OSPF)

fast-convergence [*spf-delay-interval max-spf-count*]

{**no** | **default**} **fast-convergence**

1.51.1 Purpose

Enables fast convergence for an Open Shortest Path First (OSPF) instance.

1.51.2 Command Mode

OSPF router configuration

1.51.3 Syntax Description

spf-delay-interval	Optional. Delay time, in milliseconds, between the receipt of a topology change and the start of the Shortest Path First (SPF) calculation. Valid values are 0 to 999; the default value is 100
max-spf-count	Optional. Maximum number of additional SPF calculations allowed during the SPF hold time. Valid values are 0 to 15; the default value is 3.

1.51.4 Default

Fast convergence is disabled for all OSPF instances.

1.51.5 Usage Guidelines

Use the **fast-convergence** command to enable fast convergence for an OSPF instance.

OSPF fast convergence enables networks to offer high-availability IP services to their customers by:

- Responding to important network events, such as a backbone link down.
- Quickly propagating the information to the entire domain.
- Quickly calculating new routing information based on a network topology change, which minimizes the possibility of data packet loss in the network.

This fast response not only affects the local router that has the status change but also the entire OSPF routing domain.

OSPF fast convergence response is adaptive to the frequency of network events. It reacts quickly when a sudden network change occurs, but it slows when persistent topology changes exist to offer OSPF routing stability.

Use the ***spf-delay-interval*** argument to set an SPF delay that is less than one second. When fast convergence is enabled, the ***spf-delay-interval*** argument provides an SPF delay with sub-second (millisecond) granularity, and the value for the ***delay*** argument of the **spf-timers** command in OSPF router configuration mode is ignored, regardless of whether it has been configured. Otherwise, under normal convergence, the ***delay*** argument value (in seconds) is used.

Use the ***max-spf-count*** argument to allow additional SPF calculations within the SPF hold time specified by the **spf-timers** command. Specifying a value greater than zero effectively squeezes additional SPF calculations into the SPF time interval; specifying a value of zero does not allow for squeezing additional SPF calculations into the SPF hold time and returns OSPF to the standard SPF hold time behavior.

Use the **no** or **default** form of this command to disable fast convergence for an OSPF instance.

1.51.6 Examples

The following example shows how to enable fast convergence on the OSPF instance, with an SPF delay interval of **250** milliseconds and up to **5** additional SPF calculations allowed during the SPF hold time:

```
[local]Redback#config

[local]Redback(config)#context local

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

[local]Redback(config-ospf)#fast-convergence 250 5

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

1.52 fast-hello

fast-hello count-per-second *count*

no fast-hello

default fast-hello

1.52.1 Purpose

Enables sending more than one Open Shortest Path First (OSPF) or OSPF Version 3 (OSPFv3) Hello packet per second on the interface.

1.52.2 Command Mode

- OSPF interface configuration
- OSPF3 interface configuration

1.52.3 Syntax Description

count-per-second *count*	Number of OSPF or OSPFv3 Hello packets to be sent on the specified interface each second. The range of values is 2 to 5.

1.52.4 Default

Four OSPF Hello packets are sent each second.

1.52.5 Usage Guidelines

Use the **fast-hello** command to enable the sending of more than one OSPF or OSPFv3 Hello packet per second on the interface.

Note: Using the **fast-hello** command results in faster OSPF convergence.

The following restrictions apply to the **fast-hello** command:

- After the **fast-hello** command is configured, you cannot use the **hello-interval** or **router-dead interval** command until the **fast-hello** command has been disabled.
- After the **hello-interval** or **router-dead interval** command has been configured, you cannot use the **fast-hello** command until the **hello-interval** or **router-dead interval** command has been disabled.

Use the **no** form of this command to disable the sending of more than one OSPF or OSPFv3 Hello packet per second on the interface.

Use the **default** form of this command to send four OSPF or OSPFv3 Hello packets each second.

1.52.6 Examples

The following example shows how to configure Hello packets to be sent **2** times per second, indicating that the interval between Hello packets is 500 ms:

```
[local]Redback(config-ospf-if)#fast-hello 2
```

1.53 fast-lsa-origination

fast-lsa-origination

{**no** | **default**} **fast-lsa-origination**

1.53.1 Purpose

Enables fast link-state advertisement (LSA) origination for an Open Shortest Path First (OSPF) instance.

1.53.2 Command Mode

OSPF router configuration

1.53.3 Syntax Description

This command has no keywords or arguments.

1.53.4 Default

Fast LSA origination is disabled.

1.53.5 Usage Guidelines

Use the **fast-lsa-origination** command to enable fast LSA origination for an OSPF instance.

Normally, OSPF originates an LSA every five seconds. Because there can be multiple changes to router or network LSAs during that five-second interval, the five-second LSA origination limit can slow network convergence. When fast LSA origination is enabled, up to four instances of the same LSA can be originated in the same five-second interval.

Likewise, LSA reception is normally rate limited to one new LSA instance per second. LSA instances received in less than one second after the previous LSA instance are dropped. When fast LSA origination is enabled, LSA reception is not restricted to one new instance per second.

Use the **no** or **default** form of this command to disable fast LSA origination.

1.53.6 Examples

The following example shows how to enable fast LSA origination:

```
[local]Redback(config-ctx)#router ospf 1
[local]Redback(config-ospf)#fast-lsa origination
```

1.54 fast-reroute

fast-reroute nnhop-intf-address ***ip-addr***

no fast-reroute nnhop-intf-address ***ip-addr***

1.54.1 Purpose

Configures a bypass Resource Reservation Protocol (RSVP) label-switched path (LSP) for node protection when the SmartEdge OSinteroperates with other vendor equipment.

1.54.2 Command Mode

RSVP LSP configuration

1.54.3 Syntax Description

nnhop-intf-address ***ip-addr***	Next-next-hop node interface IP address.

1.54.4 Default

None

1.54.5 Usage Guidelines

Use the **fast-reroute** command to configure a bypass RSVP LSP for node protection when the SmartEdge OS interoperates with other vendor equipment.

The **fast-reroute** command is useful when the merge-point does not send its loopback address in its RRO. The **nnhop-intf-address** ***ip-addr*** construct specifies the address that the merge point (MP) includes in the incoming-label RRO that is sent to the protected LSP. Use the **show rsvp lsp** command to obtain the
next-next-hop node interface IP address. The **fast-reroute** command is also useful for node protection in an interarea MPLS fast reroute configuration.

Note: The **fast-reroute** command is available only if the bypass RSVP LSP is configured for node protection.

Use the **no** version of this command to remove node protection configuration from bypass RSVP LSP.

1.54.6 Examples

The following example shows how to configure the RSVP LSP, **to-r1-edge**, to match the next-next-hop interface IP address, **10.2.2.2:**

```
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#lsp to-r1-edge bypass 10.1.1.1 node-protect-lsp-egress 192.168.1.1
[local]Redback(config-rsvp-lsp)#fast-reroute nnhop-intf-address 10.2.2.2
```

1.55 fast-reset (BGP neighbor configuration mode)

fast-reset ***interval***

no fast-reset ***interval***

1.55.1 Purpose

For iBGP or multihop eBGP sessions:

- Accesses Border Gateway Protocol (BGP) neighbor fast-reset configuration mode, where you create a BGP fast-reset interface list of up to ten links to a neighbor; BGP fast reset is triggered when all links in the list go down.
- Configures the interval that must pass before the BGP routing process triggers fast reset after all of the links in the BGP fast-reset interface list go down.

1.55.2 Command Mode

BGP neighbor configuration

1.55.3 Syntax Description

interval	Interval (in milliseconds) that must pass before the BGP routing process triggers fast reset after all of the links in the BGP fast-reset interface list go down. The range of values for the ***interval*** argument is 0 to 60,000 milliseconds (a maximum of 60 seconds).

1.55.4 Default

Fast-reset is disabled, and BGP sessions are dropped after the BGP hold-time value (set with the **timers** command in BGP router configuration mode) is exceeded.

1.55.5 Usage Guidelines

For iBGP or multihop eBGP sessions (where the neighbor is configured with the **ebgp-multihop** command) , use the **fast-reset** command to:

- Access BGP neighbor fast-reset configuration mode, where you create a BGP fast-reset interface list of up to ten links to a neighbor; BGP fast reset is triggered when all links in the list go down.
- Configure the interval that must pass before the BGP routing process triggers fast reset after all of the links in the BGP fast-reset interface list go down.

Use the **interface** command in BGP neighbor configuration mode to add an interface to the list of interfaces that must go down before BGP fast reset takes effect. You can add up to ten interfaces to the list. The BGP session does not come up if you configure the **fast-reset** command in BGP neighbor configuration mode without adding any interfaces to the interface list (using the **interface** command).

Consider the following rules and restrictions when configuring BGP fast reset on a multihop BGP session:

- A BGP session remains active as long as at least one of the interfaces in the BGP fast-reset interface list is up. When all of the interfaces in the list are down, BGP ignores the configured hold time (specified by the **timers** command) and, instead, waits for the specified fast-reset ***interval*** before removing its sessions with the affected neighbor.
- If none of the specified interfaces are up in the configured BGP fast-reset interface list, BGP does not establish a session with a neighbor (regardless of whether the neighbor is reachable).
- If all of the interfaces configured in a fast-reset interface list go down, the BGP session goes down and does not become active again until at least one of the down interfaces comes up.
- When configuring BGP fast reset for a neighbor that is part of a BGP peer group:
  - The BGP fast-reset configuration for a particular neighbor takes precedence over the BGP fast-reset configuration for a peer group. For example, if a BGP neighbor is configured with a fast-reset interval of 50 milliseconds, and that neighbor belongs to a peer group configured with a fast-reset interval of 20 seconds, the BGP neighbor ignores the peer group configuration and uses the BGP fast-reset interval of 50 milliseconds.
  - If a neighbor does not already have BGP fast reset configured, that neighbor inherits the fast-reset configuration from the peer group.
  - If a neighbor has its own BGP fast-reset configuration, to return that neighbor to the default (where the neighbor inherits the BGP fast-reset configuration from the peer group), remove the neighbor from the peer group and then add it back.

Use the **no** form of this command to disable BGP fast reset for an iBGP or multihop eBGP session.

1.55.6 Examples

The following example shows how to perform the following tasks on an eBGP neighbor with IP address 1.1.1.1:

- Access BGP neighbor fast-reset configuration mode

- Add three interfaces (to_red5, to_red10, and to_red15) to the BGP fast-reset interface list
- Configure the BGP routing process to wait 250 milliseconds after all of the links in the BGP fast-reset interface list go down before triggering fast reset

