Commands: c through clear mr

COMMAND DESCRIPTION

3/190 82-CRA 119 1170/1-V1 Uen K

Copyright

Disclaimer

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

Trademark List

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

Contents

1 Command Descriptions

Commands starting with “c” through commands starting with “clear mr” 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 c2byte

```
c2byte value
```

```
default c2byte
```

1.1.1 Purpose

Defines the value for the Path Signal Label (C2) byte for a Packet over SONET/SDH (POS) port.

1.1.2 Command Mode

port configuration

1.1.3 Syntax Description

value	Value to send in the C2 byte. The range of values is 0 to 255; the default value is 22 (hexadecimal 0x16).

1.1.4 Default

The default value is 22 (hexadecimal 0x16).

1.1.5 Usage Guidelines

Use the **`c2byte`** command to define the value for the C2 byte for a POS port. RFC 2615, `PPP over SONET/SDH`, specifies that a C2 byte value of 22 (hexadecimal 0x16) is used to indicate Point-to-Point Protocol (PPP) with X^43 + 1 scrambling, and the value of 207 (hexadecimal 0xCF) is used to indicate PPP without scrambling.

Note: The SmartEdge 100 router does not support POS ports.

Note: The SmartEdge router automatically configures the C2 byte to 22 (0x16) when synchronous payload envelope (SPE) scrambling is enabled, and to 207 (0xCF) when SPE scrambling is disabled; see the **`scramble`** command. To define a different C2 byte value to interoperate with another vendor's equipment and you need to enable SPE scrambling, first enable SPE scrambling (it is enabled by default), and then override the C2 byte value with this command.

Note: This command applies only to a POS port on an OC-48c/STM-16c line card, OC-12c/STM-4c line card, or OC-3c/STM-1c line card.

Note: The C2 byte for a port on any Asynchronous Transfer Mode (ATM) OC line card is fixed at 0x13 and cannot be changed.

Use the **`default`** form of this command to define the C2 byte with the default value.

1.1.6 Examples

The following example shows how to define the value **22** (hexadecimal value **0x16**) for the C2 byte for a POS port in slot **9:**

```
[local]Redback(config)#port pos 9/1

[local]Redback(config-port)#c2byte 22
```

1.2 cablelength (DS-3)

`cablelength` ***`length`***

`default cablelength`

1.2.1 Purpose

Specifies the length of the cable connected to a DS-3 port.

1.2.2 Command Mode

DS-3 configuration

1.2.3 Syntax Description

length Length of the cable in feet. The range of values is 0 to 450.0 ft. (137.2m) for a DS-3 port.

1.2.4 Default

The default cable length is 349.0 ft. (106.4m) for a DS-3 port.

1.2.5 Usage Guidelines

Use the **cablelength** command to specify the length of the cable connected to a DS-3.

Use the **default** form of this command to specify the default length.

Note: The operating system recognizes only two categories of DS-3 cables: short, which is any length up to and including 349.0 ft. (106.4m), and long, which is any length over 349.0 ft. (106.4m).

Note: This command does not apply to channelized OC-12 ports or to clear-channel E3 ports.

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

1.2.6 Examples

The following example shows how to specify a cable length of 225.0 ft. (68.6m) for a DS-3 port:

```
[local]Redback(config-ds3)#cablelength 225
```

1.3 capabilities

capabilities {**area-scope** | **as-scope**}

no capabilities {**area-scope** | **as-scope**}

1.3.1 Purpose

Enables the advertisement of router capabilities using Open Shortest Path First (OSPF) opaque link-state advertisements (LSAs).

1.3.2 Command Mode

OSPF router configuration

1.3.3 Syntax Description

`area-scope`	Advertise router capabilities using Type 10 opaque LSAs.
`as-scope`	Advertise router capabilities using Type 11 opaque LSAs.

1.3.4 Default

Advertisement of router capabilities is disabled.

1.3.5 Usage Guidelines

Use the **`capabilities`** command to enable the advertisement of router capabilities using OSPF opaque LSAs.

The capabilities LSAs advertise the optional OSPF capabilities enabled on the router to all IGP neighbors. Table 1 shows the reserved OSPF router capability bits and the associated capabilities that can be advertised.

Table 1 Reserved OSPF Router Capability Bits

Bit	Capability
0–3	Reserved
4	Graceful restart capable
5	OSPF graceful restart helper
6	Stub router support
7	Traffic engineering support
8	OSPF point-to-point over LAN
9	OSPF path computation server discovery
10–31	Future assignments

Use the **`no`** form of this command to disable advertisement of router capabilities using OSPF opaque LSAs.

1.3.6 Examples

The following example shows how to enable the advertisement of router capabilities using Type 10 (**area-scope**) opaque LSAs:

```
[local]Redback(config-ctx)#router ospf 424

[local]Redback(config-ospf)#capabilities area-scope
```

1.4 card

For cards in a SmartEdge 100 chassis, the syntax is:

`card carrier 2`

`no card carrier 2`

For cards in any other SmartEdge chassis, the syntax is:

`card` ***`card-type slot`***

`no card` ***`card-type slot`***

1.4.1 Purpose

Selects a carrier card, services card, or line card to take out of service for an on-demand diagnostic (ODD) session, or to place in service after an ODD session, and enters card configuration mode.

1.4.2 Command Mode

Global configuration

1.4.3 Syntax Description

`card-type`	Type of line card, according to one of the keywords in Table 2.
`slot`	Chassis slot number of the line card. The range of values depends on the type of card and the chassis in which the card is installed; see Table 2 for slot range data.

1.4.4 Default

None

1.4.5 Usage Guidelines

Use the **card** command to select a line or services card to take out of service for an ODD session, or to place in service after an ODD session, and enter card configuration mode.

This command is not required for any line card that is already installed; the operating system recognizes the type of each installed card. However, you can use this command to configure a line card and its associated ports, channels, and circuits before the line card is actually installed in the chassis.

If you configure a line card and then insert a different line card type in the slot, the ports on that line card do not come up.

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

Caution!

Risk of data corruption and loss of charging records. Removing an SSE card from configuration without first shutting it down can cause file corruption. To avoid the risk, do one of the following before entering the **no card sse** ***slot*** command:

- If the SSE card is in assigned to an SSE group, enter the **no bind sse group** ***name*** and **commit** commands. Wait at least 15 seconds for the card to completely shut down.
- If the SSE card is not configured for redundancy, shut down the card with the **shutdown** and **commit** commands and wait for 15 seconds before entering the **no card sse** ***slot*** command.

Table 2 lists the values for the ***card-type*** and ***slot*** arguments for any SmartEdge chassis except the SmartEdge 100; in the table, ER, IR, LR, and SR abbreviations are used for Extended Reach, Intermediate Reach, Long Reach, and Short Reach, respectively.

Table 2 Line and Services Card Types and Slots

Type of Card/Description	*card-type* Argument Keyword Options	*slot* Argument Range		
		SmartEdge 800, 1200, and 1200H	SmartEdge 400	SmartEdge 600
ATM				
ATM OC-3c/STM-1c (8-port)	`atm-oc3e-8-port`	1 to 6 and 9 to 14	1 to 4	1 to 6
ATM OC-12c/STM-4c (2-port)	`atm-oc12e-2-port`			
Channelized SONET/SDH				

Table 2 Line and Services Card Types and Slots

Type of Card/Description	`card-type` Argument Keyword Options	`slot` Argument Range		
		SmartEdge 800, 1200, and 1200H	**SmartEdge 400**	**SmartEdge 600**
Channelized 8/4-port OC-3/STM-1 or 2/1-port OC-12/STM-4	`ch-oc3oc12-8or2-port`	1 to 6 and 9 to 14	1 to 4	1 to 6
POS				
POS OC-3c/STM-1c (8-port)	`oc3e-8-port`	1 to 6 and 9 to 14	1 to 4	1 to 6
POS OC-12c/STM-4c (4-port)	`oc12e-4-port`			
POS OC-48c/STM-16c (4-port)	`oc48e-4-port`			
OC-192c/STM-64c (1-port)[1]	`oc192-1-port`			
Ethernet				
Fast Ethernet–Gigabit Ethernet (60-port FE, 2-port GE)	`fege-60-2-port`	1 to 6 and 9 to 14	1 to 4	1 to 6
Gigabit Ethernet 1020 (10-port)	`ge-10-port`			
Gigabit Ethernet 1020 (20-port)	`ge-20-port`			
Gigabit Ethernet (5-port)	`ge-5-port`			
Gigabit Ethernet DDR (10-port)	`ge2-10-port`			
Gigabit Ethernet DDR (20-port)	`ge4-20-port`			
10 Gigabit Ethernet (1-port)	`10ge-1-port`			
10 Gigabit Ethernet DDR (4-port	`10ge-4-port`			
10 Gigabit Ethernet/OC-192c DDR (1-port)	`10ge-oc192-1-port`			
ASE				
Advanced Services Engine	`ase`	1 to 6 and 9 to 14	1 to 4	1 to 6
SSE				
SmartEdge Storage Engine	`sse`	1 to 6 and 9 to 14	N/A	1 to 6

(1) This line card accepts Ericsson XFP transceivers, including IR, SR, LR, ER, and ZR types. For further information and a full list of supported transceivers, see `Transceivers for SmartEdge and SM Family Line Cards`.

1.4.6 Examples

The following example shows how to select an 8-port ATM OC-3c/STM-1c line card in slot **2** to take out of service:

```
[local]Redback(config)#card atm-oc3e-8-port 2
[local]Redback(config-card)#
```

The following example selects a 4-port 10GE DDR card in slot **3** to take out of service:

```
[local]Redback(config)#card 10ge-4-port 3
[local]Redback(config-card)#
```

The following example shows how to select a Channelized 8/4-port OC-3/STM-1or 2/1-port OC-12/STM-4 card in slot **4** to take out of service:

```
[local]Redback(config)#card ch-oc3oc12-8or2-port 4
[local]Redback(config-card)#
```

1.5 care-of-address

care-of-address ***if-name*** [***ctx-name***]

no care-of-address ***if-name*** [***ctx-name***]

1.5.1 Purpose

Specifies the interface used for the care-of-address (CoA) advertised by this foreign-agent (FA) instance.

1.5.2 Command Mode

FA configuration

1.5.3 Syntax Description

if-name	Name of the interface for the CoA.
ctx-name	Optional. Context name in which the interface exists. If the interface exists in a context other than the one you are currently in, you must specify the context name.

1.5.4 Default

The interface used for the CoA is not specified in advertisement messages.

1.5.5 Usage Guidelines

Use the **care-of-address** command to specify the interface used for the CoA advertised by this FA instance. Enter this command multiple times to specify multiple CoA interfaces. This command specifies an existing interface as the CoA interface; you must first create that interface using the **interface** command (in context configuration mode).

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

1.5.6 Examples

The following example creates the **coa** interface in the **local** context and specifies it as the CoA interface for the FA instance:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface coa
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#foreign-agent
[local]Redback(config-mip-fa)#care-of-address coa local
```

1.6 ccm

ccm

{**no** | **default**} **ccm**

1.6.1 Purpose

Enables the maintenance association endpoints (MEPs) in the current maintenance association (MA) to broadcast CCM PDUs, monitor for connectivity faults, and enter the CCM configuration mode where the CCM parameters can be configured.

1.6.2 Command Mode

MA configuration

1.6.3 Syntax Description

This command has no keywords or arguments.

1.6.4 Default

CCM is disabled. If CCM is enabled, the default settings of its parameters are as follows:

- *interval*—100 milliseconds between transmission of CCM PDUs.

- *count*—3; that is, a connectivity fault is declared if MA detects the failure of three consecutive CCMs.

1.6.5 Usage Guidelines

Use the **ccm** command to enable the MEPs in the current MA to broadcast CCM PDUs, monitor for connectivity faults, and enter the CCM configuration mode where the CCM parameters can be configured.

The CCM parameters include the frame-loss and std-interval parameters.

Use the **no** or **default** form of this command to disable CCM.

The default CCM PDU multicast address is 01:80:C2:00:00:3y, where y is the current MD level.

1.6.6 Examples

In the following example, the **ccm** command enables the SmartEdge router to monitor the **bayarea** MA for connectivity faults using CCMS PDUs. The default CCM parameters are used:

```
[local]Redback(config)#ethernet-cfm instance-1
[local]Redback(config-ether-cfm)#level 4
[local]Redback(config-ether-cfm)#domain-name abc.com
[local]Redback(config-ether-cfm)#maintenance-association bayarea
[local]Redback(config-ether-cfm-ma)#ccm
```

1.7 ccod-mode port-listen

ccod-mode port-listen

{**no** | **default**} **ccod-mode port-listen**

1.7.1 Purpose

Enables port listening mode for this Asynchronous Transfer Mode (ATM) port.

1.7.2 Command Mode

ATM OC configuration

1.7.3 Syntax Description

This command has no keywords or arguments.

1.7.4 Default

Port listening mode is disabled for all ATM ports.

1.7.5 Usage Guidelines

Use the **ccod-mode port-listen** command to enable port listening mode for this ATM port. This command is available only for ports on second-generation ATM OC line cards.

Note: Enabling port listening mode with this command must precede the configuration of any ATM VPs or PVCs on this port.

Use this command to specify the full range of ATM virtual path identifiers (VPIs) and virtual circuit identifiers (VCIs) (VCI 0 to 255, VPI 1 to 65,535) when entering the **atm pvc on-demand** command (in ATM OC configuration mode) to create listening on-demand ATM permanent virtual circuits (PVCs) for this port. Otherwise, the range specified must be within the limits for that type of port.

This command does not change the maximum number of active PVCs that are supported on the type of ATM port on which you are creating them, nor the number of active PVCs that are supported for each line class on that type of ATM port. For PVC limits for ATM ports and line classes, see the tables that specify PVC limits in *ATM Configuration Guidelines* in *Configuring Circuits*:

- *Traffic Class Combinations for ATM Priority Mode*: *Traffic Class Combinations for ATM Priority Mode*

- *Shaped VP Limits for ATM Traffic Cards*: *Shaped VP Limits for ATM Traffic Cards*

- *PVC Limits on Shaped VPs for ATM Traffic Cards*: *Shaped VP Limits for ATM Traffic Cards*

- *PVC Limits for ATM Cards Without ATMWFQ Policy*: *PVC Limits for ATM Cards Without ATMWFQ Policy*

- *PVC Limits for ATM Traffic Cards with ATMWFQ CoS Queues*: *PVC Limits for ATM Traffic Cards with ATMWFQ CoS Queues*

Use the **no** or **default** form of this command to disable port listening mode for this port.

1.7.6 Examples

The following example shows how to enable port listening mode for port **2** on the 4-port ATM OC-3c/STM-1c line card in slot **3:**

```
[local]Redback(config)#port atm 3/2
[local]Redback(config-atm-oc)#ccod-mode port-listen
```

1.8 cd

cd ***url***

1.8.1 Purpose

Changes the current working directory.

1.8.2 Command Mode

exec (10)

1.8.3 Syntax Description

url	Name of the preferred working directory. Enter **..** to change to the parent of the current directory.

1.8.4 Default

None

1.8.5 Usage Guidelines

Use the **cd** command to change the current working directory. By default, the current working directory when you log on to the system is /flash.

You must specify a directory on the local file system, with a URL in the following form:

[/***device***][/***directory***]...[/***directory***]

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

1.8.6 Examples

The following example shows how to change the current working directory to **/flash/config/old:**

```
[local]Redback>cd /flash/config/old
Current directory is now /flash/config/old
```

The following example shows how to change the current working directory to the parent directory:

```
[local]Redback>cd ..
Current directory is now /flash/config
```

The following example shows how to change the current working directory to the mass-storage device:

```
[local]Redback>cd /md
Current directory is now /md
```

1.9 cell-encap

cell-encap {**nto1-vcc** | **nto1-vpc**}

no cell-encap {**nto1-vcc** | **nto1-vpc**}

1.9.1 Purpose

Enables and configures ATM cell mode encapsulation on the specified cross-connection (XC).

1.9.2 Command Mode

L2VPN profile peer configuration

1.9.3 Syntax Description

nto1-vcc	Enable n-to-1 VCC encapsulation.
nto1-vpc	Enable n-to-1 VPC encapsulation.

1.9.4 Default

ATM cell mode encapsulation is disabled on XCs.

1.9.5 Usage Guidelines

Use the **cell-encap** command to enable and configure ATM cell mode encapsulation in an L2VPN profile. All ATM XCs that have this profile attached inherit this configuration.

After ATM cell mode encapsulation is enabled in an L2VPN profile, you cannot use the **xc** command to disable cell mode encapsulation on XCs that have that L2VPN profile attached. Instead, you must disable cell mode encapsulation in the L2VPN profile.

After ATM cell mode encapsulation is disabled in an L2VPN profile that is attached to an XC, you cannot modify the cell encapsulation setting in the L2VPN profile.

Use the **no** form of this command to disable ATM cell mode encapsulation in an L2VPN profile.

1.9.6 Examples

The following example shows how to enable and configure ATM cell mode encapsulation in an L2VPN profile called `pr1`:

```
[local]Redback(config)#l2vpn profile pr1
[local]Redback(config-l2vpn-xc-profile)#peer 111.111.111.111
[local]Redback(config-l2vpn-xc-profile-peer)#cell-encap nto1-vcc
```

1.10 ces

ces ***password*** **{encrypted | plain text passcode}** ***card-type slot-id***

no ces ***password*** **{encrypted | plain text passcode}** ***card-type slot-id***

1.10.1 Purpose

Configures the CES licensing key on a *Channelized 8-port OC-3/STM-1 or 2-port OC-12/STM-4* line card.

1.10.2 Command Mode

Config-License Configuration Mode.

1.10.3 Syntax Description

password	The password provided when the license is purchased.
encrypted 1	The password is encrypted.
plain text passcode	The password is not encrypted.

card-type The card type of the license.

slot-id The slot to which the license is to be applied or removed; accepted only for per-slot licenses.

1.10.4 Default

None.

1.10.5 Usage Guidelines

To remove all software licenses, including per-slot ones, run **no software license all-ports**.

Removing all software licenses on the chassis removes all per-slot licenses as well as all per-chassis licenses. When a per-slot license is removed, subsequent enabling of ports 5 through 8 is blocked.

1.10.6 Examples

The following example shows how to enter a license password on port 2::

```
[local]Redback(config)#software license
[local]Redback(config-license)#ces encrypted 1 $1$kYx3M5rG$aglKBVzNn8n4IM3Nc7tpR0 card ch-oc3oc12-8or2-port sl
[local]Redback(config-license)#all-ports encrypted 1 $1$EauC6mWw$sxtHeRLE9eP1bRYoB3CSN/ card ch-oc3oc12-8or2-p
```

1.11 ces excessive-packet-loss

ces excessive-packet-loss threshold ***threshold*** **set** ***declaration*** **clear** ***clearance***

no ces excessive-packet-loss

default ces excessive-packet-loss

1.11.1 Purpose

Configures the excessive packet loss settings of CESoPSN and SAToP connections.

1.11.2 Command Mode

Global Config Mode.

1.11.3 Syntax Description

threshold
: Upper limits of measurement for excessive packet loss, in percentage. The range of values is 1 to 100.

declaration
: Duration that controls declaration of the excessive packet loss alarm. The range of values is from 2.5 to 25 seconds in increments of 2.5 seconds. The default value is 2.5 seconds. Declaration time should be less than clearance time.

clearance
: Duration that controls clearance of the excessive packet loss alarm. The range is from 5 to 25 seconds in increments of 2.5 seconds. The default value is 2.5 seconds. Clearance time should be greater than declaration time.

1.11.4 Default

Excessive packet loss is disabled.

1.11.5 Usage Guidelines

Duration *T* is a system constant value which is 2.5 seconds.

Declaration time is a series of successive periods of duration *T* that experience an excessive packet loss defect.

Clearance time is a series of successive periods of duration *T* that do not experience an excessive packet loss defect.

1.11.6 Examples

The following example shows how to set excessive packet loss:

```
[local]Redback(config)#ces execessive-packet-loss thresh
old 45 set 5  clear 20
```

1.12 cesopsn

cesopsn

1.12.1 Purpose

Enable CESoPSN configuration mode on an attachment circuit.

1.12.2 Command Mode

DS0 Channel Config Mode.

1.12.3 Syntax Description

None.

1.12.4 Default

CESoPSN is not enabled.

1.12.5 Usage Guidelines

None.

1.12.6 Examples

The following example shows how to enable CESoPSN on a DS0-group attachment circuit.:

```
[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-e1-cesopsn)#
```

1.13 channel-mapping

channel-mapping ***mapping-specification***

{no | default}channel-mapping

1.13.1 Purpose

Configures the current SONET port for either STS-1 or VT-1.5 channel mapping.

1.13.2 Command Mode

- port configuration (OC-3)
- port configuration (OC-12)

1.13.3 Syntax Description

mapping-specification

- `sts1` (default)
  Maps plesiochronous digital hierarchy (PDH) frame directly into an STS-1. Use this option for ports that carry DS3 channels within SONET frames.

- `vt1.5`
  Maps structures into VT-1.5 (Virtual Tributaries), which are then mapped into VTGs and into the STS-1 frames. Use this option for ports that map DS1 channels into the SONET structure.

1.13.4 Default

STS-1

1.13.5 Usage Guidelines

1.13.5.1 Where Used

The **channel-mapping** command plays an important role in the provisioning of channelized OC-3 and OC-12 ports. For aug-mapping of channelized STM-1 and STM-4 ports, see the *aug-mapping* command. For detailed examples, the supported subchannel types, and the full context of this command, see *Configuring Channelized Ports*.

1.13.5.2 Guidelines

The port SONET mapping specifies the channel mapping used by all facilities on current OC-3 or OC-12 port. The mapping selected must match that of the far end SONET interface, and must support the types of channels required to carry the POS service.

- The port mapping limits the channel type that can be carried by the port.

- All configured channels must be removed from the port before its port mapping can be changed.

- Table 3 shows the service provided on each type of unchannelized channel with each SONET mapping option. Table 3 also shows what subchannel channel types can be multiplexed on each channelized channel type for each SONET mapping option.

Table 3 Channel Types

Channel Type	Subchannel/ Service Type	Framing	SONET Channel Mapping	SDH AUG Mapping
ds3	POS	C-Bit Parity M23	STS1	au3/no-tugs au4/tu3
channelized-ds3	DS1 E1	C-Bit Parity M23	STS1	au3/no-tugs au4/tu3
ds1	POS	SF ESF	VT1.5	au3/tu11 au4/tu11
channelized-ds1	NxDS0	SF ESF	VT1.5	au3/tu11 au4/tu11
e1	POS	CRC-4 NO-CRC-4 unframed	N/A	au3/tu12 au4/tu12
channelized-e1	NxDS0	CRC-4 NO-CRC-4	N/A	au3/tu12 au4/tu12

1.13.6 Examples

1.13.6.1 vt1.5 channel-mapping Example

```
configure

port channelized-oc12 13/1 pos
 no shutdown
 channel-mapping vt1.5
 !
 port channelized-ds1 13/1:1:1
  no shutdown
  !
 port channelized-ds1 13/1:1:2
  no shutdown
  !
  port ds0s 13/1:1:2:1
   no shutdown
   encapsulation ppp
   bind interface int2 local
   qos policy queuing pwfq-pol
```

1.13.6.2 sts1 channel-mapping Example

```
configure


port channelized-oc12 13/1 pos
 no shutdown
 channel-mapping sts1
 !
 port ds3 13/1:1
  no shutdown
  encapsulation ppp
  bind interface int2 local
  qos policy queuing pwfq-pol
!
 port channelized-ds3 13/1:2
  no shutdown
  !
  port ds0s 13/1:2:1:1
   no shutdown
   encapsulation ppp
   bind interface int2 local
   qos policy queuing pwfq-pol
```

1.14 circuit-group

circuit-group ***name*** [{{{**port** ***slot/port*** } | {**link-group** ***lg-name***}} [**virtual-port**]} | {**parent-circuit-group** ***parent-name***}]

no circuit-group ***name***

1.14.1 Purpose

Creates a circuit group and assigns to it the specified name or selects an existing circuit group, and then enters circuit-group configuration mode.

1.14.2 Command Mode

global configuration

1.14.3 Syntax Description

name	Name of a circuit group, which is an alphanumeric string comprising up to 39 characters.
port ***slot/port***	Optional. Specifies a port on which all circuits in this group should reside.
link-group ***lg-name***	Optional. Specifies an access link group on which all circuits in this circuit group should reside.

`virtual-port` — Optional. Specifies that this circuit group functions as a virtual port on the specified port or link group for Traffic Management scheduling purposes. See *Virtual Port Circuit Groups* for more information.

`parent-circuit-group` *`parent-name`* — Optional. Specifies a circuit group on which all circuits in this group are subject to inheritance from—a parent circuit group.

1.14.4 Default

By default, no circuit groups exist and no ports or link groups are associated with a newly-created circuit group.

1.14.5 Usage Guidelines

Use the **`circuit-group`** command to create a circuit group and assign it a specified name, and then enter circuit-group configuration mode. If the specified circuit group already exists, this command allows you to configure the specified circuit group by entering circuit-group configuration mode.

The following existing commands are available in circuit-group configuration mode:

- **`qos hierarchical mode`**
- **`qos policy metering`**
- **`qos policy policing`**
- **`qos policy queuing`** (for priority weighted fair queuing [PWFQ] policies only)
- **`qos profile overhead`**
- **`qos rate`**
- **`qos weight`**

A circuit group that is created specifying a port (using the **`port`** *`slot/port`* construct) or link-group (using the **`link-group`** *`lg-name`* construct) is known as a homed circuit group. A homed circuit group supports all configuration parameters and bindings, including those related to traffic management and priority weighted fair queuing (PWFQ), while a nonhomed circuit group supports only metering and policing bindings. However, a nonhomed circuit group may include circuits that span physical ports.

To change a circuit group from a homed to a nonhomed mode, delete the circuit group and then recreate it. You can add a port or link-group reference to a nonhomed circuit group to convert it to a homed circuit group only if the circuit group does not have any configured members.

A port or link group must be specified for a circuit group to enable the following QoS-related configuration command options:

- qos hierarchical mode strict
- qos policy queuing
- qos profile overhead
- qos rate
- qos weight

You can nest a circuit group within another circuit group by specifying a parent circuit group for a circuit group using the **parent-circuit-group** ***parent-name*** construct with the **circuit-group** command. Use nested circuit groups for configuring hierarchical QoS. Members of child circuit groups are subject to QoS inheritance from the child circuit group and its parent. If a parent circuit group is homed to a port or link group, its children circuit groups are implicitly homed to the same port or link group. QoS attributes configured on a parent circuit group are inheritable to its non-circuit-group members and to the members of its constituent circuit groups in a hierarchical way.

Use the **no** form of the **circuit-group** command to remove the specified circuit group, its children circuit groups, and all **circuit-group-member** commands that reference those circuit groups from the configuration.

For more information about circuit groups and VPCGs, see *Configuring Circuits for QoS*.

1.14.6 Examples

The following example shows how to create a nonhomed circuit group named **group7** and configure policing and metering policies to apply to this circuit group and its members:

```
[local]Redback(config)#circuit-group group7
[local]Redback(config-circuit-group)#qos policy policing group_policing_policy hierarchical
[local]Redback(config-circuit-group)#qos policy metering group_metering_policy inherit
```

The following example shows how to create a homed circuit group named **group8** that resides on slot 1, port 2. A queuing policy named **MyPolicy** is configured to apply to this circuit group and its members:

```
[local]Redback(config)#circuit-group group8 port 1/2
[local]Redback(config-circuit-group)#qos policy queuing MyPolicy
```

The following example shows how to define a VPCG named **vp10** that resides on slot 1, port 1. A queuing policy named **pwfq1** is configured to apply to this circuit group and its members:

```
[local]Redback(config)#circuit-group vp10 port 1/1 virtual port
[local]Redback(config-circuit-group)#qos policy queuing pwfq1
```

The following example shows nested circuit groups. In this example, a circuit group **parentCG** is defined. A hierarchical policing policy (**parent-Police**) is configured to apply to this circuit group and its members. The parent circuit group (**parent-Police**) has two children, which are also circuit groups— **childCG1** and **childCG2**. Both policing policies **parent-Police** and **child-Police** are applied to the circuit groups **childCG1** and **childCG2**. Specifying the **hierarchical** keyword on the parent circuit-group binding and the `inherit` keyword on the child circuit-group bindings allows both policies to be enforced on the members of the child circuit groups.

```
[local]Redback(config)#circuit-group parentCG port 1/1x
[local]Redback(config-circuit-group)#qos policy policing parent-Police hierarchical
[local]Redback(config)#circuit-group childCG1 parent-circuit-group parentCG
[local]Redback(config-circuit-group)#qos policy policing child-Police inherit
[local]Redback(config)#circuit-group childCG2 parent-circuit-group parentCG
[local]Redback(config-circuit-group)#qos policy policing child-Police inherit
```

The following example shows how to configure multiple levels of nested circuit groups. In the example, a circuit group **parentCG2** is defined. Policies for policing (**Hi-Police**), metering (**Hi_Meter**), and queuing (**TMPOLICY5**) are configured to apply to this circuit group and its members. For circuit group **childCG1**, the parent circuit group **parentCG2** is specified to indicate that this is the parent circuit group on which all circuits in this group (**childCG1**) are subject to inheritance from. For circuit group **childCG2**, the parent circuit group **childCG1** is specified to indicate that this is the parent circuit group on which all circuits in this group (**childCG2**) are subject to inheritance from. Lastly, For circuit group **childCG3**, the parent circuit group **childCG2** is specified to indicate that this is the parent circuit group on which all circuits in this group (**childCG3**) are subject to inheritance from. The child and grandchildren of circuit group **parentCG2** are to inherit the QoS policies configured in this circuit group:

```
[local]Redback(config)#circuit-group parentCG2 port 1/1
[local]Redback(config-circuit-group)#qos policy policing Hi-Police hierarchical
[local]Redback(config-circuit-group)#qos policy metering Hi-Meter hierarchical
[local]Redback(config-circuit-group)#qos policy queuing TMPOLICY5

[local]Redback(config)#circuit-group childCG1 parent-circuit-group parentCG2
[local]Redback(config)#circuit-group childCG2 parent-circuit-group childCG1
[local]Redback(config)#circuit-group childCG3 parent-circuit-group childCG2
```

1.15 circuit-group-member

`circuit-group-member` *`name`*

`no circuit-group-member` [*`name`*]

1.15.1 Purpose

Specifies that the 802.1Q PVC or PVCs or subscriber being configured are members of the specified circuit group.

1.15.2 Command Mode

- dot1q PVC configuration
- access link-group PVC configuration
- subscriber configuration (default subscriber profile, subscriber profile or subscriber record)

1.15.3 Syntax Description

name	Name of a configured circuit group, which is an alphanumeric string comprising up to 39 characters.

1.15.4 Default

Dot1q PVCs and subscribers are not members of circuit groups.

1.15.5 Usage Guidelines

Use the **`circuit-group-member`** command to specify that the 802.1Q PVC or PVCs or subscriber being configured are to be members of the specified circuit group.

Note: Each circuit may belong to a maximum of one circuit group.

Use the **`no`** form of this command to remove the specified dot1q PVC or PVCs from any circuit group to which it currently belongs. The ***name*** argument is optional in this case. Using the **`no`** form of this command to remove the circuit-group membership from a subscriber record or profile has no effect on the active subscriber sessions associated with the record or profile belonging to the circuit group. However, new subscriber's circuits will not become members of the circuit group once up.

Note: You must explicitly remove a circuit from an existing circuit group membership (by using the **`no`** option of **`circuit-group-member`** command) before assigning it to a new circuit group.

For more information about circuit group membership, see *Circuit Groups*.

1.15.6 Examples

The following example shows how to define a circuit group named **group7** and then specify a range of dot1q PVCs (50 through 60) that is to be a member of the circuit group:

```
[local]Redback(config)#circuit-group group7
[local]Redback(config-circuit-group)#qos policy policing group
_policing_policy hierarchical
[local]Redback(config-circuit-group)#qos policy
metering group_metering_policy inherit

[local]Redback(config)#port ethernet 12/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 50 through 60
[local]Redback(config-dot1q-pvc)#circuit-group-member group7
```

The following example shows how to define a virtual port circuit groups (VPCG) named **myVP1** and then specify a dot1q PVC tunnel that is to be a member of the VPCG:

```
[local]Redback(config)#circuit-group myVP1 port 1/1 virtual-port
[local]Redback(config)#port ethernet 1/1
[local]Redback(config-port)#dot1q pvc 1 encap 1qtunnel
[local]Redback(config-dot1q-pvc)#circuit-group-member myVP1
[local]Redback(config-dot1q-pvc)#qos rate max 1000000
[local]Redback(config-dot1q-pvc)#dot1q pvc 1:1
[local]Redback(config-dot1q-pvc)#qos policy queuing pwfq2
```

The following example shows how to define a VPCG named **myVP2** and then specify a subscriber profile named **isp2** that specifies membership in the VPCG:

```
[local]Redback(config)#circuit-group myVP2 port 1/1 virtual-port
[local]Redback(config-circuit-group)#qos policy queuing pwfq1
[local]Redback(config)#context zone1
[local]Redback(config-ctx)#subscriber profile isp2
[local]Redback(config-sub)#circuit-group-member myVP2
```

1.16 circuit mtu

```
circuit mtu size
```

```
no circuit mtu
```

1.16.1 Purpose

Configures the Intermediate System-to-Intermediate System (IS-IS) interface maximum transmission unit (MTU) size independent of the IP interface MTU size.

1.16.2 Command Mode

IS-IS interface configuration

1.16.3 Syntax Description

size MTU size. The range of values is 256 to 9,198.

1.16.4 Default

None

1.16.5 Usage Guidelines

Use the **circuit mtu** command to configure the IS-IS interface MTU size independent of the IP interface MTU size. This configuration command decouples the IS-IS packet MTU and IP packet MTU, if needed, because IS-IS link-state packets must be flooded over all the IS-IS interfaces without link fragmentation. You can use this command to ensure that the maximum size of link-state packets are be transmitted to all the neighbors while ensuring that IP packets delivery remains efficient.

Use the **no** form of this command to use the same MTU size for the IS-IS interface and the IP interface.

1.16.6 Examples

The following IS-IS interface configuration shows an IS-IS running over Ethernet. Not all the routers on this Ethernet LAN can handle IS-IS packets over 1,500 bytes, and this Ethernet interface MTU is above 1,500 bytes, thus the user sets the IS-IS MTU different from the IP interface MTU:

```
[local]Redback(config-ctx)#router isis ip-backbone
[local]Redback(config-isis)#interface ge10/1
[local]Redback(config-isis-if)#circuit mtu 1500
```

1.17 circuit protocol

```
circuit protocol encaps-type

no circuit protocol encaps-type
```

1.17.1 Purpose

Creates a child circuit on a multiprotocol Asynchronous Transfer Mode (ATM) or 802.1Q permanent virtual circuit (PVC), specifies an encapsulation for it, and enters ATM or dot1q child protocol configuration mode.

1.17.2 Command Mode

- ATM PVC configuration
- dot1Q PVC configuration

1.17.3 Syntax Description

encaps-type Type of encapsulation for the circuit, according to one of the following keywords:

- **ipv6oe**—Specifies IP Version 6 (IPv6) over Ethernet (IPv6oE) protocol.
- **pppoe**—Specifies Point-to-Point Protocol over Ethernet (PPPoE) protocol.

1.17.4 Default

No child circuit is created for a multiprotocol ATM or 802.1Q PVC.

1.17.5 Usage Guidelines

Use the **circuit protocol** command to create a child circuit on a multiprotocol ATM or 802.1Q PVC, specify a protocol for it, and then enter ATM or dot1q child protocol configuration mode.

You must have specified the **multi** keyword when you created the ATM PVC using the **atm pvc** command (in ATM OC configuration mode), or when you created the 802.1Q PVC using the **dot1q pvc** command (in port configuration mode); otherwise, you cannot create child circuits on the ATM or 802.1Q PVC.

This command, together with the **xc** command (in global configuration mode), acts as a filter on a multiprotocol ATM or 802.1Q PVC to pass only the type of packets specified by the value of the *encaps-type* argument.

Use the **no** form of this command to delete the circuit.

Use the **circuit protocol** command to create a child circuit on an 802.1Q PVC, specify a protocol for it, and then enter dot1q child protocol configuration mode.

This command, together with the **xc** command (in global configuration mode), acts as a filter on an 802.1Q PVC to pass only the type of packets specified by the value of the *encaps-type* argument.

Use the **no** form of this command to delete the circuit.

1.17.6 Examples

The following example shows how to create an ATM PVC encapsulated to support multiple protocols and creates an IPv6oE-encapsulated child circuit on that PVC. Only incoming IPv6oE-encapsulated packets are passed through the cross-connection:

```
[local]Redback(config)#port atm 3/1
[local]Redback(config-atm-oc)#atm pvc 10 10 profile pf3 encapsulation multi
[local]Redback(config-atm-pvc)#circuit protocol ipv6oe
[local]Redback(config-atm-child-proto)#
```

The following example shows how to create an 802.1Q PVC encapsulated to support multiple protocols and creates a PPPoE-encapsulated child circuit on that PVC. Only incoming IPv6oE-encapsulated packets are passed through the cross-connection:

```
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 10 profile pf2 encapsulation multi
[local]Redback(config-dot1q-pvc)#circuit protocol pppoe
[local]Redback(config-dot1q-child-proto)#
```

1.18 circuit type

circuit type {**level-1** | **level-1-2** | **level-2-only**}

no circuit type

1.18.1 Purpose

Configures the type of Intermediate System-to-Intermediate System (IS-IS) adjacency on the interface.

1.18.2 Command Mode

IS-IS interface configuration

1.18.3 Syntax Description

level-1
Establishes level 1 adjacencies on the interface.

level-1-2
Establishes level 1 and 2 adjacencies with neighbors that are configured for both levels and that share a common area. Level 2 adjacencies are established for neighbors that do not have a common area.

level-2-only
Establishes level 2 adjacencies on the interface.

1.18.4 Default

The circuit type is level 1 and level 2.

1.18.5 Usage Guidelines

Use the **circuit type** command to configure the type of IS-IS adjacency on the interface.

Use the **no** form of this command to restore the setting to the default type of level 1 and level 2.

1.18.6 Examples

The following example configures the circuit type to **level-2** for the **fa4/1** interface running the **ip-backbone** IS-IS instance. Level 1 Hello packets are not sent on the **fa4/1** interface:

```
[local]Redback(config-ctx)#router isis ip-backbone
[local]Redback(config-isis)#interface fa4/1
[local]Redback(config-isis-if)#circuit type level-2-only
```

1.19 class

class ***class-name***

no class ***class-name***

1.19.1 Purpose

Creates a class in a class-based policy and accesses policy group class configuration mode.

1.19.2 Command Mode

policy group configuration

1.19.3 Syntax Description

class-name Class name for a class of traffic packets to which the policy applies an action.

1.19.4 Default

None

1.19.5 Usage Guidelines

Use the **`class`** command to create a class in a class-based policy and access policy group class configuration mode. This command allows a forward policy, a Network Address Translation (NAT) policy, or a quality of service (QoS) policy to apply a different action to different sets (classes) of packets that are defined in the applied policy access control list (ACL).

If the ***`class-name`*** argument matches a ***`class-name`*** argument in a rule in the policy ACL, the class-based policy processes packets of that type as specified by the class-based policy. If a rule for the ***`class-name`*** argument is not specified in the policy ACL, the class-based policy considers the class to be dormant and takes no action. If a rule for the ***`class-name`*** argument is specified in the ACL, but you do not include the class in the policy (using this command), the SmartEdge router considers those packets to be in the default class.

Use the **`no`** form of this command to delete the specified class.

1.19.6 Examples

The following example applies the **QoSACL-1** policy ACL to a QoS policing policy that prioritizes incoming packets in the **Web** class using a Differentiated Service Code Point (DSCP) value of **DF**. For the **VOIP** class, incoming traffic packets are prioritized with a DSCP value of **AF11:**

```
[local]Redback(config-policy-policing)#access-group QoSACL-1 local
[local]Redback(config-policy-group)#class Web
[local]Redback(config-policy-group-class)#rate 6000 burst 3000
[local]Redback(config-policy-class-rate)#exceed mark dscp DF
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#class VOIP
[local]Redback(config-policy-group-class)#mark dscp AF11
```

The following example shows how to apply the **PBR_ACL** policy ACL to the **MirrorPolicy** forward policy, which mirrors all traffic packets in the **Web** class to the mirror output destination, **WebTraffic:**

```
[local]Redback(config)#forward policy MirrorPolicy
[local]Redback(config-policy-frwd)#access-group PBR_ACL local
[local]Redback(config-policy-group)#class Web
[local]Redback(config-policy-group-class)#mirror destination WebTraffic all
```

1.20 class-group

