ERICSSON

Commands: lj through mo

COMMAND DESCRIPTION

11/190 82-CRA 119 1170/1-V1 Uen K

Contents

1 Command Descriptions

Commands starting with “lj” through “mo” 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 llc-xid-processing

`llc-xid-processing`

`no llc-xid-processing`

1.1.1 Purpose

Enables the SmartEdge router to detect the access interface change of a mobile node (MN) based on logical link control (LLC) exchange ID (XID) messages received on a circuit.

1.1.2 Command Mode

FA configuration

1.1.3 Syntax Description

This command has no keywords or arguments.

1.1.4 Default

The detection of access interface changes of a MN based on LLC XID messages received on a circuit is enabled.

1.1.5 Usage Guidelines

Use the **llc-xid-processing** command to enable SmartEdge router to detect the access interface changes of a MN based on LLC XID messages received on a circuit.

When XID is enabled, the SmartEdge router uses the received LLC XID frame to change the access interface and circuit associated with the MN and transmits traffic to the MN over the new circuit. This feature allows for a quick traffic switchover if the relocation of an MN remains in the same FA instance.

If you disable XID, the SmartEdge router must process a Mobile IP registration message on the new interface before the MN can be moved to a new access interface.

Use the **no** form of this command to disable LLC XID message processing.

1.1.6 Examples

The following example shows how to disable LLC XID message processing:

```
[local]Redback(config)#context fa
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#foreign-agent
[local]Redback(config-mip-fa)#no llc-xid-processing
```

1.2 lns card

lns card {**selection** {**route** | **priority**} | ***slot*** **preference** ***preference***}

{**no** | **default**} **lns card** {**selection** | ***slot***}

1.2.1 Purpose

Configures slot redundancy for Layer 2 Tunneling Protocol (L2TP) sessions.

1.2.2 Command Mode

L2TP peer configuration

1.2.3 Syntax Description

selection	Selects the algorithm by which a traffic card is selected for an L2TP session.
route	Specifies the route algorithm; this is the default.
priority	Specifies the priority algorithm.
slot	Chassis slot number of a traffic card on which L2TP sessions are to be carried.
preference ***preference***	Relative preference of one traffic card over another as the choice for an L2TP session; the default value is equal preference for all traffic cards.

1.2.4 Default

The default algorithm is route, and if multiple traffic cards are available, sessions are load balanced between them (equal preference for all cards).

1.2.5 Usage Guidelines

Use the **lns card** command to configure slot redundancy for L2TP sessions between the SmartEdge router and an L2TP access concentrator (LAC). You enter this command to first select the algorithm by which a traffic card is selected to carry L2TP subscriber sessions; you enter it again one or more times to specify the traffic cards that can carry L2TP subscriber sessions. You must specify the **lns-only** keyword with the **function** command in L2TP peer configuration mode for this peer before entering this command.

The route algorithm establishes the traffic card with the route to the LAC as the preferred traffic card without explicitly specifying it. This algorithm allows you to establish the preference of one traffic card over all others when its slot is not known. The priority algorithm fixes the traffic card preferences based on an explicit configuration statement. If you specify the **priority** keyword, you must identify all the traffic cards on which L2TP sessions are to be carried.

The values that you specify for the ***preference*** argument are relative to each other and can be any integer: a smaller number has a higher preference. Cards with equal preference numbers are load balanced.

You must configure the traffic cards using the **card** command (in global configuration mode) prior to configuring slot redundancy for them. Sessions are not assigned to unconfigured traffic cards.

To display the status of slot redundancy, use the **show l2tp global** command in any mode with the **ipc** keyword.

Use the **no** or **default** form of this command to specify the default algorithm and traffic card preferences.

Note: The maximum number of sessions that a traffic card can carry is not configurable and depends on the amount of memory in each traffic card.

1.2.6 Examples

The following example shows how to enable slot redundancy by load balancing the sessions between the traffic cards in slots **10** and **11**, using the **priority** algorithm and equal preferences:

```
[local]Redback(config-l2tp)#lns card selection priority
[local]Redback(config-l2tp)#lns card 10 preference 10
[local]Redback(config-l2tp)#lns card 11 preference 10
```

The following example shows how to enable slot redundancy using the **route** algorithm; the traffic card with the route to a LAC is the preferred traffic card, and then, when that traffic card reaches its maximum number of circuits, sessions are apportioned between the traffic cards in slots **1**, **2**, and **3**, with card **1** having the highest preference and card **3** having the lowest preference. The traffic card with the route, whatever its slot, always has the highest priority:

```
[local]Redback(config-l2tp)#lns card selection route
[local]Redback(config-l2tp)#lns card 1 preference 10
[local]Redback(config-l2tp)#lns card 2 preference 20
[local]Redback(config-l2tp)#lns card 3 preference 30
```

1.3 local-address

local-address ***if-name*** [***ctx-name***]

no local-address ***if-name*** [***ctx-name***]

1.3.1 Purpose

Specifies the interface for the home agent (HA) local address used by remote foreign agent (FA) peers for this HA instance.

1.3.2 Command Mode

HA configuration

1.3.3 Syntax Description

if-name	Name of the interface for the HA.
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.

1.3.4 Default

None

1.3.5 Usage Guidelines

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

Use the **no** form of this command to remove the HA local address.

1.3.6 Examples

The following example shows how to create the local address interface in a context called `ha` and specify it as the local address interface for the HA instance:

```
[local]Redback(config)#context ha
[local]Redback(config-ctx)#interface ha
[local]Redback(config-if)#ip address 10.1.1.2/16
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#home-agent
[local]Redback(config-ha)#local-address ha
```

1.4 local-as

local-as {*asn* | *nn*:*nn*} [**no-prepend** | **replace-as**]

no local-as {*asn* | *nn*:*nn*}

1.4.1 Purpose

Configures the autonomous system number (ASN) that the Border Gateway Protocol (BGP) routing process uses to peer with the specified external BGP (eBGP) neighbor.

For inbound updates, provides the **no-prepend** option to disable local AS prepending on incoming eBGP updates.

For outbound updates, provides the **replace-as** option to replace the router's own AS with the local AS on outgoing eBGP updates.

1.4.2 Command Mode

BGP neighbor configuration

1.4.3 Syntax Description

asn	ASN in integer format. The range of values is 1 to 4,294,967,295. 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.
no-prepend	Optional. For inbound updates, do not prepend the local AS number to routes received from the BGP neighbor.
replace-as	Optional. For outbound updates, replace the router's AS with the local AS number in the AS_PATH attribute.

1.4.4 Default

None

1.4.5 Usage Guidelines

Use the **local-as** command to specify the ASN that the BGP routing process uses to peer with the specified eBGP neighbor. Under most circumstances, the BGP routing process peers with neighbors that use the same ASN, which is configured through the **router bgp** command in context configuration mode. The **local-as** command allows the configuration of a different ASN to be used with the specified eBGP neighbor. Use the **no** form of this command to remove the local ASN.

The **no-prepend** option disables the prepending of the local AS to routes received from the eBGP neighbor in inbound updates. The **replace-as** option

replaces the router's global ASN with the local AS in outbound updates. Both **no-prepend** and **replace-as** options can be used separately or together.

Note: The **no-prepend** and **replace-as** options are supported between two Autonomous systems but not between Member-AS within the same confederation.

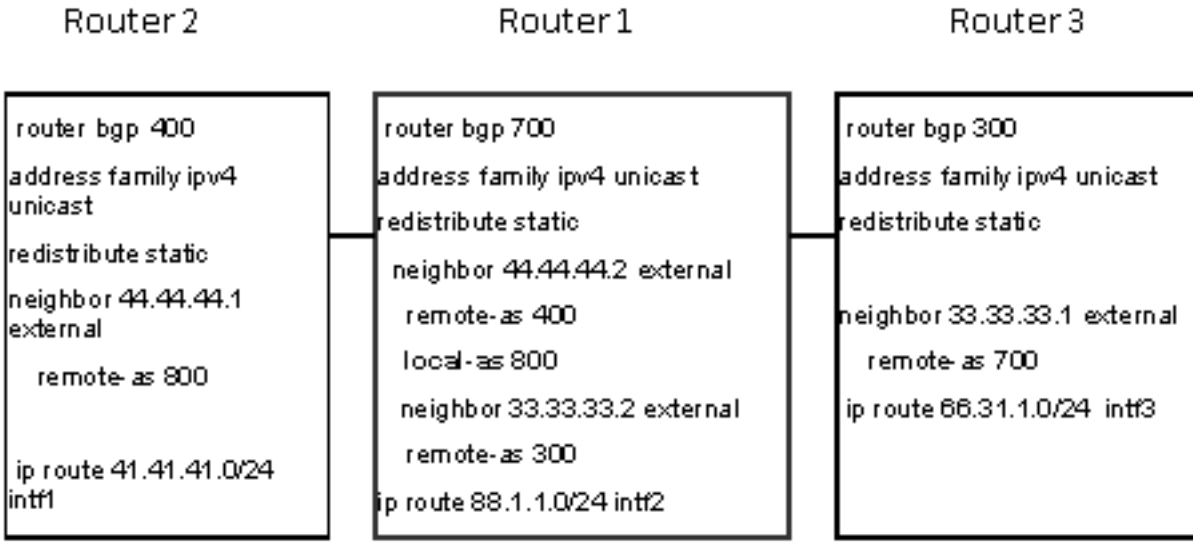
Note: The **no-prepend** and **replace-as** options have a similar effect on the as-path attribute even if the as-path attribute has been modified by commands such as **route-map**, **ext-community**, using the **set as-path prepend** option.

1.4.6 Examples

The following example shows how to configure an ASN of **100** for the SmartEdge router. The SmartEdge router peers with the neighbors at IP address, **102.210.210.1**, and IP address, **103.220.220.3**, using ASN **100**. However, it peers with the neighbor at IP address, **68.68.68.68**, using ASN **200** because of the local-AS feature.

```
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#neighbor 102.210.210.1 external
[local]Redback(config-bgp-neighbor)#remote-as 500
[local]Redback(config-bgp-neighbor)#address-family ipv4 unicast
[local]Redback(config-bgp-peer-af)#exit
[local]Redback(config-bgp-neighbor)#exit
[local]Redback(config-bgp)#neighbor 103.220.220.3 external
[local]Redback(config-bgp-neighbor)#remote-as 300
[local]Redback(config-bgp-neighbor)#address-family ipv4 unicast
[local]Redback(config-bgp-peer-af)#exit
[local]Redback(config-bgp-neighbor)#exit
[local]Redback(config-bgp)#neighbor 68.68.68.68 external
[local]Redback(config-bgp-neighbor)#remote-as 400
[local]Redback(config-bgp-neighbor)#local-as 200
[local]Redback(config-bgp-neighbor)#address-family ipv4 unicast
```

The following examples establish peering between router 1 and router 2 using the local-as feature, and peering between router 1 and router 3 without the local-as feature. They also show how to customize both the inbound and outbound update messages. By using the **no-prepend** option, the local-as is not prepended in the inbound update message. By using the **replace-as** option, the global ASN is replaced with the local-as in the outbound update message.




```
Router1(config)# router bgp 700
Router1(config-router)# neighbor 44.44.44.2 external
Router1(config-router)# remote-as 400
Router1(config-router)# local-as 800 no-prepend

show bgp route output :
On router 1 :
   Network            Next Hop                Metric  LocPrf  Weight Path
>  41.41.41.0/24      44.44.44.2                   0     100     100  400 ?
local-as 800 is not prepended to inbound update.
>  66.31.1.0/24       33.33.33.2                   0     100     100  300 ?
>  88.1.1.0/24        33.33.33.2                   0     100   32768 ?
```

```
Router1(config)#router bgp 700
Router1(config-router)# neighbor 44.44.44.2 external
Router1(config-router)# remote-as 400
Router1(config-router)# local-as 800 replace-as

On router 1 :
Network            Next Hop                Metric  LocPrf  Weight Path
>  41.41.41.0/24      44.44.44.2                    0     100     100 800 400 ?
Inbound update has local-as 800.
>  66.31.1.0/24       33.33.33.2                    0     100     100 300 ?
>  88.1.1.0/24        33.33.33.2                    0     100   32768 ?
On router 2  :
   Network            Next Hop                Metric  LocPrf  Weight Path
>  66.31.1.0/24       44.44.44.1                    0     100     100 800  300  ?
>  88.1.1.0/24        44.44.44.1                    0     100     100 800  ?
Outboud update from router 1 to router 2 replaces autonomous AS 700 with local-a
On router 3 :
   Network            Next Hop                Metric  LocPrf  Weight Path
>  41.41.41.0/24      33.33.33.1                    0     100     100 700 800 400
Inbound message has local-as and autonomous AS.
>  66.31.1.0/24       33.33.33.1                    0     100   32768 ?
>  88.1.1.0/24        33.33.33.1                    0     100     100 700 ?
```

1.5 localdir

localdir ***dir-name***

no localdir ***dir-name***

1.5.1 Purpose

Specifies the local directory on the SmartEdge router where bulkstats data for this policy is stored.

1.5.2 Command Mode

bulkstats configuration

1.5.3 Syntax Description

dir-name	Local directory where bulkstats collection files for this policy are stored.

1.5.4 Default

None

1.5.5 Usage Guidelines

Use the **localdir** command to specify the local directory where bulkstats collection files for this policy are stored.

You must first create a local directory using the **mkdir** command (in exec mode) before you enable bulkstats collection. For more information on the **mkdir** command, see the *Command List*. You can specify a directory on the local file system (/flash) or the mass-storage device (/md). (The mass-storage device is preferable due to its faster write speed.) You can limit the space allowed for bulkstats storage with the **limit** command.

You cannot change the local directory while bulkstats collection is enabled; you must first disable bulkstats collection for this policy using the **collection** command in bulkstats configuration mode and then reenable bulkstats collection after entering the **localdir** command.

Use the **no** form of this command to remove the configuration of the current local directory used to store bulkstats data for this policy. You should disable bulkstats collection for the policy using the **collection** command in bulkstats configuration mode before you delete the configuration.

1.5.6 Examples

The following example shows how to store bulkstats collection files for the policy, **bulk**, in the **/md/blksts** directory:

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

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

[local]Redback(config-bulkstats)#localdir /md/blksts
```

1.6 local-mode

local-mode {**mtu-s** | **pe-rs**}

{**no** | **default**} **local-mode**

1.6.1 Purpose

Sets the local mode of operation for the neighbor connection.

1.6.2 Command Mode

VPLS profile neighbor configuration

1.6.3 Syntax Description

mtu-s	Sets the local mode to multi-tenant unit switch (MTU-s). This mode is used when the local router is participating in hierarchical Virtual Private LAN Services (VPLS) by using a pseudowire connected to a core provider edge routers (PE-rs) device, and when the local VPLS instance does not have a mesh of pseudowire to all the core PE devices.
pe-rs	Sets the local mode to PE-rs. This mode is used at a core VPLS PE device that is providing hierarchical VPLS connectivity to other MTU-s routers.

1.6.4 Default

The PE-rs mode is set.

1.6.5 Usage Guidelines

Use the **local-mode** command to set the local mode of operation for the neighbor connection. This command applies only if a spoke connection type is configured for the neighbor. With a spoke connection type, one end of the connection must be set to MTU-s mode and the other must be set to PE-rs mode.

Note: For proper VPLS operation, ensure that the local mode at both ends is set correctly.

Use the **no** or **default** form of this command to return the local mode of operation to PE-rs.

1.6.6 Examples

The following example shows how to set the local mode to **mtu-s:**

```
[local]Redback#config

[local]Redback(config)#vpls profile foo

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

[local]Redback(config-vpls-profile-neighbor)#local-mode mtu-s

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

1.7 local-name

local-name ***local-name***

{**no** | **default**} **local-name**

1.7.1 Purpose

Creates a local name for the SmartEdge router, to be used in outbound Start-Control-Connection-Request (SCCRQ) or Start-Control-Connection-Reply (SCCRP) control messages to an Layer 2 Tunneling Protocol (L2TP) peer.

1.7.2 Command Mode

L2TP peer configuration

1.7.3 Syntax Description

local-name	Another name for the SmartEdge router to be used as the value for the Host name attribute-value pair (AVP), AVP 7, instead of the system hostname in SCCRQ or SCCRP messages to and from this L2TP peer.

1.7.4 Default

The system hostname, as specified by the **system hostname** command in global configuration mode, is used as the local name.

1.7.5 Usage Guidelines

Use the **local-name** command to create a local name for the SmartEdge router. Usually, the system hostname is used as the local name for the SmartEdge router.

You can create a different local name for the SmartEdge router for each tunnel that you configure, but the names must be unique.

The ***local-name*** argument is sent in the SCCRQ message when initializing the tunnel.

Use the **no** or **default** form of this command to specify the default local name. To change a local name, create a new one and it overwrites the existing one.

1.7.6 Examples

The following example shows how to specify the local name, **cardinal:**

```
[local]Redback(config-ctx)#l2tp-peer name peer1
[local]Redback(config-l2tp)#local-name cardinal
```

1.8 local-preference

local-preference ***pref-num***

no local-preference ***pref-num***

1.8.1 Purpose

Configures the value of the local preference number, a value that is applied to Border Gateway Protocol (BGP) routes that do not have the local-preference attribute.

1.8.2 Command Mode

BGP router configuration

1.8.3 Syntax Description

pref-num	Local preference number. The range of values is 0 to 4,294,967,295; the default value is 100.

1.8.4 Default

The default preference is 100.

1.8.5 Usage Guidelines

Use the **local-preference** command to configure the value of the local preference number.

Use the **no** form of this command to restore the default local preference value of 100.

1.8.6 Examples

The following example shows how to set the preference to **300:**

```
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#local-preference 300
```

1.9 local-protection

local-protection

no local-protection

1.9.1 Purpose

Permits a label-switched path (LSP) to be protected by a bypass Resource Reservation Protocol (RSVP) LSP.

1.9.2 Command Mode

RSVP LSP configuration

1.9.3 Syntax Description

This command has no keywords or arguments.

1.9.4 Default

Local protection is permitted.

1.9.5 Usage Guidelines

Use the **local-protection** command to permit an LSP to be protected by a bypass RSVP LSP. When configured, the LSP advertises to the ingress and

transit nodes that a bypass RSVP LSP can be used to provide Multiprotocol Label Switching (MPLS) fast reroute protection. This configuration will affect both ingress node and the transit nodes of the LSP operation.

Use the **no** form of this command to deny an LSP from being protected by a bypass RSVP LSP. Local protection can be denied for operational or resource issues.

1.9.6 Examples

The following example shows how to configure an RSVP LSP, **to-r2-core**, to deny MPLS fast reroute protection:

```
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#lsp to-r2-core
[local]Redback(config-rsvp-lsp)#no local-protection
```

1.10 logging active

logging active

{no | default} logging active

1.10.1 Purpose

Enables the logger to send logging and debug messages from the active controller card to the standby controller card.

1.10.2 Command Mode

Global configuration

1.10.3 Syntax Description

This command has no keywords or arguments.

1.10.4 Default

Logging and debug messages are sent to the standby controller card.

1.10.5 Usage Guidelines

Use the **logging active** command to enable the sending of logging and debug messages from the active controller card to the standby controller card.

Note: The SmartEdge 100 router does not support this command.

Note: If you do not specify the **short** keyword, the message is logged on the active controller card using the same severity as the original log message.