```
[local]Redback(config)#router bgp 1
[local]Redback(config-bgp)#neighbor 1.1.1.1 external
[local]Redback(config-bgp-neighbor)#fast-reset 250
[local]Redback(config-nbr-fast-reset)#interface to_red5
[local]Redback(config-nbr-fast-reset)#interface to_red10
[local]Redback(config-nbr-fast-reset)#interface to_red15
```

1.56 fast-reset (BGP peer group configuration mode)

fast-reset ***interval***

no fast-reset ***interval***

1.56.1 Purpose

For iBGP or multihop eBGP sessions:

- Accesses Border Gateway Protocol (BGP) neighbor fast-reset configuration mode, where you create a BGP fast-reset interface list of up to ten links to a neighbor; BGP fast reset is triggered when all links in the list go down.
- Configures the interval that must pass before the BGP routing process triggers fast reset after all of the links in the BGP fast-reset interface list go down.

1.56.2 Command Mode

BGP peer group configuration

1.56.3 Syntax Description

interval	Interval (in milliseconds) that must pass before the BGP routing process triggers fast reset after all of the links in the BGP fast-reset interface list go down. The range of values for the ***interval*** argument is 0 to 60,000 milliseconds (a maximum of 60 seconds).

1.56.4 Default

Fast-reset is disabled, and BGP sessions are dropped after the BGP hold-time value (set with the **timers** command in BGP router configuration mode) is exceeded.

1.56.5 Usage Guidelines

For iBGP or multihop eBGP sessions (where the neighbor is configured with the **ebgp-multihop** command) , use the **fast-reset** command to:

- Access BGP neighbor fast-reset configuration mode, where you create a BGP fast-reset interface list of up to ten links to a neighbor; BGP fast-reset is triggered when all links in the list go down.
- Configure the interval that must pass before the BGP routing process triggers fast reset after all of the links in the BGP fast-reset interface list go down.

Use the **interface** command in BGP neighbor configuration mode to add an interface to the list of interfaces that must go down before BGP fast reset takes effect. You can add up to ten interfaces to the list. The BGP session does not come up if you configure the **fast-reset** command in BGP neighbor configuration mode without adding any interfaces to the interface list (using the **interface** command).

Consider the following rules and restrictions when configuring BGP fast reset on a multihop BGP session:

- A BGP session remains active as long as at least one of the interfaces in the BGP fast-reset interface list is up. When all of the interfaces in the list are down, BGP ignores the configured hold time (specified by the **timers** command) and, instead, waits for the specified fast-reset ***interval*** before removing its sessions with the affected neighbor.

- If none of the specified interfaces are up in the configured BGP fast-reset interface list, BGP does not establish a session with a neighbor (regardless of whether the neighbor is reachable).

- If all of the interfaces configured in a fast-reset interface list go down, the BGP session goes down and does not become active again until at least one of the down interfaces comes up.

- When configuring BGP fast reset for BGP peer groups, note that:

  – The BGP fast-reset configuration for a particular neighbor takes precedence over the BGP fast-reset configuration for a peer group. For example, if a BGP neighbor is configured with a fast-reset Interval of 50 milliseconds, and that neighbor belongs to a peer group that is configured with a fast-reset interval of 20 seconds, the BGP neighbor ignores the peer group configuration and uses the BGP fast-reset interval of 50 milliseconds.

  – If a neighbor does not already have BGP fast reset configured, that neighbor inherits the fast-reset configuration from the peer group.

  – If a neighbor has its own BGP fast-reset configuration, the only way to return that neighbor to the default (where the neighbor inherits the BGP fast-reset configuration from the peer group) is to remove the neighbor from and the peer group and then add that neighbor back to the peer group.

Use the **no** form of this command to disable BGP fast reset for an iBGP or multihop eBGP session.

1.56.6 Examples

The following example shows how to perform the following tasks on an iBGP peer group called mpg1:

- Access BGP neighbor fast-reset configuration mode
- Add three interfaces (to_blue1, to_blue2, and to_blue3) to the BGP fast-reset interface list
- Configure the BGP routing process to wait 200 milliseconds after all of the links in the BGP fast-reset interface list go down before triggering fast reset

```
[local]Redback(config)#router bgp 1
[local]Redback(config-bgp)#peer-group mpg1 internal
[local]Redback(config-bgp-peer-group)#fast-reset 200
[local]Redback(config-nbr-fast-reset)#interface to_blue1
[local]Redback(config-nbr-fast-reset)#interface to_blue2
[local]Redback(config-nbr-fast-reset)#interface to_blue3
```

1.57 fast-reset (BGP router configuration mode)

fast-reset [**confed**] ***interval***

no fast-reset [**confed**] ***interval***

1.57.1 Purpose

Configures the Border Gateway Protocol (BGP) routing process to wait a specified period of time before dropping sessions with directly connected peers if the links used to reach those peers go down.

1.57.2 Command Mode

BGP router configuration

1.57.3 Syntax Description

interval	Interval, in seconds, the BGP routing process waits before dropping sessions with directly connected peers if the links use to reach those peers go down. The range of values for the ***interval*** argument when specified in seconds is 0 to 60.
confed	Optional. Fast-resets confederation peers as well as directly connected peers.

1.57.4 Default

Fast-reset is disabled, and BGP sessions are dropped after the BGP hold-time value (set with the **timers** command in BGP router configuration mode) is exceeded.

1.57.5 Usage Guidelines

Use the **fast-reset** command to configure the BGP routing process to wait a specified period of time before dropping sessions with directly connected peers if the links use to reach those peers go down. In this case, the fast-reset configuration applies to all eBGP neighbors that are directly connected to the local system.

Normally, a BGP session is dropped only after the hold time specified by the **timers** command expires. BGP fast reset allows faster route convergence by bringing down the session immediately and triggering a BGP best path calculation before the hold time expires. This fast reset minimizes routing convergence times, and therefore packet loss, during network failures.

Use the **no** form of this command to disable BGP fast reset for an instance.

To disable the application of fast reset on BGP confederation peers only, use the **fast-reset** command without the **confed** keyword.

To see the reason for a fast reset, use the **show bgp neighbor** command. To see the fast-reset configuration for a BGP neighbor or peer group, use the **show bgp neighbor** or **show bgp peer-group** command.

1.57.6 Examples

The following example shows how to configure the BGP routing process to wait 50 seconds before dropping sessions with directly connected peers if the links used to reach those peers go down:

```
[local]Redback(config)#router bgp 100

[local]Redback(config-bgp)#fast-reset 50
```

The following example shows how to configure the BGP routing process to wait 40 seconds before dropping sessions with directly connected eBGP peers or directly connected BGP confederation peers if the links used to reach those peers go down:

```
[local]Redback(config)#router bgp 1

[local]Redback(config-bgp)#fast-reset confed 40
```

1.58 filter-id

filter-id

no filter id

1.58.1 Purpose

Specifies the inbound or outbound traffic to be filtered.

1.58.2 Command Mode

Subscriber configuration.

1.58.3 Syntax Description

This command has no keywords or arguments.

1.58.4 Default

None.

1.58.5 Usage Guidelines

Use the **filter-id** command to specify inbound or outbound IPv6 traffic to be filtered. Use the ***in_v6:<name>*** and ***out_v6:<name>*** format.

1.59 flap-statistics

flap-statistics

no flap-statistics

1.59.1 Purpose

Enables route-flap statistics accounting for the address family for both internal Border Gateway Protocol (iBGP) and external BGP (eBGP) routing processes.

1.59.2 Command Mode

BGP address family configuration

1.59.3 Syntax Description

This command has no keywords or arguments.

1.59.4 Default

Route-flap statistics accounting is disabled.

1.59.5 Usage Guidelines

Use the **flap-statistics** command to enable route-flap statistics accounting for both iBGP and eBGP routing processes.

This command is useful for determining routing stability and for diagnosing problems. In particular, this command is useful for troubleshooting persistent iBGP routing loops. Use this command if the network is experiencing a high degree of route flapping.

Use the **no** form of this command to disable route-flap statistics accounting.

1.59.6 Examples

The following example shows how to enable route-flap statistics accounting:

```
[local]Redback(config-ctx)#router bgp 64001
[local]Redback(config-bgp)#address-family ipv4 multicast
[local]Redback(config-bgp-af)#flap-statistics
```

1.60 flash-update-threshold

flash-update-threshold ***seconds***

{**no** | **default**} **flash-update-threshold**

1.60.1 Purpose

Modifies the minimum interval between consecutive Routing Information Protocol (RIP) or RIP next generation (RIPng) flash updates.

1.60.2 Command Mode

- RIPng router configuration
- RIP router configuration

1.60.3 Syntax Description

seconds	Minimum number of seconds between consecutive RIP or RIPng flash updates. The range of values is 1 to 30; the default value is 5.

1.60.4 Default

The flash update threshold is five seconds.

1.60.5 Usage Guidelines

Use the **flash-update-threshold** command to modify the minimum interval between consecutive RIP or RIPng flash updates. Each flash update contains only those routes that have been changed since the most recent update.

Use the **no** or **default** form of this command to return the threshold limit to five seconds.

1.60.6 Examples

The following example shows how to set a RIP flash update threshold of **10** seconds:

```
[local]Redback(config-ctx)#router rip rip001
[local]Redback(config-rip)#flash-update-threshold 10
```

1.61 flood-reduction

flood-reduction

no flood-reduction

1.61.1 Purpose

Suppresses periodic link-state advertisement (LSA) refresh in stable topologies.

1.61.2 Command Mode

- OSPF interface configuration
- OSPF3 interface configuration

1.61.3 Syntax Description

This command has no keywords or arguments.

1.61.4 Default

Flood reduction is disabled on the interface.

1.61.5 Usage Guidelines

Use the **flood-reduction** command to suppress periodic LSA refresh in stable topologies.

Note: If demand circuit operation is implicitly or explicitly enabled, LSAs are flooded as DoNotAge LSAs on the Open Shortest Path First (OSPF) or OSPF Version 3 (OSPFv3) interface, and will not be re-flooded until the network topology changes.

Use the **no** form of this command to disable flood reduction.

1.61.6 Examples

The following example shows how to suppress periodic LSA refresh for the OSPF interface, **ETH3/4**, in area **0:**