```
class-group class-definition-name
```

```
no class-group
```

1.20.1 Purpose

Specifies a class definition and enters policy group configuration mode.

1.20.2 Command Mode

- metering policy configuration
- policing policy configuration

1.20.3 Syntax Description

`class-definition-name`	Class definition name. Alphanumeric string of up to 39 characters.

1.20.4 Default

No class definition is assigned to a policing or metering policy.

1.20.5 Usage Guidelines

Use the **`class-group`** command to specify a class definition and enter policy group configuration mode. A packet subject to the policing or metering policy being configured is assigned a class according to the referenced class definition. In policy group configuration mode, you can reference class names defined in the class definition and assign actions to perform on packets assigned to a class. You can configure any command or action that is available for policy access control list (ACL) classes or for class-definition classes.

Class-definition policing or metering is an alternative to ACL policing or metering. For each metering or policing policy, you can specify either an ACL group or a class group, but not both. Unlike ACL metering and policing policies, which require access to the packet's IP header, you can apply class-definition metering and policing policies to Layer 2 circuits, such as Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) sessions, Layer 2 Virtual Private Networks (VPNs) and cross-connections, and bridged circuits. When you apply policing and metering policies to Layer 2 circuits, you cannot use the **`mark dscp`** and **`mark precedence`** commands to mark packets and assign priority because these commands also require access to the packet's IP header. When a packet arrives, the SmartEdge router applies any ingress classification propagation and mapping to determine a packet's initial packet descriptor (PD) value. If you use a class definition to apply a policing policy, the resulting PD value for the packet determines its class.

You can use class-definition policing or metering to propagate quality of service (QoS) settings without configuring classification maps.

Use the **qos class-definition** command (in global configuration mode) to define a class definition to be referenced by a metering or policing policy.

Use the **no** form of this command to remove the class group reference.

1.21 cleanup-timer

cleanup-timer

timeout-sec

{**no** | **default**} **cleanup-timer**

1.21.1 Purpose

Configures the L2TP tunnel teardown value.

1.21.2 Command Mode

L2TP peer configuration

1.21.3 Syntax Description

timeout-sec	The number of seconds the cleanout timer is set to. Enter a number from 1 to 28,800.

1.21.4 Default

For tunnels with named peers, the L2TP tunnel does not time out even when no subscriber sessions have been connected. For tunnels with unnamed peers, the default timeout is 60 seconds.

Use the **no** or **default** form of this command to disable any timeout settings that have been configured by this command and return the L2TP tunnel to the default timeout condition.

1.21.5 Usage Guidelines

Use the **cleanup-timer** command to configure the L2TP tunnel teardown value. If no subscriber sessions have been the connected over the L2TP tunnel for a time greater than or equal to the specified time, the tunnel is disconnected.

Supported on all line cards.

1.21.6 Examples

The following example shows how this command is used:

```
[local]Redback(config-ctx)#l2tp-peer default
[local]Redback(config-l2tp)#cleanup-timer 12000
```

1.22 clear aaa route subscriber aggregate

clear aaa route subscriber aggregate

1.22.1 Purpose

Clears all routes downloaded from the route download server. In addition, if this command is issued, the SmartEdge router ceases to attempt to download the routes. However, if the interval timer expires, then the SmartEdge router initiates a download. Alternatively, a download must be manually initiated using the *download aaa route* command.

1.22.2 Command Mode

exec

1.22.3 Examples

```
[local]Redback#clear aaa route subscriber aggregate
```

1.23 clear access-group

To clear policy access control list (ACL) counters associated with a forward or quality of service (QoS) metering or policing policy, the syntax is:

clear access-group {forward | qos}{*slot/port: ch: sub* [*:subsub*]} | l2tp lns *l2tp-id* | {bvi id *id*} | {l2vpn-cross-connect [*l2vpn-profile*]} | {lg id *id*} | mip-fa [*cir-id*] | mip-ha [*cir-id*] | mp *mp-id*} {in | out} counters

To clear policy ACL counters for a Network Address Translation (NAT) policy, the syntax is:

clear access-group nat interface *if-name* in counters

To clear IP ACL counters for incoming traffic on a reverse path forwarding (RPF) interface, the syntax is:

clear access-group rpf interface *if-name* in counters

To clear administrative or IP ACL counters applied to a circuit or interface, the syntax is:

```
clear access-group ip-filter {admin | {slot/port:
ch: sub [:subsub]} | l2tp lns l2tp-id | {bvi id id} |
{l2vpn-cross-connect [l2vpn-profile]} | {lg id id} | mip-fa
[cir-id] | mip-ha [cir-id] | mp mp-id} | interface if-name}
{in | out} {all | counters | log}
```

To clear IPv6 policy access control list (ACL) counters for a forward or quality of service (QoS) metering or policing policy, the syntax is:

```
clear access-group ipv6 {forward | qos} {slot/port:
ch: sub [:subsub] | lt2p lns l2tp-id | {bvi id id} |
{l2vpn-cross-connect [l2vpn-profile]} | {lg id id} | mip-fa
[cir-id] | mip-ha [cir-id] | mp mp-id } {in | out} counters
```

To clear IPv6 administrative or IP Filter ACL counters applied to a circuit or interface, the syntax is:

```
clear access-group ipv6 filter {admin | {slot/port:
ch: sub [:subsub] | {bvi id id} | {l2vpn-cross-connect
[l2vpn-profile]} | {lg id id} | mip-fa [cir-id] | mip-ha
[cir-id] mp mp-id} | interface if-name} {in | out} {all |
counters}
```

1.23.1 Purpose

Clears counters for the ACLs that are applied to the specified port, channel, circuit, or interface.

1.23.2 Command Mode

exec (10)

1.23.3 Syntax Description

`filter`	Clears IPv6 filter ACL.
`forward`	Clears policy ACL counters for a forward policy.
`ipv6`	Clears IPv6 qos and forward policy ACL and Filter ACL
`qos`	Clears policy ACL counters for a QoS metering or policing policy.
`nat`	Clears policy ACL counters for a NAT policy.
`rpf`	Clears policy ACL counters for incoming traffic on an RPF interface.
`ip-filter`	Clears policy ACL counters applied to a circuit or interface.

circuit-filter — Circuit filter, which is defined as:

slot[/*port*[:*chan-num*[:*sub-chan-num*]] [*circuit-id*]]

l2tp lns *l2tp-id* — Layer Two Tunneling Protocol (L2TP) circuit identifier. Limits the output to the specified L2TP network server (LNS) circuit.

bvi id *id* — Bridged virtual interface ID <id>

l2vpn-cross-connect [*l2vpn-profile*] — L2VPN cross-connect circuit [<L2vpn-cross-connect profile identifier>]

lg id *id* — Link group ID <id>

mip-fa [*cir-id*] — Mobile-IP Foreign Agent [<circuit-id>]

mip-ha [*cir-id*] — Mobile-IP Home Agent [<circuit-id>]

mp *mp-id* — Merge point (MP) circuit identifier. Limits the output to the specified MP circuit.

interface *if-name* — Name of the interface for which information is to be displayed.

in — Specifies incoming traffic on the circuit.

out — Specifies outgoing traffic on the circuit. Not available for NAT policies, RPF interfaces, or administrative ACLs.

counters — Clears ACL hit counters.

admin — Clears counters for the administrative ACL.

all — Optional. Clears ACL hit counters and deny log entries. Available only with the **ip-filter** keyword.

log — Optional. Clears ACL deny log entries. Available only with the **ip-filter** keyword.

Keywords and arguments for the *circuit-filter* argument are:

slot — Chassis slot number for a particular card.

port — Optional. Port number on the specified card.

chan-num — Optional. Channel number for which circuits are displayed. If omitted, displays circuits for all channels on the specified port. The range of values depends on the type of port.

sub-chan-num — Optional. Subchannel number for which circuits are displayed. If omitted, displays circuits on all subchannels in the specified channel. The range of values depends on the type of port.

circuit-id — Optional. Circuit identifier, which is defined as:

clips *clips-id* | **dlci** *dlci* | **pppoe** *session-id* | **vlan** *vlan-id* | **vpi-vci** *vpi vci*

If omitted, clears policy ACL counters for all circuits on the specified card, port, or channel.

clips ***clips-id***

Clientless IP service selection (CLIPS) circuit on a port, channel, 802.1Q PVC, or ATM PVC. The range of values is 1 to 262144. If the CLIPS circuit is on an 802.1Q or ATM PVC, you specify this construct in addition to the circuit identifier for the 802.1Q or ATM PVC.

dlci ***dlci***

Data-link connection identifier (DLCI) for the Frame Relay permanent virtual circuit (PVC). The range of values is 16 to 991.

pppoe ***session-id***

Point-to-Point Protocol over Ethernet (PPPoE) session identifier. The range of values is 1 to 65535.

vlan ***vlan-id***

Virtual LAN (VLAN) tag value for an 802.1Q tunnel or PVC. The vlan-id argument is one of the following constructs:

- ***pvc-vlan-id***—VLAN tag value of a PVC that is not within an 802.1Q tunnel. If you specify the VLAN tag value for an 802.1Q tunnel, the output includes subscriber information for all the PVCs within the tunnel.
- ***tunl-vlan-id***—VLAN tag value of a tunnel.
- ***tunl-vlan-id:pvc-vlan-id***—VLAN tag value for the tunnel followed by the VLAN tag value for the PVC within the tunnel.

The range of values for any VLAN tag value is 1 to 4095.

vpi-vci ***vpi vci***

Virtual path identifier (VPI) and virtual circuit identifier (VCI) for an ATM PVC. The range of values is 0 to 255 and 1 to 65,535, respectively. By convention, VCI 1 to 31 are reserved for system use.

1.23.4 Default

None

1.23.5 Usage Guidelines

Use the **clear access-group** command to clear counters for the ACLs that are applied to the specified port, channel, circuit, or interface.

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

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

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

1.23.6 Examples

The following example shows how to clear forward policy ACL counters for incoming traffic on port **1** of the line card installed in slot **1:**

```
[local]Redback#clear access-group forward 1/1 in counters
```

The following example shows how to clear counters for policy ACLs used with the NAT policy applied to the `if-nat-1` interface:

```
[local]Redback#clear access-group nat interface if-nat-1 in counters
```

The following example shows how to clear QoS policy ACL counters for the incoming traffic on port **1** of the line card installed in slot **1:**

```
[local]Redback#clear access-group qos 1/1 in counters
```

The following example shows how to clear RPF hit counters for IP ACLs applied to the RPF **eth1** interface:

```
[local]Redback#clear access-group rpf interface eth1 in counters
```

The following example shows how to clear hit counters and deny log entries for the administrative port ACL:

```
[local]Redback#clear access-group ip-filter admin in all
```

The following example shows how to clear forward IPv6 policy ACL counters for incoming traffic on port 1 of the line card installed in slot 1:

```
[local]Redback#clear access-group ipv6 forward 1/1 in counters
```

The following example shows how to clear IPv6 QoS policy ACL inbound counters for L2TP LNS circuits.

```
[local]Redback#clear access-group ipv6 qos l2tp lns 1 in counters
```

1.24 clear access-line

clear access-line {**agent-circuit-id** ***string*** | **all** | **neighbor** ***ip-addr***[**:*remote-port***]}

1.24.1 Purpose

Deletes the digital subscriber line (DSL) attributes that the system has learned from the DSL access multiplexer (DSLAM) for the selected DSLs.

1.24.2 Command Mode

exec

1.24.3 Syntax Description

`agent-circuit-id` Selects the DSL with this circuit agent ID only.

`string` Circuit agent ID. A text string, with up to 63 printable characters; enclose the string in quotation marks (“ ”) if the string includes spaces.

`all` Selects all access lines.

`neighbor` Selects the DSLs attached to this Access Node Control Protocol (ANCP) neighbor peer with the specified IP address and Transmission Control Protocol (TCP) port number.

`ip-addr` IP address for the ANCP neighbor peer.

`remote-port` Optional. TCP port number for this ANCP neighbor peer. The range of values is 1 to 65535. If not specified, selects the DSLs of all neighbors with the specified IP address.

1.24.4 Default

None

1.24.5 Usage Guidelines

Use the **`clear access-line`** command to delete the DSL attributes that the system has learned from the DSLAM for the selected DSLs. This command deletes only the attributes that the system has learned from the ANCP; it does not delete those attributes learned from the signaling described in the DSL Forum TR-101, `Migration to Ethernet-Based DSL Aggregation` document.

For every selected DSL, if the DSL port on the DSLAM was signaled as down (with a Port-Down message) or if the connection to the associated ANCP neighbor peer is down, the DSL attributes are deleted.

Note: If the state of a DSL line is **SHOWTIME**, the associated DSL attributes are not deleted.

Note: This command does not delete attributes from any DSL that is signaled as up and for which an ANCP connection is still up.

1.24.6 Examples

The following example shows how to delete DSL attributes for circuit agent ID **abc-2.1:**

```
[local]Redback#clear access-line agent-circuit-id abc-2.1
```

1.25 clear administrator

`clear administrator` ***`admin-name`*** [***`tty-name`***]

1.25.1 Purpose

Terminates one or all of an administrator’s remote (Telnet or Secure Shell [SSH]) terminal sessions.

1.25.2 Command Mode

exec

1.25.3 Syntax Description

`admin-name`	Name of the administrator whose sessions are to be terminated.
`tty-name`	Optional. Name of the teletypewriter (TTY) for a particular session to be terminated.

1.25.4 Default

If you use this command without the optional ***`tty-name`*** argument, all sessions for the specified administrator are cleared.

1.25.5 Usage Guidelines

Use the **`clear administrator`** command to end one or all of an administrator’s remote terminal sessions with the following criteria:

- An administrator in the local context can end any administrator session.

- Administrators in any other context can end sessions only in their own context.

- This command does not end the current session.

Use the optional ***`tty-name`*** argument to indicate a specific terminal session to be cleared. If you use the command without this argument, all of the specified administrator’s sessions are cleared. The output of the **`show administrators`** command (in exec mode) displays the TTY names.

1.25.6 Examples

The following example shows how to clear a single terminal session for a administrator, **test:**

```
[local]Redback#clear administrator test ttyp2
```

1.26 clear ancp neighbor

clear ancp neighbor {**all** | **ip-address** ***ip-addr*:*remote-port***] | **profile** ***prof-name***} [**purge**]

1.26.1 Purpose

Terminates the Transmission Control Protocol (TCP) connection for Access Node Control Protocol (ANCP) sessions for one or more ANCP neighbor peers.

1.26.2 Command Mode

exec (10)

1.26.3 Syntax Description

all Clears all ANCP neighbor peers.

ip-address ***ip-addr*** IP address of the ANCP neighbor peer.

remote-port Optional. TCP port number. The range of values is 1 to 65,535.

profile ***prof-name*** Clears the ANCP neighbor peers that use this ANCP neighbor profile.

purge Optional. Forces all digital subscriber line (DSL) attributes that have been learned from this ANCP neighbor peer to be deleted, and to restore subscriber rates to the values specified in the quality of service (QoS) policies that are attached to the subscriber circuits.

1.26.4 Default

None

1.26.5 Usage Guidelines

Use the **clear ancp neighbor** command to terminate the TCP connection for ANCP sessions for one or more ANCP neighbor peers.

Use the **purge** keyword to delete the DSL attributes for all DSLs managed by this ANCP neighbor peer and restore the subscriber rates to the values specified in the QoS policies that are attached to the subscriber circuits. This keyword initiates a warning message that purging the attributes for the subscriber connections can possibly cause service degradation, and asks for confirmation. The DSL attributes are deleted only after all subscriber sessions are ended on this ANCP neighbor peer.

1.26.6 Examples

The following example shows how to terminate ANCP sessions with the ANCP neighbor peer with IP address **10.1.1.1:**

```
[local]Redback#clear ancp neighbor 10.1.1.1
```

1.27 clear ancp neighbor statistics

clear ancp neighbor {**all** | **ip-address** ***ip-addr***[**:*remote-port***] | **profile** ***prof-name***} **statistics**

1.27.1 Purpose

Clears Access Node Control Protocol (ANCP) neighbor statistics for one or more ANCP neighbor peers.

1.27.2 Command Mode

exec (10)

1.27.3 Syntax Description

all	Clears all ANCP neighbor peers.
ip-address *ip-addr*	IP address of the ANCP neighbor peer.
remote-port	Optional. Transmission Control Protocol (TCP) port number. The range of values is 1 to 65,535.
profile *prof-name*	Clears the ANCP neighbor peers that use this ANCP neighbor profile.

1.27.4 Default

None

1.27.5 Usage Guidelines

Use the **`clear ancp neighbor statistics`** command to clear ANCP neighbor statistics for one or more ANCP neighbor peers. Display these statistics with the **`show ancp neighbor statistics`** command (in any mode).

1.27.6 Examples

The following example shows how to clear ANCP neighbor statistics for **all** ANCP neighbor peers:

```
[local]Redback#clear ancp neighbor all statistics
```

1.28 clear arp-cache

`clear arp-cache` [*`ip-addr`*]

1.28.1 Purpose

Clears all entries from the Address Resolution Protocol (ARP) table.

1.28.2 Command Mode

exec (10)

1.28.3 Syntax Description

`ip-addr`	Optional. Specific host IP address to be cleared from the ARP table.

1.28.4 Default

No entries are cleared from the ARP table.

1.28.5 Usage Guidelines

Use the **`clear arp-cache`** command to clear all ARP table entries.

Use the *`ip-addr`* argument to clear the specified host IP address from the ARP table.

1.28.6 Examples

The following example shows how to clear all ARP table entries:

```
[local]Redback#clear arp-cache
```

The following example shows how to clear the IP address, **43.56.26.45**, from the ARP table:

```
[local]Redback#clear arp-cache 43.56.26.45
```

1.29 clear arp-cache interworking

`clear arp-cache interworking` ***`slot`*****/*****`port`*** [**`vlan`** ***`vlan-id`***]

1.29.1 Purpose

Clears information for cross-connections between Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs) and 802.1Q PVCs from the Address Resolution Protocol (ARP) table.

1.29.2 Command Mode

exec (10)

1.29.3 Syntax Description

slot	Chassis slot number.(1)
port	Line card port number.
vlan-id *vlan-id*	Optional. Virtual LAN (VLAN) tag value for the 802.1Q PVC. The range of values is 1 to 4,095. If omitted, clears the ARP cache for the entire circuit.

(1) The SmartEdge 100 router limits the value of the slot argument to 2.

1.29.4 Default

None

1.29.5 Usage Guidelines

Use the **`clear arp-cache interworking`** command to clear information for cross-connections between ATM PVCs and 802.1Q PVCs from the ARP table.

Note: The command used to configure interworking cross-connections is the **`xc`** command (in global configuration mode); for more information, see *Configuring Cross-Connections*.

1.29.6 Examples

The following example shows how to clear information for VLAN ID **1** from the ARP table:

```
[local]Redback#clear arp-cache interworking 2/1 vlan-id 1
```

1.30 clear arp-cache statistics

```
clear arp-cache statistics
```

1.30.1 Purpose

Clears traffic statistics from the Address Resolution Protocol (ARP) table.

1.30.2 Command Mode

exec (10)

1.30.3 Syntax Description

This command has no keywords or arguments.

1.30.4 Default

Statistics are not cleared from the ARP table.

1.30.5 Usage Guidelines

Use the **`clear arp-cache statistics`** command to clear traffic statistics from the ARP table.

1.30.6 Examples

The following example shows how to clear traffic statistics from the ARP table:

```
[local]Redback#clear arp-cache statistics
```

1.31 clear as-path-list

`clear as-path-list` ***`apl-name`*** **`counters`**

1.31.1 Purpose

Clears match and cache hit counts for a specified Border Gateway Protocol (BGP) autonomous system (AS) path list.

1.31.2 Command Mode

exec (10)

1.31.3 Syntax Description

`apl-name`	AS path list name.
`counters`	Clears match and cache hit counts for the specified AS path list.

1.31.4 Default

None

1.31.5 Usage Guidelines

Use the **`clear as-path-list`** command to clear match and cache hit counts for a specified BGP AS path list.

Note: A reference to an AS path list that does not exist, or does not contain any configured entries, implicitly matches and permits all AS paths.

1.31.6 Examples

The following example shows how to clear match and cache hit counts for the **aslist1** AS path list:

```
[local]Redback#clear as-path-list aslist1
```

1.32 clear atm circuit

clear atm circuit [**all**] {**all** | ***slot***/***port*** [**all** | **vpi** ***vpi*** [**all** | **vci** ***start-vci*** [**through** ***end-vci***]]]}

1.32.1 Purpose

Clears one or more Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs).

1.32.2 Command Mode

exec (10)

1.32.3 Syntax Description

all	Optional. Clears all ATM PVCs on the system, the specified port, or the specified virtual path (VP).
slot	Optional. Chassis slot number of the ATM line card with the ATM PVCs to be cleared.
port	Required if you enter the ***slot*** argument. Port number with ATM PVCs to be cleared.
vpi ***vpi***	Optional. Virtual path identifier (VPI) of the ATM PVCs to be cleared. The range of values is 0 to 255.
vci ***start-vci***	Optional. Virtual channel identifier (VCI). The range of values is 1 to 65535. By convention, values 1 to 31 are reserved for system use.
through ***end-vci***	Optional. Last VCI when clearing a range of PVCs.

1.32.4 Default

None

1.32.5 Usage Guidelines

Use the **clear atm circuit** command to clear one or more ATM PVCs and all the subscriber sessions on it. If an ATM PVC was created on demand, it is deleted. This command is available only in the local context.

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

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

Use the `all` keyword to clear all ATM PVCs on the system, specified port, or specified VP.

1.32.6 Examples

The following example shows how to clear all ATM PVCs on the system:

```
[local]Redback#clear atm circuit all
```

The following example shows how to clear all ATM PVCs on port **1** of the ATM OC-3 line card in slot **4:**