Use the **no** or **default** form of this command to disable the sending of logging and debug messages to the standby controller card.

1.10.6 Examples

The following example shows how to enable the sending of logging and debug messages to the standby controller card:

```
[local]Redback(config)#logging active
```

1.11 logging cct-valid

logging cct-valid

{no | default} logging cct-valid

1.11.1 Purpose

Enables the filtering of debug messages for valid circuits only.

1.11.2 Command Mode

Global configuration

1.11.3 Syntax Description

This command has no keywords or arguments.

1.11.4 Default

Filtering of logging and debug messages for circuits is disabled.

1.11.5 Usage Guidelines

Use the **logging cct-valid** command to enable the filtering of debug messages for valid circuits only.

Use the **no** or **default** form of this command to disable the filtering of debug messages by circuit.

1.11.6 Examples

The following example shows how to enable the filtering of debug messages for valid circuits only:

```
[local]Redback(config)#logging cct-valid
```

1.12 logging console

logging console

no logging console

1.12.1 Purpose

Enables event logging messages to the console.

1.12.2 Command Mode

Context configuration

1.12.3 Syntax Description

This command has no keywords or arguments.

1.12.4 Default

Console logging for contexts other than local is disabled.

1.12.5 Usage Guidelines

Use the **logging console** command (in context configuration mode) to quickly isolate problems by displaying event log messages directly to the console rather than to a file. Messages sent to the console can be further

constrained by using the **logging filter** command in context configuration mode to establish a logging filter.

Use the **no** form of this command to disable event logging to the console.

1.12.6 Examples

The following example shows how to enable event logging messages to the console:

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

1.13 logging debug

logging debug [active | standby]

{no | default} logging debug [active | standby]

1.13.1 Purpose

Stores messages that have been generated by all enabled debug processes in the log buffer.

1.13.2 Command Mode

Global configuration

1.13.3 Syntax Description

active	Configure the system to send debug events from the active to standby XCRP
standby	Configure the system to send debug events from the standby to active XCRP

1.13.4 Default

Debugging messages are not stored in the log buffer.

1.13.5 Usage Guidelines

Use the **logging debug** command to store messages for all enabled debugging processes in the log buffer. Use the *show log* command in any

mode to display the logged messages. Use the **active** keyword to configure the system to send debug events from the active to standby XCRP and the **standby** keyword to configure the system to send debug events from the standby to active XCRP.

The **default** and **no** forms of this command without keywords to revert to default behavior, where the system does not store debug messages in the log buffer.

After you enable the **logging debug** command, you can use **no logging debug active** or **default logging debug active** to stop sending debug messages from the active to standby XCRP, while still sending debug messages to the log buffer. Similarly, after you enable the **logging debug** command, you can use **no logging debug standby** or **default logging debug standby** to stop sending debug messages from the standby to the active XCRP, while still sending debug messages to the log buffer.

1.13.6 Examples

The following example shows how to enable the logging of debugging messages to the log buffer:

```
[local]Redback(config)#logging debug
```

The following example shows how to store messages for enabled debugging processes in the log buffer, send debug messages to standby to active XCRP, and stop sending debug messages from the active to standby XCRP.

```
[local]Redback(config)#logging debug
[local]Redback(config)#logging debug standby
[local]Redback(config)#no logging debug active
```

1.14 logging file

logging file [**text**] ***filename***

no logging file [**text**] ***filename***

1.14.1 Purpose

Enables event logging messages to a file.

1.14.2 Command Mode

Context configuration

1.14.3 Syntax Description

text	Optional. Specifies that the log file is to be saved as a text, rather than binary, file.
filename	Name of the file to which events are logged.

1.14.4 Default

If you do not use this command, events are not logged to a file. If you use this command without the optional **text** keyword, the file is saved in binary form.

1.14.5 Usage Guidelines

Use the **logging file** command to enable event logging messages to a file. You can also configure up to four log files per context.

Use the ***filename*** argument to specify the name and path of the logging file. If the full path is not specified, the file is saved to the /flash directory.

Use the **show log** command in any mode to display log files. For more information on the **show log** command, *Command List*.

Use the **no** form of this command to disable the enabling of event log messages to a file.

1.14.6 Examples

The following example shows how to enable the storing of event logs to a file, **/flash/log_file:**

```
[local]Redback(config-ctx)#logging file /flash/log_file
```

1.15 logging filter

logging filter {**console** | **file** | **monitor** | **syslog**} ***level***

default logging filter {**console** | **file** | **monitor** | **syslog**}

1.15.1 Purpose

Isolates events based on message severity in the logs and trims the flow of information.

1.15.2 Command Mode

Context configuration

1.15.3 Syntax Description

console	Specifies the console filter type.
file	Specifies the file filter type.
monitor	Specifies the monitor filter type.
syslog	Specifies the syslog server filter type.
level	Filter logging level, according to one of the following keywords (in descending priority order): • **emergency**—Logs only emergency events. • **alert**—Logs alert and more severe events. • **critical**—Logs critical and more severe events. • **error**—Logs error and more severe events. • **warning**—Logs warning and more severe events. • **notice**—Logs notice and more severe events. • **informational**—Logs informational and more severe events. • **debug**—Logs all events, including debug events.

1.15.4 Default

The default filter levels for the **console**, **file**, **monitor**, and **syslog** keywords are set to **debug**.

Table 1 describes the default input and output filter levels for each filter type.

Table 1 Default Filter Levels

Input Filter	Output Filter
console	debug
monitor	debug
runtime	informational
syslog	notice

1.15.5 Usage Guidelines

Use the **logging filter** command to isolate events based on certain severities in the logs and trim the flow of information.

Use the **show logging** command in any mode to display the configured filter levels for the current context. For more information on the **show log** command, see the *Command List*.

Use the **default** form of this command to set a logging filter back to its default level.

1.15.6 Examples

The following example shows how to modify the severity level for several log facilities:

```
[local]Redback(config-ctx)#logging filter monitor error
```

The following example shows how to modify the severity level for console:

```
[local]Redback(config-ctx)#logging filter console critical
```

1.16 logging malicious-traffic category

logging malicious-traffic category [all | failed-reassembly | filtered | malformed-ip | malformed-layer4 | other | spoofed]

no logging malicious-traffic category [all | failed-reassembly | filtered | malformed-ip | malformed-layer4 | other | spoofed]

1.16.1 Purpose

Enable logging of a specified category of malicious traffic.

1.16.2 Command Mode

context configuration

1.16.3 Syntax Description

all	Log all malicious packets.
failed-reassembly	Log failed reassemble malicious packets.
filtered	Log filtered malicious packets.
malformed-ip	Log malformed IP malicious packets.
malformed-layer4	Log malformed Layer 4 malicious packets.
other	Log other malicious traffic packets.
spoofed	Log spoofed malicious packets.

1.16.4 Default

Logging of malicious traffic is disabled by default.

1.16.5 Usage Guidelines

Use the **logging malicious-traffic category** command to enable logging of a specified category of malicious traffic.

Use the **no** form of this command to disable logging of a specified category of malicious traffic.

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

1.16.6 Examples

The following example shows how to enable logging of malformed IP malicious packets:

```
[local]Redback(config-ctx)#logging malicious-traffic category malformed-ip
```

1.17 logging malicious-traffic file

logging malicious-traffic file {***filename*** | **text** ***filename***}

no logging malicious-traffic file {***filename***| **text** ***filename***}

1.17.1 Purpose

Enable logging of malicious traffic messages to a file.

1.17.2 Command Mode

context configuration

1.17.3 Syntax Description

text	Optional. Save the log file as a text file instead of a binary file.
filename	Name of the file to which malicious traffic is logged.

1.17.4 Default

Logging of malicious traffic is disabled by default. If the file name is not specified, the log message is saved to an in-memory circular buffer. If you use this command without the optional **text** keyword, the file is saved in binary format.

1.17.5 Usage Guidelines

Use the **logging malicious-traffic file** command to enable logging of malicious traffic to a local file. You can configure up to four log files for each context. Use the ***filename*** keyword to specify the name and path of the logging file. If the full path is not specified, the file is saved to the /flash directory.

Use the **show malicious-traffic log** command in any mode to display malicious-traffic log files.

Use the **no** form of this command to disable malicious traffic logging to a local file.

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

1.17.6 Examples

The following example shows how to enable the logging of malicious traffic logs to a file named **traffic_log** on the /flash directory:

```
[local]Redback(config-ctx)#logging malicious-traffic file /flash/maltraffic_log
```

The following example shows how to enable the logging of malicious traffic logs to a local text file named **mal_txt** on the /md directory:

```
[local]Redback(config-ctx)#logging malicious-traffic file text /md/mal_txt
```

1.18 logging malicious-traffic syslog

logging malicious-traffic syslog { [*ip-address*| *ip-address* **facility** *sys-facility-name*] }

no logging malicious-traffic syslog *ip-address*

1.18.1 Purpose

Enables logging of malicious traffic messages to a remote syslog server.

1.18.2 Command Mode

context configuration

1.18.3 Syntax Description

ip-address	IP address of the syslog server.
facility *sys-facility-name*	Optional. Specify the syslog logging facility. The range of values is local0 to local7; the default value is local7.

1.18.4 Default

Logging of malicious traffic messages to a remote syslog server is disabled by default.

1.18.5 Usage Guidelines

Use the **logging malicious-traffic syslog** command to enable logging of malicious traffic messages to a remote syslog server that is reachable within the context. The remote syslog server is identified by its IP address. You can configure up to four syslog servers per context.

Use the **no** form of this command to disable logging of malicious traffic messages to a remote syslog server.

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

1.18.6 Examples

The following example shows how to enable logging of malicious traffic to a remote syslog server at IP address **10.10.7.7** in the **ABC** context:

```
[local]Redback(config-ctx)#context ABC
logging malicious-traffic syslog 10.10.7.7
```

The following example shows how to enable logging of malicious traffic to a remote syslog server using a nondefault syslog facility:

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

[local]Redback(config-ctx)#logging malicious-traffic syslog 1.2.3.4 local1
```

1.19 logging rate-limit

logging rate-limit *rate-limit* **burst** *burst-limit*

{**no** | **default**} **logging rate-limit**

1.19.1 Purpose

Specifies the rate and burst limits for malicious traffic log events.

1.19.2 Command Mode

malicious-traffic configuration mode

1.19.3 Syntax Description

rate-limit	Maximum rate in packets per second (pps) at which the packets can be received. The range of values is 20 to 1,000.
burst *burst-limit*	Maximum number of packets that can be received during a short burst. The range of values is 20 to 10,000.

1.19.4 Default

The default value for both rate and burst limits is 100.

1.19.5 Usage Guidelines

Use the **logging rate-limit** command to specify the rate and burst limits for malicious traffic log events. The specified rate and burst values are distributed evenly across all of the active PPA2 and PPA3 cards. The actual

rate limit per active card is obtained by dividing the configured rate limit by the total number of active PPA2 and PPA3 cards. The same calculation applies to obtaining the actual burst limit for each active PPA2 or PPA3 card.

Use the **no** form of this command to disable or remove the rate limit for malicious traffic log events. Use the **default** form of this command to return to the default rate of 100 pps and burst limit of 100.

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

1.19.6 Examples

The following example shows how to specify a rate limit of **500** and a burst limit of **300** for malicious traffic log events.

```
[local]Redback(config-malicious-traffic)#logging
rate-limit 500 burst 300
```

1.20 logging standby

logging standby [**short**]

{no | default} logging standby short

1.20.1 Purpose

Enables the logger to send logging and debug messages from the standby controller card to the active controller card.

1.20.2 Command Mode

Global configuration

1.20.3 Syntax Description

short	Optional. Logs a message on the active controller card using a shorter, less verbose form when a message is sent from the standby controller card to the active controller card.

1.20.4 Default

Logging and debug messages are sent from the standby controller card to the active controller card.

1.20.5 Usage Guidelines

Use the **logging standby** command to enable the sending of logging and debug messages from the standby controller card to the active controller card.

Use the **short** keyword to display a message on the active controller card using a shorter, less verbose form.

Note: The SmartEdge 100 router does not support this command.

Note: If you do not specify the **short** keyword, the message is logged on the active controller card using the same severity as the original log message.

Use the **no** or **default** form of this command to disable the sending of logging and debug messages from the standby controller card to the active controller card.

1.20.6 Examples

The following example shows how to enable the sending of logging and debug messages to the standby controller card:

```
[local]Redback(config)#logging standby
```

1.21 logging syslog

logging syslog *ip-addr* [**facility** *sys-fac-name*]

no logging syslog *ip-addr*

1.21.1 Purpose

Enables the logging of system events to a remote syslog server that is reachable within the context.

1.21.2 Command Mode

Context configuration

1.21.3 Syntax Description

ip-addr	IP address of the syslog server.
facility ***sys-fac-name***	Optional. System logging facility. The range of values is local0 to local6; the default value is local6.

1.21.4 Default

System events logging is disabled.

1.21.5 Usage Guidelines

Use the **logging syslog** command to enable the logging of system events to a remote syslog server that is reachable within the context. The remote syslog server is identified by its IP address. You can also configure up to four syslog servers per context.

Use the **no** form of this command to disable the logging of system events to a remote syslog server.

1.21.6 Examples

The following example shows how to enable logging to a remote syslog server at IP address, **10.10.3.46**, in the **newworld** context:

```
[local]Redback(config)#context newworld
[local]Redback(config-ctx)#logging syslog 10.10.3.46
```

The following example shows a configuration using a non-default syslog facility:

```
[local]Redback(config)#context gretzky
[local]Redback(config-ctx)#logging syslog 1.2.3.4 local4
```

1.22 logging timestamp millisecond

logging timestamp millisecond

{no | default} logging timestamp millisecond

1.22.1 Purpose

Enables the display of logged system event messages with a millisecond resolution timestamp.

1.22.2 Command Mode

Global configuration

1.22.3 Syntax Description

This command has no keywords or arguments.

1.22.4 Default

Millisecond resolution is disabled and is not displayed.

1.22.5 Usage Guidelines

Use the **logging timestamp millisecond** command to enable the display of logged system event messages with a millisecond resolution timestamp.

Use the **no** or **default** form of this command to disable the display of logged system event messages with millisecond resolution.

1.22.6 Examples

The following example shows how to enable the display of logged system event messages with millisecond resolution:

```
[local]Redback(config)#logging timestamp millisecond
```

The following example displays system event log messages when millisecond resolution is enabled:

```
Oct 21 03:44:47.697: [0001]: %ISIS-7-ADJ: sent PTPT IIH on inter-ctx intf black
Oct 21 03:44:48.610: [0002]: %ISIS-7-ADJ:
 rcvd L2 LAN IIH from 001e.1000.0002 seq 16835 on inter-ctxintf bluefoo
```

1.23 log-neighbor-changes

log-neighbor-changes

no log-neighbor-changes

1.23.1 Purpose

Configures the Border Gateway Protocol (BGP) routing process to log BGP neighbor resets.

1.23.2 Command Mode

BGP router configuration

1.23.3 Syntax Description

This command has no keywords or arguments.

1.23.4 Default

BGP neighbor resets are logged.

1.23.5 Usage Guidelines

Use the **log-neighbor-changes** command to configure the BGP routing process to log BGP neighbor resets. Frequent resets could indicate excessive packet loss or other network problems.

Use the **no** form of this command to ensure that resets are not logged.

1.23.6 Examples

The following example shows how to configure the BGP routing process so that BGP neighbor resets are not logged:

```
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#no log-neighbor-changes
```

1.24 log-neighbor-up-down

log-neighbor-up-down

no log-neighbor-up-down

1.24.1 Purpose

Logs an informational message when a neighbor transitions to or from the full adjacency state.

1.24.2 Command Mode

- OSPF router configuration
- OSPF3 router configuration

1.24.3 Syntax Description

This command has no keywords or arguments.

1.24.4 Default

Transitions are not logged.

1.24.5 Usage Guidelines

Use the **log-neighbor-up-down** command to log an informational message when a neighbor transitions to or from the full adjacency state.

Use the **no** form of this command to disable the logging of messages for neighbor transition events.

1.24.6 Examples

The following example shows how to log neighbor transitions:

```
[local]Redback(config-ospf)#log-neighbor-up-down
```

1.25 log-lsp-up-down

log-lsp-up-down

no log-lsp-up-down

1.25.1 Purpose

Enables the logging of RSVP-INFO messages when any Resource Reservation Protocol (RSVP) label-switched path (LSP) changes state.

1.25.2 Command Mode

RSVP router configuration

1.25.3 Syntax Description

This command has no keywords or arguments.

1.25.4 Default

RSVP-INFO messages are not logged.

1.25.5 Usage Guidelines

Use the **log-lsp-up-down** command to enable the logging of RSVP-INFO messages when any RSVP LSP changes state. The state can change from Up to Down, or from Down to Up.

Note: The generation of RSVP-INFO messages cannot be disabled using the **no terminal monitor** command.

Use the **no** form of this command to disable the logging of RSVP-INFO messages.

1.25.6 Examples

The following example shows how to enable logging of RSVP-INFO messages when any RSVP LSP changes state:

```
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#log-lsp-up-down
```

1.26 log-pw-up-down

log-pw-up-down

no log-pw-up-down

1.26.1 Purpose

Logs the state of any XCs that have the specified L2VPN profile attached.

1.26.2 Command Mode

L2VPN profile peer configuration

1.26.3 Syntax Description

This command has no keywords or arguments.

1.26.4 Default

The state of an XC is not logged.

1.26.5 Usage Guidelines

Use the **log-pw-up-down** command to log the state of any XCs that have the specified L2VPN profile attached.

A log is created each time an XC transitions to the down, up, and standby states. The logs are saved in the ex syslog file or in a user-specified log file.

Use the **no** form of this command to disable the state logging for any XCs attached to the specified L2VPN profile.

1.26.6 Examples

The following example shows how to enable state logging for any XCs that have the L2VPN profile called `profile1 attached:`

```
[local]Redback(config)#l2vpn profile profile1
[local]Redback(config-l2vpn-xc-profile)#peer 100.100.100.1
[local]Redback(config-l2vpn-xc-profile-peer)#log-pw-up-down
```

1.27 log-state-changes

log-state-changes

no log-state-changes

1.27.1 Purpose

Enables the generation of a **TUNNEL-INFO** or **GRE-INFO** message each time the tunnel changes state (from up to down or down to up).

1.27.2 Command Mode

Tunnel configuration

1.27.3 Syntax Description

This command has no keywords or arguments.

1.27.4 Default

The generation of **TUNNEL-INFO** messages is disabled.

1.27.5 Usage Guidelines

Use the **log-state-changes** command to enable the generation of a message each time the tunnel changes state (from up to down or down to up).

Enables the generation of a **TUNNEL-INFO** or **GRE-INFO** message each time the tunnel changes state (from up to down or down to up).

To display the **TUNNEL-INFO** or **GRE-INFO** messages, enter the **show log** command (in any mode).

Note: You cannot disable the generation of **TUNNEL-INFO** or **GRE-INFO** messages with the **no terminal monitor** command (in exec mode).

Use the **no** form of this command to disable the generation of **TUNNEL-INFO** or **GRE-INFO** messages.

1.27.6 Examples

The following example shows how to enable the generation of a **TUNNEL-INFO** message each time the overlay tunnel, **DenverTn1**, in the **local** context changes state:

```
[local]Redback(config)#tunnel ipv6v4-manual DenverTnl
[local]Redback(config-tunnel)#log-state-changes
```

1.28 loopback (ATM, POS, Ethernet, WAN-PHY)

For an Ethernet port (not in WAN-PHY operating mode), the syntax in port configuration mode is:

loopback

no loopback

For a WAN-PHY Ethernet port, the syntax in port configuration mode is:

loopback {internal | line | payload}

no loopback

For a port on a 4-port ATM OC-3c/STM-1c traffic card or an ATM OC MIC, the syntax in ATM OC configuration mode is:

loopback {**internal** | **line** | **payload**}

no loopback

For a port on any other ATM OC traffic card or a Packet over SONET/SDH (POS) port, the syntax in ATM OC or port configuration mode is:

loopback {**internal** | **line**}

no loopback

1.28.1 Purpose and Usage Guidelines

Changes the operation of an ATM OC, Ethernet, WAN-PHY, or POS port to a loopback state.

Use the **no** form of this command to restore the port operation to a normal state.

Use the **show port detail** command (in any mode) to display the administrative state of the port. The Admin state field must be up to verify the remote link connectivity and quality with the **remote** keyword.

1.28.2 Command Mode

- ATM OC configuration
- Port configuration

1.28.3 Syntax Description

internal	Tests the internal functions of an ATM OC, POS, or WAN-PHY port by looping the transmit line to the receive line. The **internal** keyword for all ATM OC, POS, or WAN-PHY ports (with the exception of a port on a second-generation ATM OC traffic card) causes all transmitted traffic to be looped back and not sent to the remote site; instead, the remote site receives a loss of signal (LOS). For a port on a second-generation ATM OC traffic card, the port software injects an alarm indication signal-line (AIS-L) and then resumes transmitting traffic.
line	Tests the line operation of an ATM OC, POS, or WAN-PHY port by looping the receive line to the transmit line.
payload	Indicates that when the DS-3 frame on the SDH or SONET or WAN-PHY payload, is received and the frame or payload is extracted, it is to be reframed and returned.

1.28.4 Default

Port operation is in a normal state.

1.28.5 Examples

The following example shows how to change the port operation of an ATM OC port to loop transmitted frames back to the receive line:

```
[local]Redback(config)#port atm 3/1
[local]Redback(config-atm-oc)#loopback internal
```

The following example shows how to change the port operation of an Ethernet port to a loopback state:

```
[local]Redback(config)#port ethernet 5/1
[local]Redback(config-port)#loopback
```

1.29 loopback (CFM)

loopback

{no | default} loopback

1.29.1 Purpose

The **no** and **default** forms of this command specify that the maintenance points in the current maintenance domain (MD) not respond to loopback messages (LBMs).

1.29.2 Command Mode

CFM configuration

1.29.3 Syntax Description

This command has no keywords or arguments.

1.29.4 Default

Maintenance points respond to LBMs, unless disabled by this command.

1.29.5 Usage Guidelines

Use the **no loopback** or **default loopback** command to specify that the maintenance points in the current MD do not respond to LBM.

The **no loopback** or **default loopback** commands allow a MEP to initiate loopback messages and respond only to messages it initiates.

Use the **loopback** command to enable responses.

1.29.6 Examples

In the following example, the **no loopback** command disables responses to LBMs in the **sbc** CFM instance (**sbc.com** maintenance domain):

```
[local]Redback(config)#ethernet-cfm instance-1
[local]Redback(config-ether-cfm)#level 4
[local]Redback(config-ether-cfm)#no loopback
```

1.30 loopback (channels)

For a channelized OC-3 or STM-1 port, the syntax in port or STM-1 configuration mode is:

loopback {internal | line}

no loopback

For a channelized OC-12 or STM-4 port, the syntax in port or STM-4 configuration mode is:

loopback {internal | line}

no loopback

For a DS-3 channel, the syntax in DS-3 configuration mode is:

loopback {internal | line | remote}

no loopback

For a DS-1 channel, the syntax in DS-1 configuration mode is:

loopback {local | network ***net-type*** **| remote** ***rem-type*****}**

no loopback

For an E1 channel, the syntax in E1 configuration mode is:

loopback {line | local}

no loopback

For an DS-0 group, the syntax in DS-0 configuration mode is:

loopback line

no loopback

1.30.1 Purpose

Changes the operation of a OC-3/STM-1 port, OC-12/STM-4 port, DS-3 channel, DS-1 channel, or E1 channel, to a loopback state.

1.30.2 Command Mode

- Port configuration (channelized OC-3 or OC-12)
- STM-1 configuration
- STM-4 configuration
- DS-3 configuration
- DS-1 configuration
- E1 configuration
- DS-0 group configuration

1.30.3 Syntax Description

internal	Tests the internal functions of the port by looping the transmit line to the receive line. Use the **internal** keyword to test the internal functions of the port.
line	Tests the line operation of the channel or port by looping the receive line to the transmit line. Use the **line** keyword to loop received frames back to the transmit line.
local	Tests the internal functions of the channel or port by looping the transmit line to the receive line. Use the **local** keyword to loop transmitted frames back to the receive line without actually transmitting them.
remote	Verifies remote link connectivity and quality of the DS-3 channel or port at the DS-3 signal level. This option is available only if the DS-3 channel or port has C-bit framing and its admin state is up. Use the **remote** keyword to verify remote link connectivity and quality at the DS-3 signal level. This option is available only if the DS-3 channel or port has C-bit framing and the admin state is up.

network *net-type*	Type of loopback state for the DS-1 channel: • **line**—Specifies a full loopback (all bits) from the receive line to the transmit line. Use the **line** keyword to loop all received bits (a full loopback) to the transmit line. The time slots (for DS-0 channels) must be set to the default (1–24). • **payload**—Specifies a payload loopback from the receive line to the transmit line. Use the **payload** keyword to loop back only the received payload to the transmit line. The time slots (for DS-0 channels) must be set to the default (1–24).
remote *rem-type*	Type of loopback state for the far-end equipment: • **line fdl ansi**—Specifies a facility data link (FDL) ANSI loopback. The DS-1 channel must have Extended Superframe Format (ESF) framing. Use the **line fdl ansi** keywords to request the remote end, using the FDL, to loop back the bits transmitted by the local end. This option is available only if the DS-1 channel has ESF framing and its admin state is up. • **line fdl bellcore**—Specifies an FDL Bellcore loopback. The DS-1 channel must have ESF framing. Use the **line fdl bellcore** keywords to request the remote end, using the FDL, to loop back the bits transmitted by the local end. This option is available only if the DS-1 channel has ESF framing and its admin state is up. • **line inband**—Specifies an in-band loopback. This option is compatible with either ESF or Superframe Format (SF) framing, and is available only if the admin state of the DS-1 channel is up. Use the **line inband** keywords to request within the payload, that the remote end perform a full loopback. This option is available only if the admin state of the DS-1 channel is up. • **payload**—Specifies a payload loopback. This option is compatible only with ESF framing. Use the **payload** keyword to request that the remote end loop back only the payload. This option is available only if the DS-1 channel has ESF framing and its admin state is up.

1.30.4 Default

Port or channel operation is in a normal state.

1.30.5 Usage Guidelines

Caution!

Risk of data loss when operating in a remote loopback state.

If you specify a different framing for a DS-1 channel, and the DS-1 channel is operating in a remote (**line fdl ansi**, **line inband**, or **payload**) loopback state, and the new framing is not compatible with the type of remote loopback that you have operating, the system terminates the remote loopback (change the DS-1 channel operation to a normal state) before changing the framing. To reduce the risk, postpone issuing the **framing** command until you are ready to terminate the remote loopback.

After changing a DS-1 channel to the loopback state, you can use the **bert** command to perform a bit error rate test (BERT) to qualify the link.

After changing a DS-3 channel or port or E3 port to the loopback state, you can use the **bert** command to perform a bit error rate test (BERT) to qualify the links.

Use the **no** form of this command to restore the port or channel operation to a normal state.

1.30.6 Examples

The following example shows how to change the channel operation of a DS-1 channel to a loopback state to verify remote link connectivity:

```
[local]Redback(config)#port ds1 3/1:1
[local]Redback(config-ds1)#loopback remote
```

The following example shows how to change the channel operation of a DS-3 channel **1** to a loopback state to verify remote link connectivity:

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

The following example shows how to test the internal functions of port **1** on the channelized E1 traffic card in slot **1** by looping the transmit line to the receive line:

```
[local]Redback(config)#port e1 1/1:3:2
[local]Redback(config-e1)#loopback line
```

The following example shows how to test the line operation of the channelized STM-1 port **1** on the E1 traffic card in slot **1** by looping the receive line to the transmit line:

```
[local]Redback(config)#port channelized-stm1 1/1 pos
[local]Redback(config-stm1)#loopback line
```

1.31 loop-detection

In bridge configuration mode, enables loop detection and blocking based on MAC moves:

loop-detection

no loop-detection

In bridge profile configuration mode, enables configuration of loop detection priority applied to a circuit, port, or pseudowire:

loop-detection

{**no** | **default**} **loop-detection**

1.31.1 Purpose

In bridge configuration mode, enables or disables loop detection and blocking based on MAC moves. In bridge profile configuration mode, enables or disables configuration of loop detection priority applied to a circuit, port, pseudowire, or link group.

1.31.2 Command Mode

- Bridge configuration
- Bridge profile configuration

1.31.3 Syntax Description

This command has no keywords or arguments.

1.31.4 Default

In bridge configuration mode, detection of bridging loops using the MAC moves process is disabled. In bridge profile configuration mode, loop detection circuit priority is disabled.

1.31.5 Usage Guidelines

Use the **loop-detection** command (in bridge configuration mode) to enable loop detection based on MAC moves. Use the **loop-detection** command (in bridge profile configuration mode) to enable loop detection circuit priority.

This command does not interfere with the spanning-tree process of detecting bridging loops.

1.31.6 Examples

The following example shows how the **loop-detection** command (in bridge configuration mode) enables loop detection, and sets the loop detection interval attribute to **10** seconds:

```
[local]Redback(config)#context ink
[local]Redback(config-ctx)#bridge lbdl
[local]Redback(config-bridge)#loop-detection
[local]Redback(config-ld)#interval 10
```

In the following example, the **loop-detection** command (in bridge profile configuration mode) is used to enable setting the loop-detection priority for circuits associated with the bridge profile (**plow**) to the value 2:

```
[local]Redback(config)#bridge profile plow
[local]Redback(config-bridge-profile)#loop-detection
[local]Redback(config-bridge-profile-ld)#priority 2
```

1.32 lossless-large-mtu

lossless-large-mtu port-group {[*n1*] [*n2*]...[*n8*] | **all**}

{**no** | **default**} **lossless-large-mtu**

1.32.1 Purpose

Enables guaranteed lossless flow control for jumbo frames (packet sizes 1,519 to 9,600 bytes) and specifies the port groups for which this capability is enabled.

1.32.2 Command Mode

Card configuration

1.32.3 Syntax Description

port-group	Specifies that individual port groups are to be enabled for guaranteed lossless flow control.
[*n1*] [*n2*]... [*n8*]	Optional. Port groups that this command enables for guaranteed lossless flow control. Enter one or more port groups, numbered from 1 to 8, space separated.
all	Specifies that all port groups on this traffic card are to be enabled for guaranteed lossless flow control.

1.32.4 Default

Guaranteed lossless flow control is not enabled for any port group.

1.32.5 Usage Guidelines

Use the **lossless-large-mtu** command to enable guaranteed lossless flow control for jumbo packets (packet sizes 1,519 to 9,600 bytes) and specify the port groups for which this capability is enabled. This command is available for ports on Fast Ethernet-Gigabit Ethernet (FE-GE) cards only.

Note: The GE ports on an FE-GE traffic card support lossless flow control for jumbo frames (packet sizes 1,519 to 9,600 bytes) without the use of this command.

FE ports are organized into port groups; each group has either six or eight member ports. When you configure a port group for guaranteed lossless flow control, two of the member ports are enabled; these ports are guaranteed to support lossless flow control for maximum transmission unit (MTU) sizes up to 9,600 bytes. The other ports in the group are shut down.

FE ports in groups that are not explicitly enabled by this command also support lossless flow control but only for oversized frames (MTU sizes to up to 2,000 bytes). You can specify larger MTUs (up to 9,600 bytes) for these ports, but lossless flow control is not guaranteed.

Use the **all** keyword to enable all port groups for guaranteed lossless flow control.

Caution!

Risk of data loss. This command causes the FE-GE traffic card to reload. To reduce the risk, do not enter this command when the ports on the card are active.

Note: If you enter this command more than once, each succeeding entry overwrites the data you previously entered. For example, if you have configured one or more port groups for lossless flow control and later configure other port groups using this command, you must also specify all the port groups that you previously configured.

Table 2 lists the ports that are members of each port group and the ports that are enabled or shut down for lossless flow control.

Table 2 Port Groups and Their Members

Port Group	Member Ports	Ports Enabled	Ports Shut Down
1	49, 50, 51, 52, 53, 54, 55, 56	49, 53	50, 51, 52, 54, 55, 56
2	37, 38, 39, 40, 57, 58, 59, 60	37, 57	38, 39, 40, 58, 59, 60
3	41, 42, 43, 44, 45, 46, 47, 48	41, 45	42, 43, 44, 46, 47, 48
4	25, 26, 27, 28, 29, 30	25, 29	26, 27, 28, 30
5	13, 14, 31, 32, 33, 34, 35, 36	31, 35	13, 14, 32, 33, 34, 36
6	15, 16, 17, 18, 19, 20, 21, 22	15, 19	16, 17, 18, 20, 21, 22
7	1, 2, 3, 4, 5, 6, 23, 24	3, 23	1, 2, 4, 5, 6, 24
8	7, 8, 9, 10, 11, 12	7, 11	8, 9, 10, 12

Use the **no** or **default** form of this command to disable lossless flow control for all port groups.

1.32.6 Examples

The following example shows how to configure port groups `1` and `2` for guaranteed lossless flow control. In this instance the command enables ports 49 and 53 (in group 1) and ports 37 and 57 (in group 2), and shuts down all the other ports (50 to 52, 54 to 56, 38 to 40, and 58 to 60) in those groups:

```
[local]Redback(config)#card fege-60-2-port 1
[local]Redback(config-card)#lossless-large-mtu port-group 1 2
```

1.33 lsp

lsp ***lsp-name*** [**backup-for** ***lsp-name*** | **bypass** ***ip-addr*** [**node-protect-lsp-egress** ***ip-addr***]]

no lsp ***lsp-name*** [**backup-for** ***lsp-name*** | **bypass** ***ip-addr*** [**node-protect-lsp-egress** ***ip-addr***]]

1.33.1 Purpose

When entered in MPLS static router configuration mode, creates a static label-switched path (LSP), and enters MPLS static LSP configuration mode.

When entered in RSVP router configuration mode, creates an Resource Reservation Protocol (RSVP) LSP, and enters RSVP LSP configuration mode.

1.33.2 Command Mode

- MPLS static router configuration
- RSVP router configuration

1.33.3 Syntax Description

lsp-name	Name of the LSP.
backup-for ***lsp-name***(1)	Optional. Creates a backup or backup-to-backup RSVP LSP. You can create a backup LSP for a primary LSP, or for another backup LSP, as follows: • To create an LSP that backs up a primary LSP, replace the ***lsp-name*** argument with the name of the primary LSP you are creating this backup LSP for. • To create a backup-to backup LSP (an LSP that backs up another backup LSP), replace the ***lsp-name*** argument with the name of the primary LSP you are creating this backup LSP for. This configuration is called a backup-to-backup LSP.
bypass ***ip-addr***	Optional. Bypass LSP for next-hop fast reroute (NFRR) link protection. The ***ip-addr*** argument is the IP address of the directly connected next-hop node being protected. This option is only available when configuring a signaled LSP in RSVP LSP configuration mode.
node-protect-lsp-egress ***ip-addr***	Optional. Bypass LSP for NFRR node protection. The ***ip-addr*** argument specifies the egress IP address of the bypass LSP. This option is only available when configuring a signaled LSP in RSVP LSP configuration mode, and when the LSP is being configured as a bypass LSP.

(1) This construct is only available when configuring an RSVP LSP in RSVP LSP configuration mode.

1.33.4 Default

None

1.33.5 Usage Guidelines

Use the **lsp** command in MPLS static router configuration mode to create a static LSP, and enter MPLS static LSP configuration mode.

Use the **lsp** command in RSVP router configuration mode to create an RSVP LSP, and enter RSVP LSP configuration mode.

Use the **backup-for** *lsp-name* construct to create a backup RSVP LSP for a primary RSVP LSP, or for another backup RSVP LSP in a backup-to-backup LSP configuration. A backup RSVP LSP remains in hot standby, which means that it is always consuming resources and available for passing traffic. If RSVP signals that the primary RSVP LSP has gone down, the backup RSVP LSP immediately begins passing traffic. If that backup RSVP LSP goes down, then the RSVP LSP that backs up that backup RSVP LSP begins passing traffic.

Backup and backup-to-backup RSVP LSP tunnels are configured on a one-to-one, end-to-end path backup basis. Failover occurs in a hierarchy: if the primary LSP fails, traffic fails over to the backup LSP; if the backup LSP also fails, traffic fails over to the backup to the backup LSP. In both cases, failover is revertive: if the higher-order LSP becomes active again, traffic reverts to the higher-order LSP.

Switchover to the backup RSVP LSP occurs within 100 milliseconds (ms) after the primary LSP goes down.

The operating system also supports fast failover to a backup or backup-to-backup LSP when the ingress router fails.

Switchover to the backup LSP occurs within 100 milliseconds after one of the following errors is received by the LSP on the ingress router:

- RSVP Reservation Tear message
- RSVP Hello timeout

Switchover over to the backup LSP occurs within 50 ms if a link-down event at the ingress router causes a failure.

Use the **bypass** *ip-addr* construct to configure the RSVP LSP as a bypass LSP for NFRR link protection. A bypass LSP is no different from any other RSVP LSP, except that it does not carry traffic under normal conditions. It is configured to reach the next-hop router in the event of a link failure. Any type of traffic intended to use the next hop can be switched onto the bypass LSP.

Use the **node-protect-lsp-egress** *ip-addr* construct to use the bypass LSP for NFFR node protection. In the event of a link failure or a next-hop node

failure, traffic is switched to the bypass LSP. If a bypass LSP is configured without enabling node protection, then the bypass LSP is used only for link protection.

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

1.33.6 Examples

The following example shows how to configure the static LSP, **sl10**, to use the next-hop label-switched router (LSR), **192.168.1.24**, the egress LSR, **192.168.100.2**, and to set the outgoing label value to **3:**

```
[local]Redback(config-ctx)#router mpls-static
[local]Redback(config-mpls-static)#lsp sl10
[local]Redback(config-mpls-static-lsp)#next-hop 192.168.1.24
[local]Redback(config-mpls-static-lsp)#egress 192.168.100.2
[local]Redback(config-mpls-static-lsp)#out-label 3
```

The following example configures the RSVP LSP, **12**, to use the ingress LSR, **13.1.1.1**, the egress LSR, **14.1.1.1**, and the explicit route **two** as its source path:

```
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#lsp 12
[local]Redback(config-rsvp-lsp)#ingress 13.1.1.1
[local]Redback(config-rsvp-lsp)#egress 14.1.1.2
[local]Redback(config-rsvp-lsp)#source-path two
```

The following example shows how to configure the RSVP LSP `12-bkup as a backup for the primary LSP 12 and the RSVP LSP 12-bkup2 as a backup for the backup RSVP LSP 12-bkup:`

```
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#lsp 12-bkup backup-for 12
[local]Redback(config-rsvp-lsp)#exit
[local]Redback(config-rsvp)#lsp 12-bkup-2 backup-for 12-bkup
```

The following example configures the RSVP LSP, **to-r2-core**, as a bypass LSP for link protection:

```
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#lsp to-r2-core bypass 10.1.1.1
[local]Redback(config-rsvp-lsp)#egress 192.168.1.1
```

1.34 lsp block-flooding

lsp block-flooding [**level-1** | **level-2**]

```
no lsp block-flooding [level-1 | level-2]
```

1.34.1 Purpose

Prevents intermediate link-state protocol data units (LSPs) from being flooded out through the Intermediate System-to-Intermediate System (IS-IS)-enabled interface.

1.34.2 Command Mode

IS-IS interface configuration

1.34.3 Syntax Description

`level-1`	Optional. Enables block flooding on IS-IS level 1 routing independently.
`level-2`	Optional. Enables block flooding on IS-IS level 2 routing independently.

1.34.4 Default

LSPs are flooded over IS-IS-enabled interfaces. When you enter this command without specifying either level 1 or level 2 routing, LSPs are flooded on both IS-IS levels 1 and 2.

1.34.5 Usage Guidelines

Use the **`lsp block-flooding`** command to prevent LSPs from being flooded out through the IS-IS-enabled interface. When a network topology has many redundant connections among IS-IS devices, LSPs can be flooded excessively inside the network, costing extra CPU cycles and bandwidth consumption. This feature is especially useful in a large, fully-meshed IS-IS topology.

Note: This command is typically used for point-to-point (P2P) IS-IS interfaces.

Note: Avoid blocking some LSPs completely.

Use the **`no`** form of this command to restore to the default behavior of flooding LSPs on the interface.

1.34.6 Examples

The following example shows how to block LSP flooding on level 1 only for the **fa4/1** interface running the IS-IS instance **ip-backbone:**

```
[local]Redback(config-ctx)#router isis ip-backbone
[local]Redback(config-isis)#interface oc48-4/1
[local]Redback(config-isis-if)#lsp block-flooding level-1
```

1.35 lsp gen-interval

lsp gen-interval *interval* [**level-1** | **level-2**]

no lsp gen-interval

1.35.1 Purpose

Controls how frequently a link-state protocol data unit (LSP) can be regenerated with new content for the Intermediate System-to-Intermediate System (IS-IS) instance.

1.35.2 Command Mode

IS-IS router configuration

1.35.3 Syntax Description

interval	Frequency, in seconds, at which an LSP can be regenerated with new content. The range of values is 1 to 120; the default value is 10.
level-1	Optional. Sets the frequency at which an LSP can be regenerated for level 1 independently.
level-2	Optional. Sets the frequency at which an LSP can be regenerated for level 2 independently.

1.35.4 Default

An LSP can be regenerated every 10 seconds.

1.35.5 Usage Guidelines

Use the **lsp gen-interval** command to control how frequently an LSP can be regenerated with new content for the IS-IS instance.

Decreasing the frequency at which an LSP can be regenerated with new content can stabilize a network at the cost of slower convergence. New versions of LSPs with updated content are generated less often and produce less load on the network than the load caused by flooding and route recomputation. Typically, the value set by the **lsp gen-interval** command should be lower than the values set through the **lsp max-lifetime** and **lsp refresh-interval** commands in IS-IS router configuration mode.

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

1.35.6 Examples

The following example shows how to set the LSP regeneration frequency for IS-IS **level-1** to **30** seconds:

```
[local]Redback(config-ctx)#router isis ip-backbone
[local]Redback(config-isis)#lsp gen-interval 30 level-1
```

1.36 lsp interval

lsp interval ***interval***

no lsp interval

1.36.1 Purpose

Controls the pace at which link-state protocol data unit (LSP) transmissions are flooded on the interface to Intermediate System-to-Intermediate System (IS-IS) neighbors.

1.36.2 Command Mode

IS-IS interface configuration

1.36.3 Syntax Description

interval	Interval, in milliseconds, between successive LSPs. The range of values is 10 to 65,535; the default value is 33.

1.36.4 Default

The minimum delay time is set to 33 milliseconds.

1.36.5 Usage Guidelines

Use the **lsp interval** command to control the pace at which LSPs are flooded on the interface to IS-IS neighbors. In dense-meshed IS-IS network topologies with a large number of devices and IS-IS neighbors, LSP flooding is the key scaling factor. Ensure that devices are not overloaded by LSPs from neighbors.

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

1.36.6 Examples

The following example shows how to configure the SmartEdge router to transmit LSPs every **100** milliseconds (10 packets per second) on the **serial1/1** interface:

```
[local]Redback(config-ctx)#router isis ip-backbone
[local]Redback(config-isis)#interface serial1/1
[local]Redback(config-isis-if)#lsp interval 100
```

1.37 lsp max-lifetime

lsp max-lifetime ***lifetime***

no lsp max-lifetime

1.37.1 Purpose

Modifies the length of time that Intermediate System-to-Intermediate System (IS-IS) link-state protocol data units (LSPs) can live on the network before timing out.

1.37.2 Command Mode

IS-IS router configuration

1.37.3 Syntax Description

lifetime	Maximum lifetime, in seconds, of an LSP. The range of values is 120 to 65,535; the default value is 1,200.

1.37.4 Default

The maximum lifetime of an LSP is 1,200 seconds.

1.37.5 Usage Guidelines

Use the **lsp max-lifetime** command to modify the length of time LSPs can live on the network before timing out. Use this command in conjunction with the **lsp refresh-interval** command in the case of large networks. Longer-lived LSPs allow for less flooding and higher stability.

The value set by the **lsp max-lifetime** command should be at least 60 seconds more than the value set through the **lsp refresh-interval** command, and should also be more than the value set through the **lsp gen-interval** command.

Use the **no** form of this command to restore the default maximum lifetime value of 1,200 seconds.

1.37.6 Examples

The following example shows how to set the maximum lifetime for LSPs to **900** seconds, which is **300** seconds more than the LSP refresh interval:

```
[local]Redback(config-isis)#lsp refresh-interval 600
[local]Redback(config-isis)#lsp max-lifetime 900
```

1.38 lsp receive-only-mode

lsp receive-only-mode

no lsp receive-only-mode

1.38.1 Purpose

Prevents the specified Intermediate System-to-Intermediate System (IS-IS) interface from forwarding link-state protocol data units (LSPs).

1.38.2 Command Mode

IS-IS interface configuration

1.38.3 Syntax Description

This command has no keywords or arguments.

1.38.4 Default

None

1.38.5 Usage Guidelines

Use the **lsp receive-only-mode** command to prevent the specified IS-IS interface from forwarding LSPs.

Caution!

Risk of leaked routing information. This command is used for internal lab test situations only and is relevant only for a stub IS-IS area where the goal is to import the network routing information from the operational network without exporting lab environment routing information into the operational network. After enabling IS-IS on an interface using the **interface** command in IS-IS router configuration mode, a delay in entering the **lsp receive-only-mode** command can result in lab routing information leaking into the operational network. To reduce the risk, immediately enter the **lsp receive-only-mode** command after enabling IS-IS on an interface using the **interface** command in IS-IS router configuration mode.

Use the **no** form of this command to reestablish forwarding of LSPs.

1.38.6 Examples

The following example show how to prevent the IS-IS interface, **isis1**, on a lab router from forwarding LSPs:

```
[local]Redback(config-ctx)#router isis ip-backbone
[local]Redback(config-isis)#interface isis1
[local]Redback(config-isis-if)#lsp receive-only-mode
```

1.39 lsp refresh-interval

lsp refresh-interval ***interval***

no lsp refresh-interval

1.39.1 Purpose

Controls how frequently a link-state protocol data units (LSPs) can be regenerated for the Intermediate System-to-Intermediate System (IS-IS) instance.

1.39.2 Command Mode

IS-IS router configuration

1.39.3 Syntax Description

interval	Frequency, in seconds, with which an LSP can be regenerated. The range of values is 30 to 65,535; the default value is 900.

1.39.4 Default

LSPs can be regenerated every 900 seconds.

1.39.5 Usage Guidelines

Use the **lsp refresh-interval** command to control how frequently an LSP can be regenerated for the specified IS-IS instance.

Use this command in conjunction with the **lsp max-lifetime** command in the case of large networks. Longer-lived LSPs allow for less flooding and higher stability. This value should be at least 60 seconds less than the value set through the **lsp max-lifetime** command, and should also be less than the value set through the **lsp gen-interval** command. This LSP refresh interval also determines the IS-IS periodical Shortest Path First (SPF) calculations on the system.

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

1.39.6 Examples

The following example shows how to set the LSP refresh interval to **600** seconds, which is **300** seconds less than the maximum lifetime value:

```
[local]Redback(config-isis)#lsp refresh-interval 600

[local]Redback(config-isis)#lsp max-lifetime 900
```

1.40 lsp retransmit-interval

lsp retransmit-interval ***interval***

no lsp retransmit-interval

1.40.1 Purpose

Configures the length of time the system should wait for an acknowledgment from the neighbor before resending Intermediate System-to-Intermediate System (IS-IS) link-state protocol data units (LSPs).

1.40.2 Command Mode

IS-IS interface configuration

1.40.3 Syntax Description

interval	Interval, in seconds, between LSP retransmissions. The range of values is 0 to 65,535; the default value is 5.

1.40.4 Default

The retransmission interval is five seconds.

1.40.5 Usage Guidelines

Use the **lsp retransmit-interval** command to configure how long the system should wait for an acknowledgment from the neighbor before resending an IS-IS LSP. The number of seconds should be greater than the expected round-trip delay between any two devices on the attached network.

This command has no effect on LAN interfaces. On point-to-point links, the ***interval*** argument can be increased to enhance network stability. The retransmission interval can be larger for serial lines. More neighbors and paths over which LSPs are flooded allow for a longer interval.

Use the **no** form of this command to restore the default retransmission interval of five seconds.

1.40.6 Examples

The following example shows how to configure the **pos11/1** interface to retransmit LSPs every **10** seconds:

```
[local]Redback(config-ctx)#router isis ip-backbone
[local]Redback(config-isis)#interface pos11/1
[local]Redback(config-isis-if)#lsp retransmit-interval 10
```

1.41 mac-address (ATM)

mac-address ***mac-addr***

default mac-address

1.41.1 Purpose

Assigns a medium access control (MAC) address on an Asynchronous Transfer Mode (ATM) OC port.

1.41.2 Command Mode

ATM OC configuration

1.41.3 Syntax Description

mac-addr	MAC address to be used for the port in the form ***hh:hh:hh:hh:hh:hh***.

1.41.4 Default

When the ATM OC traffic card or ATM OC MIC is inserted in the SmartEdge router, the MAC address is extracted from the Electrically Erasable Programmable Read-Only Memory (EEPROM) and assigned to each port on the card as sequential addresses starting with the base address for port 1.

1.41.5 Usage Guidelines

Use the **mac-address** command to assign a MAC address on an ATM port.

Use the **default** form of this command to return the MAC address to the address that has been extracted from the EEPROM on the ATM OC traffic card.

1.41.6 Examples

The following example shows how to assign **00:03:04:10:a4:bc** as the MAC address on port **1** of the ATM OC traffic card in slot **3:**

```
[local]Redback(config)#port atm 3/1
[local]Redback(config-atm-ds3)#mac-address 00:03:04:10:a4:bc
```

1.42 mac-address (DHCP)

mac-address ***mac-addr*** **ip-address** ***ip-addr***

no mac-address ***mac-addr*** **ip-address** ***ip-addr***

1.42.1 Purpose

Creates a static mapping between a medium access control (MAC) address and an IP address in this subnet.

1.42.2 Command Mode

DHCP subnet configuration

1.42.3 Syntax Description

mac-addr	MAC address for the subnet.
ip-address ***ip-addr***	IP address to which the MAC address is to be mapped.

1.42.4 Default

No mapping exists between the MAC address and an IP address.

1.42.5 Usage Guidelines

Use the **mac-address** command to create a static mapping between a MAC address and an IP address in this subnet.

The value for the ***ip-addr*** argument must be an IP address within this subnet, but not within any range of IP addresses that you have specified using the **range** command (in DHCP subnet configuration mode).

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

1.42.6 Examples

The following example shows how to create a static mapping between a MAC address and an IP address:

```
[local]Redback(config)#context dhcp
[local]Redback(config-ctx)#dhcp server policy
[local]Redback(config-dhcp-server)#subnet 12.1.1.0/24 name sub2
[local]Redback(config-dhcp-subnet)#range 12.1.1.50 12.1.1.100
[local]Redback(config-dhcp-subnet)#mac-address 02:12:34:56:78:90 ip-address 12.1.1.10
```

1.43 mac-address (Dot1Q PVC)

mac-address ***mac-addr***

{**no** | **default**} **mac-address** ***mac-addr***

1.43.1 Purpose

Assigns a medium access control (MAC) address to an 802.1Q permanent virtual circuit (PVC).

1.43.2 Command Mode

dot1q PVC configuration

1.43.3 Syntax Description

mac-addr	MAC address to be used for the port in the form ***hh*:*hh*:*hh*:*hh*:*hh*:*hh***.

1.43.4 Default

When the Gigabit or Fast Ethernet traffic card is inserted in the SmartEdge router, the MAC address is extracted from the EEPROM and assigned to each port on the Gigabit or Fast Ethernet traffic card as sequential addresses starting with the base address for port 1. Every tunnel and PVC on a port has the same default address as the port.

1.43.5 Usage Guidelines

Use the **mac-address** command to assign a MAC address on a Gigabit or Fast Ethernet port.

The **mac-address** command is only available under the dot1q PVC configuration mode. This command is not available when configuring 802.1Q PVCs virtual LAN (VLAN) link group.

Note: Do not enter a point-to-multipoint MAC address. There must not be an odd number in the first byte of the ***mac-addr*** argument.

Use the **no** or **default** form of this command to return the MAC address to the MAC address of the parent circuit.

1.43.6 Examples

The following example shows how to assign **02:03:04:05:06:07** as the MAC address on an 802.1Q PVC within a tunnel on port **2** of the Gigabit or Fast Ethernet traffic card in slot **1:**

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

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

[local]Redback(config-port)#encapsulation dot1q

[local]Redback(config-port-dot1q)#dot1q pvc 2 1qtunnel

[local]Redback(config-port-dot1q)#dot1q pvc 2:1

[local]Redback(config-dot1q-pvc)#mac-address 02:03:04:05:06:07
```

As a result, the port and the 802.1Q tunnel have the same default address stored in the EEPROM. Only the 802.1Q PVC has an assigned MAC address.

1.44 mac-address (link group)

mac-address {***mac-addr*** | **auto**}

no mac-address [***mac-addr*** | ***auto***]

1.44.1 Purpose

Specifies or automatically generates a medium access control (MAC) address for the Ethernet, 802.1Q, or access link group.

1.44.2 Command Mode

Link group configuration

1.44.3 Syntax Description

mac-addr	MAC address to be used for the link group in the form ***hh:hh:hh:hh:hh:hh***. Optional when using the **no** form of this command.
auto	Specifies that the system automatically generate a link group MAC address whenever the default MAC address is not available.

1.44.4 Default

The MAC address of a constituent FE or GE port in the link group is used as the MAC address for the link group.

1.44.5 Usage Guidelines

Use the **mac-address** command to specify or automatically generate a MAC address for the Ethernet, 802.1Q, or access link group.

If the command includes the `auto` keyword, the link group uses the address of its constituent FE or GE port whenever it is available and automatically generates a new MAC address whenever the port address is not available, such as when the traffic card containing the port is removed.

Note: This command is applicable only to an Ethernet, 802.1Q, or access link group.

You must use this command to specify a MAC address when configuring an access link group.

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

1.44.6 Examples

The following example shows how to specify `00:00:26:26:26:26` as the MAC address for the Ethernet link group:

```
[local]Redback(config)#link-group lg-ether ether
[local]Redback(config-link-group)#mac-address 00:00:26:26:26:26
```

1.45 mac-address (Port PW)

mac-address ***address***

no mac-address ***address***

1.45.1 Purpose

Sets the MAC address for a port pseudowire (PW) connection.

1.45.2 Command Mode

port configuration

1.45.3 Syntax Description

address	MAC address of the port PW connection in the format *NN:NN:NN:NN:NN:NN*.

1.45.4 Default

None

1.45.5 Usage Guidelines

Use the **mac-address** command to set the MAC address of the port PW connection.

Use the **no** form of this command to set the MAC address of the port PW connection to the previously set value.

1.45.6 Examples

The following example shows how to set the MAC address of the port PW connection to **11:22:33:44:55:66:**

```
[local]Redback(config-port)#mac-address 11:22:33:44:55:66
```

1.46 mac-entry

mac-entry drop ***mac-addr***

no mac-entry drop ***mac-addr***

1.46.1 Purpose

Specifies a medium access control (MAC) address that is not allowed on this bridge.

1.46.2 Command Mode

Bridge configuration

1.46.3 Syntax Description

drop	Discards all packets on the specified MAC address.
mac-addr	MAC address that is not allowed on this bridge, in the form ***hh:hh:hh:hh:hh:hh***.

1.46.4 Default

Packets with any MAC address are accepted.

1.46.5 Usage Guidelines

Use the **mac-entry** command to specify a MAC address that is not allowed on this bridge. Packets with this MAC address, either as source or destination, are dropped unconditionally.

Use the **no** form of this command to remove the MAC address from the list of MAC addresses that are not allowed on this bridge.

1.46.6 Examples

The following example shows how to specify the MAC addresses that are not allowed on this bridge:

```
[local]Redback(config)#context bridge
[local]Redback(config-ctx)#bridge isp1
[local]Redback(config-bridge)#mac-entry drop 00:0d:ab:40:8d:50
[local]Redback(config-bridge)#mac-entry drop 00:a0:a0:40:d8:60
```

1.47 mac-limit

mac-limit {*max-num* | **unlimited**}

{**no** | **default**} **mac-limit**

1.47.1 Purpose

Specifies the maximum number of medium access control (MAC) addresses that can be learned by the bridge or specified manually for any port, circuit, or Virtual Private LAN Service (VPLS) pseudowire circuit to which this profile is assigned.

1.47.2 Command Mode

Bridge profile configuration

1.47.3 Syntax Description

max-num	Maximum number of learned MAC addresses. The range of values is 1 to 16,000.
unlimited	Does not impose a limit to the number of learned MAC addresses.

1.47.4 Default

The maximum number of learned MAC addresses is four for a tributary circuit to which a profile is assigned. Trunk and VPLS circuits have no MAC limit.

1.47.5 Usage Guidelines

Use the **mac-limit** command to specify the maximum number of MAC addresses that can be learned by the bridge or specified manually for any port, circuit, or VPLS pseudowire circuit to which this profile is assigned. For more information about VPLS pseudowire circuits, see *Configuring VPLS*.

MAC addresses are specified manually using the **bridge mac-entry** command (in dot1q PVC, ATM PVC, or port configuration mode).