```
[local]Redback(config-ospf)#area 0
[local]Redback(config-ospf-area)#interface ETH3/4
[local]Redback(config-ospf-if)#flood-reduction
```

1.62 flow admission-control profile

flow admission-control profile ***profile***

no flow admission-control

1.62.1 Purpose

Creates a flow admission control (FAC) profile and enters flow configuration mode.

1.62.2 Command Mode

Global configuration

1.62.3 Syntax Description

profile	Name of the profile.

1.62.4 Default

No flow admission control profiles are configured.

1.62.5 Usage Guidelines

Use the **flow admission-control profile** command to create a FAC profile and enter flow configuration mode. You use this profile to apply flow attributes to a circuit.

Use the **no** form of this command to remove a FAC profile.

1.62.6 Examples

The following example shows how to create a FAC profile called profile1:

```
[local]Redback(config)#flow admission-control profile profile1
```

1.63 flow apply admission-control profile

flow apply admission-control profile *name* {**in** | **out** | **bidirectional**}

no flow apply admission-control

1.63.1 Purpose

Applies a flow admission control (FAC) profile to a circuit for a specified traffic direction.

1.63.2 Command Mode

Circuit configuration

1.63.3 Syntax Description

name	Name of the FAC profile.
in	Specifies that the FAC profile applies to ingress traffic on the circuit.
out	Specifies that the FAC profile applies to egress traffic on the circuit.
bidirectional	Specifies that the FAC profile applies to both ingress and egress traffic on the circuit.

1.63.4 Default

None

1.63.5 Usage Guidelines

Use the **flow apply admission-control profile** command to apply a FAC profile to a circuit for a specified traffic direction.

Use the **no** form of this command to remove a FAC profile from a circuit.

1.63.6 Examples

The following example shows how to apply FAC profile profile1 to bidirectional traffic on circuit **dot1q pvc 1:**

```
[local]Redback(config)#port ethernet 1/1
[local]Redback(config-port)#dot1q pvc 1
[local]Redback(config-dot1q-pvc)#flow apply admission-control profile profile1 bidirectional
```

1.64 flow apply ip profile

flow apply ip profile *profile-name* {**in** | **out** | **both**}

no flow apply ip profile *profile-name*

1.64.1 Purpose

Attaches a specified RFlow profile to a circuit.

1.64.2 Command Mode

- Port configuration
- dot1q PVC configuration

1.64.3 Syntax Description

profile-name	The profile that you want to apply to the circuit.
in	Applies the profile to the circuit in the ingress direction only.
out	Applies the profile to the circuit in the egress direction only.
both	Applies the profile to the circuit in both the ingress and egress directions.

1.64.4 Default

None.

1.64.5 Usage Guidelines

Use the **flow apply ip profile** command to attach a specified RFlow profile to a circuit.

Note: The physical circuit must be bound to an IP interface for flow accounting to work.

Use the **no** form of this command to remove an RFlow profile from a circuit.

Note: If no RFlow profiles are attached to the circuit, then RFlow is disabled on the circuit.

1.64.6 Examples

The following example shows how to attach an RFlow profile called **p1** to the dot1q circuit on port 4/1:

```
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#bind interface if1_1 local
[local]Redback(config-port)#flow apply ip profile p1 in
```

1.65 flow collector

flow collector *collector-name*

1.65.1 Purpose

Enters flow collector configuration mode, where you configure access to an external collector.

1.65.2 Command Mode

Context configuration

1.65.3 Syntax Description

collector-name	Name that identifies this external collector.

1.65.4 Default

None.

1.65.5 Usage Guidelines

Use the **flow collector** command to enter flow collector configuration mode, where you configure access to an external collector.

1.65.6 Examples

The following example shows how to enter flow collector configuration mode for an external collector called **c1:**

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#flow collector c1
[local]Redback(config-flow-collector)#
```

1.66 flow-control

For a GE port, the syntax is:

flow-control [*flow-control*]

{**no** | **default**} **flow-control**

For a 10GE port, the syntax is:

flow-control

{**no** | **default**} **flow-control**

1.66.1 Purpose

For a Gigabit Ethernet (GE) port, sets the flow control mode on a port to be applied when auto-negotiation is disabled or fails with force mode enabled. For a 10GE port, sets the flow control mode on a port to be applied unconditionally for both transmitted and received traffic because these ports do not support auto-negotiation.

1.66.2 Command Mode

Port configuration

1.66.3 Syntax Description

flow-control	Optional. Specifies the direction flow control is to be applied, according to one of the following keywords: • **tx**—Applies flow control only to transmitted traffic. For example, the port honors flow-control indications received from the far end and temporarily suspends transmission. • **rx**—Applies flow control only to received traffic. For example, the port asserts flow-control indications to the far end when traffic is being received faster than it can be processed. This is the default. • **tx&rx**—Applies flow control to both transmitted and received traffic. This argument is only available for GE ports.

1.66.4 Default

Flow control is applied to received traffic on a GE port. For 10GE ports, flow-control is enabled by default for both transmitted and received traffic. However, for the oversubscribe-capable 4-port 10GE card, receive flow control

(in this case, transmission of Ethernet PAUSE frames) is always disabled whenever more than two of the four ports of the card are placed in service by using the **no shutdown** command.

1.66.5 Usage Guidelines

For a GE port, use the **flow-control** command to set the flow control mode on a GE port to be applied when auto-negotiation is disabled or fails with force mode enabled. The flow control mode set using this command is applied when:

- Auto-negotiation is disabled on the port.
- Auto-negotiation is enabled and force mode is also enabled and the negotiation fails.

Otherwise, the value set using this command is ignored and flow control is negotiated using the parameters specified in the auto-negotiate command in port configuration mode.

For a 10GE port, use the **flow-control** command to set the flow control mode on a port to be applied unconditionally for both transmitted and received traffic because these ports do not support auto-negotiation.

Use the **default** form of this command to set flow control to its default value.

Note: This command does not apply to ports on Fast Ethernet (FE) traffic cards.

Use the **no** form of this command to disable all flow control on the port.

1.66.6 Examples

The following example shows how to disable receive and transmit flow control on a 10GE port:

```
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#no flow-control
```

The following example shows how to apply flow control to traffic both transmitted from and received on GE port **1** in slot **4:**

```
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#flow-control tx&rx
```

1.67 flow enable

flow enable circuit ***circuit-handle direction***

no flow enable

1.67.1 Purpose

Enables flows on a circuit.

1.67.2 Command Mode

exec

1.67.3 Syntax Description

circuit-handle	Handle of the circuit to which flows apply. A circuit handle occurs in the following syntax: ***slot***/***port***:***channel***:***sub-channel***/***circuit-id***.
slot	Chassis slot number of a traffic card to which the circuit is mapped.
port	Required if you enter the ***slot*** argument. Port number for the circuit.
channel	Channel number of the circuit.
sub-channel	Sub-channel number of the circuit.
circuit-id	Circuit ID number to which flows apply.
direction	Direction of the flow on the circuit. The range of value can be **in**, **out**, or **bidirectional**.

1.67.4 Default

Flows are disabled.

1.67.5 Usage Guidelines

Use the **flow enable** command to enable flows on a circuit.

Use the **no** form of this command to disable flows on a circuit.

1.67.6 Examples

The following example shows how to enable flows on circuit **3/1:1023:63/1/2/81922:**

```
[local]Redback#flow enable circuit 3/1:1023:63/1/2/81922 in
```

1.68 flow ip application-list

flow ip application-list ***list-name***

no application-list ***list-name***

1.68.1 Purpose

Creates a flow IP application list and accesses flow IP application-list configuration mode.

1.68.2 Command Mode

Flow IP configuration

1.68.3 Syntax Description

list-name	Application list name.

1.68.4 Default

None.

1.68.5 Usage Guidelines

Use the **flow ip application-list** command to create a flow IP application list and access flow IP application-list configuration mode.

In flow IP application-list configuration mode, you can classify the IP traffic that is being sent over the system (for example Telnet, FTP, HTTP, SMTP, and BGP). Applications, based on IP protocol number and port number may be defined within an application list, providing flexibility in the definition of the applications you want to monitor.

Use the **no** version of this command to remove a flow IP application list configuration.

1.68.6 Examples

Use the **flow ip application-list** command to access flow IP application-list configuration mode for an application list called **applist10**:

```
[local]Redback(config)# flow ip application-list applist10
[local]Redback(config-flow-ip-app-list)#
```

1.69 flow ip profile

flow ip profile ***profile-name***

no flow ip profile ***profile-name***

1.69.1 Purpose

Creates an RFlow IP profile and enters flow IP profile configuration mode.

1.69.2 Command Mode

Global configuration

1.69.3 Syntax Description

profile-name	Identifies the IP profile.

1.69.4 Default

None.

1.69.5 Usage Guidelines

Use the **flow ip profile** command to create an RFlow IP profile and enter flow IP profile configuration mode.

Use the **no** form of this command to delete an RFlow profile.

1.69.6 Examples

The following example shows how to create an RFlow IP profile called **p1** and enter flow IP profile configuration mode for that profile:

```
[local]Redback#configure
[local]Redback(config)#flow ip profile p1
[local]Redback(config-flow-ip-profile)#
```

1.70 flow ip sampling

flow ip sampling

1.70.1 Purpose

Accesses flow IP sampling configuration mode.

1.70.2 Command Mode

Global configuration

1.70.3 Syntax Description

This command has no keywords or arguments.

1.70.4 Default

None.

1.70.5 Usage Guidelines

Use the **flow ip sampling** command to access flow IP sampling configuration mode.

In flow IP sampling configuration mode, you can use the command so globally specify the packet sampling interval to be used when sampling is enabled.

Note: To enable packet sampling for a flow, you must first use the **sampling** command in flow IP profile configuration mode to enable packet sampling in an Rflow IP profile. All flows using that profile have packet sampling enabled.