```
[local]Redback#clear atm circuit 4/1 all
```

1.33 clear atm counters

clear atm counters [**all**] [*slot*/*port* [**vpi** *vpi* [**vci** *start-vci* [**through** *end-vci*]]]]

1.33.1 Purpose

Clears the traffic counters for one or more Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs).

1.33.2 Command Mode

exec (10)

1.33.3 Syntax Description

all — Optional. Clears counters for all PVCs in all contexts. This option is available only in the local context.

slot — Optional. Chassis slot number of the ATM line card with a port for which counters are cleared.

port — Optional. Port number of the ATM port for which counters are cleared.

vpi *vpi* — Optional. Virtual path identifier (VPI). The range of values is 0 to 255.

vci ***start-vci***	Optional. The start virtual channel identifier (VCI). The range of values is 1 to 65535. By convention, values 1 to 30 are reserved for system use.
through ***end-vci***	Optional. Last VCI when clearing counters for a range of PVCs.

1.33.4 Default

Clears all ATM counters for all ATM PVCs.

1.33.5 Usage Guidelines

Use the **clear atm counters** command to clear traffic counters for one or more ATM PVCs.

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

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

You must specify the **vpi** ***vpi*** and **vci** ***start-vci*** constructs to clear only the counters for a specific ATM PVC. Use the **through** ***end-vci*** construct to clear the counters for a range of VCIs. If you do not specify any optional constructs, the **clear atm counters** command clears all ATM counters for all ATM PVCs on the port in the current context.

1.33.6 Examples

The following example shows how to clear the traffic counters for the ATM PVC on port **1** on the ATM line card in slot **3:**

```
[local]Redback#clear atm counters 3/1
```

1.34 clear bgp

clear bgp {***** | **as** {***asn*** | ***nn*****:*****nn***} [**notify** | **soft** [**in** | **out**]]

1.34.1 Purpose

Resets Border Gateway Protocol (BGP) connections or forces BGP updates to be generated.

Note: The **clear bgp** command is used for test purposes only, and using it to apply new routing policies is no longer required, because routing policies are automatically updated.

1.34.2 Command Mode

exec (10)

1.34.3 Syntax Description

`*`	Resets or forces BGP updates for all BGP neighbor connections.
`as`	Resets or applies new routing policies for BGP neighbor connections in the specified autonomous system number (ASN).
`asn`	ASN in integer format. The range of values is 1 to 65,535. The subrange 64,512 to 65,535 is reserved for private autonomous systems. Resets or forces BGP updates for connections with the peers that belong to the specified AS.
`nn:nn`	ASN in 4-byte integer format, where the first *`nn`* indicates the two higher-order bytes and the second *`nn`* denotes the two lower-order bytes. Resets or forces BGP updates for connections with the peers that belong to the specified AS.
`notify`	Optional. Sends a notification message to neighbors. When neighbors receive the notification message, they immediately drop their connection.
`soft`	Optional. Does not drop the BGP connection, but forces BGP updates for the connection. If the `soft` keyword is not specified, the BGP connection is immediately dropped.
`in`	Optional. Forces inbound BGP updates for the connections only. Used only with the `soft` keyword. If the `in` or `out` optional keyword is not specified, both inbound and outbound BGP updates are forced for the connections.
`out`	Optional. Forces outbound BGP updates for the connections only. Used only with the `soft` keyword. If the `in` or `out` optional keyword is not specified, both inbound and outbound BGP updates are forced for the connections.

1.34.4 Default

None

1.34.5 Usage Guidelines

Use the `clear bgp` command to reset BGP connections, or to force BGP updates to be generated.

Note: The `clear bgp` command is used for test purposes only, and using it to apply new routing policies is no longer required, because routing policies are automatically updated.

Caution!

Risk of dropped connection. A hard reset can impact network connectivity. The **`soft`** keyword for inbound only takes effect if the BGP neighbor supports the refresh capability. The **`soft`** keyword for outbound is a local matter, and does not require the capability. To see if a BGP neighbor supports the refresh capability, use the **`show bgp neighbor summary`** command (in exec mode). Specify the **`soft`** keyword if you do not want the BGP neighbor connection dropped. To reduce the risk, only use a hard reset as a last resort.

Note: Prior to Release 2.5, when there was a change in an inbound or outbound routing policy, such as a prefix list, autonomous system (AS) path list, or route map, for a BGP peer, the **`clear bgp neighbor`** ***`ip-addr`*** **`soft`** [**`in`** | **`out`**] command had to be manually issued to make the policy change effective. Currently, routing policy changes automatically take effect, and issuing the **`clear bgp neighbor`** ***`ip-addr`*** **`soft`** [**`in`** | **`out`**] construct to update routing policies can cause updates to be unnecessarily sent; therefore, it is not recommended.

To aggregate multiple policy changes, the operating system performs the necessary action 15 seconds after a policy change.

1.34.6 Examples

The following example shows how to reset all BGP connections:

```
[local]Redback#clear bgp *
```

1.35 clear bgp external

`clear bgp external` [**`notify`** | **`soft`** [**`in`** | **`out`**]]

1.35.1 Purpose

Resets external Border Gateway Protocol (eBGP) connections or forces BGP updates to be generated for eBGP connections without dropping the connections.

1.35.2 Command Mode

exec (10)

1.35.3 Syntax Description

`notify` Optional. Sends a notification message to neighbors. When neighbors receive the notification message, they immediately drop their connection.

`soft` Optional. Does not drop the BGP connection, but forces BGP updates for the connection. If the **`soft`** keyword is not specified, the BGP connection is immediately dropped.

`in` Optional. Forces inbound BGP updates for the connections only. Used only with the **`soft`** keyword. If the **`in`** or **`out`** optional keyword is not specified, both inbound and outbound BGP updates are forced for the connections.

`out` Optional. Forces outbound BGP updates for the connections only. Used only with the **`soft`** keyword. If the **`in`** or **`out`** optional keyword is not specified, both inbound and outbound BGP updates are forced for the connections.

1.35.4 Default

None

1.35.5 Usage Guidelines

Use the **`clear bgp external`** command to reset eBGP connections or force BGP updates to be generated for eBGP connections without causing a hard reset (which drops connections immediately).

Caution!

Risk of dropped connection. A hard reset can impact network connectivity. The **`soft`** keyword for inbound only takes effect if the BGP neighbor supports the refresh capability. The **`soft`** keyword for outbound is a local matter, and does not require the capability. To see if a BGP neighbor supports the refresh capability, use the **`show bgp neighbor summary`** command (in exec mode). Specify the **`soft`** keyword if you do not want the BGP neighbor connection dropped. To reduce the risk, only use a hard reset as a last resort.

Note: Prior to Release 2.5, when there was a change in an inbound or outbound routing policy, such as a prefix list, autonomous system (AS) path list, or route map, for a BGP peer, the **`clear bgp neighbor`** ***`ip-addr`*** **`soft`** [**`in`** | **`out`**] command had to be manually issued to make the policy change effective. Currently, routing policy changes automatically take effect, and issuing the **`clear bgp neighbor`** ***`ip-addr`*** **`soft`** [**`in`** | **`out`**] command to update routing policies can cause updates to be unnecessarily sent; therefore, it is not recommended.

To aggregate multiple policy changes, the operating system performs the necessary action 15 seconds after a policy change.

1.35.6 Examples

The following example shows how to reset all eBGP connections:

```
[local]Redback#clear bgp external
```

1.36 clear bgp flap-statistics

`clear bgp flap-statistics` [***`ip-addr/prefix-length`*** | **`neighbor`** ***`ip-addr`*** | **`regex`** ***`reg-exp`***]

1.36.1 Purpose

Clears Border Gateway Protocol (BGP) connection route-flap statistics.

1.36.2 Command Mode

exec (10)

1.36.3 Syntax Description

`ip-addr`	Optional. IP address, in the form ***`A.B.C.D`***, and the prefix length, separated by the slash (`/`) character. The range of values for the ***`prefix-length`*** argument is 0 to 32.
`prefix-length`	Required when the ***`ip-addr`*** argument is used. The range of values is 0 to 32. Clears route-flap statistics for the specified prefix.
`neighbor` ***`ip-addr`***	Optional. Route-flap statistics for only the specified neighbor.
`regex` ***`reg-exp`***	Optional. Route-flap statistics for only routes matching the specified AS path regular expression.

1.36.4 Default

None

1.36.5 Usage Guidelines

Use the `clear bgp flap-statistics` command to clear BGP route-flap statistics.

1.36.6 Examples

The following example shows how to clear all BGP route-flap statistics:

```
[local]Redback#clear bgp flap-statistics
```

1.37 clear bgp ipv4 mdt

```
clear bgp ipv4 mdt {* | as {asn | nn:nn}} [soft [in | out]]
```

1.37.1 Purpose

Resets Border Gateway Protocol (BGP) IP Version 4 (IPv4) address connections or forces BGP updates to be generated for connections using multicast distribution tree (MDT) routes without dropping the connections.

1.37.2 Command Mode

exec (10)

1.37.3 Syntax Description

`*` Resets or forces BGP updates for all BGP neighbor connections.

`as` Resets or forces BGP updates to be generated for BGP neighbor connections in the specified autonomous system number (ASN).

`asn` ASN in integer format. The range of values is 1 to 65535. The subrange 64512 to 65535 is reserved for private autonomous systems. Resets or forces BGP updates for connections with the peers that belong to the specified AS.

`nn:nn` ASN in 4-byte integer format, where the first *`nn`* indicates the two higher-order bytes and the second *`nn`* denotes the two lower-order bytes. Resets or forces BGP updates for connections with the peers that belong to the specified AS.

soft	Optional. Does not drop the BGP connection, but forces BGP updates for the connection. If the **soft** keyword is not specified, the BGP connection is immediately dropped.
in	Optional. Forces inbound BGP updates for the connections only. Used only with the **soft** keyword. If the **in** or **out** optional keyword is not specified, both inbound and outbound BGP updates are forced for the connections.
out	Optional. Forces outbound BGP updates for the connections only. Used only with the **soft** keyword. If the **in** or **out** optional keyword is not specified, both inbound and outbound BGP updates are forced for the connections.

1.37.4 Default

None

1.37.5 Usage Guidelines

Use the **clear bgp ipv4 mdt** command to reset BGP IPv4 address connections or force BGP updates to be generated for connections using MDT routes without causing a hard reset (which drops the connection immediately).

Caution!

Risk of dropped connection. A hard reset can impact network connectivity. The **soft** keyword for inbound only takes effect if the BGP neighbor supports the refresh capability. The **soft** keyword for outbound is a local matter, and does not require the capability. To see if a BGP neighbor supports the refresh capability, use the **show bgp neighbor summary** command (in exec mode). Specify the **soft** keyword if you do not want the BGP neighbor connection dropped. To reduce the risk, only use a hard reset as a last resort.

Note: Prior to Release 2.5, when there was a change in an inbound or outbound routing policy, such as a prefix list, autonomous system (AS) path list, or route map, for a BGP peer, the **clear bgp neighbor** ***ip-addr*** **soft** [**in** | **out**] command had to be manually issued to make the policy change effective. Currently, routing policy changes automatically take effect, and issuing the **clear bgp neighbor** ***ip-addr*** **soft** [**in** | **out**] command to update routing policies can cause updates to be unnecessarily sent; therefore, it is not recommended.

To aggregate multiple policy changes, the operating system performs the necessary action 15 seconds after a policy change.

1.37.6 Examples

The following example shows how to reset all BGP MDT connections using IPv4 address prefixes:

```
[local]Redback#clear bgp ipv4 mdt *
```

1.38 clear bgp ipv4 multicast

clear bgp ipv4 multicast {***** | **as** {*asn* | *nn*:*nn*}} [**soft** [**in** | **out**]]

1.38.1 Purpose

Resets Border Gateway Protocol (BGP) IP Version 4 (IPv4) multicast address connections or forces BGP updates to be generated for connections using multicast address prefixes without dropping the connections.

1.38.2 Command Mode

exec (10)

1.38.3 Syntax Description

*****

Resets or forces BGP updates for all BGP neighbor connections.

as

Resets or forces BGP updates to be generated for BGP neighbor connections in the specified autonomous system number (ASN).

asn

ASN in integer format. The range of values is 1 to 65535. The subrange 64512 to 65535 is reserved for private autonomous systems. Resets or forces BGP updates for connections with the peers that belong to the specified AS.

nn:*nn*

ASN in 4-byte integer format, where the first *nn* indicates the two higher-order bytes and the second *nn* denotes the two lower-order bytes. Resets or forces BGP updates for connections with the peers that belong to the specified AS.

soft

Optional. Does not drop the BGP connection, but forces BGP updates for the connection. If the **soft** keyword is not specified, the BGP connection is immediately dropped.

`in`	Optional. Forces inbound BGP updates for the connections only. Used only with the **`soft`** keyword. If the **`in`** or **`out`** optional keyword is not specified, both inbound and outbound BGP updates are forced for the connections.
`out`	Optional. Forces outbound BGP updates for the connections only. Used only with the **`soft`** keyword. If the **`in`** or **`out`** optional keyword is not specified, both inbound and outbound BGP updates are forced for the connections.

1.38.4 Default

None

1.38.5 Usage Guidelines

Use the **`clear bgp ipv4 multicast`** command to reset BGP IPv4 address connections or force BGP updates to be generated for connections using multicast address prefixes without causing a hard reset (which drops the connection immediately).

Caution!

Risk of dropped connection. A hard reset can impact network connectivity. The **`soft`** keyword for inbound only takes effect if the BGP neighbor supports the refresh capability. The **`soft`** keyword for outbound is a local matter, and does not require the capability. To see if a BGP neighbor supports the refresh capability, use the **`show bgp neighbor summary`** command (in exec mode). Specify the **`soft`** keyword if you do not want the BGP neighbor connection dropped. To reduce the risk, only use a hard reset as a last resort.

Note: Prior to Release 2.5, when there was a change in an inbound or outbound routing policy, such as a prefix list, autonomous system (AS) path list, or route map, for a BGP peer, the **`clear bgp neighbor`** ***`ip-addr`*** `soft` [`in` | `out`] command had to be manually issued to make the policy change effective. Currently, routing policy changes automatically take effect, and issuing the **`clear bgp neighbor`** ***`ip-addr`*** `soft` [`in` | `out`] command to update routing policies can cause updates to be unnecessarily sent; therefore, it is not recommended.

To aggregate multiple policy changes, the operating system performs the necessary action 15 seconds after a policy change.

1.38.6 Examples

The following example shows how to reset all BGP multicast connections using IPv4 address prefixes:

```
[local]Redback#clear bgp ipv4 multicast *
```

1.39 clear bgp ipv4 unicast

clear bgp ipv4 unicast {***** | **as** {*asn* | *nn***:***nn*}} [**soft** [**in** | **out**]]

1.39.1 Purpose

Resets Border Gateway Protocol (BGP) IP Version 4 (IPv4) address connections or forces BGP updates to be generated for connections using unicast address prefixes without dropping the connections.

1.39.2 Command Mode

exec (10)

1.39.3 Syntax Description

*****	Resets or forces BGP updates for all BGP neighbor connections.
as	Resets or forces BGP updates to be generated for BGP neighbor connections in the specified autonomous system number (ASN).
asn	ASN in integer format. The range of values is 1 to 65535. The subrange 64512 to 65535 is reserved for private autonomous systems. Resets or forces BGP updates for connections with the peers that belong to the specified AS.
*nn***:***nn*	ASN in 4-byte integer format, where the first *nn* indicates the two higher-order bytes and the second *nn* denotes the two lower-order bytes. Resets or forces BGP updates for connections with the peers that belong to the specified AS.
soft	Optional. Does not drop the BGP connection, but forces BGP updates for the connection. If the **soft** keyword is not specified, the BGP connection is immediately dropped.

`in`	Optional. Forces inbound BGP updates for the connections only. Used only with the **`soft`** keyword. If the **`in`** or **`out`** optional keyword is not specified, both inbound and outbound BGP updates are forced for the connections.
`out`	Optional. Forces outbound BGP updates for the connections only. Used only with the **`soft`** keyword. If the **`in`** or **`out`** optional keyword is not specified, both inbound and outbound BGP updates are forced for the connections.

1.39.4 Default

None

1.39.5 Usage Guidelines

Use the **`clear bgp ipv4 unicast`** command to reset BGP IPv4 address connections, or force BGP updates to be generated for connections using unicast address prefixes without causing a hard reset (which drops the connection immediately).

Caution!

Risk of dropped connection. A hard reset can impact network connectivity. The **`soft`** keyword for inbound only takes effect if the BGP neighbor supports the refresh capability. The **`soft`** keyword for outbound is a local matter, and does not require the capability. To see if a BGP neighbor supports the refresh capability, use the **`show bgp neighbor summary`** command (in exec mode). Specify the **`soft`** keyword if you do not want the BGP neighbor connection dropped. To reduce the risk, only use a hard reset as a last resort.

Note: Prior to Release 2.5, when there was a change in an inbound or outbound routing policy, such as a prefix list, autonomous system (AS) path list, or route map, for a BGP peer, the **`clear bgp neighbor`** ***`ip-addr`*** `soft` [`in` | `out`] command had to be manually issued to make the policy change effective. Currently, routing policy changes automatically take effect, and issuing the **`clear bgp neighbor`** ***`ip-addr`*** `soft` [`in` | `out`] command to update routing policies can cause updates to be unnecessarily sent; therefore, it is not recommended.

To aggregate multiple policy changes, the operating system performs the necessary action 15 seconds after a policy change.

1.39.6 Examples

The following example shows how to reset all BGP unicast connections using IPv4 address prefixes:

```
[local]Redback#clear bgp ipv4 unicast *
```

1.40 clear bgp ipv4 vpn

clear bgp ipv4 vpn {***** | **as** {*asn* | *nn***:***nn*}} [**soft** [**in** | **out**]]

1.40.1 Purpose

Resets Border Gateway Protocol (BGP) IP Version 4 (IPv4) address connections or forces BGP updates to be generated for connections using Virtual Private Network (VPN) prefixes without dropping the connections.

1.40.2 Command Mode

exec (10)

1.40.3 Syntax Description

***** Resets or forces BGP updates for all BGP neighbor connections.

as Resets or forces BGP updates to be generated for BGP neighbor connections in the specified autonomous system number (ASN).

asn ASN in integer format. The range of values is 1 to 65,535. The subrange 64,512 to 65,535 is reserved for private autonomous systems. Resets or forces BGP updates for connections with the peers that belong to the specified AS.

*nn***:***nn* ASN in 4-byte integer format, where the first *nn* indicates the two higher-order bytes and the second *nn* denotes the two lower-order bytes. Resets or forces BGP updates for connections with the peers that belong to the specified AS.

soft Optional. Does not drop the BGP connection, but forces BGP updates for the connection. If the **soft** keyword is not specified, the BGP connection is immediately dropped.

in — Optional. Forces inbound BGP updates for the connections only. Used only with the **soft** keyword. If the **in** or **out** optional keyword is not specified, both inbound and outbound BGP updates are forced for the connections.

out — Optional. Forces outbound BGP updates for the connections only. Used only with the **soft** keyword. If the **in** or **out** optional keyword is not specified, both inbound and outbound BGP updates are forced for the connections.

1.40.4 Default

None

1.40.5 Usage Guidelines

Use the **clear bgp ipv4 vpn** command to reset BGP IPv4 connections or force BGP updates to be generated for connections using VPN prefixes without causing a hard reset (which drops the connection immediately).

Caution!

Risk of dropped connection. A hard reset can impact network connectivity. The **soft** keyword for inbound only takes effect if the BGP neighbor supports the refresh capability. The **soft** keyword for outbound is a local matter, and does not require the capability. To see if a BGP neighbor supports the refresh capability, use the **show bgp neighbor summary** command (in exec mode). Specify the **soft** keyword if you do not want the BGP neighbor connection dropped. To reduce the risk, only use a hard reset as a last resort.

Note: Prior to Release 2.5, when there was a change in an inbound or outbound routing policy, such as a prefix list, autonomous system (AS) path list, or route map, for a BGP peer, the **clear bgp neighbor** ***ip-addr*** **soft** [**in** | **out**] command had to be manually issued to make the policy change effective. Currently, routing policy changes automatically take effect, and issuing the **clear bgp neighbor** ***ip-addr*** **soft** [**in** | **out**] command to update routing policies can cause updates to be unnecessarily sent; therefore, it is not recommended.

To aggregate multiple policy changes, the operating system performs the necessary action 15 seconds after a policy change.

1.40.6 Examples

The following example shows how to perform a route refresh to all iBGP neighbors for the IPv4 VPN address family:

```
[local]Redback#clear bgp ipv4 vpn * soft out
```

1.41 clear bgp ipv6 unicast *

```
clear bgp ipv6 unicast * soft [in | out]
```

1.41.1 Purpose

Resets or forces updates for all Border Gateway Protocol (BGP) unicast neighbor connections that use IP Version 6 (IPv6) address prefixes without dropping the connection.

1.41.2 Command Mode

exec (10)

1.41.3 Syntax Description

`soft` Does not drop the BGP connection, but forces BGP updates for the connections. The `soft` keyword works only if the peer router advertises the route-refresh capability.

`in` Forces inbound BGP updates for the connections only. Used only with the soft keyword.

`out` Forces outbound BGP updates for the connections only. Used only with the soft keyword.

1.41.4 Default

None

1.41.5 Usage Guidelines

Use the `clear bgp ipv6 unicast *` command to reset or force updates for all BGP unicast neighbor connections that use IPv6 address prefixes without dropping the connection.

Note: The `soft` keyword works only if the peer router advertises the route-refresh capability.

1.41.6 Examples

The following example forces the reset of all BGP unicast connections using IPv6 address prefixes:

```
[local]SE1#clear bgp ipv6 unicast * soft
```

The following example shows how to force the reset of all outbound BGP unicast connections using IPv6 address prefixes:

```
[local]SE1#clear bgp ipv6 unicast * soft out
```

1.42 clear bgp ipv6 unicast as

```
clear bgp ipv6 unicast as {as-number | nn:nn} soft [in | out}
```

1.42.1 Purpose

Resets or forces Border Gateway Protocol (BGP) inbound updates to be generated for BGP IPv6 unicast neighbor connections in the specified autonomous system number (ASN) without dropping the connection.

1.42.2 Command Mode

exec (10)

1.42.3 Syntax Description

as-number ASN in integer format. The range of values is 1 to 65,535. The subrange 64,512 to 65,535 is reserved for private autonomous systems.

nn:nn ASN in 4-byte integer format, where the first *nn* indicates the two higher-order bytes and the second *nn* denotes the two lower-order bytes.

soft Does not drop the BGP connection, but forces BGP updates for the connection.

The **soft** keyword works only if the peer router advertises the route-refresh capability.

in Forces inbound BGP updates for the connections only. Used only with the **soft** keyword.

out Forces outbound BGP updates for the connections only. Used only with the **soft** keyword.

1.42.4 Default

None

1.42.5 Usage Guidelines

Use the **clear bgp ipv6 as** command to reset or force BGP inbound updates to be generated for BGP IPv6 unicast neighbor connections in the specified autonomous system number (ASN) without dropping the connection.

Note: The **soft** keyword works only if the peer router advertises the route-refresh capability.

1.42.6 Examples

The following example shows how to reset or force BGP inbound updates to be generated for BGP IPv6 unicast neighbor connections in the ASN 600:

```
[local]SE1#clear bgp ipv6 unicast ipv6 as 600 soft in
```

1.43 clear bgp ipv6 unicast external

clear bgp ipv6 unicast external soft [**in** | **out**]

1.43.1 Purpose

Resets or forces Border Gateway Protocol (BGP) updates for all external IP Version 6 (IPv6) BGP neighbor unicast connections.

1.43.2 Command Mode

exec (10)

1.43.3 Syntax Description

external	Resets or forces BGP updates for all external BGP neighbor unicast connections.
soft	Does not drop the BGP connection, but forces BGP updates for the connection. The **soft** keyword works only if the peer router advertises the route-refresh capability.

in Forces inbound BGP updates for the connections only. Used only with the **soft** keyword.

out Forces outbound BGP updates for the connections only. Used only with the **soft** keyword.

1.43.4 Default

None

1.43.5 Usage Guidelines

Use the **clear bgp ipv6 unicast external** command to reset or force BGP updates for all external IPv6 BGP neighbor unicast connections.

Note: The **soft** keyword works only if the peer router advertises the route-refresh capability.

1.43.6 Examples

The following example shows how to reset or force BGP updates for all external IPv6 BGP neighbor unicast connections:

```
[local]SE1#clear bgp ipv6 unicast external soft
```

1.44 clear bgp ipv6 unicast flap-statistics

clear bgp ipv6 unicast flap-statistics {*ip-addr/prefix-length* | **neighbor** *ip-addr* | **regexp** *as-path-string..*}

1.44.1 Purpose

Clears Border Gateway Protocol (BGP) IP Version 6 (IPv6) unicast connection route-flap statistics.

1.44.2 Command Mode

exec (10)

1.44.3 Syntax Description

ip-addr/prefix-length	IP address, in the form **A.B.C.D**, and the prefix length, separated by the slash (/) character. The range of values for the prefix-length argument is 0 to 32.
neighbor *ip-addr*	Route-flap statistics for only the specified neighbor.
regexp *as-path-string* ..	Route-flap statistics for only routes matching the specified AS path strings.

1.44.4 Default

None

1.44.5 Usage Guidelines

Use the **clear bgp ipv6 unicast flap-statistics** command to clear BGP IPv6 unicast connection route-flap statistics.

1.44.6 Examples

The following example shows how to clear the unicast connection route-flap statistics for the BGP IPv6 address 172.29.32.129/10:

```
[local]SE1#clear bgp ipv6 unicast flap-statistics 172.29.32.129/30
```

The following example shows how to clear the unicast connection route-flap statistics for BGP IPv6 routes that match the AS paths 64137 and 14207:

```
[local]SE1#clear bgp ipv6 unicast flap-statistics 64137 14207
```

1.45 clear bgp ipv6 unicast message-statistics

clear bgp ipv6 unicast message-statistics [**neighbor** *ip-addr*]

1.45.1 Purpose

Clears message statistics for Border Gateway Protocol (BGP) IP Version 6 (IPv6) unicast routes.

1.45.2 Command Mode

exec (10)

1.45.3 Syntax Description

neighbor *ip-addr*	Specifies a BGP neighbor IP address. Clears BGP message statistics for only the specified neighbor.

1.45.4 Default

None

1.45.5 Usage Guidelines

Use the **`clear bgp ipv6 unicast message-statistics`** command to clear message statistics for BGP IPv6 unicast routes.

1.45.6 Examples

The following example shows how to clear message statistics for all BGP IPv6 unicast routes:

```
[local]SE1#clear bgp ipv6 unicast message-statistics
```

1.46 clear bgp ipv6 unicast neighbor

`clear bgp ipv6 unicast neighbor` {*ip-addr*}

1.46.1 Purpose

Resets or forces Border Gateway Protocol (BGP) updates for the specified BGP IP Version 6 (IPv6) neighbor connection.

1.46.2 Command Mode

Exec (10)

1.46.3 Syntax Description

ip-addr	IP address of the neighbor.

1.46.4 Default

None

1.46.5 Usage Guidelines

Use the **`clear bgp ipv6 unicast neighbor`** command to reset or force BGP updates for the specified BGP IPv6 neighbor unicast connection.

1.46.6 Examples

The following example shows how to reset or force BGP updates for the BGP IPv6 neighbor unicast connection whose IP address is 120.19.18.193

```
[local]SE1#clear bgp ipv6 unicast neighbor 120.19.18.193
```

1.47 clear bgp ipv6 unicast peer-group

`clear bgp ipv6 unicast peer-group` *`group-name`* **`soft`** [**`in`** | **`out`**]

1.47.1 Purpose

Resets or forces Border Gateway Protocol (BGP) updates for the specified BGP IP Version 6 (IPv6) unicast connection with the specified peer group without dropping the connection.

1.47.2 Command Mode

exec (10)

1.47.3 Syntax Description

`group-name`	Name of peer group to be cleared.
`soft`	Does not drop the BGP connection, but forces BGP updates for the connection. If the **`soft`** keyword is not specified, the BGP connection is immediately dropped. The **`soft`** keyword works only if the peer router advertises the route-refresh capability.
`in`	Forces inbound BGP updates for the connections only. Used only with the soft keyword.
`out`	Forces outbound BGP updates for the connections only. Used only with the **`soft`** keyword.

1.47.4 Default

None

1.47.5 Usage Guidelines

Use the **`clear bgp ipv6 unicast peer-group`** command to reset or force BGP updates for the specified BGP IPv6 unicast connection with the specified peer group without dropping the connection.

Note: The **`soft`** keyword works only if the peer router advertises the route-refresh capability.

1.47.6 Examples

The following example shows how to reset the unicast connection with the peer group called `groupA`:

```
[local]SE1#clear bgp ipv6 unicast peer-group groupA
```

1.48 clear bgp ipv6 vpn *

`clear bgp ipv6 vpn * soft` [**`in`** | **`out`**]

1.48.1 Purpose

Resets or forces updates for all Border Gateway Protocol (BGP) VPN neighbor connections that use IP Version 6 (IPv6) address prefixes without dropping the connection.

1.48.2 Command Mode

exec (10)

1.48.3 Syntax Description

`soft`
Does not drop the BGP connection, but forces BGP updates for the connections. The **`soft`** keyword works only if the peer router advertises the route-refresh capability.

`in`
Forces inbound BGP updates for the connections only. Used only with the soft keyword.

`out`
Forces outbound BGP updates for the connections only. Used only with the soft keyword.

1.48.4 Default

None

1.48.5 Usage Guidelines

Use the `clear bgp ipv6 vpn *` command to reset or force updates for all BGP VPN neighbor connections that use IPv6 address prefixes without dropping the connection.

Note: The `soft` keyword works only if the peer router advertises the route-refresh capability.

1.48.6 Examples

The following example shows how to force the reset of all BGP VPN connections using IPv6 address prefixes:

```
[local]SE1#clear bgp ipv6 vpn * soft
```

The following example shows how to force the reset of all outbound BGP VPN connections using IPv6 address prefixes:

```
[local]SE1#clear bgp ipv6 vpn * soft out
```

1.49 clear bgp ipv6 vpn as

`clear bgp ipv6 vpn as` {*as-number* | *nn*:*nn*} **`soft`** [**`in`** | **`out`**}

1.49.1 Purpose

Resets or forces Border Gateway Protocol (BGP) inbound updates to be generated for BGP IPv6 VPN neighbor connections in the specified autonomous system number (ASN) without dropping the connection.

1.49.2 Command Mode

exec (10)

1.49.3 Syntax Description

`as-number` ASN in integer format. The range of values is 1 to 65,535. The subrange 64,512 to 65,535 is reserved for private autonomous systems.

nn:*nn* ASN in 4-byte integer format, where the first *nn* indicates the two higher-order bytes and the second *nn* denotes the two lower-order bytes.

`soft`	Does not drop the BGP connection, but forces BGP updates for the connection. The **`soft`** keyword works only if the peer router advertises the route-refresh capability.
`in`	Forces inbound BGP updates for the connections only. Used only with the **`soft`** keyword.
`out`	Forces outbound BGP updates for the connections only. Used only with the **`soft`** keyword.

1.49.4 Default

None

1.49.5 Usage Guidelines

Use the **`clear bgp ipv6 vpn as`** command to reset or force BGP inbound updates to be generated for BGP IPv6 VPN neighbor connections in the specified autonomous system number (ASN) without dropping the connection.

Note: The **`soft`** keyword works only if the peer router advertises the route-refresh capability.

1.49.6 Examples

The following example shows how to reset or force BGP inbound updates to be generated for BGP IPv6 VPN neighbor connections in the ASN 600:

```
[local]SE1#clear bgp ipv6 vpn ipv6 as 600 soft in
```

1.50 clear bgp ipv6 vpn external

`clear bgp ipv6 vpn external soft` [**`in`** | **`out`**]

1.50.1 Purpose

Resets or forces Border Gateway Protocol (BGP) updates for all external IP Version 6 (IPv6) BGP neighbor VPN connections.

1.50.2 Command Mode

exec (10)

1.50.3 Syntax Description

`external`	Resets or forces BGP updates for all external BGP neighbor VPN connections.
`soft`	Does not drop the BGP connection, but forces BGP updates for the connection. The **`soft`** keyword works only if the peer router advertises the route-refresh capability.
`in`	Forces inbound BGP updates for the connections only. Used only with the **`soft`** keyword.
`out`	Forces outbound BGP updates for the connections only. Used only with the **`soft`** keyword.

1.50.4 Default

None

1.50.5 Usage Guidelines

Use the **`clear bgp ipv6 vpn external`** command to reset or force BGP updates for all external IPv6 BGP neighbor VPN connections.

Note: The **`soft`** keyword works only if the peer router advertises the route-refresh capability.

1.50.6 Examples

The following example shows how to reset or force BGP updates for all external IPv6 BGP neighbor VPN connections:

```
[local]SE1#clear bgp ipv6 vpn external soft
```

1.51 clear bgp ipv6 vpn flap-statistics

`clear bgp ipv6 vpn flap-statistics` {*`ip-addr/prefix-length`*| **`neighbor`** *`ip-address`* | **`regexp`** *`as-path-string..`*}

1.51.1 Purpose

Clears Border Gateway Protocol (BGP) IP Version 6 (IPv6) VPN connection route-flap statistics.

1.51.2 Command Mode

exec (10)

1.51.3 Syntax Description

`ip-addr/prefix-length`	IP address, in the form *A.B.C.D*, and the prefix length, separated by the slash (/) character. The range of values for the prefix-length argument is 0 to 32.
`neighbor ip-address`	Route-flap statistics for only the specified neighbor.
`regexp as-path-string ..`	Route-flap statistics for only routes matching the specified AS path strings.

1.51.4 Default

None

1.51.5 Usage Guidelines

Use the **`clear bgp ipv6 vpn flap-statistics`** command to clear BGP IPv6 VPN connection route-flap statistics.

1.51.6 Examples

The following example shows how to clear the VPN connection route-flap statistics for the BGP IPv6 address 172.29.32.129/10:

```
[local]SE1#clear bgp ipv6 vpn flap-statistics 172.29.32.129/30
```

The following example shows how to clear the VPN connection route-flap statistics for BGP IPv6 routes that match the AS paths 64137 and 14207:

```
[local]SE1#clear bgp ipv6 vpn flap-statistics 64137 14207
```

1.52 clear bgp ipv6 vpn message-statistics

`clear bgp ipv6 vpn message-statistics` [**`neighbor`** *`ip-addr`*]

1.52.1 Purpose

Clears message statistics for Border Gateway Protocol (BGP) IP Version 6 (IPv6) VPN routes.

1.52.2 Command Mode

exec (10)

1.52.3 Syntax Description

neighbor *ip-addr* Specifies a BGP neighbor IP address. Clears BGP message statistics for only the specified neighbor.

1.52.4 Default

None

1.52.5 Usage Guidelines

Use the **clear bgp ipv6** command to clear message statistics for BGP IPv6 VPN routes.

1.52.6 Examples

The following example shows how to clear message statistics for all BGP IPv6 VPN routes:

```
[local]SE1#clear bgp ipv6 vpn message-statistics
```

1.53 clear bgp ipv6 vpn neighbor

clear bgp ipv6 vpn neighbor {ip-addr}

1.53.1 Purpose

Resets or forces Border Gateway Protocol (BGP) updates for the specified BGP IP Version 6 (IPv6) neighbor connection.

1.53.2 Command Mode

Exec (10)

1.53.3 Syntax Description

ip-addr IP address of the neighbor.

1.53.4 Default

None

1.53.5 Usage Guidelines

Use the **`clear bgp ipv6 vpn neighbor`** command to reset or force BGP updates for the specified BGP IPv6 neighbor VPN connection.

1.53.6 Examples

The following example shows how to reset or force BGP updates for the BGP IPv6 neighbor VPN connection whose IP address is 120.19.18.193:

```
[local]SE1#clear bgp ipv6 vpn neighbor 120.19.18.193
```

1.54 clear bgp ipv6 vpn peer-group

`clear bgp ipv6 vpn peer-group` ***`group-name`*** **`soft`** [**`in`** | **`out`**]

1.54.1 Purpose

Resets or forces Border Gateway Protocol (BGP) updates for the specified BGP IP Version 6 (IPv6) VPN connection with the specified peer group without dropping the connection.

1.54.2 Command Mode

Exec (10)

1.54.3 Syntax Description

`group-name` Name of peer group to be cleared.

`soft` Does not drop the BGP connection, but forces BGP updates for the connection. If the soft keyword is not specified, the BGP connection is immediately dropped. The **`soft`** keyword works only if the peer router advertises the route-refresh capability.

`in` Forces inbound BGP updates for the connections only. Used only with the **`soft`** keyword.

`out` Forces outbound BGP updates for the connections only. Used only with the **`soft`** keyword.

1.54.4 Default

None

1.54.5 Usage Guidelines

Use the **clear bgp ipv6 vpn peer-group** command to reset or force BGP updates for the specified BGP IPv6 VPN connection with the specified peer group without dropping the connection.

Note: The **soft** keyword works only if the peer router advertises the route-refresh capability.

1.54.6 Examples

The following example shows how to reset the VPN connection with the peer group called `groupA`:

```
[local]SE1#clear bgp ipv6 vpn peer-group groupA
```

1.55 clear bgp message-statistics

clear bgp message-statistics [**neighbor** ***ip-addr***]

1.55.1 Purpose

Clears Border Gateway Protocol (BGP) message statistics.

1.55.2 Command Mode

exec (10)

1.55.3 Syntax Description

neighbor ***ip-addr***	Optional. BGP neighbor IP address. Clears BGP message statistics for only the specified neighbor.

1.55.4 Default

None

1.55.5 Usage Guidelines

Use the **clear bgp message-statistics** command to clear BGP message statistics.

1.55.6 Examples

The following example shows how to clear BGP message statistics:

```
[local]Redback#clear bgp message-statistics
```

1.56 clear bgp neighbor

`clear bgp neighbor` ***`ip-addr`*** [**`notify`** | **`soft`** [**`in`** | **`out`**]]

1.56.1 Purpose

Resets Border Gateway Protocol (BGP) neighbor connections or forces BGP updates to be generated without dropping the connections.

1.56.2 Command Mode

exec (10)

1.56.3 Syntax Description

`ip-addr`

IP address of the neighbor. Resets or applies new routing policies for only the specified BGP neighbor.

`notify`

Optional. Sends a notification message to neighbors. When neighbors receive the notification message, they immediately drop their connections.

`soft`

Optional. Does not drop the BGP connection, but forces BGP updates for the connection. If the **`soft`** keyword is not specified, the BGP connection is immediately dropped.

`in`

Optional. Forces inbound BGP updates for the connections only. Used only with the **`soft`** keyword. If the **`in`** or **`out`** optional keyword is not specified, both inbound and outbound BGP updates are forced for the connections.

`out`

Optional. Forces outbound BGP updates for the connections only. Used only with the **`soft`** keyword. If the **`in`** or **`out`** optional keyword is not specified, both inbound and outbound BGP updates are forced for the connections.

1.56.4 Default

None

1.56.5 Usage Guidelines

Use the **`clear bgp neighbor`** command to reset BGP neighbor connections or force BGP updates to be generated for connections without causing a hard reset (which drop connections immediately).

Caution!

Risk of dropped connection. A hard reset can impact network connectivity. The **`soft`** keyword for inbound only takes effect if the BGP neighbor supports the refresh capability. The **`soft`** keyword for outbound is a local matter, and does not require the capability. To see if a BGP neighbor supports the refresh capability, use the **`show bgp neighbor summary`** command (in exec mode). Specify the **`soft`** keyword if you do not want the BGP neighbor connection dropped. To reduce the risk, only use a hard reset as a last resort.

Note: Prior to Release 2.5, when there was a change in an inbound or outbound routing policy, such as a prefix list, autonomous system (AS) path list, or route map, for a BGP peer, the **`clear bgp neighbor`** ***`ip-addr`*** **`soft`** [**`in`** | **`out`**] command had to be manually issued to make the policy change effective. Currently, routing policy changes automatically take effect, and issuing the **`clear bgp neighbor`** ***`ip-addr`*** **`soft`** [**`in`** | **`out`**] command to update routing policies can cause updates to be unnecessarily sent; therefore, it is not recommended.

To aggregate multiple policy changes, the operating system performs the necessary action 15 seconds after a policy change.

1.56.6 Examples

The following example shows how to cause a hard reset in which the connection to the BGP neighbor at IP address, **10.11.48.170**, is immediately dropped:

```
[local]Redback#clear bgp neighbor 10.11.48.170

 Jan 5 19:32:02: %BGP-6-INFO: 10.11.48.170 DOWN - User action
 Jan 5 19:32:07: %BGP-6-INFO: 10.11.48.170 UP
```

The following example displays output from the **`show bgp neighbor summary`** command:

```
[local]Redback>show bgp neighbor summary
BGP router identifier: 1.1.1.71, local AS number: 64001
Neighbors Configured: 10, Established: 9
Neighbor      AS     MsgRcvd   MsgSent InQ OutQ Reset Up/Down  State
10.11.64.170  64001  45        55        0    0     1 01:32:17 Connect
CapSent : refresh restart unicast
```

1.57 clear bgp peer-group

`clear bgp peer-group` *`group-name`* [**`notify`** | **`soft`** [**`in`** | **`out`**]]

1.57.1 Purpose

Resets Border Gateway Protocol (BGP) peer group connections or forces BGP updates to be generated without dropping the connections.

1.57.2 Command Mode

exec (10)

1.57.3 Syntax Description

`group-name`	Name of peer group to be cleared.
`notify`	Optional. Sends a notification message to neighbors. When neighbors receive the notification message, they immediately drop their connections.
`soft`	Optional. Does not drop the BGP connection, but forces BGP updates for the connection. If the **`soft`** keyword is not specified, the BGP connection is immediately dropped.
`in`	Optional. Forces inbound BGP updates for the connections only. Used only with the **`soft`** keyword. If the **`in`** or **`out`** optional keyword is not specified, both inbound and outbound BGP updates are forced for the connections.
`out`	Optional. Forces outbound BGP updates for the connections only. Used only with the **`soft`** keyword. If the **`in`** or **`out`** optional keyword is not specified, both inbound and outbound BGP updates are forced for the connections.

1.57.4 Default

None

1.57.5 Usage Guidelines

Use the **`clear bgp peer-group`** command to reset BGP peer group connections or force BGP updates to be generated for connections without causing a hard reset (which drop connections immediately).

Caution!

Risk of dropped connection. A hard reset can impact network connectivity. The **soft** keyword for inbound only takes effect if the BGP neighbor supports the refresh capability. The **soft** keyword for outbound is a local matter, and does not require the capability. To see if a BGP neighbor supports the refresh capability, use the **show bgp neighbor summary** command (in exec mode). Specify the **soft** keyword if you do not want the BGP neighbor connection dropped. To reduce the risk, only use a hard reset as a last resort.

Note: Prior to Release 2.5, when there was a change in an inbound or outbound routing policy, such as a prefix list, autonomous system (AS) path list, or route map, for a BGP peer, the **clear bgp neighbor** ***ip-addr*** **soft** [**in** | **out**] command had to be manually issued to make the policy change effective. Currently, routing policy changes automatically take effect, and issuing the **clear bgp neighbor** ***ip-addr*** **soft** [**in** | **out**] command to update routing policies can cause updates to be unnecessarily sent; therefore, it is not recommended.

To aggregate multiple policy changes, the operating system performs the necessary action 15 seconds after a policy change.

1.57.6 Examples

The following example shows how to reset the connection with peer group, **groupA:**