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

1.47.6 Examples

The following example shows how to specify **10** as the maximum number of MAC addresses for this profile:

```
[local]Redback(config)#bridge profile prof-isp1
[local]Redback(config-bridge-profile)#mac-limit 10
```

1.48 mac-list

mac-list ***MAC-list-name***

no mac-list ***MAC-list-name***

1.48.1 Purpose

Creates a list of MAC addresses that can be used drop incoming packets when their source MAC address matches any entry in the MAC list.

1.48.2 Command Mode

Global configuration

1.48.3 Syntax Description

MAC-list-name	Name of the list of MAC addresses.

1.48.4 Default

No default

1.48.5 Usage Guidelines

Use the **mac-list** command to create a list of MAC addresses that can be used drop incoming packets when their source MAC address matches any entry in the MAC list. The examples below show how a bridge filter with one or more MAC can be applied to an 802.1Q PVC bound to a bridge.

To configure a MAC list on an 802.1Q PVC, follow these steps:

1. Specify the name of the MAC list and press Enter :

   mac-list ***MAC-list-name***

2. When you see the `config-mac-list` prompt, enter the first address in the MAC list.

   - To add an address to the MAC list, type the MAC address and press Enter; that is, the subcommand that adds MAC addresses to the MAC

list is the ***MAC-address*** argument without keywords. In other words, the **mac-list** command creates a container for a list of MAC addresses called a MAC list, and these addresses can be applied to PVCs bound to bridges to filter incoming packets.

- To remove an address, enter the **no *MAC-address*** form of the subcommand.

3. Add or remove as many addresses as needed by repeating step 2.
4. Include the MAC list in a bridge profile. You can include multiple MAC lists in any bridge profile.

   Use the **drop source** command (in **bridge profile** configuration mode) to include a MAC list filter in a bridge profile.
5. Use the **bridge profile** command to apply the MAC lists it contains to a bridged 802.1Q PVC.

   The 802.1Q PVC must be bound to the interface of a bridge.

Use the **show circuit counters detail** command to show the dropped packets.

Use the **show circuit counters detail** command to see the dropped packets statistics. The field, **MAC filter Drops**, appears among the other bridge counters. It displays the count in bytes and packets.

The following restrictions apply to MAC list filters:

- A maximum of 10 MAC addresses can be contained in each MAC list
- No more than eight unique MAC lists can be applied to a bridge.

  For example, there are two 802.1Q PVCs bound to a bridge. The first PVC specifies bridge profile `Profile-A` and the second PVC specifies `Profile-B`. In addition:

  – `Profile-A includes three MAC-lists: MAC-list-2, MAC-list-3, and MAC-list-5.`

  – `Profile-B includes two MAC-lists: MAC-list-4 and MAC-list-5.` The number of unique MAC lists applied to the bridge in this example is four. They are: `MAC-list-2, MAC-list-3, MAC-list-4, and MAC-list-5.`
- MAC lists are not supported on VPLS pseudowire circuits.
- MAC lists are supported on learning bridges only.
- MAC list filtering on circuits aggregated in link groups is not supported.
- MAC list filtering has less than a 3% impact on the overall Layer 2 forwarding performance of the SmartEdge router.

1.48.6 Examples

The following example illustrates how to create a MAC list named “noloops” with the **mac-list** command:

```
[local]Redback(config)#mac-list noloops
[local]Redback(config-mac-list)#11:11:11:ab:cd:cd
[local]Redback(config-mac-list)#11:13:44:ab:cd:ab
[local]Redback(config-mac-list)#end
```

The following example shows how to incorporate the created list in a bridge profile:

```
[local]Redback(config)#bridge profile mynetworkbridges
[local]Redback(config-bridge-profile)#drop source noloops
[local]Redback(config-bridge-profile)#end
```

The following example shows how to apply the bridge profile with the MAC list filter to a 802.1Q PVC that interfaces to a bridge where the filter is required:

```
[local]Redback(config)#port ethernet 5/2
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 5
[local]Redback(config-dot1q-pvc)#bridge profile mynetworkbridges
[local]Redback(config-bridge-profile)#end
```

1.49 mac-move-drop

mac-move-drop

{**no** | **default**} **mac-move-drop**

1.49.1 Purpose

Enables the legacy method of detection of bridging loops.

1.49.2 Command Mode

Bridge configuration

1.49.3 Syntax Description

This command has no keywords or arguments.

1.49.4 Default

The legacy method of detecting bridging loops is enabled by default, but only if the loop detection command (in bridge configuration mode) is not enabled. When loop-detection is enabled, the legacy method is disabled.

1.49.5 Usage Guidelines

The **mac-move-drop** command enables the legacy method of detection of bridging loops; however, you cannot enable the legacy method if loop-detection has been enabled.

Use the **no** or **default** form of this command to disable the legacy method of detection of bridging loops.

1.49.6 Examples

The following example shows how to configure a bridge to use the legacy method of detecting bridging loops:

```
[local]Redback(config-bridge)#mac-move-drop
```

1.50 macro

macro {**exec** | **inherit** | ***mode***} ***macro-name***

no macro {**exec** | **inherit** | ***mode***} ***macro-name***

1.50.1 Purpose

Defines an alias for a sequence of commands and accesses macro configuration mode.

1.50.2 Command Mode

Global configuration

1.50.3 Syntax Description

exec	Specifies that the macro be available in exec mode.
inherit	Specifies that the macro be available in exec mode.

mode	Configuration mode in which the macro is available. See Table 3 for exceptions.
macro-name	Name of the macro to be defined.

1.50.4 Default

No macros are defined.

1.50.5 Usage Guidelines

Use the **macro** command to define an alias for a sequence of commands. After entering macro configuration mode, you enter the commands to be included in the macro using the **seq** command (in macro configuration mode).

Table 3 lists all the mode prompts and keyword exceptions for the **macro** command. Except for the modes listed in Table 3, the keyword for the ***mode*** argument is the command mode prompt. For a list of all keywords, see the command-line interface (CLI) online Help.

Table 3 Mode Prompts and Keyword Exceptions for the macro Command

Mode Description	Mode Prompt	Mode Keyword
Network Address Translation (NAT) access control list	**policy-acl**	**nat-policy-acl**
NAT access control list class	**policy-acl-class**	**nat-policy-acl-class**

Use the **exit** command (in macro configuration mode) to complete the macro and exit to global configuration mode.

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

1.50.6 Examples

The following example shows how to define a macro, **show-port-all**, to display port information:

```
[local]Redback(config)#macro inherit show-port-all
[local]Redback(config-macro)#seq 10 show port $1/$2
[local]Redback(config-macro)#seq 20 show circuit $1/$2
[local]Redback(config-macro)#exit
```

The following example displays port data for port **3** of the traffic card in slot **4** using the **show-port-all** macro:

```
[local]Redback>#show-port-all 4 3
```

The following example defines the macro, **show-all**, that uses the **$** character:

```
[local]Redback(config)#macro inherit show-all
[local]Redback(config-macro)#seq 10 show config $*
[local]Redback(config-macro)#seq 30 show circuit $*
[local]Redback(config-macro)#exit
```

The following example displays how to run the **show-port-all** macro for Asynchronous Transfer Mode (ATM) and Frame Relay configuration and circuits:

```
[local]Redback>show-all atm frame-relay
```

1.51 malicious-traffic

malicious-traffic

no malicious-traffic

1.51.1 Purpose

In global configuration mode, configures malicious traffic parameters and enters malicious-traffic configuration mode. In context configuration mode, configures malicious traffic parameters and enters malicious-traffic context configuration mode.

1.51.2 Command Mode

- global configuration mode
- context configuration mode

1.51.3 Syntax Description

This command has no keywords or arguments.

1.51.4 Default

None

1.51.5 Usage Guidelines

Use the **malicious-traffic** command in global configuration mode to configure malicious traffic parameters and enter malicious-traffic configuration mode. Use the command in context configuration mode to configure malicious-traffic parameters for the given context and enter malicious-traffic context configuration mode.

Use the **no** form of this command in global configuration mode to disable or remove malicious-traffic parameters. These global malicious-traffic parameters will use the default values. Use the **no** form of this command in context configuration mode to disable or remove malicious-traffic parameters for the given context.

For information about detecting and monitoring malicious traffic, see *Configuring Malicious Traffic Detection and Monitoring*.

1.51.6 Examples

The following example shows how to enter malicious-traffic configuration mode:

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

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

The following example shows how to enter malicious-traffic context configuration mode to configure malicious traffic parameters for the context **ABC**:

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

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

1.52 maintenance-association

maintenance-association [icc] ***ma-short-name***

no maintenance-association

1.52.1 Purpose

Creates a maintenance association (MA) on an Ethernet or VLAN-based circuit to verify the integrity of the circuit. If the MA already exists, the command simply enters the MA configuration mode.

1.52.2 Command Mode

CFM configuration

1.52.3 Syntax Description

icc	By default, the MAID is entered in IEEE 802.1ag format. Enabling **icc** allows the MAID to be specified in ICC (Y.1731) format instead. When ICC is enabled, both the domain name and MA name must be specified in ICC format; the ICC ME group (MEG) ID/MAID is 13 characters, where the first bit is 0 followed by a 6-character ICC code and a 6-character unique MEG ID code (UMC). Mismatch of MAIDs are reported as configuration errors.
ma-short-name	Specifies the name used to identify the MA to CFM users who have access to the current MD. A maximum of 43 characters are allowed for the ***ma-short-name*** argument. The total length of MD name and the ***ma-short-name*** argument must be less than or equal to 48 characters.

1.52.4 Default

No MA exists.

1.52.5 Usage Guidelines

Use the **maintenance-association** command to create a MA on an Ethernet or VLAN-based circuit to verify the integrity of the circuit. If the MA already exists, the command simply enters the MA configuration mode.

When the MD is divided into multiple maintenance associations (MAs) (as shown in level 3 in the following illustration), the maintenance association endpoints (MEPs) can be adjacent, but cannot overlap.

Each Ethernet or VLAN-based circuit is a single Ethernet Virtual Connection (EVC); that is a single customer service instance.

An MA is defined as a mesh of MEPs, each of which has a Domain Service Access Point (DSAP) to which a user can connect for CFM operations. In addition the network mesh can contain intermediate maintenance points not having DSAPs. If an intermediate maintenance point is configured to be reported in the CFM user's domain, it is called a maintenance association intermediate point (MIP) in the MA.

The Continuity Check Message (CCM) PDU is broadcast by an MA endpoint (MEP), is used to check the continuity of the MA.

Maintenance points are ingress and egress Ethernet ports, Ethernet circuit interfaces, or interfaces to emulated Ethernet circuits. See *CFM Supported Circuits* in `Configuring Ethernet CFM` for details.

The following drawing illustrates two Operator MAs. Each MA is corresponds to separate VLAN. If the two VLANs are operated by separate companies and have DSAPs, they should be created in separate MDs. If they are supplied by the same company, they should be created in a single domain:

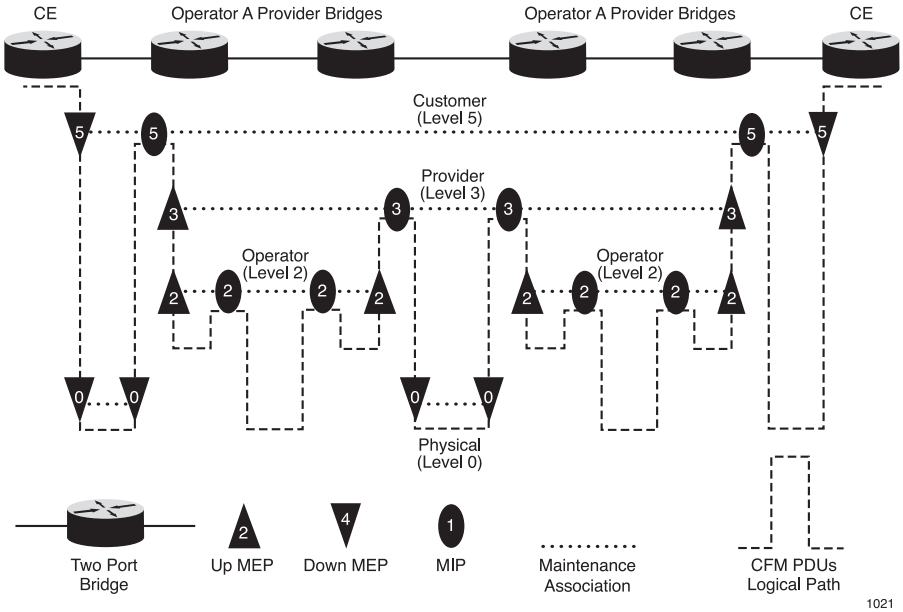


Figure 1 Operator MAs

1.52.6 Examples

The following example shows how to use this command to create an MA **bayarea** in the MD named **sbc.com:**

```
[local]Redback(config)#ethernet-cfm instance-1
[local]Redback(config-ether-cfm)#level 4
[local]Redback(config-ether-cfm)#domain-name sbc.com
[local]Redback(config-ether-cfm)#disable-linktrace
[local]Redback(config-ether-cfm)#group-mac 01:01:01:01:01:01
[local]Redback(config-ether-cfm)#maintenance-association bayarea
```

1.53 mapping-schema

mapping-schema {**8P0D** | **7P1D** | **6P2D** | **5P3D**}

{**no** | **default**} **mapping-schema**

1.53.1 Purpose

Defines the default quality of service (QoS) translation schema to use with a classification map.

1.53.2 Command Mode

Class map configuration

1.53.3 Syntax Description

8P0D	Specifies that 8P0D 802.1p Priority Code Point (PCP) encoding is the default schema. The 8P0D schema propagates the three Multiprotocol Label Switching (MPLS) experimental (EXP) or 802.1p bits to the priority bits of the packet descriptor (PD) QoS value on ingress, and performs the reverse on egress. The PD drop-precedence bits are set to zero on ingress, and ignored on egress. For the default values for 8P0D ingress and egress mappings, see Table 4 and Table 5, respectively.
7P1D	Specifies that 7P1D 802.1p PCP is the default schema. The 7P1D schema maps between the eight possible EXP or 802.1p values and seven different PD QoS priority levels, one of which includes two levels of drop-precedence. For the default values for 7P1D ingress and egress mappings, see Table 6 and Table 7, respectively.

6P2D	Specifies that 6P2D 802.1p PCP is the default schema. The 6P2D schema maps between the eight possible EXP or 802.1p values and six different PD QoS priority levels, two of which include two levels of drop-precedence. For the default values for 6P2D ingress and egress mappings, see Table 8 and Table 9, respectively.
5P3D	Specifies that 5P3D 802.1p PCP is the default schema. The 5P3D schema maps between the eight possible EXP or 802.1p values and five different PD QoS priority levels, three of which include two levels of drop-precedence. For the default values for 5P3D ingress and egress mappings, see Table 10 and Table 11, respectively.

1.53.4 Default

Maps all entries to the default 8P0D values.

1.53.5 Usage Guidelines

Use the **mapping-schema** command to define the default QoS translation schema to use with a classification map that translates external to internal to external QoS priority markings. This command overrides any existing configuration for the classification map.

You can use this command to specify default values for all mapping entries, then override that value for a subset of entries by entering subsequent mapping commands.

Use the **no** or **default** form of this command to revert values for all map entries to the default 8P0D values.

Table 4 lists the default values for 8P0D ingress mappings.

Table 4 8P0D Mapping, Ingress from MPLS EXP and Ethernet 802.1p

Ethernet 802.1p	MPLS EXP	PD QoS Priority	PD Drop Precedence	IP Precedence	DSCP
7	7	0	0	7	Network Control
6	6	1	0	6	Reserved
5	5	2	0	5	cs5
4	4	3	0	4	cs4
3	3	4	0	3	cs3
2	2	5	0	2	cs2

Table 4 8P0D Mapping, Ingress from MPLS EXP and Ethernet 802.1p

Ethernet 802.1p	MPLS EXP	PD QoS Priority	PD Drop Precedence	IP Precedence	DSCP
1	1	6	0	1	cs1
0	0	7	0	0	DF

Table 5 lists the default values for 8P0D egress mappings.

Table 5 8P0D Mapping, Egress to MPLS EXP and Ethernet 802.1p

PD QoS Priority	PD Drop Precedence	IP Precedence	DSCP	Ethernet 802.1p	MPLS EXP
0	NA	7	Network Control	7	7
1	NA	6	Reserved	6	6
2	NA	5	EF	5	5
3	NA	4	AF4[1,2,.3]	4	4
4	NA	3	AF3[1,2,3]	3	3
5	NA	2	AF2[1,2,3]	2	2
6	NA	1	AF1[1,2,3]	1	1
7	NA	0	DF	0	0

Table 6 lists the default values for 7P1D ingress mappings.

Table 6 7P1D Mapping, Ingress from MPLS EXP and Ethernet 802.1p

MPLS EXP	Ethernet 802.1p	PD QoS Priority	PD Drop Precedence	DSCP	IP Precedence
7	7	0	0	Network Control	7
6	6	1	0	Reserved	6
5	5	3	2	AF 4[1]	4
4	4	3	6	AF 4[3]	4
3	3	4	2	AF 3[1]	3
2	2	5	2	AF2[1]	2
1	1	6	2	AF 1[1]	1
0	0	7	0	DF	0

Table 7 lists the default values for 7P1D egress mappings.

Table 7 7P1D Mapping, Egress to MPLS EXP and Ethernet 802.1p

PD QoS Priority	PD Drop Precedence	DSCP	IP Precedence	MPLS EXP	Ethernet 802.1p
0	NA	Network Control	7	7	7
1	NA	Reserved	6	6	6
2	NA	EF	5	5	5
3	0, 1, 2	AF 4[1]	4	5	5
3	<> [0, 1, 2]	AF 4[2,3]	4	4	4
4	NA	AF3[1,2,3]	3	3	3
5	NA	AF2[1,2,3]	2	2	2
6	NA	AF1[1,2,3]	1	1	1
7	NA	DF	0	0	0

Table 8 lists the default values for 6P2D ingress mappings.

Table 8 6P2D Mapping, Ingress from MPLS EXP and Ethernet 802.1p

MPLS EXP	Ethernet 802.1p	PD QoS Priority	PD Drop Precedence	DSCP	IP Precedence
7	7	0	0	Network Control	7
6	6	1	0	Reserved	6
5	5	3	2	AF 4[1]	4
4	4	3	6	AF 4[3]	4
3	3	5	2	AF 2[1]	2
2	2	5	6	AF 2[3]	2
1	1	6	2	AF 1[1]	1
0	0	7	0	DF	0

Table 9 lists the default values for 6P2D egress mappings.