Use the **no** version of this command to remove a flow ip sampling configuration.

1.70.6 Examples

The following example shows how to access flow IP sampling configuration mode:

```
[local]Redback(config)# flow ip sampling
[local]Redback(config-flow-ip-sampling)#
```

1.71 flow monitor circuit

flow monitor circuit {**count** | **list** | **log**}

no flow monitor circuit

1.71.1 Purpose

Initiates monitoring of flows on a circuit.

1.71.2 Command Mode

Flow configuration

1.71.3 Syntax Description

count	Indicates that flows are to be counted on the current circuit.
list	Indicates that flows are to be tracked on the current circuit.
log	Indicates that flow events are to be logged on the current circuit.

1.71.4 Default

Flows are not monitored.

1.71.5 Usage Guidelines

Use the **flow monitor circuit** command to initiate monitoring of flows on a circuit.

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

1.71.6 Examples

The following example shows how to initiate the counting of flows on a circuit:

```
[local]Redback(config-ac-profile)#flow monitor circuit count
```

1.72 foreach

foreach ***param-name-list***

no foreach

1.72.1 Purpose

Specifies a field in a RADIUS standard attribute, Redback vendor-specific attribute (VSA) provided by Ericsson AB, or service attribute that can have multiple values and accesses parameter array loop configuration mode.

1.72.2 Command Mode

Service profile configuration

1.72.3 Syntax Description

param-name-list	Name of the field that can have multiple values.

1.72.4 Default

No fields are specified in any attribute in the service profile.

1.72.5 Usage Guidelines

Use the **foreach** command to specify a field in a RADIUS standard attribute, Redback VSA provided by Ericsson AB, or service attribute that can have multiple values and access parameter array loop configuration mode.

The ***param-name-list*** argument is the one you specified for the field in the **parameter** command in service profile configuration mode. When the ***param-name-list*** argument is inserted in the string for the **attribute** command in parameter array loop configuration mode, include a dollar sign (**$**) immediately before the field name.

Use the **no** form of this command to remove the **foreach** command and the **attribute** command that follows it from the service profile.

1.72.6 Examples

The following example shows how to define the **tcp-port** field in Redback VSA 164 provided by Ericsson AB (**Dynamic-Policy-Filter**) to have multiple values:

```
[local]Redback(config-ctx)#radius service profile redirect

[local]Redback(config-svc-profile)#parameter list tcp-port

[local]Redback(config-svc-profile)#foreach tcp-port

[local]Redback(config-param-array-loop)#attribute Dynamic-Policy-Filter
 "ip in forward tcp dstport = $tcp-port class redirect fwd"
```

1.73 foreign-agent

foreign-agent

no foreign-agent

1.73.1 Purpose

Creates or selects a foreign-agent (FA) instance in this context and accesses FA configuration mode.

1.73.2 Command Mode

Mobile IP configuration

1.73.3 Syntax Description

This command has no keywords or arguments.

1.73.4 Default

No FAs are created.

1.73.5 Usage Guidelines

Use the **foreign-agent** command to create or select an FA instance in this context and access FA configuration mode. You can only create one FA instance in a context. You can also apply a dynamic tunnel profile.

Use the **no** form of this command to delete the FA instance in this context.

1.73.6 Examples

The following example shows how to create an FA instance in the **fa** context:

```
[local]Redback(config)#context fa
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#foreign-agent
[local]Redback(config-mip-fa)#
```

1.74 foreign-agent-peer

foreign-agent-peer ***ip-addr***

no foreign-agent-peer ***ip-addr***

1.74.1 Purpose

Creates or selects a foreign-agent (FA) peer for this home-agent (HA) instance and accesses FA peer configuration mode.

1.74.2 Command Mode

HA configuration

1.74.3 Syntax Description

ip-addr	IP address for this FA peer.

1.74.4 Default

No FA peers are created.

1.74.5 Usage Guidelines

Use the **foreign-agent-peer** command to create or select an FA peer for this HA instance and access FA peer configuration mode. If a Mobile IP registration is received from an FA peer that isn't configured, one is created dynamically. FA and HA authentication and dynamic tunnel configuration are inherited from the HA instance.

Use the **no** form of this command to delete the FA peer with the specified IP address.

1.74.6 Examples

The following example shows how to create an FA peer with IP address `172.16.2.1` for the HA instance in the `ha` context:

```
[local]Redback(config)#context ha
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#home-agent
[local]Redback(config-ha)#foreign-agent-peer 172.16.2.1
[local]Redback(config-fapeer)#
```

1.75 format media-device

`format media-device`

1.75.1 Purpose

Reformats the mass-storage device installed in the external slot of the controller card to which you are connected, or the compact-flash (CF) card installed in the external slot of the SmartEdge 100 chassis.

1.75.2 Command Mode

exec (10)

1.75.3 Syntax Description

This command has no keywords or arguments.

1.75.4 Default

The mass-storage device or CF card is shipped pre-formatted with three partitions, one of which is essential for obtaining kernel core dumps more quickly.

1.75.5 Usage Guidelines

Use the **`format media-device`** command to reformat mass-storage device installed in the external slot of the controller card to which you are connected, or the CF card installed in the external slot of the SmartEdge 100 chassis.

Because the device is formatted when shipped, you do not need to enter this command unless the device becomes unusable. The reformat operation duplicates the original formatting.

Caution!

Risk of data loss. If the mass-storage device or CF card (the /md partition) has any useful information (configuration or Packet Processing ASIC [PPA] crash dumps, and so on), that information is destroyed during the format operation. To reduce the risk, archive useful information before you enter this command.

Note: To reformat the mass-storage device installed in the standby controller card, you must be connected to the Craft 2 port on the standby controller card.

1.75.6 Examples

The following example shows how to format the mass-storage device installed in the external slot of the active controller card:

```
[local]Redback#format media-device
```

The following example shows how to format the mass-storage device installed in the external slot of the standby controller card; the administrator is connected to the Craft 2 port on the standby controller card:

```
[local]standby#format media-device
```

The following example shows how to reformat the CF card in a SmartEdge 100 chassis:

```
[local]Redback#format media-device
```

1.76 format sse

format sse ***slot disk_num***

1.76.1 Command Mode

exec

1.76.2 Syntax Description

slot	Chassis slot number of the SSE card.
disk_num	Disk number on the SSE card. Values: 1 or 2.

1.76.3 Default

None.

1.76.4 Usage Guidelines

Formats the specified disk on the SSE card, removing all user-configured partitions and data.

The SSE card cannot be bound to an SSE group when you issue this command.

1.76.5 Examples

```
[local]Redback#format sse 2 2
```

1.77 forward-all

forward-all

no forward-all

1.77.1 Purpose

Forwards packets to all other external Dynamic Host Configuration Protocol (DHCP) servers in a DHCP server group.

1.77.2 Command Mode

DHCP relay server configuration

1.77.3 Syntax Description

This command has no keywords or arguments.

1.77.4 Default

Packets are not forwarded to the other DHCP servers in the DHCP server group.

1.77.5 Usage Guidelines

When a DHCP server is unreachable, DHCP request packets can be forwarded to all other DHCP servers in its DHCP server group. Use the **forward-all** command to forward packets to all other DHCP servers in a server group.

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

Use the **no** form of this command to disable the forward all option.

1.77.6 Examples

The following example shows how to forward packets to all other DHCP servers in DHCP server group, **int-grp**, when the DHCP server, **10.30.40.50**, is unreachable:

```
[local]Redback(config-ctx)#dhcp relay server 10.30.40.50
[local]Redback(config-dhcp-relay)#server-group int-grp
[local]Redback(config-dhcp-relay)#forward-all
```

1.78 forward-delay

forward-delay ***sec***

{default | no} forward-delay

1.78.1 Purpose

Sets forward delay time.

1.78.2 Command Mode

spanning-tree configuration

1.78.3 Syntax Description

sec Forward delay time in seconds (4 to 30). The forward delay time minus one second must be in whole seconds and greater than or equal to half the maximum age of the received Bridge Protocol Data Units (BPDUs) set in the **max-age** command; that is, it must conform to the following formula:

2 * (forward-delay - 1.0) >= max-age >= 2 * (hello-interval + 1.0)

1.78.4 Default

The default forward delay is 15 seconds.

1.78.5 Usage Guidelines

Use the **forward-delay** command to set the forward delay time; that is, the time spent in the listening state. This command applies when the current bridge is the root bridge.

1.78.6 Examples

The following example shows how to set the forward-delay, max-age, and hello-interval:

```
[local]Redback(config)#context bridge
[local]Redback(config-ctx)#bridge isp1
[local]Redback(config-bridge)#spanning-tree
[local]Redback(config-bridge-stp)#forward-delay 20
[local]Redback(config-bridge-stp)#max-age 38
[local]Redback(config-bridge-stp)#hello-interval 2
```

1.79 forward output (circuit)

forward output *dest-name*

no forward output *dest-name*

1.79.1 Purpose

Specifies a circuit as the output destination for mirrored or redirected traffic.

1.79.2 Command Mode

- ATM PVC configuration
- Frame Relay PVC configuration
- Port configuration
- dot1Q PVC configuration

1.79.3 Syntax Description

dest-name	Output destination name for mirrored or redirected traffic.

1.79.4 Default

No output destination for mirrored or redirected traffic is specified.

1.79.5 Usage Guidelines

Use the **forward output** command to specify a circuit as an output destination for mirrored or redirected traffic.

Note: You can specify an Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC), an Ethernet port, Frame Relay PVC, Packet over SONET/SDH (POS) port, or a Generic Routing Encapsulation (GRE) tunnel as the output destination for mirrored or redirected traffic.

Note: You can specify an Ethernet port or a Generic Routing Encapsulation (GRE) tunnel as the output destination for mirrored or redirected traffic.

You cannot use the circuit referencing the forward policy as the forward output port. The selected circuit must be different from the circuit used for the traffic being mirrored or redirected.

Use the **mirror destination** or **redirect destination circuit** commands in forward policy or policy group class configuration mode to mirror or redirect traffic to this circuit.

Use the **no** form of this command to remove the circuit as the output destination for mirrored or redirected traffic.