```
[local]Redback#clear bgp peer-group groupA
```

1.58 clear bridge loop-detection

clear bridge loop-detection {***bridge-name*** | **all**} ***context-name***

1.58.1 Purpose

Unblocks all circuits on the specified bridge that are blocked by MAC moves loop detection and clears the bridge MAC moves loop-detection counters.

1.58.2 Command Mode

exec

1.58.3 Syntax Description

bridge-name	Name of the bridge.
context-name	Name of the context that contains the bridge.
all	Clears all bridges in the specified context.

1.58.4 Default

None

1.58.5 Usage Guidelines

Use the **clear bridge loop-detection** command to unblock all circuits on the specified bridge that are blocked by MAC moves loop detection and clears the bridge MAC moves loop-detection counters.

1.58.6 Examples

The following example shows how to unblock all circuits in the **brdgrp1** bridge:

```
[local]Redback#clear bridge loop-detection brdgrp1 all
```

1.59 clear bridge table

clear bridge table *bridge-name*

1.59.1 Purpose

Clears the bridge table for the specified bridge.

1.59.2 Command Mode

exec

1.59.3 Syntax Description

bridge-name	Name of the bridge with the table to be cleared.

1.59.4 Default

None

1.59.5 Usage Guidelines

Use the **`clear bridge table`** command to clear the bridge table for the specified bridge.

1.59.6 Examples

The following example shows how to clear the bridge table for the **isp1** bridge:

```
[local]Redback#clear bridge table isp1
```

1.60 clear ces excessive-packet-loss

```
clear ces excessive-packet-loss [slot/port:ds3-channel:ds1-c
hannel:ds0-channel-group]
```

1.60.1 Purpose

Clears all excessive packet loss counters or only the counters of a specific CESoPSN or SAToP. circuit.

1.60.2 Command Mode

Global Config Mode.

1.60.3 Syntax Description

`slot:port`	Slot and port of the circuit.
`ds3-channel`	Channel of the circuit.
`ds1-channel`	Sub-channel of the circuit.
`ds0-channel-group`	Sub-sub-channel group ID of the circuit.

1.60.4 Default

Clears all CES excessive packet loss counters.

1.60.5 Usage Guidelines

Circuit handle is optional which is used to clear specific circuit excessive packet counters. The clear scope can be slot, port, or channel (DS1/E1 channel or DS0 group channel).

The following Entry information is reset to zero:

- Time Stamp
- Total Packet Loss
- Time minute

The follwing Exit information is reset to zero:

- Packet Loss Time
- Total Packet Loss Time
- Total number of times the channel in packet loss

1.60.6 Examples

The following example shows how to clear excessive packet loss counters on a specific circuit.:

```
[local]Redback(config)#clear ces execessive-packet-loss 3/2:3:1:1
```

1.61 clear ces outage

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

1.61.1 Purpose

Clears all outage counters or only the counters of a specific CESoPSN or SAToP. circuit.

1.61.2 Command Mode

SNMP Server Config Mode.

1.61.3 Syntax Description

slot:port	Slot and port of the circuit.
ds3-channel	Channel of the circuit.
ds1-channel	Sub-channel of the circuit.
ds0-channel-group	Sub-sub-channel group ID of the circuit.

1.61.4 Default

All CES MIB traps are disabled.

1.61.5 Usage Guidelines

Circuit handle is optional which is used to clear specific circuit excessive packet counters. The clear scope can be slot, port, or channel (DS1/E1 channel or DS0 group channel).

The following information is reset to zero:

- Latest Outage Time
- Last Outage Time
- Last UP Time
- Cumulative Outage Time
- UP Time
- Number of Outages

1.61.6 Examples

The following example shows how to clear excessive packet loss counters on a specific circuit.:

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

1.62 clear circuit counters

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

clear circuit counters [*slot/port* [*circuit-id*]] [*circuit-type*]

1.62.1 Purpose

Clears circuit counters for one or more circuits in the system.

1.62.2 Command Mode

exec (10)

1.62.3 Syntax Description

slot Optional. Chassis slot number for the line card for which counters are cleared. If omitted, counters are cleared for all circuits in the system.

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

chan-num Optional. Channel number for which counters are cleared. If omitted, clears counters for all channels on the specified port. The range of values depends on the type of port.

sub-chan-num Optional. Subchannel number for which counters are cleared. If omitted, clears counters for all subchannels on the specified channel. The range of values depends on the type of port.

circuit-id Optional. Circuit identifier, according to one of the constructs listed in Table 4. If omitted, clears counters for all circuits on the specified port or channel.

circuit-type Optional. Type of circuit for which counters are cleared, according to one of the keywords listed in Table 5. If omitted, clears counters for all types of circuits.

1.62.4 Default

Clears circuit counters for all circuits of all types in the system.

1.62.5 Usage Guidelines

Use the **`clear circuit counters`** command to clear circuit counters.

Table 4 lists the values for the ***circuit-id*** argument.

Table 4 Values for the circuit-id Argument

Construct	Description
	Data-link connection identifier (DLCI) for the Frame Relay PVC. The range of values is 16 to 991.

Table 4 Values for the circuit-id Argument

Construct	Description
`lsp` *`lsp`*	Multiprotocol label switching (MPLS) label-switched path (LSP) number. The range of values is 1 to 65535.
`vlan-id` *`vlan-id`*	Virtual LAN (VLAN) tag value for an 802.1Q tunnel or PVC. The *`vlan-id`* argument is one of the following constructs: • *`pvc-vlan-id`*—VLAN tag value of a PVC that is not within an 802.1Q tunnel. • *`tunl-vlan-id`*—VLAN tag value of a tunnel. • *`tunl-vlan-id`*:*`pvc-vlan-id`*—VLAN tag value for the tunnel followed by the VLAN tag value for the PVC within the tunnel. The range of values for either VLAN tag value is 1 to 4095.
`vpi-vci` *`vpi vci`*	Virtual path identifier (VPI) and virtual circuit identifier (VCI) for an ATM permanent virtual circuit (PVC). The range of values is 0 to 255 and 1 to 65535, respectively.

Table 5 lists the values for the *`circuit-type`* argument.

Table 5 Keywords for the circuit-type Argument

Keyword	Description
`atm`	ATM circuits
`chdlc`	Cisco High-Level Data Link Control (HDLC) circuits
`dot1q`	802.1Q circuits
`ether`	Ethernet circuits
`fr`	Frame Relay circuits
`gre`	Generic Routing Encapsulation (GRE) tunnel circuits
`mpls`	MPLS circuits.

Note: The SmartEdge 100 router does not support the `chdlc` and `fr` keywords.

If you enter the optional *`slot`*, *`port`*, or *`chan-num`* arguments, the command clears the counters for the specified card, port, or channel; if you enter the optional *`sub-chan-num`* argument, the command clears the counters for the DS-1 channel or the DS-0 channel group.

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

Note:

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

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

If you enter the optional *circuit-id* argument, the command clears the counters for the specified circuit.

If you specify the VLAN tag value for an 802.1Q tunnel, the command clears the counters for all the PVCs within the tunnel.

If you enter the optional *circuit-type* argument, the command clears the counters for all circuits of the specified type.

1.62.6 Examples

The following example shows how to clear all Cisco HDLC circuit counters on port **1** in slot **6:**

```
[local]Redback#clear circuit counters 6/1 chdlc
```

1.63 clear circuit counters (ces)

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

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

1.63.1 Purpose

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

1.63.2 Command Mode

All modes.

1.63.3 Syntax Description

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

1.63.4 Default

Clears all CES circuit counters.

1.63.5 Usage Guidelines

The optional circuit handle specifies a specific circuit. The clear scope can be slot, port, or channel (DS1 channel or DS0 group channel on CESoPSN; DS1/E1 channel on SAToP).

1.63.6 Examples

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

```
[local]Redback#clear circuit counters 3/2:3:1:1
```

1.64 clear circuit counters vpls

clear circuit counters vpls [***circuit-id***]

1.64.1 Purpose

Clears circuit counters for Virtual Private LAN Services (VPLS) circuits in the system.

1.64.2 Command Mode

Exec (10)

1.64.3 Syntax Description

circuit-id — Optional. System-generated ID for the VPLS circuit. The range of values is 1 to 65535. Clears the counters for the specified VPLS circuit.

1.64.4 Default

None

1.64.5 Usage Guidelines

Use the **clear circuit counters vpls** command to clear circuit counters for VPLS circuits in the system.

Use the **clear circuit counters vpls** *circuit-id* command to clear circuit counters for a single VPLS circuit. You can use the **show vpls peer** command (in any mode) to display a list of all VPLS circuit IDs.

1.64.6 Examples

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

```
[local]Redback>clear circuit counters vpls
```

The following example shows how to clear circuit counters for the VPLS circuit, **1250:**

```
[local]Redback>clear circuit counters vpls 1250
```

1.65 clear circuit loop-detection

clear circuit loop-detection *circuit-id*

1.65.1 Purpose

Disables MAC moves loop detection on the specified circuits.

1.65.2 Command Mode

exec

1.65.3 Syntax Description

circuit-id Specifies circuits on the bridge. See Table 6 for the expanded syntax for the *circuit-id* argument.

1.65.4 Default

none

1.65.5 Usage Guidelines

Use the clear circuit loop-detection command to disable MAC moves loop detection on the specified circuits. If blocked, the circuits are unblocked and their loop-detection counters cleared.

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

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

Table 6 describes the components of the *circuit-id* argument:

Table 6 Building Blocks of the circuit-id Argument

Field	Description
slot	Chassis slot number of the line card with the bridged circuit.
port	Port number of the port with the bridged circuit.
vpls *vpls-id*	A filter that limits the command to a specified Virtual Private LAN Service (VPLS) circuit. The VPLS circuit identifier is a system-generated ID. The range of values is 1 to 65,535.
vlan *vlan-id*	A filter that limits the command to a specified virtual LAN (VLAN) 802.1Q tunnel or PVC. The *vlan-id* argument is one of the following constructs: • *pvc-vlan-id*—VLAN tag value of a PVC that is not within an 802.1Q tunnel. • *tunl-vlan-id*—VLAN tag value of an 802.1Q tunnel. • *tunl-vlan-id*:*pvc-vlan-id*—VLAN tag value of an 802.1Q tunnel followed by the VLAN tag value for the PVC within the tunnel. If you specify the VLAN tag value for an 802.1Q tunnel, this command clears subscriber sessions on all the PVCs within the tunnel. The range of values for any VLAN tag value is 1 to 4,095.

1.65.6 Examples

The following example shows how to disable MAC moves loop detection on the VPLS **1225** circuit in slot 2, port 1:

```
[local]Redback#clear bridge loop-detection 2/1 vpls 1225
```

1.66 clear clips counters

`clear clips counters`

1.66.1 Purpose

Clears clientless IP service selection (CLIPS) counters.

1.66.2 Command Mode

exec (10)

1.66.3 Syntax Description

This command has no keywords or arguments.

1.66.4 Default

None

1.66.5 Usage Guidelines

Use the **`clear clips counters`** command to clear CLIPS counters.

1.66.6 Examples

The following example shows how to clear CLIPS counters:

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

1.67 clear community-list

`clear community-list` ***`cl-name`*** **`counters`**

1.67.1 Purpose

Clears match and cache hit counts for the specified Border Gateway Protocol (BGP) community list.

1.67.2 Command Mode

exec (10)

1.67.3 Syntax Description

`cl-name`	Community list name.
`counters`	Clears match and cache hit counts for the specified community list.

1.67.4 Default

None

1.67.5 Usage Guidelines

Use the **`clear community-list`** command to clear match and cache hit counts for the specified BGP community list.

1.67.6 Examples

The following example shows how to clear match and cache hit counts for the **commlist2** community-list:

```
[local]Redback#clear community-list commlist2
```

1.68 clear-df

`clear-df`

{**`no`** | **`default`**} **`clear-df`**

1.68.1 Purpose

Clears the IP header Don’t Fragment (DF) flag in all packets that are transmitted on an IP-in-IP or a Generic Routing Encapsulation (GRE) tunnel.

1.68.2 Command Mode

Tunnel configuration

1.68.3 Syntax Description

This command has no keywords or arguments.

1.68.4 Default

The IP header DF flag is honored.

1.68.5 Usage Guidelines

Use the **`clear-df`** command to clear the IP header DF flag in all packets that are transmitted on an IP-in-IP or a GRE tunnel. If the IP packet length exceeds the tunnel interface maximum transmission unit (MTU), the packet is fragmented.

If you enter the **`ip clear-df`** command (in interface configuration mode) for the tunnel interface, instead of this command, the DF flag is cleared only in transmitted packets that must be fragmented. If you enter both commands, the **`clear-df`** command takes precedence for this tunnel, and clears the DF flag in all packets transmitted on this tunnel.

Use the **`no`** or **`default`** form of this command to honor the DF flag in inbound packets.

1.68.6 Examples

The following example shows how to specify that the DF flag in all transmitted packets be cleared in the specified GRE tunnel:

```
[local]Redback(config)#tunnel gre HartfordTnl
[local]Redback(config-tunnel)#clear-df
```

1.69 clear-df (dynamic tunnel)

`clear-df`

{**`no`** | **`default`**} **`clear-df`**

1.69.1 Purpose

Clears the IP header Don’t Fragment (DF) flag in all packets that are transmitted on an IP-in-IP or a Generic Routing Encapsulation (GRE) tunnel.

1.69.2 Command Mode

Dynamic Tunnel Profile

1.69.3 Syntax Description

This command has no keywords or arguments.

1.69.4 Default

The IP header DF flag is not cleared.

1.69.5 Usage Guidelines

Use the **clear-df** command to clear the IP header DF flag in all packets that are transmitted on an IP-in-IP or a GRE tunnel. If the IP packet length exceeds the tunnel interface maximum transmission unit (MTU), the packet is fragmented.

Use the **no** or **default** form of this command to honor the DF flag in inbound packets.

1.69.6 Examples

The following example shows how to specify that the DF flag in all transmitted packets be cleared in the GRE and IP-in-IP tunnels:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#dynamic-tunnel-profile prof1
[local]Redback(config-mip-dyn-tun1-profile)#clear-df
[local]Redback(config-mip-dyn-tun1-profile)#end
```

1.70 clear dhcp host

clear dhcp host ***ip-addr***

1.70.1 Purpose

Clears Dynamic Host Configuration Protocol (DHCP) host entries and corresponding host route and Address Resolution Protocol (ARP) entries from the routing table.

1.70.2 Command Mode

exec (10)

1.70.3 Syntax Description

ip-addr	Specific IP address that is cleared.

1.70.4 Default

None

1.70.5 Usage Guidelines

Use the **clear dhcp host** command to clear DHCP host entries, and corresponding host route and ARP entries, from the routing table.

1.70.6 Examples

The following example shows how to clear the host entry and corresponding host route and ARP entries from the routing table, for the **10.1.1.1** IP address:

```
[local]Redback#clear dhcp host 10.1.1.1
```

1.71 clear dhcp stats

clear dhcp stats [{**circuit** *slot/port circuit-id* [**pending** *mac-addr*] | **context** *ctx-name* **interface** *if-name* [**pending** *mac-addr*]}]

1.71.1 Purpose

Clears Dynamic Host Configuration Protocol (DHCP) statistics.

1.71.2 Command Mode

exec (10)

1.71.3 Syntax Description

`circuit` *`slot/port`*
Slot and port numbers for the line card that holds the circuit to be cleared.

`circuit-id`
Circuit identifier, according to one of the constructs listed in Table 7.

`pending` *`mac-addr`*
Optional. DHCP host entry for the specified medium access control (MAC) address.

`context` *`ctx-name`*
Context for which DHCP statistics are cleared.

`interface` *`if-name`*
Interface in the specified context for which DHCP statistics are cleared.

1.71.4 Default

None

1.71.5 Usage Guidelines

Use the `clear dhcp stats` command to clear DHCP statistics.

Table 7 lists the values for the *`circuit-id`* argument.

Table 7 Values for the circuit-id Argument

Construct	Description
`vlan-id` *`vlan-id`*	Virtual LAN (VLAN) tag value for an 802.1Q tunnel or permanent virtual circuit (PVC). The *`vlan-id`* argument is one of the following constructs: • *`pvc-vlan-id`*—VLAN tag value of a PVC that is not within an 802.1Q tunnel. • *`tunl-vlan-id`*—VLAN tag value of a tunnel. • *`tunl-vlan-id:pvc-vlan-id`*—VLAN tag value for the tunnel followed by the VLAN tag value for the PVC within the tunnel. The range of values for either VLAN tag value is 1 to 4095.
`vpi-vci` *`vpi vci`*	Virtual path identifier (VPI) and virtual circuit identifier (VCI) for an Asynchronous Transfer Mode (ATM) PVC. The range of values is 0 to 255 and 1 to 65535, respectively.

1.71.6 Examples

The following example shows how to clear DHCP statistics for the specified circuit:

```
[local]Redback#clear dhcp stats circuit 11/5 vlan-id 10
```

1.72 clear dhcpv6 log

```
clear dhcpv6 log
```

1.72.1 Purpose

Clears Dynamic Host Configuration Protocol version 6 (DHCPv6) logs from the router memory.

1.72.2 Command Mode

exec (10)

1.72.3 Syntax Description

This command has no keywords or arguments.

1.72.4 Default

None

1.72.5 Usage Guidelines

Use the **`clear dhcpv6 log`** command to clear DHCPv6 logs from the router memory.

1.72.6 Examples

The following example shows how to clear DHCPv6 logs from the router memory:

```
[local]Redback#clear dhcpv6 log
```

1.73 clear dhcpv6 statistics

```
clear dhcpv6 statistics
```

1.73.1 Purpose

Clears Dynamic Host Configuration Protocol version 6 (DHCPv6) statistics from the router memory.

1.73.2 Command Mode

exec (10)

1.73.3 Syntax Description

This command has no keywords or arguments.

1.73.4 Default

None

1.73.5 Usage Guidelines

Use the **`clear dhcpv6 statistics`** command to clear DHCPv6 statistics from the router memory.

1.73.6 Examples

The following example shows how to clear DHCPv6 statistics from the router memory:

```
[local]Redback#clear dhcpv6 statistics
```

1.74 clear diag on-demand

For SmartEdge 100 controller or I/O carrier cards, the syntax is:

`clear diag on-demand` {**`all`** | **`card`** *`slot`* | **`history`**}

For SmartEdge line and services cards or standby controller cards, the syntax is:

`clear diag on-demand` {**`all`** | **`card`** *`slot`* | **`mesh`** | **`standby`** | **`history`**}

For SSE cards, the syntax is:

`clear diag on-demand card` *`slot`* [**`disk`** *`disk_num`*]

1.74.1 Purpose

Clears the log entries for one or more on-demand diagnostic (ODD) sessions for one or more cards.

1.74.2 Command Mode

exec

1.74.3 Syntax Description

`all`	Clears the log entries for all carrier, line, services, or standby controller cards.
`card` ***`slot`***	Chassis slot number of the carrier, line, services, or standby controller card for which results are cleared. The range of values depends on the type of card and the chassis in which the card is installed. For the SmartEdge 100 carrier card, the range of values is 1 to 2; for line cards, see Table 8 for slot range data. Optional. Clears the latest results for the fan and alarm unit in the SmartEdge 800 chassis or the fan tray in the SmartEdge 400 chassis.
`mesh`	Clears the log entry for packet mesh test.
`standby`	Clears the log entry for the standby controller card.
`history`	Clears all entries in the history.
`disk` ***`disk_num`***	Optional. Disk number on the SSE card. Values: 1 or 2. The rest of the SSE card continues operation while diagnostics run on the specified disk.

1.74.4 Default

None

1.74.5 Usage Guidelines

Use the **`clear diag`** command to clear the log entries from one or more ODD sessions for one or more cards.

For a SmartEdge 400 chassis, the standby controller is in slot 5 or 6.

For an SmartEdge 600, 800, 1200, or 1200H chassis the standby controller is in slot 7 or 8.

For a SmartEdge 100 chassis, the controller carrier card is in slot 1.

Table 8 lists the values for the *slot* argument; in the table, the IR, LR, and SR abbreviations are used for Intermediate Reach, Long Reach, and Short Reach, respectively.