Table 9 6P2D Mapping, Egress to MPLS EXP and Ethernet 802.1p

PD QoS Priority	PD Drop Precedence	DSCP	IP Precedence	MPLS EXP	Ethernet 802.1p
0	NA	Network Control	7	7	7

Table 9 6P2D Mapping, Egress to MPLS EXP and Ethernet 802.1p

PD QoS Priority	PD Drop Precedence	DSCP	IP Precedence	MPLS EXP	Ethernet 802.1p
1	NA	Reserved	6	6	6
2	NA	EF	5	5	5
3	0, 1, 2	AF 4[1]	4	5	5
3	<>[0, 1, 2]	AF 4[2,3]	4	4	4
4	0, 1, 2	AF 3[1]	3	3	3
4	<>[0, 1, 2]	AF 3[2,3]	3	2	2
5	0, 1, 2	AF 2[1]	2	3	3
5	<>[0, 1, 2]	AF 2[2,3]	2	2	2
6	NA	AF1[1,2,3]	1	1	1
7	NA	DF	0	0	0

Table 10 lists the default values for 5P3D ingress mappings

Table 10 5P3D Mapping, Ingress from MPLS EXP and Ethernet 802.1p

PD QoS Priority	PD Drop Precedence	DSCP	IP Precedence	MPLS EXP	Ethernet 802.1p
0	0	Network Control	7	7	7
1	0	Reserved	6	6	6
3	2	AF 4[1]	4	5	5
3	6	AF 4[3]	4	4	4
3	3	3	3	3	3
5	6	AF 2[3]	2	3	2
7	0	DF	0	1	1
7	6	DF-	0	0	0

Table 11 lists the default values for 5P3D egress mappings.

Table 11 5P3D Mapping, Egress to MPLS EXP and Ethernet 802.1p

SmartEdge PD Priority	SmartEdge PD Drop	DSCP	IP Precedence	MPLS EXP	Ethernet 802.1p
0	NA	Network Control	7	7	7
1	NA	Reserved	6	6	6

Table 11 5P3D Mapping, Egress to MPLS EXP and Ethernet 802.1p

SmartEdge PD Priority	SmartEdge PD Drop	DSCP	IP Precedence	MPLS EXP	Ethernet 802.1p
2	NA	EF	5	5	5
3	0, 1, 2	AF 4[1]	4	5	5
3	<>[0, 1, 2]	AF 4[2,3]	4	4	4
4	0, 1, 2	AF 3[1]	3	3	3
4	<> [0, 1, 2]	AF 3[2,3]	3	2	2
5	0, 1, 2	AF 2[1]	2	3	3
5	<>[0, 1, 2]	AF 2[2,3]	2	2	2
6	0, 1, 2	AF 1[1]	1	1	1
6	<>[0, 1, 2]	AF 1[2,3]	2	0	0
7	0	DF	0	1	1
7	<>0	DF-	0	0	0

1.53.6 Examples

The following example shows how to define the classification map **pd-to-exp** for PD values on egress, then to define the default mapping schema as **6P2D**. It overrides the default mapping for PD user priority value **af33** to MPLS EXP value **4**, and specifies the default DSCP-to-EXP mapping for PD value **13:**

```
[local]Redback(config)#qos class-map pd-to-exp mpls out
[local]Redback(config-class-map)#mapping-schema 6P2D
[local]Redback(config-class-map)#qos af33 to mpls 4
[local]Redback(config-class-map)#qos 13 use-ip
```

1.54 mark dscp

mark dscp ***dscp-class***

no mark dscp ***dscp-class***

1.54.1 Purpose

Assigns a quality of service (QoS) Differentiated Services Code Point (DSCP) priority to IP packets. For IPv4 packets, the DSCP marking is the upper six bits

of the IPv4 header Type of Service (ToS) field. For IPv6 packets, the DSCP marking is the upper six bits of the IPv6 header Traffic Class field.

1.54.2 Command Mode

- Metering policy configuration
- Policy ACL class configuration
- Policing policy configuration

1.54.3 Syntax Description

dscp-class	Priority with which packets are marked. Values can be: • Integer from 0 to 63. • One of the keywords listed in Table 12.

1.54.4 Default

Packets are not assigned a DSCP priority.

1.54.5 Usage Guidelines

Use the **mark dscp** command to assign a QoS DSCP priority to packets.

Caution!

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

Table 12 lists the keywords for the ***dscp-class*** argument.

Table 12 DSCP Class Keywords

DSCP Class	Keyword	DSCP Class	Keyword
Assured Forwarding (AF) Class 1/ Drop precedence 1	**af11**	Class Selector 0 (same as default forwarding)	**cs0** (same as **df**)

Table 12 DSCP Class Keywords

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

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

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

1.54.6 Examples

The following example shows how to configure the policy, **GE-in policing**, to mark all packets within the **VOIP** class as high-priority packets, while all packets within the **best-effort** class are marked as low-priority packets:

```
[local]Redback(config)#qos policy GE-in policing
[local]Redback(config-policy-policing)#access-group myacl cont2
[local]Redback(config-policy-group)#class VOIP
[local]Redback(config-policy-group-class)#mark dscp ef
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#class best-effort
[local]Redback(config-policy-group-class)#mark dscp df
```

1.55 mark dscp destination

mark dscp destination

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

1.55.1 Purpose

Sets the Differentiated Services Code Point (DSCP) byte, based on Border Gateway Protocol (BGP) attributes, such as community list and autonomous system (AS) path, for incoming IP traffic on the specified interface.

1.55.2 Command Mode

Interface configuration

1.55.3 Syntax Description

This command has no keywords or arguments.

1.55.4 Default

Disabled

1.55.5 Usage Guidelines

Use the **mark dscp destination** command to set the DSCP byte, based on BGP attributes, such as community list and autonomous AS path, for incoming IP traffic on the specified interface.

BGP destination-based quality of service (QoS) provides multiple levels of service based on a customer's IP destination. BGP routes can be assigned a DSCP value based on the BGP traffic indexing and table map features associated with route maps. BGP routes can be assigned a traffic index. The byte and packet counters for the traffic index are incremented based on the route traversed by IP traffic received on the ingress interface.

When a packet is received on an interface with **mark dscp destination** enabled and the packet is routed using a route with associated DSCP, the packet's DSCP is updated and the IP header checksum is recalculated.

Caution!

Risk of overriding configurations. Because marking can be configured at different levels, the SmartEdge router checks for and applies marking in a specific order. To reduce the risk, remember the following points: Circuit-based marking overrides class-based marking. Circuit-based marking is configured through the **conform** and **exceed** commands in QoS policy rate configuration mode. Class-based marking is configured through the **class** command in policy ACL configuration mode and the **mark** command in policy ACL class configuration mode and BGP destination-based marking, through route maps, overrides both circuit-based and class-based marking.

Use the **no** form of this command to disable the DSCP byte marking for incoming IP traffic for the specified interface.

1.55.6 Examples

The following example shows how to enable BGP-based marking on the appropriate ingress interface:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface CustomerOne
[local]Redback(config-if)#ip address 10.200.1.1/30
[local]Redback(config-if)#mark dscp destination
```

1.56 mark precedence

mark precedence *prec-value*

no mark precedence ***prec-value***

1.56.1 Purpose

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

1.56.2 Command Mode

- Metering policy configuration
- Policy ACL class configuration
- Policing policy configuration

1.56.3 Syntax Description

prec-value	Drop precedence value. See Table 13.

1.56.4 Default

Packets are not marked with an explicit drop precedence value.

1.56.5 Usage Guidelines

Use the **mark precedence** command to assign a QoS drop precedence value to packets.

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

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

In general, the level of forwarding assurance of an IP packet is based on: (1) , (2), (3) ().

- Resources allocated to the AF class to which the packet belongs
- Current load of the AF class and, in case of congestion, within the class
- Drop precedence of the packet. In case of congestion,

The drop precedence of a packet determines the relative importance of the packet within the assured forwarding (AF) Differentiated Services Code Point (DSCP) class. Packets with a lower drop precedence value are preferred and protected from being lost, while packets with a higher drop precedence value are discarded.

For more information see RFC 2597, *Assured Forwarding PHB Group*.With AF classes AF1 (AF11, AF12, AF13), AF2 (AF21, AF22, AF23), AF3 (AF31, AF32, AF33), and AF4 (AF41, AF42, AF43), the second integer represents a drop precedence value. Table 13 shows how the AF drop precedence value of an incoming packet is changed when it exits the SmartEdge router after being tagged with a new drop precedence. (See also RFC 2597, *Assured Forwarding PHB Group*.)

Table 13 Drop Precedence Values

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

Caution!

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

1.56.6 Examples

The following example shows how to configure the policy, **GE-in policing**, to mark all packets within the **VOIP** class as preferred packets, while all packets within the **best-effort** class are marked as less-preferred packets:

```
[local]Redback(config)#qos policy GE-in policing
[local]Redback(config-policy-policing)#access-group myacl cont2
[local]Redback(config-policy-group)#class VOIP
[local]Redback(config-policy-group-class)#mark precedence 1
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#class best-effort
[local]Redback(config-policy-group-class)#mark precedence 3
```

1.57 mark priority

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

no mark priority

1.57.1 Purpose

Sets the internal packet descriptor (PD) quality of service (QoS) classification value for specified packets, while preserving the packet's IP header Differentiated Services Code Point (DSCP) value.

1.57.2 Command Mode

- Metering policy configuration
- Policing policy configuration
- Policy group class configuration

1.57.3 Syntax Description

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

1.57.4 Default

The PD QoS values for a packet are not modified.

1.57.5 Usage Guidelines

Use the **mark priority** command to set the internal PD QoS classification value for specified packets, while preserving the packet's IP header DSCP value.

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

The SmartEdge router uses the factory preset, or default, mapping of a PD QoS priority group to a queue, according to the number of queues configured on a circuit; see Table 14.

Table 14 Default Mapping of Priority Groups

PD QoS Priority Group	8 Queues	4 Queues	2 Queues	1 Queue
0	Queue 0	Queue 0	Queue 0	Queue 0
1	Queue 1	Queue 1	Queue 1	Queue 0

Table 14 Default Mapping of Priority Groups

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

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

Caution!

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

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

If neither the **drop-precedence** nor the **af-drop** keyword is specified, the priority bits are set to the specified value and the drop-precedence bits are cleared.

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

1.57.6 Examples

The following example shows how to configure the policy, **GE-in policing**, to mark all packets within the **VOIP** class as high-priority packets, while all packets within the **best-effort** class are marked as low-priority packets:

```
[local]Redback(config)#qos policy GE-in policing
[local]Redback(config-policy-policing)#access-group myacl cont2
[local]Redback(config-policy-group)#class VOIP
[local]Redback(config-policy-group-class)#mark priority 2
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#class best-effort
[local]Redback(config-policy-group-class)#mark priority 7
```

1.58 master

master

no master

1.58.1 Purpose

Configures the current bridge as a Rapid Spanning Tree Protocol (RSTP) master bridge.

1.58.2 Command Mode

Spanning-tree configuration

1.58.3 Syntax Description

This command has no keywords or arguments.

1.58.4 Default

Current bridge is not an RSTP master.

1.58.5 Usage Guidelines

Use the **master** command to configure the current bridge as an RSTP master bridge.

Bridges that are not running RSTP and are enabled for tracking by the `track spanning-tree` command are called *client* bridges. The state of all client bridge circuits on the same port as a master bridge circuit follow the state of the RSTP master. When the state of the circuit controlled by the master bridge changes to blocking, forwarding, or flushing, all circuits on the same port of the tracking client bridges change to the same state.

Use the **no** form of this command to disable tracking of the RSTP master bridge.

1.58.6 Examples

The following example shows how configure an RSTP master bridge and a client bridge configured for tracking:

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#bridge blue
[local]Redback(config-bridge)#spanning-tree
[local]Redback(config-bridge-stp)#master
[local]Redback(config-bridge-stp)#end
!
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#bridge green
[local]Redback(config-bridge)#track spanning-tree blue local
[local]Redback(config-bridge)#end
```

1.59 match as-path-list

match as-path-list *apl-name*

no match as-path-list *apl-name*

1.59.1 Purpose

Permits or denies routes that include the specified Border Gateway Protocol (BGP) autonomous system (AS) path list.

1.59.2 Command Mode

Route map configuration

1.59.3 Syntax Description

apl-name	AS path list name.

1.59.4 Default

There are no preconfigured route map match conditions.

1.59.5 Usage Guidelines

Use the **match as-path-list** command to permit or deny routes that include the specified BGP AS path list. A route map can have several entries. Any route that does not match at least one match clause corresponding to a route map is ignored; that is, the route is not advertised for outbound route maps and is not accepted for inbound route maps. To modify only some data, you must configure a second route map section with an explicit match condition specified.

Use the **no** form of this command to remove the match condition.

1.59.6 Examples

The following example shows how to permit routes that include AS path list **5:**

```
[local]Redback(config-ctx)#route-map asp-regex permit 10
[local]Redback(config-route-map)#match as-path-list 5
```

1.60 match community-list

match community-list *cl-name* [**exact-match**]

no match community-list *cl-name*

1.60.1 Purpose

Permits or denies routes with an associated Border Gateway Protocol (BGP) community attribute that matches the specified community list.

1.60.2 Command Mode

Route map configuration

1.60.3 Syntax Description

cl-name	Name of the community list.
exact-match	Optional. Defines communities in the community list that must match exactly.

1.60.4 Default

There are no preconfigured route map match conditions.

1.60.5 Usage Guidelines

Use the **match community-list** command to permit or deny routes with an associated BGP community attribute that matches the specified community list.

When the **exact-match** keyword is specified, the community list entries must match the BGP community attribute exactly. In other words, the community list

must have the same number of entries as the BGP community attribute, and each community list entry, community number, or well-known community must be present in the BGP community attribute. In addition, the community list used for exact matching must not have any deny entries or any entries with a regular expression specification.

A route map can have several sequenced entries. Any route that does not satisfy all the match conditions associated with a route map entry is ignored and the next higher sequenced route map entry is examined.

See the **community-list** command in context configuration mode for more information.

Use the **no** form of this command to disable the match condition.

1.60.6 Examples

The following example shows how to permit any route that includes the attribute community list **1:**

```
[local]Redback(config-ctx)#community-list 1
[local]Redback(config-community-list)#permit 11
[local]Redback(config-community-list)#exit
[local]Redback(config-ctx)#route-map map_A
[local]Redback(config-route-map)#match community-list 1
```

1.61 match ext-community-list

match ext-community-list *ecl-name* [**exact-match**]

no match community-list *ecl-name*

1.61.1 Purpose

Permits or denies routes with an associated Border Gateway Protocol (BGP) extended community attribute that matches the specified extended community list.

1.61.2 Command Mode

Route map configuration

1.61.3 Syntax Description

ecl-name	Name of the extended community list.
exact-match	Optional. Defines extended communities in the extended community list that must match exactly.

1.61.4 Default

There are no preconfigured route map match conditions.

1.61.5 Usage Guidelines

Use the **match ext-community-list** command to permit or deny routes with an associated BGP extended community attribute that matches the specified extended community list.

When the **exact-match** keyword is specified, the extended community list entries must match the BGP extended community attribute exactly. In other words, the extended community list must have the same number of entries as the BGP extended community attribute, and each extended community list entry, extended community number, or well-known extended community must be present in the BGP extended community attribute. In addition, the extended community list used for exact matching must not have any deny entries or any entries with a regular expression specification.

A route map can have several sequenced entries. Any route that does not satisfy all the match conditions associated with a route map entry is ignored and the next higher sequenced route map entry is examined.

See the **ext-community-list** command in context configuration mode for more information.

Use the **no** form of this command to disable the match condition.

1.61.6 Examples

The following example shows how to permit any route that includes the extended community list **1** attribute:

```
[local]Redback(config-ctx)#ext-community-list 1
[local]Redback(config-community-list)#permit 11
[local]Redback(config-community-list)#exit
[local]Redback(config-ctx)#route-map map_A
[local]Redback(config-route-map)#match ext-community-list 1
```

1.62 match ip address prefix-list

match ip address prefix-list *pl-name*

no match ip address prefix-list *pl-name*

1.62.1 Purpose

Permits or denies routes with a destination IP address permitted by the specified IP prefix list.

1.62.2 Command Mode

Route map configuration

1.62.3 Syntax Description

pl-name	Name of the IP prefix list used to match route destinations.

1.62.4 Default

There are no preconfigured route map match conditions.

1.62.5 Usage Guidelines

Use the **match ip address prefix-list** command to permit or deny routes with a destination IP address permitted by the specified IP prefix list. To create an IP prefix list, use the **ip prefix-list** command in context configuration mode.

Use the **no** form of this command to disable IP address matching.

1.62.6 Examples

The following example shows how to permit routes that have destination IP addresses specified in an IP prefix list, **prefix8:**

```
[local]Redback(config-ctx)#route-map rmap_B
[local]Redback(config-route-map)#match ip address prefix-list prefix8
```

1.63 match ip next-hop prefix-list

match ip next-hop prefix-list *pl-name*

no match ip next-hop prefix-list *pl-name*

1.63.1 Purpose

Permits or denies routes with a next-hop IP address that is permitted by the specified IP prefix list.

1.63.2 Command Mode

Route map configuration

1.63.3 Syntax Description

pl-name	Name of the IP prefix list used to match the next-hop IP address.

1.63.4 Default

There are no preconfigured route map match conditions.

1.63.5 Usage Guidelines

Use the **match ip next-hop prefix-list** command to permit or deny routes with a next-hop IP address permitted by the specified IP prefix list. To create an IP prefix list, use the **ip prefix-list** command in context configuration mode.

Use the **no** form of this command to disable next-hop IP address matching.

1.63.6 Examples

The following example shows how to permit routes that have a next-hop IP address permitted by either prefix list, **prefix11** or **prefix98:**

```
[local]Redback(config-ctx)#route-map rmap_C
[local]Redback(config-route-map)#match ip next-hop prefix-list prefix11 prefix98
```

1.64 match ipv6 address prefix-list

match ipv6 address prefix-list *ipv6-pl-name*

no match ipv6 address prefix-list *ipv6-pl-name*

1.64.1 Purpose

Permits or denies routes with a destination IP Version 6 (IPv6) address permitted by the specified IPv6 prefix list.

1.64.2 Command Mode

Route map configuration

1.64.3 Syntax Description

ipv6-pl-name	Name of the IPv6 prefix list used to match route destinations.

1.64.4 Default

There are no preconfigured route map match conditions.

1.64.5 Usage Guidelines

Use the **match ipv6 address prefix-list** command to permit or deny routes with a destination IPv6 address permitted by the specified IPv6 prefix list. To create an IPv6 prefix list, use the **ipv6 prefix-list** command in context configuration mode.

Use the **no** form of this command to disable IPv6 address matching.

1.64.6 Examples

The following example shows how to permit routes that have destination IPv6 addresses specified in an IPv6 prefix list, **prefix8:**

```
[local]Redback(config-ctx)#route-map rmap_B
[local]Redback(config-route-map)#match ipv6 address prefix-list prefix8
```

1.65 match ipv6 next-hop prefix-list

match ip next-hop prefix-list ***ipv6-pl-name***

no match ip next-hop prefix-list ***ipv6-pl-name***

1.65.1 Purpose

Permits or denies routes with a next-hop IP Version 6 (IPv6) address that is permitted by the specified IPv6 prefix list.

1.65.2 Command Mode

Route map configuration

1.65.3 Syntax Description

ipv6-pl-name	Name of the IPv6 prefix list used to match the next-hop IPv6 address.

1.65.4 Default

There are no preconfigured route map match conditions.

1.65.5 Usage Guidelines

Use the **match ipv6 next-hop prefix-list** command to permit or deny routes with a next-hop IPv6 address permitted by the specified IPv6 prefix list. To create an IPv6 prefix list, use the **ipv6 prefix-list** command in context configuration mode.

Use the **no** form of this command to disable next-hop IPv6 address matching.