GRE tunnels only support IP datagram mirrored data. If a forward policy specifies a GRE tunnel as the mirror destination, the ip-datagrams option must be used with the mirror destination command.

1.79.6 Examples

The following example shows how to specify two forward outputs, **snoop1** and **snoop2** on Ethernet ports:

```
[local]Redback(config)#port ethernet 5/12
[local]Redback(config-port)#forward output snoop1
[local]Redback(config-port)#exit
[local]Redback(config)#port ethernet 7/1
[local]Redback(config-port)#forward output snoop2
```

1.80 forward output (tunnel)

forward output ***tunl-out-name***

no forward output ***tunl-out-name***

1.80.1 Purpose

Specifies the name of a tunnel to which the output of the current tunnel is forwarded.

1.80.2 Command Mode

Tunnel configuration

1.80.3 Syntax Description

tunl-out-name	Name of a tunnel to which the output of the current tunnel is forwarded.

1.80.4 Default

Output is not forwarded.

1.80.5 Usage Guidelines

Use the **forward output** command to specify the name of the tunnel to which the output of the current tunnel is forwarded.

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

1.80.6 Examples

The following example shows how to forward output from the **DenverTnl** tunnel to the **ColoradoSpringsTnl** tunnel:

```
[local]Redback(config)#tunnel gre DenverTnl
[local]Redback(config-tunnel)#forward output ColoradoSpringsTnl
```

1.81 forward policy

forward policy *name* [**radius-guided**]

no forward policy *name*

1.81.1 Command Mode

Global configuration

1.81.2 Syntax Description

name	Forward policy name.
radius-guided	Optional. Specifies a Remote Authentication Dial-In User Service (RADIUS) guided policy and allows the policy to be modified by dynamic access control lists (ACLs).

1.81.3 Default

No forward policy is configured.

1.81.4 Usage Guidelines

Use the **forward policy** command to create or select a forward policy and access forward policy configuration mode. A forward policy can contain a combination of mirror, redirect, and drop functions.

Use the **radius-guided** keyword to specify a RADIUS-guided policy and to allow the policy to be modified by dynamic ACLs. You cannot remove a dynamic policy ACL from the policy after you have configured it, nor can you change the policy type from static to RADIUS-guided. To remove the dynamic policy ACL or change its type, delete the policy and then recreate it as a static policy.

Use the **no** form of this command to remove the forward policy from the configuration.

1.81.5 Examples

The following example shows how to create the forward policy, **MirrorPolicy**, and access forward policy configuration mode:

```
[local]Redback(config)#forward policy MirrorPolicy
[local]Redback(config-policy-frwd)#
```

1.82 forward policy in

forward policy *name* **in** [**[ip] [ipv6] acl-counters**]

no forward policy *name* **in**

1.82.1 Command Mode

- ATM OC configuration
- ATM PVC configuration
- dot1q PVC configuration
- Frame Relay PVC configuration
- Port configuration
- Subscriber configuration

1.82.2 Syntax Description

name	Forward policy name.
ip acl-counters	Optional. Enables per-rule IPv4 access control list (ACL counters for the number of packets mirrored, redirected, or dropped by a policy access-group associated with the policy.
ipv6 acl-counters	Optional. Enables per-rule access control list (ACL) counters for the number of packets mirrored, redirected, or dropped by a policy access-group associated with the policy. For dual stack counters use the **ip ipv6 acl-counters** construct.

1.82.3 Default

No policy is attached.

1.82.4 Usage Guidelines

Use the **forward policy in** command to attach a forward policy to incoming traffic on a circuit, port, or subscriber record.

Forward policies are not supported for dynamic 802.1Q permanent virtual circuit (PVC) ranges.

Use the **no** form of this command to remove a forward policy from a circuit, port, or subscriber record.

1.82.5 Examples

The following example shows how to attach the forward policy, **MP1**, to incoming traffic on an Ethernet port and enable IPv4 and IPv6 ACL counters:

```
[local]Redback(config)#port ethernet 2/1
[local]Redback(config-port)#forward policy MP1 in ip ipv6 acl-counters
```

1.83 forward policy out

forward policy *name* **out** [**[ip] [ipv6] acl-counters**]

no forward policy *name* **out**

1.83.1 Purpose

Attaches a forward policy that mirrors traffic to outgoing traffic on a circuit, port, or subscriber record.

1.83.2 Command Mode

- ATM OC configuration
- ATM PVC configuration
- dot1q PVC configuration
- Frame Relay PVC configuration
- Port configuration
- Subscriber configuration

1.83.3 Syntax Description

name	Forward policy name.
ip acl-counters	Optional. Enables per-rule access control list (ACL counters for a policy access-group associated with the policy. Specify ip acl-counters for an IPv4 ACL.
ipv6 acl-counters	Optional. Enables per-rule access control list (ACL) counters for a policy access-group associated with the policy. Specify "ipv6 acl-counters" to enable counters for an IPv6 ACL, or "ip ipv6 acl-counters" to enable counters for both IPv4 and IPv6, if applicable.

1.83.4 Default

No policy is attached.

1.83.5 Usage Guidelines

Use the **forward policy out** command to attach a forward policy that mirrors traffic to outgoing traffic on a circuit, port, or subscriber record.

Note: You can apply a forward policy with redirect or drop functions only to incoming traffic, which requires that you use the **forward policy in** command.

Forward policies are not supported for dynamic 802.1Q permanent virtual circuit (PVC) ranges.

Use the **no** form of this command to remove a forward policy from a circuit, port, or subscriber record.

1.83.6 Examples

The following example shows how to attach the forward policy, **MirrorPolicy**, to outgoing traffic on an Asynchronous Transfer Mode (ATM) port:

```
[local]Redback(config)#port atm 13/1
[local]Redback(config-atm-oc)#forward policy MirrorPolicy out
```

1.84 forwarding scheme

forwarding scheme {**source-mac**}

{**no** | **default**} **forwarding scheme**

1.84.1 Purpose

Specifies how the IP route used for packet forwarding for a mobile node (MN) is determined.

1.84.2 Command Mode

FA configuration

1.84.3 Syntax Description

source-mac	Use the source medium access control (MAC) address to look up the IP route.

1.84.4 Default

The forwarding scheme uses the source MAC address.

1.84.5 Usage Guidelines

Use the **forwarding scheme** command to specify the means by which IP route used for packet forwarding for a MN is determined.

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

1.84.6 Examples

The following example shows how to specify forwarding based on the source MAC address:

```
[local]Redback(config)#context fa
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#foreign-agent
[local]Redback(config-mip-fa)#forwarding scheme source-
mac validate-source-ip
```

1.85 forwarding traffic

forwarding traffic routed-ip

no forwarding traffic routed-ip

1.85.1 Purpose

Enables the forwarding of non-Mobile IP traffic for this foreign-agent (FA) instance.

1.85.2 Command Mode

FA configuration

1.85.3 Syntax Description

routed-ip	Forward routed IP (non-Mobile IP) traffic.

1.85.4 Default

Routing of non-Mobile IP traffic is enabled.

1.85.5 Usage Guidelines

Use the **forwarding traffic** command to enable the forwarding of non-Mobile IP traffic for this foreign-agent (FA) instance. Non-Mobile IP traffic is routed IP traffic received on an interface that is enabled for Mobile IP services.

Use the **no** form of this command to disable the forwarding of non-Mobile IP traffic.

1.85.6 Examples

The following example shows how to disable the forwarding of non-Mobile IP traffic:

```
[local]Redback(config)#context fa
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#foreign-agent
[local]Redback(config-mip-fa)#no forwarding traffic routed-ip
```

1.86 framed-route allow-ecmp

framed-route allow-ecmp

no framed-route allow-ecmp

1.86.1 Purpose

Configures multiple framed routes for IPv4 traffic using the Framed-Route RADIUS attribute to allow for equal-cost multipath (ECMP) routing over no more than eight subscriber links.

1.86.2 Command Mode

Subscriber configuration

1.86.3 Syntax Description

This command has no keywords or arguments.

1.86.4 Default

By default, redundant routes exist across the multiple subscriber links.

1.86.5 Usage Guidelines

Use the **framed-route allow-ecmp** command to configure multiple framed routes for IPv4 traffic using the Framed-Route RADIUS attribute to allow for ECMP routing over no more than eight subscriber links. Configure this command for the default subscriber within a context. The configuration applies to all other subscribers that are configured within the context.

Use the **no** form of this command to remove the configured Framed-Route attributes.

For more information about the Framed-Route attribute (standard attribute 22), see *RADIUS Attributes*.

1.86.6 Examples

The following example shows how to configure the **framed-route allow-ecmp** command for a default subscriber profile within the `xyz` context:

```
[local]Redback(config)#config
[local]Redback(config)#context xyz
[local]Redback(config-ctx)#subscriber default
[local]Redback(config-sub)#framed-route allow-ecmp
```

1.87 frame-loss

frame-loss *count*

{**no** | **default**} **frame-loss**

1.87.1 Purpose

Configures the continuity check message (CCM) frame-loss criteria in the current maintenance association (MA).

1.87.2 Command Mode

CCM configuration

1.87.3 Syntax Description

frame-loss *count*	Sets the number of consecutive CCM PDUs failures that are considered a connectivity fault. By default, the failure of a MEP to receive three consecutive CCM PDUs from any one of the other MEPs in the MA is considered as a connectivity fault. A connectivity fault causes an SNMP trap to be transmitted to the SNMP network manager.

1.87.4 Default

Connectivity fault declared after the failure to receive three (3) consecutive CCM PDUs from any one of the other MEPs in the MA.

1.87.5 Usage Guidelines

Use the **frame-loss** command to configure the CCM frame-loss criteria in the current MA.

Enter an integer value for the *count* argument from **3** to **100**.

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

1.87.6 Examples

In the following example, the **frame-loss** command changes the default frame-loss count setting of the MEPs in the **bayarea** MA from the default of **3** to **10:**

```
[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)#maintenance-association bayarea
[local]Redback(config-ether-cfm-ma)#ccm
[local]Redback(config-ether-cfm-ma-ccm)#frame-loss 10
```

1.88 frame-relay auto-detect

frame-relay auto-detect

{**no** | **default**} **frame-relay auto-detect**

1.88.1 Purpose

Enables the automatic detection of the type of Local Management Interface (LMI) for a Frame Relay-encapsulated channel or port, or Multilink Frame Relay (MFR) bundle.