Table 8 Line and Services Card Types and Slots

Type of Card/Description	***card-type* Argument Keyword Options**	***slot* Argument Range**		
		SmartEdge 800, 1200, or 1200H	**SmartEdge 400**	**SmartEdge 600**
ATM				
ATM OC-3c/STM-1c (8-port)	`atm-oc3e-8-port`	1 to 6 and 9 to 14	1 to 4	1 to 6
ATM OC-12c/STM-4c (2-port)	`atm-oc12e-2-port`			
Channelized SONET/SDH				
Channelized 8/4-port OC-3/STM-1 or 2/1-port OC-12/STM-4	`ch-oc3oc12-8or2-port`	1 to 6 and 9 to 14	1 to 4	1 to 6
POS OC-3c/STM-1c (8-port)	`oc3e-8-port`	1 to 6 and 9 to 14	1 to 4	1 to 6
POS OC-12c/STM-4c (4-port)	`oc12e-4-port`			
POS OC-48c/STM-16c (4-port)	`oc48e-4-port`			
OC-192c/STM-64c (1-port)[1]	`oc192-1-port`			
Ethernet				
Fast Ethernet–Gigabit Ethernet (60-port FE, 2-port GE)	`fege-60-2-port`	1 to 6 and 9 to 14	1 to 4	1 to 6
Gigabit Ethernet 1020 (10-port)	`ge-10-port`			
Gigabit Ethernet 1020 (20-port)	`ge-20-port`			
Gigabit Ethernet (5-port)	`ge-5-port`			
Gigabit Ethernet DDR (10-port)	`ge2-10-port`			
Gigabit Ethernet DDR (20-port)	`ge4-20-port`			
10 Gigabit Ethernet (1-port)	`10ge-1-port`			
10 Gigabit Ethernet DDR (4-port	`10ge-4-port`			
10 Gigabit Ethernet/OC-192c DDR (1-port)	`10ge-oc192-1-port`			
ASE				
Advanced Services Engine	`ase`	1 to 6 and 9 to 14	1 to 4	1 to 6
SSE				
SmartEdge Storage Engine	`sse`	1 to 6 and 9 to 14	N/A	1 to 6

[1] This line card accepts Ericsson XFP transceivers, including IR, SR, LR, ER, and ZR types. For further information and a full list of supported transceivers, see `Transceivers for SmartEdge and SM Family Line Cards.`

The latest results for each card are kept in a log, which is stored on the compact-flash card for low-level software and in main memory. Use the **card** *slot* construct to clear the log entry for the specified card; use the **all** keyword to clear the log entries for all cards.

A history file of the 100 previous sessions is also stored on the compact-flash card for low-level software; use the **history** keyword to clear all entries stored in the history file.

1.74.6 Examples

The following example shows how to clear the log entry for the line card in slot **2**:

```
[local]Redback#clear diag on-demand card 2
```

The following example shows how to clear the log entry for disk 2 on the SSE card in slot 3:

```
[local]Redback#clear diag on-demand card 3 disk
2 level 3 loop 4
```

1.75 clear disk sse counters

clear disk sse counters [*slot* [*disk_num*]]

1.75.1 Command Mode

exec

1.75.2 Syntax Description

slot	Optional. Chassis slot number of the SSE card.
disk_num	Optional. Disk number on the SSE card.

1.75.3 Usage Guidelines

Clears counters on all SSE cards. Use the *slot* argument to clear counters on the SSE in the specified slot; use the *disk_num* argument to clear counters on the specified SSE disk of the SSE card.

1.75.4 Examples

```
[local]Redback#clear disk sse counters 2 1
```

1.76 clear dot1q counters

clear dot1q counters [*slot*/*port* [**vlan-id** *vlan-id*]]

1.76.1 Purpose

Clears counters for one or more 802.1Q tunnels or permanent virtual circuits (PVCs) in the system.

1.76.2 Command Mode

exec (10)

1.76.3 Syntax Description

slot	Optional. Chassis slot number of a line card for which counters are cleared. If omitted, counters are cleared for all 802.1Q tunnels and PVCs in the system.
port	Required if you enter the *slot* argument. Port number for which counters are cleared.
vlan-id *vlan-id*	Optional. Virtual LAN (VLAN) tag value of the 802.1Q tunnel or PVC to be cleared. The *vlan-id* argument has one of the following formats: • *pvc-vlan-id*—VLAN tag value of a PVC that is not within an 802.1Q tunnel. • *tunl-vlan-id*—VLAN tag value of a tunnel. • *tunl-vlan-id*:*pvc-vlan-id*—VLAN tag value for the tunnel followed by the VLAN tag value for the PVC within the tunnel. The range of values for either VLAN tag value is 1 to 4095.

1.76.4 Default

Clears 802.1Q circuit counters for all 802.1Q tunnels and PVCs in the system.

1.76.5 Usage Guidelines

Use the **clear dot1q counters** command to clear circuit counters for one or more 802.1Q circuits in the system.

The **clear dot1q counters** command is an alias for the **clear circuit counters dot1q** command (in exec mode).

If you enter the optional *slot* and *port* arguments, the command clears circuit counters for all the circuits configured on the specified card or port.

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

Note:

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

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

If you enter the optional **vlan-id** *vlan-id* construct, the output clears the counters for the specified circuit.

If you specify the VLAN tag value for an 802.1Q tunnel, the command clears the counters for all the PVCs within the tunnel.

1.76.6 Examples

The following example shows how to clear all circuit counters for all 802.1Q PVCs on port **1** in slot **13**:

```
[local]Redback#clear dot1q counters 13/1
```

1.77 clear dot1q pvc on-demand

```
clear dot1q pvc on-demand slot/port[:ch[:sub[:subsub]]]
vlan-id vlan-id
```

1.77.1 Purpose

Clears the specified on-demand Ethernet permanent virtual circuit (PVC).

1.77.2 Command Mode

exec (10)

1.77.3 Syntax Description

slot Chassis slot number of the Ethernet line card with the PVC to be cleared.

port Port slot number with the PVC to be cleared.

ch Channel number. Applies if the port is channelized.

sub Subchannel number. Applies if the port is channelized to the subchannel level.

ch Subsubchannel number. Applies if the port is channelized to the subsubchannel level.

vlan-id *vlan-id* Optional. Virtual LAN (VLAN) tag value of the 802.1Q tunnel or PVC to be cleared. The *vlan-id* argument has one of the following formats:

- *pvc-vlan-id*—VLAN tag value of a PVC that is not within an 802.1Q tunnel.
- *tunl-vlan-id*—VLAN tag value of a tunnel.
- *tunl-vlan-id*:*pvc-vlan-id*—VLAN tag value for the tunnel followed by the VLAN tag value for the PVC within the tunnel.

The range of values for either VLAN tag value is 1 to 4095.

1.77.4 Default

None

1.77.5 Usage Guidelines

Clears the specified on-demand Ethernet PVC.

1.77.6 Examples

```
[local]Redback#clear dot1q pvc on-demand 5/1 vlan-id 15:145
```

1.78 clear dvsr statistics

clear dvsr statistics

1.78.1 Purpose

Clears all dynamically verified static routing (DVSR) statistics in the DVSR summary table.

1.78.2 Command Mode

exec

1.78.3 Syntax Description

This command has no keywords or arguments.

1.78.4 Default

None

1.78.5 Usage Guidelines

Use the **`clear dvsr statistics`** command to clear all DVSR statistics in the DVSR summary table.

1.78.6 Examples

The following example displays the DVSR summary table before and after the DVSR statistics have been cleared:

```
[local]Redback>show dvsr summary
DVSR summary:
dvsr profiles: 4                    dvsr routes: 5
routes alive: 5                     routes fail: 0
total ping sent: 19163              total recv icmp replies: 19163
total icmp timeout: 12              total icmp no reply: 0
total reply no route: 0             total nexthop invalid: 2
avg round trip delay(msec): 0       max round trip delay(msec): 3070
avg ping time(msec): 0              max ping time(msec): 10170
total ping operation: 11498         total ping error: 0
total route state changes: 7        max pings in a batch: 2
```

```
[local]Redback#clear dvsr statistics
[local]Redback>show dvsr summary
DVSR summary:
dvsr profiles: 4                    dvsr routes: 5
routes alive: 5                     routes fail: 0
total ping sent: 0                  total recv icmp replies: 0
total icmp timeout: 0               total icmp no reply: 0
total reply no route: 0             total nexthop invalid: 0
avg round trip delay(msec): 0       max round trip delay(msec): 0
avg ping time(msec): 0              max ping time(msec): 0
total ping operation: 0             total ping error: 0
total route state changes: 0        max pings in a batch: 0
```

1.79 clear ethernet-cfm counters

clear ethernet-cfm counters [*instance-name*] [domain *domain-name*]

1.79.1 Purpose

Clears loopback and link-trace counters for each MEP, but does not clear Continuity-Check Message (CCM) counters.

1.79.2 Command Mode

exec (10)

1.79.3 Syntax Description

instance-name	The name of the CFM service instance.
[domain *domain-name*]	The name of the maintenance domain (MD).

1.79.4 Default

None

1.79.5 Usage Guidelines

Use the **clear ethernet-cfm counters** command to clear loopback and link-trace counters for each MEP. It does not clear Continuity-Check Message (CCM) counters.

1.79.6 Examples

```
[local]Redback#clear ethernet-cfm counters myservice domain myservice
```

1.80 clear ext-community-list

clear ext-community-list *ecl-name* counters

1.80.1 Purpose

Clears match and cache hit counts for a specified Border Gateway Protocol (BGP) extended community list.

1.80.2 Command Mode

exec (10)

1.80.3 Syntax Description

ecl-name	Extended community list name.
`counters`	Clears match and cache hit counts for the specified community list.

1.80.4 Default

None

1.80.5 Usage Guidelines

Use the **`clear ext-community-list`** command to clear match and cache hit counts for the specified BGP extended community list.

1.80.6 Examples

The following example shows how to clear match and cache hit counts for the **excommlist2** extended community list:

```
[local]Redback#clear ext-community-list excommlist2
```

1.81 clear flow counters

`clear flow counters`

1.81.1 Purpose

Removes all counters from the flow counter list.

1.81.2 Command Mode

Exec

1.81.3 Syntax Description

This command has no keywords or arguments.

1.81.4 Default

None

1.81.5 Usage Guidelines

Use the **`clear flow counters`** command to remove all counters from the flow counter list.

1.81.6 Examples

The following example shows how to clear flow counters:

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

1.82 clear flow ip cache

`clear flow ip cache` ***`profile-name`*** **`statistics [application]`**

1.82.1 Purpose

Clear RFlow information gathered as part of statistics collection for a specified profile.

1.82.2 Command Mode

exec

1.82.3 Syntax Description

`profile-name`	Profile name for which to clear statistics.

1.82.4 Default

None

1.82.5 Usage Guidelines

Use the **`clear flow ip statistics`** command to clear RFlow statistics information collected or in the cache. Clearing summary statistics affects summary-period statistics.

1.82.6 Examples

The following examples shows how to clear existing statistics, clear statistics for all configured applications, and verifiy that they have been cleared:

```
[local]Redback#clear flow ip cache p1 statistics
[local]Redback#clear flow ip cache p1 statistics application

[local]Redback#show flow ip cache p1 statistics

 Last cleared: Thu Aug 13 19:42:37 2009
 Current time: Thu Aug 13 19:42:49 2009

 Profile : p1
 Context : isp

 Statistics:
  PPA flows received     : 0
  PPA flows processed    : 0
  PPA flows discarded    : 0
  Processing errors      : 0
  Cache entries created  : 0
  Cache entries updated  : 0
  Cache entries aged     : 0
  Cache entries fast-aged: 0
  Entries in cache       : 0
  Ager walks             : 0

 Collector Stream Information:
 Collector       ExportID   Seq Number       Generated           Send Errors
                                          Packets  Records    Packets  Records
 ---------       --------   ----------    -------- ---------- -------- ----------
 c               1          0x2           1        2          0        0

[local]Redback# show flow ip cache p1 statistics application

Last cleared: Thu Aug 13 19:42:35 2009
Current time: Thu Aug 13 19:42:56 2009

Application        Total     Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
-----------        Flows      /Sec     /Flow  /Pkt     /Sec       /Flow     /Flow
TCP-Telnet             0       0.0         0     0      0.0        0.0       0.0
TCP-FTP                0       0.0         0     0      0.0        0.0       0.0
TCP-FTPD               0       0.0         0     0      0.0        0.0       0.0
TCP-HTTP               0       0.0         0     0      0.0        0.0       0.0
TCP-SMTP               0       0.0         0     0      0.0        0.0       0.0
TCP-BGP                0       0.0         0     0      0.0        0.0       0.0
TCP-NNTP               0       0.0         0     0      0.0        0.0       0.0
TCP-Other              0       0.0         0     0      0.0        0.0       0.0
UDP-DNS                0       0.0         0     0      0.0        0.0       0.0
UDP-NTP                0       0.0         0     0      0.0        0.0       0.0
UDP-TFTP               0       0.0         0     0      0.0        0.0       0.0
UDP-Other              0       0.0         0     0      0.0        0.0       0.0
ICMP                   0       0.0         0     0      0.0        0.0       0.0
IGMP                   0       0.0         0     0      0.0        0.0       0.0
Other                  0       0.0         0     0      0.0        0.0       0.0
```

1.83 clear flow log

```
clear flow log
```

1.83.1 Purpose

Removes all entries from the flow log.

1.83.2 Command Mode

Exec

1.83.3 Syntax Description

This command has no keywords or arguments.

1.83.4 Default

None

1.83.5 Usage Guidelines

Use the **`clear flow log`** command to remove all entries from the flow log.

1.83.6 Examples

The following example shows how to remove all entries from the flow log:

```
[local]Redback#clear flow log
```

1.84 clear frame-relay counters

For ports on Packet over SONET/SDH (POS) line cards, the syntax is:

`clear frame-relay counters` [*`slot/port`*] [**`dlci`** *`dlci`*]]

1.84.1 Purpose

Clears all Frame Relay counters for one or more Frame Relay permanent virtual circuits (PVCs).

1.84.2 Command Mode

exec (10)

1.84.3 Syntax Description

slot	Optional. Chassis slot number of the line card for which the Frame Relay counters are cleared.
port	Required if you enter the *slot* argument. Port number of the port for which the Frame Relay counters are cleared.
chan-num	Optional. Channel number for which Frame Relay counters are cleared. If omitted, clears Frame Relay counters for all channels on the specified port. The range of values depends on the type of port.
sub-chan-num	Optional. Subchannel number for which Frame Relay counters are cleared. If omitted, clears Frame Relay counters for all subchannels on the specified channel. The range of values depends on the type of port.
dlci *dlci*	Optional. Data-link connection identifier (DLCI) of the configured PVC for which Frame Relay counters are cleared. The range of values is 16 to 991.

1.84.4 Default

Clears all Frame Relay counters on all Frame Relay PVCs.

1.84.5 Usage Guidelines

Use the **clear frame-relay counters** command to clear Frame Relay counters for one or more Frame Relay PVCs.

The **clear frame-relay counters** command is an alias for the **clear circuit counters fr** command (in exec mode).

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

You must specify the *chan-num* argument to clear only the counters on a specific channel; you must specify the *sub-chan-num* argument to clear only the counters on a specific subchannel.

You must specify the **dlci** *dlci* construct to clear only the counters for a specific Frame Relay PVC.

1.84.6 Examples

The following example shows how to clear the counters for PVC **301** on a POS port:

```
[local]Redback#clear frame-relay counters 3/1 dlci 301
```

1.85 clear frame-relay lmi-counters

For ports on Packet over SONET/SDH (POS) line cards, the syntax is:

```
clear frame-relay lmi-counters slot/port
```

1.85.1 Purpose

Clears Frame Relay Local Management Interface (LMI) statistics and error counters.

1.85.2 Command Mode

exec (10)

1.85.3 Syntax Description

slot	Chassis slot number of the line card for which the LMI statistics and error counters are cleared.
port	Port number of the port for which the LMI statistics and error counters are cleared.
chan-num	Optional. Channel number for which the LMI statistics and error counters are cleared. If omitted, clears LMI statistics and error counters for all channels on the specified port. The range of values depends on the type of port.
sub-chan-num	Optional. Subchannel number on the channel for which the LMI statistics and error counters are cleared. If omitted, clears LMI statistics counters for all subchannels on the specified channel. The range of values depends on the type of port.

1.85.4 Default

Clears all Frame Relay LMI statistics and error counters on the specified port.

1.85.5 Usage Guidelines

Use the `clear frame-relay lmi-counters` command to clear Frame Relay LMI statistics and error counters. This command only affects the counters available to the command line. Corresponding Simple Network Management Protocol (SNMP) counters are not cleared.

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

You must specify the ***chan-num*** argument to clear the statistics counters for a specific channel; you must specify the ***sub-chan-num*** argument to clear the statistics counters for a specific DS-1 channel of DS-0 channel group.

1.85.6 Examples

The following example shows how to clear LMI statistics counters for port **1** on the POS line card in slot **3:**

```
[local]Redback#clear frame-relay lmi-counters 3/1
```

1.86 clear igmp group

```
clear igmp group [group-addr [interface-name]]
```

1.86.1 Purpose

Clears the specified Internet Group Management Protocol (IGMP) cache tables.

1.86.2 Command Mode

exec (10)

1.86.3 Syntax Description

group-addr	IP address of the IGMP group. If not specified, all IGMP group tables are cleared.
interface-name	Name of the multicast interface.

1.86.4 Default

None

1.86.5 Usage Guidelines

Use the **clear igmp group** command to clear specified IGMP cache tables.

Use the ***group-addr*** argument to clear only the specified IGMP group.

1.86.6 Examples

The following example shows how to clear all dynamically learned IGMP groups from the IGMP cache table:

```
[local]Redback#clear igmp group
```

The following example shows how to clear the IGMP group, `224.1.1.1`:

```
[local]Redback#clear igmp group 224.1.1.1
```

1.87 clear igmp snooping

clear igmp snooping mroute [bridge *bridge-name*] [group *group-addr* [source *source-adr*]]

1.87.1 Purpose

Clears IGMP snooping multicast routing table of rows that apply to a specified bridge, multicast group, or multicast source-multicast group in multicast table.

1.87.2 Command Mode

exec (10)

1.87.3 Syntax Description

mroute	Specifies the system IGMP snooping multicast routing table.
bridge *bridge-name*	Clears rows that apply only to the specified bridge.
group *group-addr*	Clears rows that apply to the multicast group specified by its IP address.
source *source-adr*	Clears rows that apply only to hosts in a multicast routing table as specified by their IP address and their multicast group as specified by its IP address.

1.87.4 Default

IGMP snooping table is not cleared.

1.87.5 Usage Guidelines

Use the **clear igmp snooping** to clear the IGMP snooping multicast routing table of rows that apply to a specified bridge, multicast group, or multicast source-multicast group in multicast table.

1.87.6 Examples

The following example shows how to clear the IGMP snooping table of rows that apply to the **blue** bridge on which IGMP snooping has been enable and only to the 233.1.1.1 multicast group in the bridge's set of rows:

```
[local]Redback#clear igmp snooping mroute bridge blue group 233.1.1.1
```

1.88 clear igmp traffic

clear igmp traffic

1.88.1 Purpose

Clears all traffic statistics maintained by Internet Group Management Protocol (IGMP).

1.88.2 Command Mode

exec (10)

1.88.3 Syntax Description

This command has no keywords or arguments.

1.88.4 Default

None

1.88.5 Usage Guidelines

Use the **clear igmp traffic** command to clear all traffic statistics maintained by IGMP.

1.88.6 Examples

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

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

1.89 clear ip maximum-routes

clear ip maximum-routes [**multicast**]

1.89.1 Purpose

Removes routes and a maximum route flag from the IP routing table.

1.89.2 Command Mode

exec

1.89.3 Syntax Description

multicast	Optional. Removes routes and a maximum route flag from the IP multicast routing table.

1.89.4 Default

Routes and maximum route flag are removed from unicast table.

1.89.5 Usage Guidelines

Use the **clear ip maximum-routes** command to remove routes and a maximum route flag from the IP routing table.

After the upper limit for the number of prefixes installed in a routing table is reached, new routes are rejected, which can cause the loss of routing or forwarding information. To restore normal operation, enter the **clear ip maximum-routes** command to clear all routes and a flag that rejects the addition of new routes.

1.89.6 Examples

The following example shows how to remove routes and a maximum route flag from the IP routing table:

```
[local]Redback#clear ip maximum-routes
```

1.90 clear ip mroute

clear ip mroute {*group-addr* [*src-addr*]} | *****

1.90.1 Purpose

Clears source and group entries from the Protocol Independent Multicast (PIM) routing table.

1.90.2 Command Mode

exec (10)

1.90.3 Syntax Description

group-addr	IP address of the Internet Group Management Protocol (IGMP) group.
src-addr	Optional. IP address of the multicast source that is transmitting to the group. A source does not need to be a member of the group.
*****	Clears all entries from the multicast routing table.

1.90.4 Default

None

1.90.5 Usage Guidelines

Use the **clear ip mroute** command to clear source address and group address entries from the PIM routing table.