1.88.2 Command Mode

- Link-group configuration
- Port configuration

1.88.3 Syntax Description

This command has no keywords or arguments.

1.88.4 Default

Auto-detection is enabled.

1.88.5 Usage Guidelines

Use the **frame-relay auto-detect** command to enable the automatic detection of the type of LMI for a Frame Relay-encapsulated channel or port, or MFR bundle. The auto-detect feature tells the system to look at the first LMI message received from the remote end, determine from the message the LMI type of the remote end, and reconfigure the LMI type at the local end to match.

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

The original “group of 4” LMI uses DLCI number 1023 as the PVC number; both the ANSI and ITU LMI use DLCI number 0. If the LMI type is not set to group-of-4 (using the **frame-relay lmi-type** command in link group, or port configuration mode) and the local Frame Relay interface type is data communications equipment (DCE), this command allows the software to detect which LMI type is being used by the remote end, and use that same LMI type at the local end.

Because the default interface type is data terminal equipment (DTE), the auto-detect function does not normally operate. However, if you configure the

interface type to be DCE, then the auto-detect function takes effect (unless previously disabled using the **no** form of this command).

Use the **no** form of this command to disable the automatic detection of the LMI type.

Use the **default** form of this command to enable the automatic detection of the LMI type.

1.88.6 Examples

The following example shows how to enable automatic detection of the LMI type for a Packet over SONET/SDH (POS) port in slot **9:**

```
[local]Redback(config)#port pos 9/1

[local]Redback(config-port)#frame-relay auto-detect
```

1.89 frame-relay intf-type

frame-relay intf-type {**dce** | **dte**}

1.89.1 Purpose

Configures the Frame Relay interface as data communications equipment (DCE) or data terminal equipment (DTE) for a Frame Relay-encapsulated channel or port or Multilink Frame Relay (MFR) bundle.

1.89.2 Command Mode

- Link-group configuration
- Port configuration

1.89.3 Syntax Description

dce	Specifies that the port functions as a Frame Relay switch connected to a router.
dte	Specifies that the port is connected to a Frame Relay network.

1.89.4 Default

Frame Relay interfaces are set to DTE.

1.89.5 Usage Guidelines

Use the **frame-relay intf-type** command to configure the interface type for a Frame Relay-encapsulated channel or port or MFR bundle.

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

If you configure the interface type as DCE and the Local Management Interface (LMI) is not disabled, LMI Status Enquiries are expected to be received by the port, and Status messages are sent as a response.

If you configure the interface type as DTE and LMI is not disabled, LMI Status Enquiries are sent by the port, and Status messages are expected to be received.

Note: The **default** form of this command does not exist for the link-group configuration mode.

1.89.6 Examples

The following example shows how to configure a Packet over SONET/SDH (POS) port in slot **9** as a **DCE** interface:

```
[local]Redback(config)#port pos 9/1
[local]Redback(config-port)#frame-relay intf-type dce
```

1.90 frame-relay keepalive

frame-relay keepalive *seconds*

{**no** | **default**} **frame-relay keepalive**

1.90.1 Purpose

Enables the Frame Relay keepalive function and specifies the interval between the transmissions of keepalive messages by a data terminal equipment (DTE) interface for a Frame Relay-encapsulated channel or port, or Multilink Frame Relay (MFR) bundle.

1.90.2 Command Mode

- Link-group configuration
- Port configuration

1.90.3 Syntax Description

seconds	Number of seconds between keepalive messages. The range of values is 0 to 60; the default value is 10.

1.90.4 Default

The Frame Relay keepalive function is enabled, with a 10-second interval between messages.

1.90.5 Usage Guidelines

Use the **frame-relay keepalive** command to enable the Frame Relay keepalive function and specify the interval between the transmissions of keepalive messages by a DTE interface for a Frame Relay-encapsulated channel or port, or MFR bundle.

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

Use the **no** form of this command (or the **frame-relay keepalive 0** command) to disable the transmission of keepalive messages completely. This allows connections to time out and terminate during periods of inactivity.

Use the **default** form of this command to specify the default values.

1.90.6 Examples

The following example shows how to specify the Frame Relay keepalive interval on a Packet over SONET/SDH (POS) port to **20** seconds:

```
[local]Redback(config)#port pos 9/1
[local]Redback(config-port)#frame-relay keepalive 20
```

1.91 frame-relay lmi-n391dte

frame-relay lmi-n391dte ***exchanges***

default frame-relay lmi-n391dte

1.91.1 Purpose

Specifies the number of keepalive messages to be sent before a request for a full status message is sent for a Frame Relay-encapsulated channel or port, or Multilink Frame Relay (MFR) bundle.

1.91.2 Command Mode

- Link-group configuration (MFR)
- Port configuration

1.91.3 Syntax Description

exchanges	Number of keepalive messages (exchanges) to be sent before a full status request message is sent. The range of values is 0 to 255; the default value is 6.

1.91.4 Default

The number of keepalive messages sent is 6.

1.91.5 Usage Guidelines

Use the **frame-relay lmi-n391dte** command to specify the number of keepalive messages to be sent before a request for a full status message is sent for a Frame Relay-encapsulated channel or port, or MFR bundle.

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

Use the **default** form of this command to specify the default value.

Note: The **default** form of this command does not exist for the link-group MFR configuration mode.

1.91.6 Examples

The following example shows how to specify **10** as the number of keepalive messages before a request for a full status message is sent on a Packet over SONET/SDH (POS) port:

```
[local]Redback(config)#port pos 9/1
[local]Redback(config-port)#frame-relay lmi-n391dte 10
```

1.92 frame-relay lmi-n392dce

frame-relay lmi-n392dce *threshold*

default frame-relay lmi-n392dce

1.92.1 Purpose

Sets the error threshold before the Local Management Interface (LMI) is considered to have failed on a data communications equipment (DCE) interface for a Frame Relay-encapsulated channel or port, or Multilink Frame Relay (MFR) bundle.

1.92.2 Command Mode

- Link-group configuration (MFR)
- Port configuration

1.92.3 Syntax Description

threshold	Error threshold in number of errors. The range of values is 0 to 10; the default value is 3.

1.92.4 Default

The threshold is 3.

1.92.5 Usage Guidelines

Use the **frame-relay lmi-n392dce** command to set the error threshold before LMI is considered to have failed on a DCE interface for a Frame Relay-encapsulated channel or port, or MFR bundle. You can only use this command when you have configured the Frame Relay interface type as DCE (using the **frame-relay intf-type** command in link group or port configuration mode).

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

The error threshold should never be greater than the monitored event count (configured with the **frame-relay lmi-n393dce** command in link group or port configuration mode) because when the error threshold meets or exceeds the monitored event count, the LMI is considered to have failed.

Use the **default** form of this command to set the error threshold to the default value of 3.

Note: The **default** form of this command does not exist for the link-group MFR configuration mode.

1.92.6 Examples

The following example shows how to set the error threshold to **5** on a **DCE** interface:

```
[local]Redback(config)#port pos 9/1
[local]Redback(config-port)#frame-relay intf-type dce
[local]Redback(config-port)#frame-relay lmi-n392dce 5
```

1.93 frame-relay lmi-n392dte

frame-relay lmi-n392dte *threshold*

default frame-relay lmi-n392dte

1.93.1 Purpose

Specifies the error threshold before the Local Management Interface (LMI) is considered to have failed on a Frame Relay data terminal equipment (DTE) interface for a Frame Relay-encapsulated channel or port, or Multilink Frame Relay (MFR) bundle.

1.93.2 Command Mode

- Link-group configuration (MFR)
- Port configuration

1.93.3 Syntax Description

threshold	Error threshold in number of errors. The range of values is 0 to 10; the default value is 3.

1.93.4 Default

The threshold is 3.

1.93.5 Usage Guidelines

Use the **frame-relay lmi-n392dte** command to specify the error threshold before the LMI is considered to have failed on a Frame Relay DTE interface for a Frame Relay-encapsulated channel or port, or MFR bundle.

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

The error threshold should never be greater than the monitored event count (configured with the **frame-relay lmi-n393dte** command in link group or port configuration mode). When the error threshold meets or exceeds the monitored event count, the LMI is considered to have failed.

Use the **default** form of this command to specify the default value.

Note: The **default** form of this command does not exist for the link-group MFR configuration mode.

1.93.6 Examples

The following example shows how to specify **5** as the error threshold on a **DTE** interface on a Packet over SONET/SDH (POS) port:

```
[local]Redback(config)#port pos 9/1
[local]Redback(config-port)#frame-relay lmi-n392dte 5
```

1.94 frame-relay lmi-n393dce

frame-relay lmi-n393dce *event-count*

{**no** | **default**} **frame-relay lmi-n393dce**

1.94.1 Purpose

Sets the monitored event count on a data communications equipment (DCE) interface for a Frame Relay-encapsulated channel or port, or Multilink Frame Relay (MFR) bundle.

1.94.2 Command Mode

- Link-group configuration (MFR)
- Port configuration

1.94.3 Syntax Description

event-count	Number of events (receipts of messages across the interface) to be included in the monitored event count. The range of values is 0 to 10; the default value is 4.

1.94.4 Default

The monitored event count is enabled and set to 4.

1.94.5 Usage Guidelines

Use the **frame-relay lmi-n393dce** command to set the monitored event count on a DCE interface. You can only use this command if you have configured the Frame Relay interface type as DCE for a Frame Relay-encapsulated channel or port, or MFR bundle.

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

The event count should never be less than the error threshold count (configured by the **frame-relay lmi-n392dce** command in link group or port configuration mode). When the error threshold meets or exceeds the monitored event count, the Local Management Interface (LMI) is considered to have failed.

Use the **no** form of this command to set the monitored event count value to 0.

Use the **default** form of this command to set the monitored event count to the default value of 4.

Note: The **default** and **no** forms of this command does not exist for the link-group MFR configuration mode.

1.94.6 Examples

The following example shows how to set the monitored event count to **5** on a **DCE** interface:

```
[local]Redback(config)#port pos 9/1
[local]Redback(config-port)#frame-relay intf-type dce
[local]Redback(config-port)#frame-relay lmi-n393dce 5
```

1.95 frame-relay lmi-n393dte

frame-relay lmi-n393dte *event-count*

default frame-relay lmi-n393dte

1.95.1 Purpose

Specifies the monitored event count on a data terminal equipment (DTE) interface for a Frame Relay-encapsulated channel or port, or Multilink Frame Relay (MFR) bundle.

1.95.2 Command Mode

- Link-group configuration (MFR)
- Port configuration

1.95.3 Syntax Description

event-count	Number of events (receipts of messages across the interface) to be included in the monitored event count. The range of values is 0 to 10; the default value is 4.

1.95.4 Default

The monitored event count is 4.

1.95.5 Usage Guidelines

Use the **frame-relay lmi-n393dte** command to specify the monitored event count on a DTE interface for a Frame Relay-encapsulated channel or port, or MFR bundle.

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

The event count should never be less than the error threshold count, which you specify by entering the **frame-relay lmi-n392dte** command in link group or port configuration mode. When the error threshold meets or exceeds the monitored event count, the Local Management Interface (LMI) is considered to have failed.

Use the **default** form of this command to specify the default value.

Note: The **default** form of this command does not exist for the link-group configuration mode.

1.95.6 Examples

The following example shows how to specify **5** as the monitored event count on a **DTE** interface on a Packet over SONET/SDH (POS) port:

```
[local]Redback(config)#port pos 9/1
[local]Redback(config-port)#frame-relay lmi-n393dte 5
```

1.96 frame-relay lmi-t392dce

frame-relay lmi-t392dce *seconds*

default frame-relay lmi-t392dce

1.96.1 Purpose

Specifies the interval for the polling verification timer when the interface type is data communications equipment (DCE) for a Frame Relay-encapsulated channel or port, or Multilink Frame Relay (MFR) bundle.

1.96.2 Command Mode

- Link-group configuration (MFR)
- Port configuration

1.96.3 Syntax Description

seconds	Number of seconds after which an error is counted if a message has not been received. The range of values is 5 to 60; the default value is 15.

1.96.4 Default

The timer interval is 15 seconds.

1.96.5 Usage Guidelines

Use the **frame-relay lmi-t392dce** command to specify the interval for the polling verification timer when the interface type is DCE for a Frame Relay-encapsulated channel or port, or MFR bundle.

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

The polling verification timer starts each time a keepalive message is received from the remote end. If no keepalive message is received before the timer expires, an error is counted. If the number of errors exceeds the error threshold, the LMI is declared down. The value specified for the timer should be greater than the keepalive timer that is set by the remote end.

Use the **default** form of this command to specify the default interval of 15 seconds.

Note: The **default** form of this command does not exist for the link-group MFR configuration mode.

1.97 frame-relay lmi-type

frame-relay lmi-type {**ansi** | **group-of-4** | **itu**}

default frame-relay lmi-type

1.97.1 Purpose

Specifies the Frame Relay Local Management Interface (LMI) type for a Frame Relay-encapsulated channel or port, or Multilink Frame Relay (MFR) bundle.

1.97.2 Command Mode

- Link-group configuration
- Port configuration

1.97.3 Syntax Description

ansi	Specifies the LMI type for Annex D as defined by ANSI standard T1.617; this is the default.
group-of-4	Specifies the original LMI as defined by Cisco, DEC, Northern Telecom, and StrataCom.
itu	Specifies the LMI type for ITU-T Q933 Annex A (formerly labeled as “CCITT”).

1.97.4 Default

The LMI type is ANSI.

1.97.5 Usage Guidelines

Use the **frame-relay lmi-type** command to specify the LMI type for the Frame Relay interface for a Frame Relay-encapsulated channel or port, or MFR bundle.

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

Note: A Packet over SONET/SDH (POS) ports support only the ANSI LMI type.

Use the **default** form of this command to specify the default LMI type.

Note: The **default** form of this command does not exist for the link-group MFR configuration mode.

1.97.6 Examples

The following example shows how to specify an LMI type of ITU-T Q933 Annex A for a POS port:

```
[local]Redback(config)#port pos 9/1

[local]Redback(config-port)#frame-relay lmi-type itu
```

1.98 frame-relay multilink

frame-relay multilink {**ack-delay** *seconds* | **hello-interval** *seconds* | **retries** *count*}

{**no**} **frame-relay multilink** {**ack-delay** | **hello-interval** | **retries**}

1.98.1 Purpose

Specifies the timing for Hello and acknowledgement messages for a channel in a Multilink Frame Relay (MFR) bundle.

1.98.2 Command Mode

- DS-1 configuration
- E1 configuration

1.98.3 Syntax Description

ack-delay *seconds*	Interval, in seconds, to wait for an inbound acknowledgement message to an outgoing control message before taking action. The range of values is 1 to 10; the default value is 4.
hello-interval *seconds*	Interval, in seconds, between sending outbound Hello messages. The range of values is 1 to 180; the default value is 10.
retries *count*	Number of times to resend an Hello message before receiving an acknowledgement message. The range of values is 1 to 5; the default value is 2.

1.98.4 Default

Timing for Hello and acknowledgement messages is enabled according to the defaults.

1.98.5 Usage Guidelines

Use the **frame-relay multilink** command to specify the timing for Hello and acknowledgement messages for a channel or port in an MFR bundle. You can enter this command multiple times to specify each construct for each channel or port in the MFR bundle.

Note: The SmartEdge 100 router does not support Frame Relay bundles.

You must add the channel or port to the MFR bundle by using the **link-group** command in DS-1 or E1 configuration mode before you can enter the **frame-relay multilink** command.

Hello messages inform the peer at the remote end that the link is up; acknowledgement messages notify the peer that a control message from the peer has been received by the SmartEdge router.

Control messages add a link, remove a link, notify the peer that the link is up, or notify the peer that an invalid control message has been received.

Note: If an inbound acknowledgement message to an outgoing control message is not received before the acknowledgement timer expires, the system removes the affected DS-1 channel, E1 channel, or E1 port from the MFR bundle (no user data is sent out and incoming user data is ignored). When the system can successfully exchange control messages with the remote site, the system adds the DS-1 channel, E1 channel, or E1 port to the MFR bundle.

Use the **no** form of this command to specify the default values for the timing for Hello and acknowledgement messages.

1.98.6 Examples

The following example shows how to specify the timing for Hello and acknowledgement messages for a DS-1 channel that is added to an MFR link group, **lg-mfr:**

```
[local]Redback(config)#port ds1 2/1:1
[local]Redback(config-ds1)#encapsulation frame-relay
[local]Redback(config-ds1)#link-group lg-mfr
[local]Redback(config-ds1)#frame-relay multilink ack-delay 5
[local]Redback(config-ds1)#frame-relay multilink hello-interval 5
[local]Redback(config-ds1)#frame-relay multilink retries 3
```

1.99 frame-relay profile

frame-relay profile *prof-name*

no frame-relay profile *prof-name*

1.99.1 Purpose

Creates a new Frame Relay profile or selects an existing one for modification, and enters Frame Relay profile configuration mode.

1.99.2 Command Mode

Global configuration

1.99.3 Syntax Description

prof-name	Alphanumeric string to be used as the name of the particular profile.

1.99.4 Default

No Frame Relay profiles are defined.

1.99.5 Usage Guidelines

Use the **frame-relay profile** command to create a new Frame Relay profile or to select an existing profile for modification, and enter Frame Relay profile configuration mode.

Note: You must create a Frame Relay profile before you can configure Frame Relay permanent virtual circuits (PVCs) that reference the profile.

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

Use the **no** form of this command to delete a Frame Relay profile. This form deletes any PVCs that reference that profile.

1.99.6 Examples

The following example shows how to configure the Frame Relay profile, **fr-pro**, and enters Frame Relay profile configuration mode:

```
[local]Redback(config)#frame-relay profile fr-pro
[local]Redback(config-fr-profile)#
```

1.100 frame-relay pvc

In link-group configuration mode, the syntax is:

frame-relay pvc ***dlci***

no frame-relay pvc ***dlci***

In all other configuration modes, the syntax is:

frame-relay pvc {***dlci*** | **default** [**profile** ***prof-name***]}

no frame-relay pvc ***dlci***

1.100.1 Purpose

Creates or selects a Frame Relay permanent virtual circuit (PVC) on a Frame Relay-encapsulated channel or port, or Multilink Frame Relay (MFR) bundle, and enters Frame Relay PVC or link PVC configuration mode.

1.100.2 Command Mode

- Link-group configuration
- Port configuration

1.100.3 Syntax Description

dlci	Data-link connection identifier (DLCI) of the individual circuit be created. The range of values is 16 to 991.
default	Specifies the default profile and encapsulation. Not available in link-group configuration mode.
profile ***prof-name***	Optional. Name of an existing Frame Relay profile. Not available in link-group configuration mode.

1.100.4 Default

No Frame Relay PVCs are defined.

1.100.5 Usage Guidelines

Use the **frame-relay pvc** command to create or select a Frame Relay PVC on a Frame Relay-encapsulated channel or port, or MFR bundle, and enter Frame Relay PVC or link PVC configuration mode.

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

When entered in link-group configuration mode, this command creates or selects an aggregated Frame Relay PVC in the MFR bundle. When a DS-1 channel, or clear-channel E1 channel or port, is added to the MFR bundle, a Frame Relay PVC with the specified ***dlci*** is created on that channel or port.

When entered in port configuration mode, creates or selects a Frame Relay PVC on the single-link channel, channel group, or port.

Use the **no** form of this command to delete a previously configured Frame Relay PVC.