When the *src-addr* argument is set to 0, the **clear ip mroute** command is treated as a deletion command for all source address and group address entries for the same group. When the *group-addr* argument is set to 0, the entire multicast routing table is cleared.

1.90.6 Examples

The following example shows how to clear all entries for the multicast group, **224.1.1.1**, and for the source transmitting to the group, **1.1.1.1:**

```
[local]Redback#clear ip mroute 224.1.1.1 1.1.1.1
```

The following example clears all entries from the PIM routing table:

```
[local]Redback#clear ip mroute *
```

1.91 clear ip prefix-list

clear ip prefix-list ***pl-name*** **counters**

1.91.1 Purpose

Clears match and cache hit counts for a specified IP prefix list.

1.91.2 Command Mode

exec (10)

1.91.3 Syntax Description

pl-name	IP prefix list name.
counters	Clears match and cache hit counts for the specified IP prefix list.

1.91.4 Default

None

1.91.5 Usage Guidelines

Use the **clear ip prefix-list** command to clear match and cache hit counts for a specified IP prefix list.

1.91.6 Examples

The following example shows how to clear match and cache hit counts for the **prlist3** ip prefix list:

```
[local]Redback#clear ip prefix-list prlist3
```

1.92 clear ip route

clear ip route [**multicast**] *****

1.92.1 Purpose

Removes routes from the IP routing or IP multicast routing table. Issuing the command without the multicast keyword clears all routes from the RIB. Subsequently, the AAA process propagates all routes in shared memory to the RIB; however, the SmartEdge router does not attempt to download routes from the route download server again.

1.92.2 Command Mode

exec

1.92.3 Syntax Description

multicast	Optional. Clears routes from the IP multicast routing table only.
*	Clears all routes from either the IP routing table or from the IP multicast routing table.

1.92.4 Default

None

1.92.5 Usage Guidelines

Use the **clear ip route** command to remove routes from the IP routing table or from the IP multicast routing table.

1.92.6 Examples

The following example shows how to clear all routes from the IP routing table:

```
[local]Redback#clear ip route *
```

1.93 clear ipv6 prefix-list

clear ipv6 prefix-list *ipv6-pl-name* **counters**

1.93.1 Purpose

Clears match and cache hit counts for a specified IP Version 6 (IPv6) prefix list.

1.93.2 Command Mode

exec (10)

1.93.3 Syntax Description

ipv6-pl-name	IPv6 prefix list name.
`counters`	Clears match and cache hit counts for the specified IPv6 prefix list.

1.93.4 Default

None

1.93.5 Usage Guidelines

Use the **`clear ipv6 prefix-list`** command to clear match and cache hit counts for a specified IPv6 prefix list.

1.93.6 Examples

The following example shows how to clear match and cache hit counts for the **ipv6prlist62** IPv6 prefix list:

```
[local]Redback#clear ipv6 prefix-list ipv6prlist62
```

1.94 clear isis adaptive-holdtime

`clear isis adaptive-holdtime interface` *`if-name`*

1.94.1 Purpose

Resets the Intermediate System-to-Intermediate System (IS-IS) Hello holdtime to its original value on the interface.

1.94.2 Command Mode

exec (10)

1.94.3 Syntax Description

`interface` ***`if-name`*** Name of the interface for which the IS-IS Hello holdtime is to be reset.

1.94.4 Default

None

1.94.5 Usage Guidelines

Use the **`clear isis adaptive-holdtime`** command to reset the IS-IS Hello holdtime to its original value on the interface. When the IS-IS interface is configured for the adaptive millisecond mode, the holdtime may be dynamically adjusted to a larger value.

This **`clear`** command resets the holdtime to its original value, which is the product of the Hello interval and the Hello multiplier rounded up to the nearest second. Use the **`show isis interfaces detail`** command (in any mode) to check if the holdtime has been dynamically adjusted.

1.94.6 Examples

The following example shows how to reset the IS-IS Hello holdtime to its original value on the `to-isp` interface:

```
[local]Redback#clear isis adaptive-holdtime interface to-isp
```

1.95 clear isis adjacency

`clear isis` [*`instance-name`*] **`adjacency`** {**`all`** | **`interface`** ***`if-name`*** {**`all`** | ***`sys-id`***} | **`is`** sys-id}

1.95.1 Purpose

Resets the Intermediate System-to-Intermediate System (IS-IS) adjacencies with neighbors.

1.95.2 Command Mode

exec (10)

1.95.3 Syntax Description

`instance-name`	Optional. IS-IS instance name. Required only if more than one instance is configured for the context.
`all`	Clears all adjacencies on all IS-IS interfaces.
`interface` *`if-name`*	Name of the interface for which adjacencies are cleared.
`all`	Clears all adjacencies on the specified interface.
`sys-id`	ID (*`xxxx.xxxx.xxxx`* format) or hostname of the system attached to the specified interface. Only adjacencies to the specified system are cleared.
`is` *`sys-id`*	ID (*`xxxx.xxxx.xxxx`* format) or hostname of the system on which adjacencies are cleared.

1.95.4 Default

None

1.95.5 Usage Guidelines

Use the **`clear isis adjacency`** command to reset IS-IS adjacencies with neighbors.

1.95.6 Examples

The following example shows how to clear adjacencies to the **ns-edge** system connected to the **ericsson** interface:

```
[local]Redback#clear isis adjacency interface ericsson is ns-edge
```

1.96 clear isis instance

`clear isis` [*`instance-name`*] **`instance`**

1.96.1 Purpose

Clears all Intermediate System-to-Intermediate System (IS-IS) adjacencies and recalculates the routes for an IS-IS instance.

1.96.2 Command Mode

exec (10)

1.96.3 Syntax Description

instance-name	Optional. IS-IS instance name. Required only if more than one instance is configured for the context.

1.96.4 Default

None

1.96.5 Usage Guidelines

Use the **clear isis instance** command to clear all IS-IS adjacencies and recalculate the routes for an IS-IS instance.

1.96.6 Examples

The following example shows how to clear all IS-IS adjacencies and recalculates the routes for the one IS-IS instance that is configured:

```
[local]Redback#clear isis instance
```

1.97 clear isis log

clear isis [*instance-name*] **log** [**level-1** | **level-2**] {**adjacency** {**all** | **interface** *if-name* | **spf**}}

1.97.1 Purpose

Clears Intermediate System-to-Intermediate System (IS-IS) logs.

1.97.2 Command Mode

exec (10)

1.97.3 Syntax Description

instance-name	Optional. IS-IS instance name. Required only if more than one instance is configured for the context.
level-1	Optional. Clears level 1 adjacency or Shortest Path First (SPF) logs.
level-2	Optional. Clears level 2 adjacency or SPF logs.

adjacency	Clears adjacency logs.
all	Clears all adjacency logs on all IS-IS interfaces.
interface ***if-name***	Name of the interface for which adjacency logs are cleared.
spf	Clears SPF logs.

1.97.4 Default

When entered without specifying either level 1 or level 2 routing, this command clears logs for both levels of IS-IS routing.

1.97.5 Usage Guidelines

Use the **clear isis log** command to clear IS-IS logs.

1.97.6 Examples

The following example shows how to clear the adjacency log for the **gre0** interface:

```
[local]Redback#clear isis log adjacency interface gre0
```

1.98 clear isis routes

clear isis [*instance-name*] **routes** [**level-1** | **level-2**] [**redistribute**]

1.98.1 Purpose

Clears existing routes from the Intermediate System-to-Intermediate System (IS-IS) routing table and repopulates the table with updated route information.

1.98.2 Command Mode

exec (10)

1.98.3 Syntax Description

instance-name	Optional. IS-IS instance name. Required only if more than one instance is configured for the context.
level-1	Optional. Clears existing IS-IS level 1 routes from the routing table.
level-2	Optional. Clears existing IS-IS level 2 routes from the routing table.
redistribute	Optional. Clears existing routes learned by other routing protocols or methods that have been redistributed into the IS-IS instance.

1.98.4 Default

When entered without specifying either level 1 or level 2 routing, this command clears existing routes for both levels of IS-IS routing from the routing table.

1.98.5 Usage Guidelines

Use the **clear isis routes** command to clear existing routes from the IS-IS routing table and to repopulate the table with updated route information.

1.98.6 Examples

The following example shows how to clear all IS-IS level 1 and level 2 routes from the routing table:

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

1.99 clear isis statistics

clear isis [***instance-name***] **statistics** [**level-1** | **level-2**]

1.99.1 Purpose

Clears Intermediate System-to-Intermediate System (IS-IS) statistics.

1.99.2 Command Mode

exec (10)

1.99.3 Syntax Description

instance-name Optional. IS-IS instance name. Required only if more than one instance is configured for the context.

level-1 Optional. Clears level 1 IS-IS statistics.

level-2 Optional. Clears level 2 IS-IS statistics.

1.99.4 Default

When entered without specifying either level 1 or level 2 routing, this command clears statistics for both levels of IS-IS routing.

1.99.5 Usage Guidelines

Use the **clear isis statistics** command to clear IS-IS statistics.

1.99.6 Examples

The following example shows how to clear IS-IS statistics for **level-2** routing:

```
[local]Redback#clear isis statistics level-2
```

1.100 clear isp-log

clear isp-log

1.100.1 Purpose

Clears all entries in the ISP log file.

1.100.2 Command Mode

exec (15)

1.100.3 Syntax Description

This command has no keywords or arguments.

1.100.4 Default

None

1.100.5 Usage Guidelines

Use the **clear isp-log** command to clear the ISP log file. When you enter the command, the system prompts you whether you want to clear the ISP log file. Select **y** to clear all entries from the ISP log file.

1.100.6 Examples

The following example shows how to clear the ISP log file:

```
[local]Redback#clear isp-log
Are you sure you want to clear ISP log (y/n)?y
[local]Redback#
```

1.101 clear l2tp

clear l2tp {**peer** ***peer-name*** [**tunnel** ***tunl-num*** [**session** ***ses-num***]]}

1.101.1 Purpose

Shuts down all or specified tunnels or sessions to a Layer 2 Tunneling Protocol (L2TP) peer or to the members of an L2TP group.

1.101.2 Command Mode

exec (10)

1.101.3 Syntax Description

peer ***peer-name***	Name of an L2TP peer or its domain alias.
tunnel ***tunl-num***	Optional when you use the **peer** ***peer-name*** construct. Tunnel number of a particular L2TP tunnel to be shut down.
session ***ses-num***	Optional when you use the **tunnel** ***tunl-num*** construct. Session number of a particular L2TP session to be shut down.

1.101.4 Default

No tunnels are cleared.

1.101.5 Usage Guidelines

Use the **clear l2tp** command to shut down L2TP tunnels or sessions. You can shut down all tunnels to a specified peer if you use this command without any optional constructs. To shut down a specific tunnel and all the sessions within that tunnel, specify it by using the **`tunnel`** ***`tunl-num`*** construct. To shut down a specific session, specify the tunnel and session by using both the **`tunnel`** ***`tunl-num`*** and **`session`** ***`ses-num`*** constructs. You can determine the values for the ***`tunl-num`*** and ***`ses-num`*** arguments with the **`show l2tp peer`** command (in any mode).

For a Remote Authentication Dial-In User Service (RADIUS) based configuration, this command is useful to implement a new configuration. After this command is issued, the next RADIUS connection reads the new configuration.

1.101.6 Examples

The following example shows how to shut down all tunnels to an L2TP peer, **lns.net:**

```
[local]Redback#clear l2tp peer lns.net
```

1.102 clear ldp

`clear ldp` [**`*`** | **`neighbor`** *`ip-addr`*] [**`notify`**]

1.102.1 Purpose

Clears Label Distribution Protocol (LDP) sessions for all neighbors or a specific neighbor.

1.102.2 Command Mode

Exec (10)

1.102.3 Syntax Description

`*`	Optional. Clears LDP sessions for all neighbors.
`neighbor` *`ip-addr`*	Optional. Neighbor IP address, in the form *`A.B.C.D`*, for which to clear LDP sessions. LDP sessions are cleared only for the neighbor at the specified IP address.
`notify`	Optional. Sends a notification message to neighbors. When neighbors receive the notification message, they immediately drop their connection.

1.102.4 Default

None

1.102.5 Usage Guidelines

Use the **`clear ldp`** command to clear LDP sessions for all neighbors or a specific neighbor.

1.102.6 Examples

The following example shows how to clear LDP sessions for all neighbors:

```
[local]Redback>clear ldp *
```

The following example shows how to clear LDP sessions for a specific neighbor. In this example, the user specifies that a notification message is sent to the neighbor at the IP address 10.1.1.1:

```
[local]Redback>clear ldp neighbor 10.1.1.1 notify
```

1.103 clear log

`clear log`

1.103.1 Purpose

Clears the system event log buffer.

1.103.2 Command Mode

exec (10)

1.103.3 Syntax Description

This command has no keywords or arguments.

1.103.4 Default

None

1.103.5 Usage Guidelines

Use the **clear log** command to clear the system event log buffer. Use the **save log** command (in exec mode) to keep the current log buffer before you clear it.

1.103.6 Examples

The following example shows how to clear the system event log buffer:

```
[local]Redback#clear log
```

1.104 clear logger statistics drop-counter

clear logger statistics drop-counter {**all** | **debug** | **log**}

1.104.1 Purpose

Clears one or more statistics drop counters for the logging facility (logger).

1.104.2 Command Mode

Exec (10)

1.104.3 Syntax Description

all	Clears all drop counters for the logger.
debug	Clears the debug message drop counter for the logger.
log	Clears the log message drop counter for the logger.

1.104.4 Default

None

1.104.5 Usage Guidelines

Use the **clear logger statistics drop-counter** command to clear one or more statistics drop counters for the logger.

1.104.6 Examples

The following example shows how to clear the debug message drop counter for the logger:

```
[local]Redback#clear logger statistics drop-counter debug
```

1.105 clear malicious-traffic log

clear malicious-traffic log [**file** ***filename***]

1.105.1 Purpose

Clear malicious traffic data.

1.105.2 Command Mode

Exec

1.105.3 Syntax Description

file ***filename***	Optional. Clear malicious traffic in a log file. Specify the name of a log file.

1.105.4 Default

None

1.105.5 Usage Guidelines

Use the **clear malicious-traffic log** command to clear malicious traffic data. To clear malicious traffic data stored in the in-memory buffer or in a specified file (binary or text format), use the **clear malicious-traffic log file** command. If a file is specified, all versions of the file are cleared and then logging to these files resumes again.

Note: When using the **clear malicious-traffic log file** command from a non-local context, only files configured for that context can be cleared.

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

1.105.6 Examples

The following example shows how to clear malicious traffic data:

```
[local]Redback#clear malicious-traffic log
```

1.106 clear mobile-ip binding

`clear mobile-ip binding` {*`ip-addr`* | **`nai`** *`nai`*}

1.106.1 Purpose

Clears mobile node (MN) binding maintained by the home-agent (HA) instance.

1.106.2 Command Mode

Exec (10)

1.106.3 Syntax Description

`nai` *`nai`*	Network Access Identifier (NAI) of the MN.
`ip-addr`	IP address of the MN.

1.106.4 Default

None

1.106.5 Usage Guidelines

Use the **`clear mobile-ip binding`** command to clear an MN binding maintained by the HA instance. If revocation is configured and negotiated for the binding, a registration revocation is sent to the foreign agent (FA) serving the MN.

1.106.6 Examples

The following example shows how to clear MN bindings on the HA instance with an IP address **172.16.2.1:**

```
[local]Redback#clear mobile-ip binding 172.16.2.1
```

1.107 clear mobile-ip counters

`clear mobile-ip counters`

1.107.1 Purpose

Clears Mobile IP counters for a foreign-agent (FA) instance or home-agent (HA) instance.

1.107.2 Command Mode

Exec (10)

1.107.3 Syntax Description

This command has no keywords or arguments.

1.107.4 Default

None

1.107.5 Usage Guidelines

Use the **`clear mobile-ip counters`** command to clear Mobile IP counters for an FA instance or an HA instance depending on what is configured on the context.

1.107.6 Examples

The following example shows how to clear the counters for an FA instance:

```
[local]Redback#clear mobile-ip counters
```

1.108 clear mobile-ip dynamic-keys

clear-mobile-ip dynamic-keys {**`home-agent-peer`** ***`ip-address`*** | **`foreign-agent-peer`** ***`ip-address`*** | **`local-address`** ***`if-name`*** [**`context`** ***`ctx-name`***]} **`[spi`** ***`spi-num]`***

1.108.1 Purpose

Clear Mobile IP dynamic FA-HA authentication keys corresponding to the specified home-agent (HA) peer, foreign-agent (FA) peer, or (HA) local-address.

1.108.2 Command Mode

Exec (10)

1.108.3 Syntax Description

home-agent-peer *ip-addr*	IP address for an HA peer
foreign-agent-peer *ip-addr*}	IP address for an FA peer.
local-address *if-name*	Name of the local interface on the HA for which dynamic keys have to be cleared.
context *ctx-name*	Optional. Context name in which the interface exists. If the interface exists in a context other than the one you are currently in, you must specify the context name.
spi *spi-num*	Optional. SPI index number. The range of values is 256 to 4294967295.

1.108.4 Default

None

1.108.5 Usage Guidelines

Use the **clear mobile-ip dynamic-keys** command to clear Mobile IP dynamic FA-HA authentication keys corresponding to the specified HA peer, FA peer, or HA local-address.

1.108.6 Examples

The following example show how to clear dynamic keys for `10.1.1.2 HA` peer:

```
[local]Redback#clear mobile-ip home-agent-peer 10.1.1.2 context local
```

1.109 clear mobile-ip foreign-agent-peer

clear mobile-ip foreign-agent-peer *ip-addr* {**bindings** | **counters**}

1.109.1 Purpose

Clears foreign-agent (FA) peer bindings by shutting down FA peer and bringing it back up, or clears the FA peer counters.

1.109.2 Command Mode

Exec (10)

1.109.3 Syntax Description

ip-addr	IP address of the FA peer.
bindings	Clears bindings for the FA peer.
counters	Clears counters for the FA peer.

1.109.4 Default

None

1.109.5 Usage Guidelines

Use the **clear mobile-ip foreign-agent-peer** command to clear the FA peer bindings by shutting down the FA peer and bringing it back up, or to clear FA peer counters.

1.109.6 Examples

The following example shows how to clear counters for the FA peer with the IP address **172.16.2.1**:

```
[local]Redback#clear mobile-ip foreign-agent-peer 172.16.2.1 counters
```

1.110 clear mobile-ip home-agent-peer

clear mobile-ip home-agent-peer *ip-addr* (**visitors** | **counters**)

1.110.1 Purpose

Clears home-agent (HA) peer visitors by shutting down the HA peer and bringing it back up on a foreign-agent (FA) instance, or clears HA peer counters.

1.110.2 Command Mode

Exec (10)

1.110.3 Syntax Description

ip-addr	IP address of the HA peer to be cleared.
counters	HA peer counters.
visitors	HA peer visitors.

1.110.4 Default

None

1.110.5 Usage Guidelines

Use the **clear mobile-ip home-agent-peer** command to clear HA peer visitors by shutting down the HA peer and bringing it back up on an FA instance, or to clear HA peer counters.

1.110.6 Examples

The following example shows how to clear HA peer counters on an FA instance with an IP address **172.16.2.1**:

```
[local]Redback#clear mobile-ip home-agent-peer 172.16.2.1 counters
```

1.111 clear mobile-ip interface

clear mobile-ip interface *if-name* (**visitors** | **counters**)

1.111.1 Purpose

Clears counters associated with the foreign-agent (FA) instance access interface, or to clear the FA instance access interface, including all Mobile IP visitors associated with the access interface.

1.111.2 Command Mode

Exec (10)

1.111.3 Syntax Description

if-name FA access interface to be cleared.

visitors FA access interface, including all Mobile IP visitors associated with the interface.

counters Counters associated with the specified FA access interface.

1.111.4 Default

None

1.111.5 Usage Guidelines

Use the **clear mobile-ip interface** command to clear counters associated with the FA access interface or to clear the FA access interface, including all Mobile IP visitors associated with the access interface.

1.111.6 Examples

The following example shows how to clear counters associated with the FA access interface **interface1**:

```
[local]Redback#clear mobile-ip interface interface1 counters
```

1.112 clear mobile-ip visitor

clear mobile-ip visitor {*ip-addr* | **nai** *nai*}

1.112.1 Purpose

Clears a visiting mobile node (MN) on a foreign agent (FA) instance.

1.112.2 Command Mode

exec (10)

1.112.3 Syntax Description

ip-addr IP address of the visitor MN to be cleared.

nai *nai* Network Access Identifier (NAI) of the visitor MN.

1.112.4 Default

None

1.112.5 Usage Guidelines

Use the **clear mobile-ip visitor** command to clear a visitor MN on an FA instance.

1.112.6 Examples

The following example shows how to clear the visitor MN on an FA instance with the IP address **10.1.1.20:**

```
[local]Redback#clear mobile-ip visitor 10.1.1.20
```

Glossary

PDH
Plesiochronous Digital Hierarchy

STS-1
Synchronous transport signal level 1

VT-1.5
Virtual tributary 1.5