1.100.6 Examples

The following example shows how to encapsulate a POS port for Frame Relay, create a Frame Relay PVC with DLCI **16**, and enter Frame Relay PVC configuration mode:

```
[local]Redback(config)#frame-relay profile frame20
[local]Redback(config-fr-profile)#bulkstats schema fr-port
[local]Redback(config-fr-profile)#exit
[local]Redback(config)#port pos 3/1
[local]Redback(config-port)#encapsulation frame-relay
[local]Redback(config-port)#frame-relay pvc 16 profile frame20
[local]Redback(config-fr-pvc)#
```

The following example shows how to create a Frame Relay link group and two aggregated Frame Relay PVCs with DLCIs **26** and **27** for two sets of constituent Frame Relay PVCs to be aggregated in the MFR bundle **lg1:**

```
[local]Redback(config)#link-group lg1 mfr
[local]Redback(config-link-group)#frame-relay pvc 26
[local]Redback(config-link-pvc)#exit
[local]Redback(config-link-group)#frame-relay pvc 27
[local]Redback(config-link-pvc)#exit
```

1.101 framing (ATM, POS, WAN-PHY)

For an ATM OC or Packet over SONET/SDH (POS) port, the syntax in ATM OC or port configuration mode is:

framing {sdh | sonet}

default framing

For an Ethernet WAN-PHY port, the syntax in port configuration mode is:

framing {sdh | sonet}

1.101.1 Purpose

Specifies the framing for an ATM OC, Ethernet WAN-PHY, or POS port.

1.101.2 Command Mode

- ATM OC configuration
- Port configuration

1.101.3 Syntax Description

sdh	Specifies Synchronous Digital Hierarchy (SDH) framing for an ATM OC or POS or Ethernet WAN-PHY port.
sonet	Specifies Synchronous Optical Network (SONET) framing for an ATM OC or POS or Ethernet WAN-PHY port; this is the default framing.

1.101.4 Default

The default framing for an ATM OC, Ethernet WAN-PHY, or POS port is SONET.

1.101.5 Usage Guidelines

Use the **framing** command to specify the framing for an ATM OC, Ethernet WAN-PHY, or POS port.

Note: This command does not apply to channelized OC-12 ports.

The system provides the following error message if you attempt to change the framing on a port with PVCs:

```
Cannot change Framing while PVCs/VPs exist on any port on this card - Please remove all PVCs/VPs on this card
try again
```

The framing on all ports must be the same.

Use the **default** form of this command to set the framing to the default setting.

1.101.6 Examples

The following example shows how to set the framing for an ATM OC port to **cbit-plcp:**

```
[local]Redback(config)#port atm 3/1
[local]Redback(config-atm-ds3)#framing cbit-plcp
```

The following example shows how to set the framing for an WAN-PHY port to **sdh:**

```
[local]Redback(config)#port ethernet 3/1 wan-phy
[local]Redback(config-port)#framing sdh
```

1.102 framing (DS-1, DS-3, E1)

For a clear-channel DS-3 channel or port, the syntax in DS-3 configuration mode is:

framing {**c-bit** | **m13**}

default framing

For a channelized DS-3 channel or port, the syntax in DS-3 configuration mode is:

framing {**c-bit** | **m23**}

default framing

For a DS-1 channel, the syntax in DS-1 configuration mode is:

framing {**esf** | **sf**}

default framing

For an E1 channel or port, the syntax is in E1 configuration mode:

framing {**crc4** | **no-crc4** | **unframed**}

{**no** | **default**} **framing**

1.102.1 Purpose

Specifies the framing for a clear-channel or channelized DS-3 channel or port, a DS-1 channel, or an E1 channel or port.

1.102.2 Command Mode

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

1.102.3 Syntax Description

c-bit	Specifies C-bit format. Available only for DS-3 channels or ports, either channelized or clear-channel; this is the default for clear-channel DS-3 channels or ports.
g751	Specifies ITU-T G.751 format. Available only for clear-channel E3 ports; this is the default.

m13	Specifies M13 framing. Available only for clear-channel DS-3 channels or ports. This option is not currently supported.
m23	Specifies M23 format. Available only for channelized DS-3 channels or ports; this is the default for channelized DS-3 channels or ports.
esf	Specifies Extended Superframe Format (ESF). Available only for DS-1 channels; this is the default.
sf	Specifies Superframe Format (SF). Available only for DS-1 channels.
crc4	Specifies CRC-4 framing. Available only for E1 channels or ports; this is the default, which channelizes the E1 channel or port.
no-crc4	Specifies non-CRC-4 framing. Available only for E1 channels or ports, it removes the channelization for an E1 channel or port.
unframed	Specifies no framing. Available only for E1 channels or ports, it removes the channelization for an E1 channel or port.

1.102.4 Default

The framing for clear-channel and channelized DS-3 channels or ports is C-bit format. The framing for E3 ports is G.751 format. The framing for DS-1 channels is ESF. The framing for E1 channels or ports is CRC-4 format.

1.102.5 Usage Guidelines

Use the **framing** command to specify the framing for a channelized DS-3 channel or port, E3 port, DS-1 channel, or E1channel or port.

For clear-channel E3 ports, use the **no** form of this command to specify the framing as unframed.

For DS-1 channels, the following caution applies:

Caution!

Risk of data loss. To specify a different framing for a DS-1 channel, where the DS-1 channel is operating in a remote (line fdl ansi, line in-band, or payload) loopback state, and the new framing is not compatible with the type of remote loopback that you have operating, the system terminates the remote loopback (change the DS-1 channel operation to a normal state) before changing the framing. To reduce the risk, postpone issuing the **framing** command until you are ready to terminate the remote loopback. The description of the **loopback** command in this document includes the framing format compatible with each type of remote loopback.

For E1 channels or ports, the following guidelines apply:

- Specify the **crc4** or **no-crc4** keyword to create a channelized E1 channel or port. If an E1 channel or port is channelized, you can create a DS-0 channel group that consists of one or more DS-0 time slots.
- Use the **unframed** keyword specify a clear-channel E1 channel or port.
- Specify the **no** form of this command to return the E1 channel or port to its default CRC-4 framing.

Use the **default** form of this command to set the framing to the default, regardless of channel or port type.

1.102.6 Examples

The following example shows how to set the framing for a channelized DS-3 channel **2** on port **1** to C-bit format (**c-bit**):

```
[local]Redback(config)#port channelized-ds3 3/1:2
[local]Redback(config-ds3)#framing c-bit
```

The following example shows how to configure a clear-channel E1 port:

```
[local]Redback(config)#port e1 4/1
[local]Redback(config-e1)#framing unframed
```

1.103 frr-auto-revert-delay

frr-auto-revert-delay ***delay-interval***

no frr-auto-revert-delay

1.103.1 Purpose

Sets the amount of time that RSVP waits after a failed interface comes back up before traffic is switched back to the primary LSP from a bypass LSP.

1.103.2 Command Mode

RSVP router configuration mode

1.103.3 Syntax Description

delay-interval	Amount of time, in seconds, that RSVP waits after a failed interface comes back up before traffic is switched back to the primary LSP from a bypass LSP. The range of values is 0 to 65,535.

1.103.4 Default

The **frr-auto-revert-delay** command is disabled and bypass LSPs do not switch back to primary LSPs.

1.103.5 Usage Guidelines

Use the **frr-auto-revert-delay** command to set the amount of time that RSVP waits after a failed interface comes back up before traffic is switched back to the primary LSP from a bypass LSP.

When the ***delay-interval*** value is changed, and it is lower than the delay interval set for any existing bypass RSVP LSPs that are scheduled to switch back to their primary LSPs, then their delay timer is reset to the new, lower value.

From Release 2.6.5.2 to Release 5.0.3.1 of the SmartEdge router ,when the NFRR auto-revert delay is enabled, traffic is automatically switched to the primary LSP after the specified delay interval has elapsed. Starting with Release 5.0.3.2, after the delay interval has elapsed, a new instance of the primary LSP must be established before traffic is switched to it; otherwise, traffic continues to use the bypass LSP.

Note: If the interface goes down before the specified delay interval has elapsed, the traffic does not switch back to the primary LSP, but continues to use the bypass LSP. The delay timer is in effect only when a previously failed interface comes back up and stays up.

Use the **no** form of this command to disable the NFRR auto-revert delay. If the NFRR auto-revert delay is disabled, then all existing bypass LSPs do not switch back to their primary LSPs, even if their delay timer has started.

1.103.6 Examples

The following example shows how to enable an RSVP instance to restart gracefully:

```
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#frr-auto-revert-delay
```

1.104 full-name

full-name ***text***

no full-name

1.104.1 Purpose

Associates a full name or textual description with an administrator account.

1.104.2 Command Mode

Administrator configuration

1.104.3 Syntax Description

text	Alphanumeric string representing a new or existing administrator.

1.104.4 Default

No full name is associated with an administrator account.

1.104.5 Usage Guidelines

Use the **full-name** command to associate a full name or text description with an administrator account. You can enter a full name with embedded spaces by enclosing the entire name in double quotation marks; for example, **"Fred Q. Lynch"**.

Use the **no** form of this command to remove the full name text for an administrator.

1.104.6 Examples

The following example shows how to configure the full name for an administrator, **Fred:**

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

[local]Redback(config-administrator)#full-name "Fred Q. Lynch, x1234"
```

1.105 function

function {**lac-only** | **lns-only**}

{**no** | **default**} **function**

1.105.1 Purpose

Specifies the role that the SmartEdge router assumes with this Layer 2 Tunneling Protocol (L2TP) peer, either as an L2TP access concentrator (LAC) or as an L2TP network server (LNS).

1.105.2 Command Mode

L2TP peer configuration

1.105.3 Syntax Description

lac-only	Specifies that the SmartEdge router can send incoming call requests to, but cannot receive them from, this peer.
lns-only	Specifies that the SmartEdge router can receive incoming call requests from, but cannot send them to, this peer.

1.105.4 Default

The SmartEdge router functions as a LAC only for this peer.

1.105.5 Usage Guidelines

Use the **function** command to specify the role that the SmartEdge router assumes with this L2TP peer, either as a LAC or as an LNS. The LAC-only role prevents the acceptance of Incoming-Call-Request (ICRQ) control messages from a LAC peer. The LNS-only role prevents the generation of ICRQ control messages based on incoming Point-to-Point Protocol (PPP) sessions to an LNS peer.

Note: We recommend that you specify the **lns-only** keyword if you are configuring an anonymous (unnamed) peer.

Use the **default** or **no** form of this command to disable any specification.

1.105.6 Examples

The following example shows how to specify that the SmartEdge router function as a LAC with the named L2TP peer:

```
[local]Redback(config-ctx)#l2tp-peer name peer1
[local]Redback(config-l2tp)#function lac-only
```

Glossary

MP
Merge Point.

The point at which traffic exits the tail end router of a bypass RSVP LSP.