1.65.6 Examples

The following example shows how to permit routes that have a next-hop IPv6 address permitted by either IPv6 prefix list, **ipv6pl4** or **ipv6pl72:**

```
[local]Redback(config-ctx)#route-map rmap_C
[local]Redback(config-route-map)#match ipv6 next-hop prefix-list ipv6pl4 ipv6pl72
```

1.66 match metric

match metric ***metric***

no match metric ***metric***

1.66.1 Purpose

Permits or denies routes with a specified metric value.

1.66.2 Command Mode

Route map configuration

1.66.3 Syntax Description

metric	Route metric value. The range of values is 0 to 4294967295.

1.66.4 Default

There are no preconfigured route map match conditions.

1.66.5 Usage Guidelines

Use the **match metric** command to permit or deny routes with a specified metric value.

Use the **no** form of this command to disable the match condition.

1.66.6 Examples

The following example shows how to permit routes with a metric value of **5:**

```
[local]Redback(config-ctx)#route-map rmap_D
[local]Redback(config-route-map)#match metric 5
```

1.67 match route-type

match route-type {**internal** | **external** [**type-1** | **type-2**] | **level-1** | **level-2** | **nssa-external** [**type-1** | **type-2**] | **dvsr**}

no match route-type

1.67.1 Purpose

Permits or denies routes that match a specified route type.

1.67.2 Command Mode

Route map configuration

1.67.3 Syntax Description

internal	Matches internal Open Shortest Path First (OSPF) intra-area and inter-area routes.
external	Specifies Border Gateway Protocol (BGP) and OSPF external routes.
type-1	Optional. Matches OSPF Type 1 external routes when used with the **external** keyword. Matches OSPF not-so-stubby-area (NSSA) Type 1 external routes when used with the **nssa-external** keyword.
type-2	Optional. Matches OSPF Type 2 external routes when use with the **external** keyword. Matches OSPF NSSA Type 2 external routes when used with the **nssa-external** keyword.
level-1	Matches Intermediate System-to-Intermediate System (IS-IS) Level 1 routes.
level-2	Matches IS-IS Level 2 routes.
nssa-external	Matches OSPF NSSA external routes.
dvsr	Matches dynamically verified static routing (DVSR) subtype of static route.

1.67.4 Default

There are no preconfigured route map match conditions.

1.67.5 Usage Guidelines

Use the **match route-type** command to permit or deny routes that match a specified route type.

Use the **no** form of this command to disable route type matching.

1.67.6 Examples

The following example shows how to permit or deny internal OSPF routes:

```
[local]Redback(config-ctx)#route-map map_E
[local]Redback(config-route-map)#match route-type internal
```

1.68 match tag

match tag *tag*

no match tag

1.68.1 Purpose

Permits or denies routes that match a specified route tag value.

1.68.2 Command Mode

Route map configuration

1.68.3 Syntax Description

tag	Unsigned integer. The range of values is 0 to 4,294,967,295.

1.68.4 Default

There are no preconfigured route map match conditions.

1.68.5 Usage Guidelines

Use the **match tag** command to permit or deny routes that match a specified route tag value.

Use the **no** form of this command to disable route tag matching.

1.68.6 Examples

The following example shows how to permit routes using a route tag value of **5:**

```
[local]Redback(config-ctx)#route-map map_F
[local]Redback(config-route-map)#match tag 5
```

1.69 max-age

max-age *sec*

{**no** | **default**} **max-age**

1.69.1 Purpose

Sets the maximum age of received bridge protocol data units (BPDUs).

1.69.2 Command Mode

spanning-tree configuration

1.69.3 Syntax Description

sec	Maximum age in seconds (6 to 40). The maximum age must be in whole seconds and within the following range: 2 * (forward-delay - 1.0) >= max-age >= 2 * (hello-interval + 1.0).

1.69.4 Default

20 seconds

1.69.5 Usage Guidelines

Use the **max-age** command to set the maximum age of the received BPDUs; that is, the maximum time received BPDU information is saved, after which it is discarded. This command applies when the current bridge is the root bridge.

1.69.6 Examples

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

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

1.70 max-flows-per-circuit

max-flows-per-circuit *value*

default max-flows-per-circuit

1.70.1 Purpose

Sets the maximum number of flows the system can create on a circuit.

1.70.2 Command Mode

Flow configuration

1.70.3 Syntax Description

value	Maximum number of flows the system can create on a circuit. The range of values is 1 to 2097152.

1.70.4 Default

None

1.70.5 Usage Guidelines

Use the **max-flows-per-circuit** command to set the maximum number of flows the system can create on a circuit.

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

1.70.6 Examples

The following example shows how to set the maximum number of flows the system can generate on the current circuit to **2000:**

```
[local]Redback(config-ac-profile)#max-flows-per-circuit 2000
```

1.71 max-groups

max-groups *count* [**drop-old**]

no max-groups

1.71.1 Purpose

Configures the maximum number of groups a single circuit can join.

1.71.2 Command Mode

- IGMP service profile configuration
- IGMP snooping profile configuration

1.71.3 Syntax Description

count	Maximum number of joined groups. Range is from 1 to 100000 groups.
drop-old	Optional. Drops the oldest IGMP group on the interface and accepts the new IGMP report.

1.71.4 Default

Unlimited number of groups.

1.71.5 Usage Guidelines

Use the **max-groups** command to configure the maximum number of groups a single circuit can join.

If the addition of a new group on an interface causes the total number of joined groups to exceed the maximum number allowed, either of the following actions is taken:

- If the **drop-old** keyword is specified for the service profile, the oldest IGMP group on the interface is dropped and the new IGMP report accepted.
- If the **drop-old** keyword is not specified for the service profile, the new IGMP membership report is refused.

Use the **no** form of this command to remove the maximum number of IGMP-joined groups restriction.

1.71.6 Examples

The following example shows how to configure a maximum of `3 joined groups for each interface:`

```
[local]Redback(config-ctx)#profile bar
[local]Redback(config-igmp-service-profile)#max-groups 3
```

The following example shows how to configure the maximum groups setting in an IGMP profile called `sanjose1`. If this profile is associated with a circuit, then the maximum number of groups that circuit can join is set to `3`. If the circuit joins more than 3 groups, then the circuit drops its join with the oldest group:

```
[local]Redback#configure
[local]Redback(config)#igmp snooping profile sanjose
[local]Redback(config-igmp-snooping-profile)#max-groups 3
```

1.72 max-hops

max-hops ***count***

{**no** | **default**} **max-hops** ***count***

1.72.1 Purpose

Configures the maximum hop count allowed for Dynamic Host Configuration Protocol (DHCP) requests.

1.72.2 Command Mode

DHCP relay server configuration

1.72.3 Syntax Description

count	Hop count. The range of values is 1 to 16.

1.72.4 Default

The default hop count is four.

1.72.5 Usage Guidelines

Use the **max-hops** command to configure the maximum hop count allowed for DHCP requests.

Use the **no** or **default** form of this command to return to the default DHCP relay server maximum hop count of four.

1.72.6 Examples

The following example shows how to configure a maximum of **12** hops allowed for DHCP requests to DHCP server, **10.30.40.50:**

```
[local]Redback(config-ctx)#dhcp relay server 10.30.40.50
[local]Redback(config-dhcp-relay)#max-hops 12
[local]Redback(config-dhcp-relay)#
```

1.73 maximum ip-packet-size

maximum ip-packet-size ***size***

no maximum ip-packet-size ***size***

1.73.1 Purpose

Configures the maximum size of the IP packet in bytes for a NAT logging profile.

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

1.73.2 Command Mode

NAT logging configuration.

1.73.3 Syntax Description

size-in-bytes	Maximum size of the IP packet in bytes. The range 200 to 65520.

1.73.4 Default

1200 bytes

1.73.5 Example

The following example shows how to configure the maximum size of the IP packet for a NAT logging profile.

```
[local]Redback#configuration
Enter configuration commands, one per line, 'end' to exit
[local]Redback(config)#context nat-context
[local]Redback(config-ctx)#nat logging-profile nat-log-profile
[local]Redback(config-nat-profile)#maximum ip-packet-size 1400
```

1.74 maximum-links

maximum-links ***max-active***

{**no** | **default**} **maximum-links**

1.74.1 Purpose

Specifies the maximum number of active links in the 802.1Q, Ethernet, or access link group.

1.74.2 Command Mode

Link group configuration

1.74.3 Syntax Description

max-active	Maximum number of active links in the link group. The range of values depends on the type of Fast Ethernet (FE) or Gigabit Ethernet (GE) port and the type of link group; see Table 15 for the range of values for each type of port and link group. The default value is 1 for an access link group and 8 for any other type of link group.

1.74.4 Default

The number of active links in a link group is one for any type of link group.

1.74.5 Usage Guidelines

Use the **maximum-links** command to specify the maximum number of active links in the 802.1Q, Ethernet, or access link group.

Table 15 lists the range of values for the ***max-active*** argument when configuring an 802.1Q, Ethernet, or access link group with SmartEdge 100 native ports, FE and GE ports on media interface cards (MICs), or SmartEdge 400 and SmartEdge 800 traffic cards.

Table 15 Range of Values for max-active Argument

Port Type	Link Group Type	Range of Values
GE3, GE1020, 10GE	Access	1 to 2(1)
	Ethernet	1 to 8
	802.1Q	1 to 8
FE, GE (all other versions)	Access	1 to 8
	Ethernet	1 to 8
	802.1Q	1 to 8

(1) Configuring a value of 2 is subject to configuration restrictions. See the paragraph immediately following this table.

In general, an access link group with GE3, GE1020, or 10GE ports can have only one active port (in the up state) among the constituent circuits in the group; however, you can specify two active ports with this command, subject to the following restrictions:

- The two active ports cannot be on the same traffic card.
- The standby ports can be on the same traffic card as one of the active ports or on a different traffic card.
- Priority weighted fair queuing (PWFQ) policies are not supported.

- Quality of service (QoS) hierarchical nodes configured with strict mode are not supported.

If you add more ports to the link group than the maximum number of active links specified by the ***max-active*** argument, the remaining links are treated as hot standby links. The system communicates the standby state for these links to the partner system using Link Aggregation Control Protocol (LACP).

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

1.74.6 Examples

The following example shows how to configure the **lg-ether** link group with a maximum of **2** active links:

```
[local]Redback(config)#link-group lg-ether ether
[local]Redback(config-link-group)#maximum-links 2
```

1.75 maximum paths (IS-IS)

maximum paths ***paths***

{**no** | **default**} **maximum paths**

1.75.1 Purpose

Changes the router's default number of multiple equal-cost Intermediate System-to-Intermediate System (IS-IS) paths for load balancing of outgoing traffic packets.

1.75.2 Command Mode

IS-IS router configuration

1.75.3 Syntax Description

paths	Maximum number of equal-cost paths used as the best paths. The range of values is 1 to 8.

1.75.4 Default

The maximum number of equal-cost paths is 8.

1.75.5 Usage Guidelines

Use the **maximum paths** command to change the router's default number of multiple equal-cost IS-IS paths for load balancing of outgoing traffic packets. The SmartEdge router load balances among these IS-IS paths if, in the routing table, they are the best paths among paths provided by all running routing protocols.

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

1.75.6 Examples

The following example shows how to set the maximum number of paths to **4:**

```
[local]Redback(config-ctx)#router isis isis01
[local]Redback(config-isis)#maximum paths 4
```

1.76 maximum-paths (RIP)

maximum-paths *path-num*

{**no** | **default**} **maximum-paths**

1.76.1 Purpose

Modifies the number of multiple equal-cost Routing Information Protocol (RIP) or RIP next generation (RIPng) routes that can be used as the best paths for load balancing outgoing traffic packets.

1.76.2 Command Mode

- RIPng router configuration
- RIP router configuration

1.76.3 Syntax Description

path-num	Maximum number of equal-cost routes used as the best paths. The range of values is 1 to 16; the default value is 8.

1.76.4 Default

The default number of equal-cost routes is 8.

1.76.5 Usage Guidelines

Use the **maximum-paths** command to modify the number of multiple equal-cost RIP or RIPng routes that can be used as the best paths for load balancing outgoing traffic packets. The SmartEdge router enables load balancing among these RIP or RIPng paths if, in the routing table, they are the best paths among paths provided by all running routing protocols.

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

1.76.6 Examples

The following example shows how to enable load balancing between two RIP paths for outgoing traffic packets:

```
[local]Redback(config-ctx)#router rip rip001

[local]Redback(config-rip)#maximum-paths 2
```

1.77 maximum prefix

maximum prefix *max-prefix* [**threshold** *threshold*] [**downtime** *interval* | **warning-only**]

no maximum prefix *max-prefix* [**threshold** *threshold*] [**downtime** *interval* | **warning-only**]

1.77.1 Purpose

Specifies how the Border Gateway Protocol (BGP) routing process responds when the maximum number of prefixes sent by the BGP neighbor or BGP peer group for the specified address family is exceeded.

1.77.2 Command Mode

BGP neighbor address family configuration

1.77.3 Syntax Description

max-prefix	Maximum number of prefixes that can be sent by the neighbor. The range of values is 1 to 4,294,967,295; the default is an unlimited number of prefixes.
threshold ***threshold***	Optional. Warning that is generated when the specified threshold value, expressed as a percentage, is reached. The range of values is 1 to 100; the default value is 75.
downtime ***interval***	Optional. Interval, in seconds, for which the connection to the neighbor is down once the specified maximum number of prefixes is exceeded. If this keyword construct is not enabled, the connection remains down until the **clear bgp** ***ip-address*** command in exec mode is issued.
warning-only	Optional. Issues a warning to the neighbor once the specified maximum number of prefixes is exceeded. The connection remains intact.

1.77.4 Default

The BGP routing process accepts an unlimited number of prefixes. If you enter this command without any keywords, the BGP session will be torn down once the ***max-prefix*** argument value is exceeded. The session remains down until the **clear bgp** ***ip-address*** command is issued. The threshold is 75.

1.77.5 Usage Guidelines

Use the **maximum prefix** command to specify how the BGP routing process responds when the maximum number of prefixes sent by the BGP neighbor or BGP peer group for the specified address family is exceeded.

Use the **no** form of this command to return the BGP routing process to the default behavior of allowing an unlimited number of routes and to reset the system to the default behavior of dropping the BGP session when the maximum number of prefixes is exceeded.

1.77.6 Examples

The following example shows how to allow a maximum number of **10000** unicast routes from the neighbor at IP address **102.210.210.1** and generates a warning after 90% of the routes (**9000**) are received:

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

[local]Redback(config-bgp)#neighbor 102.210.210.1 external

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

[local]Redback(config-bgp-peer-af)#maximum prefix 10000 threshold 90
```

Once 10,000 unicast routes are received, the BGP routing process drops the BGP session. The session remains down until the **clear bgp 102.210.210.1** command in exec mode is issued.

1.78 maximum redistribute (IS-IS)

maximum redistribute ***prefixes*** [**retry-interval** ***interval***]

no maximum redistribute

1.78.1 Purpose

Limits the maximum number of routes that can be redistributed into the specified Intermediate System-to-Intermediate System (IS-IS) instance.

1.78.2 Command Mode

IS-IS router configuration

1.78.3 Syntax Description

prefixes	Maximum number of prefixes that can be redistributed into the IS-IS routing instance. The range of values is 1 to 1,000,000.
retry-interval ***interval***	Optional. Amount of time, in seconds, before IS-IS attempts to redistribute routes after the maximum prefix value is exceeded. The range of values is 120 to 7,200; the default value is 600.

1.78.4 Default

There is no maximum limit for the number of prefixes that can be redistributed. The retry interval is 600 seconds.

1.78.5 Usage Guidelines

Use the **maximum redistribute** command to limit the maximum number of routes that can be redistributed into the specified IS-IS instance.

If the maximum number of redistributed prefixes is reached, IS-IS stops redistributing external routes for the duration specified by the **retry-interval** *interval* construct.

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

1.78.6 Examples

The following example shows how to redistribute up to **50000** prefixes into the **isis01** IS-IS instance. If this number is exceeded, routes are not redistributed again for **300** seconds (5 minutes):

```
[local]Redback(config-ctx)#router isis isis01
[local]Redback(config-isis)#maximum redistribute 50000 retry-interval 300
```

1.79 maximum redistribute (OSPF)

maximum redistribute *prefixes* [**retry-interval** *interval*]

no maximum redistribute

1.79.1 Purpose

Sets a maximum limit on the number of routes that can be redistributed into the specified Open Shortest Path First (OSPF) or OSPF Version 3 (OSPFv3) instance.

1.79.2 Command Mode

- OSPF router configuration
- OSPF3 router configuration

1.79.3 Syntax Description

prefixes	Maximum number of routes that can be redistributed into the OSPF or OSPFv3 routing instance. The range of values is 1 to 100,000.
retry-interval *interval*	Optional. Amount of time, in minutes, before OSPF or OSPFv3 attempts to redistribute routes after the maximum prefix value is exceeded. The range of values is 1 to 120.

1.79.4 Default

No maximum.

1.79.5 Usage Guidelines

Use the **maximum redistribute** command to set a maximum limit on the number of routes that can be redistributed into the specified OSPF or OSPFv3 instance.

If the maximum number of redistributed prefixes is reached, OSPF or OSPFv3 stops redistributing external routes for the duration specified by the ***interval*** argument.

Use the **no** form of this command to return to the default setting, which is an unlimited number of routes.

1.79.6 Examples

The following example shows how to limit redistribution of routes into the OSPF routing instance, **650** to **5000:**

```
[local]Redback(config-ctx)#router ospf 650
[local]Redback(config-ospf)#maximum redistribute 5000
```

1.80 maximum redistribute-quantum

maximum redistribute-quantum ***prefixes***

no maximum redistribute-quantum

1.80.1 Purpose

Sets a maximum limit on the number of routes that can be redistributed per second into the Open Shortest Path First (OSPF) or OSPF Version 3 (OSPFv3) instance.

1.80.2 Command Mode

- OSPF router configuration
- OSPF3 router configuration

1.80.3 Syntax Description

prefixes	Maximum number of routes that can be redistributed per second into the OSPF or OSPFv3 routing instance. The range of values is 1 to 10,000; the default value is 2,000.

1.80.4 Default

The maximum number of routes that can be redistributed per second into the OSPF or OSPFv3 routing instance is 2,000.

1.80.5 Usage Guidelines

Use the **maximum redistribute-quantum** command to set a maximum limit on the number of routes that can be redistributed per second into the OSPF or OSPFv3 routing instance.

Use the **no** form of this command to return the limit to its default value of 2,000 routes per second.

1.80.6 Examples

The following example shows how to the maximum number of routes that can be redistributed per second into the OSPF routing instance **30** to **1000:**

```
[local]Redback(config-ctx)#router ospf 30
[local]Redback(config-ospf)#maximum redistribute-quantum 1000
```

1.81 maximum restart-time

maximum restart-time ***interval***

no maximum restart-time ***interval***

1.81.1 Purpose

Sets the maximum amount of time that it will take for a local Border Gateway Protocol (BGP) peer to come up after it has been reset.

1.81.2 Command Mode

- BGP neighbor configuration

- BGP router configuration

1.81.3 Syntax Description

interval	Maximum time, in seconds, that a remote peer will hold the routes received from a local bgp peer after the local peer has been reset during BGP graceful restart. The range of values is 10 to 180; the default value is 120.

1.81.4 Default

The command is disabled. When enabled, the local BGP speaker attempts to reconnect with the remote peer after 120 seconds.

1.81.5 Usage Guidelines

Use the **maximum restart-time** command to set the maximum amount of time that it will take for a local BGP peer to come up after it has been reset.

This graceful restart capability allows a BGP speaker to indicate its ability to preserve its forwarding state during BGP restart.

Use the **no** form of this command to disable a maximum restart time.

1.81.6 Examples

The following example shows how to configure the BGP routing process for autonomous system, **64001**, to attempt to reconnect with the remote peer within **40** seconds after a reset has occurred:

```
[local]Redback(config-ctx)#router bgp 64001
[local]Redback(config-bgp)#maximum restart-time 40
```

The following example shows how to configure the external BGP (eBGP) neighbor, **10.1.1.1**, to attempt to reconnect with the remote peer within **45** seconds after a reset has occurred:

```
[local]Redback(config-bgp)#neighbor 10.1.1.1 external
[local]Redback(config-bgp-neighbor)#maximum restart-time 45
```

1.82 maximum retain-time

maximum retain-time *interval*

no maximum retain-time *interval*

1.82.1 Purpose

Configures the maximum amount of time the local Border Gateway Protocol (BGP) speaker retains routes it previously received from a remote peer once that remote peer restarts the connection.

1.82.2 Command Mode

- BGP neighbor configuration
- BGP router configuration

1.82.3 Syntax Description

interval	Maximum amount of time, in seconds, that the local BGP speaker retains routes it has previously received from the remote peer. The range of values is 30 to 300; the default value is 180 seconds.

1.82.4 Default

The command is disabled. When enabled, the local BGP speaker retains routes it has previously received from the remote peer for 180 seconds, or 3 minutes.

1.82.5 Usage Guidelines

Use the **maximum retain-time** command to set the maximum amount of time the local BGP speaker retains routes it previously received from a remote peer once that remote peer restarts the connection.

Any routes that have not been updated by the remote peer are deleted by the local peer after the local peer receives the end-of-routing information base (RIB) marker from the remote peer, or after the timer expires. An end-of-RIB marker from the remote peer indicates that its initial update has been completed.

Use the **no** form of this command to disable the maximum retain time.

1.82.6 Examples

The following example shows how to configure the BGP routing process for autonomous system, **64001**, to retain routes that have been received from a remote peer once the remote peer restarts the connection for **120** seconds, or 2 minutes:

```
[local]Redback(config-ctx)#router bgp 64001
[local]Redback(config-bgp)#maximum retain-time 120
```

The following example shows how to configure the external BGP (eBGP) neighbor, **10.1.1.1**, to attempt to retain routes from a remote peer once the remote peer restarts the connection for **90** seconds:

```
[local]Redback(config-bgp)#neighbor 10.1.1.1 external
[local]Redback(config-bgp-neighbor)#maximum retain-time 90
```

1.83 maximum update-delay

maximum update-delay ***interval***

no maximum update-delay ***interval***

1.83.1 Purpose

Sets the maximum delay time for the Border Gateway Protocol (BGP) routing process after a reset has occurred before performing initial best-path calculations.

1.83.2 Command Mode

BGP router configuration

1.83.3 Syntax Description

interval	Maximum amount of time, in seconds, that the BGP routing process waits after reset before performing initial best-path calculations. The range of values is 1 to 300.

1.83.4 Default

The command is disabled.

1.83.5 Usage Guidelines

Use the **maximum update-delay** command to set the maximum delay time for the BGP routing process after a reset has occurred before performing initial best-path calculations.

This feature is useful in the case where not all peers support a graceful restart, and in the case where a peer may not send an end-of-Routing Information Base (RIB) marker. Best-path calculations are performed after all peers have send an end-of-RIB marker, or when the timer expires.

Use the **no** form of this command to disable the maximum delay time.

1.83.6 Examples

The following example shows how to configure the BGP routing process for autonomous system, **64001**, to wait **60** seconds, or 1 minute, after a reset has occurred before performing initial best-path calculations:

```
[local]Redback(config-ctx)#router bgp 64001
[local]Redback(config-bgp)#maximum update-delay 60
```

1.84 max-lease-time

max-lease-time *seconds*

no max-lease-time *seconds*

1.84.1 Purpose

Specifies the maximum allowed time for the lease for this internal Dynamic Host Configuration Protocol (DHCP) server or one of its subnets.

1.84.2 Command Mode

- DHCP server configuration
- DHCP subnet configuration

1.84.3 Syntax Description

seconds	Maximum allowed time for the lease (in seconds). The range of values is 180 seconds 900 seconds (15 minutes) to 31,536,000 seconds (1 year).

1.84.4 Default

24 hours

1.84.5 Usage Guidelines

Use the **max-lease-time** command to specify the maximum allowed lease time for this internal DHCP server or one of its subnets. Enter this command in DHCP server configuration mode to specify the maximum allowed lease time for all subnets; enter it in DHCP subnet configuration mode to specify the maximum allowed lease time for that subnet. The value that you specify for a subnet overrides the global value for the server.

Note: If the default lease time is set very low, it will affect the performance of the SmartEdge router, causing some subscribers to lose their leases.

Use the **no** form of this command to specify the default value for the maximum allowed lease time.

1.84.6 Examples

The following example shows how to specify a maximum allowed lease time of 48 hours (**172800**) for the DHCP server and all its subnets:

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

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

[local]Redback(config-dhcp-server)#maximum-lease-time 172800
```

1.85 max-pending-registrations

max-pending-registrations ***maximum***

no max-pending-registrations ***maximum***

1.85.1 Purpose

Specifies the maximum number of pending registrations permitted for this home-agent (HA) peer.

1.85.2 Command Mode

HA peer configuration

1.85.3 Syntax Description

maximum	Maximum number of pending registrations permitted for this HA peer. The range of values is 1 to 65535.

1.85.4 Default

Pending registrations are unlimited.

1.85.5 Usage Guidelines

Use the **max-pending-registrations** command to specify maximum number of pending registrations permitted for this HA peer.

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

1.85.6 Examples

The following example shows how to specify that a maximum of **10** pending registrations are permitted for this HA peer:

```
[local]Redback(config)#context fa
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#foreign-agent
[local]Redback(config-mip-fa)#home-agent-peer 10.1.1.1
[local]Redback(config-mip-ha-peer)#max-pending-registrations 10
```

1.86 max-session

max-session ***sessions***

{**no** | **default**} **max-session** ***sessions***

1.86.1 Purpose

Enables the creation of pseudo-circuits for the Label Distribution Protocol (LDP) label-switched paths (LSPs), and configures the maximum number of LDP sessions allowed on the router.

1.86.2 Command Mode

LDP router configuration

1.86.3 Syntax Description

sessions	Optional. Maximum number of LDP peer sessions allowed on this router.

1.86.4 Default

1200 LDP sessions

1.86.5 Usage Guidelines

Use the **max-session** command to change the maximum number of LDP peer sessions.

Use the **default** form of this command to return to the default value of 1200 sessions.

Use the **no** form of this command to disable the creation of pseudo-circuits for the LDP LSPs.

Use the **show ldp summary** command to display the maximum number of LDP sessions currently configured on this router.

Use the **show configuration ldp** command to display the LDP commands that are configured in the current context.

1.86.6 Examples

The following example shows how to set the maximum number of LDP session for the LSR to 1000:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router ldp
[local]Redback(config-ldp)#max-session 1000
```

1.87 max-sessions

max-sessions ***max-ses-num***

no max-sessions

1.87.1 Purpose

Specifies the maximum number of sessions allowed for a Layer 2 Tunneling Protocol (L2TP) tunnel to a peer or context.

1.87.2 Command Mode

- L2TP peer configuration
- Context configuration

1.87.3 Syntax Description

max-ses-num	Maximum number of sessions allowed for a tunnel or context. The range of values is 1 to 65,535; the default value is 65,535.

1.87.4 Default

65,535

1.87.5 Usage Guidelines

Use the **max-sessions** command to specify the maximum number of sessions allowed for an L2TP tunnel to a peer. For User Datagram Protocol (UDP) tunnels, a new tunnel opens if the ***max-ses-num*** argument value has been reached for the current tunnel and the maximum number of tunnels (***max-tunl-num*** argument value for the **max-tunnels** command in L2TP peer configuration mode) has not been exceeded.

You cannot use this command if you entered L2TP peer configuration mode using the **l2tp-peer** command with the **default** keyword (in context configuration mode).

Use the **max-sessions** command to configure the maximum number of sessions allowed in a given context. This value is applied to all peers configured in this context. If you are using the **max-sessions** command at context level, use this command to enforce the maximum number of L2TP sessions that all the LNS Peers configured in a given context may establish.

Use the **no** or **default** form of this command (in any configuration mode) to set the maximum number of sessions to the default.

1.87.6 Examples

The following example shows how to set the maximum number of sessions allowed per tunnel to a peer to **1000:**

```
[local]Redback(config-ctx)#l2tp-peer name peer1
[local]Redback(config-l2tp)#max-sessions 1000
```

The following example shows how to set the maximum number of sessions allowed per tunnel to a context to **1000:**

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#l2tp max-sessions 1000
```

1.88 max-tunnels

max-tunnels *max-tunl-num*

{**no** | **default**} **max-tunnels**

1.88.1 Purpose

Specifies the maximum number of tunnels allowed to a Layer 2 Tunneling Protocol (L2TP) peer.

1.88.2 Command Mode

L2TP peer configuration

1.88.3 Syntax Description

max-tunl-num	Maximum number of tunnels allowed. The range of values is 1 to 32,767; the default value is 32,767.

1.88.4 Default

32,767

1.88.5 Usage Guidelines

Use the **max-tunnels** command to specify the maximum number of tunnels allowed to an L2TP peer.

Use the **no** or **default** form of this command to set the maximum number of tunnels allowed to the default.

1.88.6 Examples

The following example shows how to set the maximum number of tunnels allowed to **2:**

```
[local]Redback(config-ctx)#l2tp-peer name peer1
[local]Redback(config-l2tp)#max-tunnels 2
```

1.89 mdt default-group

mdt default-group ***ip-addr***

no mdt default-group ***ip-addr***

1.89.1 Purpose

Specifies the default multicast distribution tree (MDT) group.

1.89.2 Command Mode

Interface configuration

1.89.3 Syntax Description

ip-addr	IP address of the default MDT group in the form ***A.B.C.D***.

1.89.4 Default

No default MDT group is specified.

1.89.5 Usage Guidelines

Use the **mdt default-group** command to define the default MDT group.

You must configure the **mdt default-group** command on an intercontext interface in a Virtual Private Network (VPN) context. The intercontext interface creates an intercontext circuit between the VPN context and the local context.

To configure a Protocol Independent Multicast source-specific multicast (PIM-SSM) MDT default group, use a multicast IP address in the range configured for PIM-SSM (using the **pim ssm** command in context configuration mode).

Use the **no** form of this command to disable the default MDT group.

1.89.6 Examples

The following example shows how to specify the default MDT group, **239.1.1.1**, on a point-to-point intercontext interface, **to-local**, in a VPN context, **VPN1**:

```
[local]Redback(config)#context VPN1 vpn-rd 101:202
[local]Redback(config-ctx)#interface to-local intercontext p2p 2
[local]Redback(config-if)#mdt default-group 239.1.1.1
```

The following example shows how to configure the MDT default group for PIM-SSM. The PIM-SSM address range of addresses is set to the default range, 232.0.0.0/8. The MDT default group is specified within the multicast VPN context **mvpn** with the route distinguisher **1:1**. In this context, a point-to-point intercontext interface **test-if** is defined for interfacing to the default MDT group. This interface is assigned intercontext group number **1** and IP address

10.10.10.1/32. The MDT default group is then specified with IP address **232.1.1.1**.

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#pim ssm default
[local]Redback(config-ctx)#exit
[local]Redback(config)#context test-mvpn vpn-rd 1:1
[local]Redback(config-ctx)#interface test-if intercontext p2p 1
[local]Redback(config-if)#ip address 10.10.10.1/32
[local]Redback(config-if)#mdt default-group 232.1.1.1
```

1.90 mdt encapsulation

mdt encapsulation {**gre** | **ip**}

no mdt encapsulation {**gre** | **ip**}

1.90.1 Purpose

Specifies the multicast domain tree (MDT) encapsulation type.

1.90.2 Command Mode

Interface configuration

1.90.3 Syntax Description

gre	Uses the Generic Routing Encapsulation (GRE) encapsulation type.
ip	Uses the IP-in-IP encapsulation type.

1.90.4 Default

No MDT encapsulation type is specified.

1.90.5 Usage Guidelines

Use the **mdt encapsulation** command to specify the MDT encapsulation type.

You must configure this command on a loopback interface in the local context. The loopback interface is used to source multicast packets on the MDT.

Note: The Protocol Independent Multicast Sparse-Mode (PIM-SM) explicit join mechanism is optimal only for sparsely populated groups.

Use the **no** form of this command to remove the MDT encapsulation type.

1.90.6 Examples

The following example sets the MDT encapsulation type on the point-to-point intercontext interface **to-vpn1** (with intercontext group number **1**) to GRE.

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface to-vpn1 intercontext p2p 1
[local]Redback(config-if)#mdt encapsulation gre
```

The following example shows how to specify the MDT encapsulation type for a PIM-SM configuration. The loopback interface **loop0** is configured with IP address **192.168.128.251/32**. PIM-SM is enabled in passive mode, and the MDT encapsulation is set to GRE:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface loop0 loopback
[local]Redback(config-if)#ip address 192.168.128.251/32
[local]Redback(config-if)#pim sparse-mode passive
[local]Redback(config-if)#mdt encapsulation gre
```

1.91 medium (fast-ethernet)

medium {**auto** | **speed** *speed* **duplex** *mode*}

{**no** | **default**} **medium**

1.91.1 Purpose

Specifies the port speed and duplex mode for all Fast Ethernet (FE) ports on this Fast Ethernet-Gigabit Ethernet (FE-GE) traffic card.

1.91.2 Command Mode

Card configuration

1.91.3 Syntax Description

auto	Specifies that the ports on this card automatically detect the speed and duplex mode of the segments to which they are connected; this setting is recommended and is the default for FE ports.
speed *speed*	FE port speed, according to one of the following keywords: • **10**—10 Mbps • **100**—100 Mbps
duplex *mode*	Port duplex mode, according to one of the following keywords: • **half**—Half-duplex mode • **full**—Full-duplex mode

1.91.4 Default

FE ports automatically sense the speed in full-duplex mode.

1.91.5 Usage Guidelines

Use the **medium** command to specify the speed and duplex mode for all FE ports on this FE-GE traffic card. Use the **speed** and **duplex** keywords to force the ports to use the specified speed and duplex mode.

Note: This command does not apply to the GE ports on this FE-GE traffic card.

Note: The FE ports do not come up if the medium speed or the duplex mode is configured incorrectly.

You can override the speed and mode settings for individual FE ports by using this command in port configuration mode.

Use the **no** or **default** form of this command to restore the default speed and duplex mode.

1.91.6 Examples

The following example shows how to specify the speed at `100 Mbps and full-duplex mode for all FE ports on the FE-GE traffic card in slot 4:`

```
[local]Redback(config)#card fege-60-2-port 4
[local]Redback(config-port)#medium speed 100 duplex full
```

1.92 medium (ethernet)

medium {**auto** | **speed** ***speed*** **duplex** ***mode***}

{**no** | **default**} **medium**

1.92.1 Purpose

Specifies the Ethernet port speed and duplex mode.

1.92.2 Command Mode

Port configuration

1.92.3 Syntax Description

auto	Specifies that the port automatically detects the speed and duplex mode of the segment to which it is connected; this setting is recommended and is the default.
speed ***speed***	Ethernet port speed, according to one of the following keywords: • **10**—10 Mbps • **100**—100 Mbps
duplex ***mode***	Port duplex mode, according to one of the following keywords: • **half**—half-duplex mode • **full**—full-duplex mode

1.92.4 Default

10/100 Ethernet ports auto-sense the speed in full-duplex mode.

1.92.5 Usage Guidelines

Use the **medium** command to specify the Ethernet port speed and duplex mode. Use the **speed** and **duplex** keywords to force an Ethernet port to use the specified speed and duplex mode.

Note:

- This command applies to 10/100 ports on Fast Ethernet-Gigabit Ethernet (FE-GE) traffic cards.
- This command does not apply to ports on Gigabit Ethernet traffic cards.
- The port does not come up if the medium speed or the duplex mode is configured incorrectly.
- If you have specified a speed and mode for all FE ports on an FE-GE traffic card (using this command in card configuration mode), entering this command in port configuration mode overrides those settings for this port only.

Use the **no** or **default** form of this command to restore the default speed and duplex mode.

1.92.6 Examples

The following example shows how to specify the speed at **10** Mbps and **full**-duplex mode for port **1** in slot **4:**

```
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#medium speed 10 duplex full
```

1.93 medium-type

medium-type {**copper** | **optical-fiber**}

no medium-type {**copper** | **optical-fiber**}

1.93.1 Purpose

Specifies the physical interface for this native port on the SmartEdge 100 router.

1.93.2 Command Mode

Port configuration

1.93.3 Syntax Description

copper	Specifies the 1000Base-T interface.
optical-fiber	Specifies the 1000Base-FX interface; this is the default.

1.93.4 Default

1000Base-FX interface

1.93.5 Usage Guidelines

Use the **medium-type** command to specify the physical connection for this SmartEdge 100 native port. Each native port supports either a copper or an optical fiber connection. To configure the port, you must specify the type of connector to which the cable is attached; a mismatch causes the port to be inoperable. For example, if the cable is attached to the copper connector and you enter this command with the **optical-fiber** keyword, the port cannot transmit or receive traffic.

If you specify the **copper** keyword, you can also specify the port speed and duplex mode by using the **duplex** and **speed** commands (in port configuration mode).

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

1.93.6 Examples

The following example shows how to configure the physical interface for native port **2/1** as **optical-fiber:**

```
[local]se100-01(config)#port ethernet 2/1
[local]se100-01(config-port)#medium-type optical-fiber
```

1.94 mep-local

mep-local *mep-id* {*circuit* | *link-group*} [*vlan* | *transport*] [*direction*]

{**no** | **default**} **mep-local** *mep-id* {*circuit* | *link-group*} [*vlan* | *transport*] [*direction*]

1.94.1 Purpose and Usage Guidelines

Binds an Ethernet link group, circuit, transport circuit, or port to a local maintenance association endpoint (MEP) in the current maintenance association (MA).

- When bound to a transport circuit, a MEP or MIP is matched to the circuit that best matches the VLANs configured under it.

  When a VLAN range is configured on a transport circuit on which an MP (MEP or MIP) is already configured, the existing MP configuration on that circuit is deleted and remapped to the new transport circuit. CCMs are sent out on the new circuit instead of the previously associated transport circuit.

  When multiple MPs qualify for the same transport circuit, the MP with the lowest starting VLAN-id valid within the range of VLANs supported under the transport circuit is mapped to the circuit regardless of whether or not the transport circuit is already associated to an MP at the same level. If the transport circuit was associated with another MP, the new MP (with the lowest starting VLAN-id) replaces the old one and the old MP will be best matched to another transport circuit if present on the SmartEdge router .

  On deletion of a best matched circuit on which MP is configured, the MP will be remapped to the next transport circuit present in the box which supports the VLANs configured under the MP. Similarly on deletion of an MP, the circuit associated with the MP is best matched to any other MP which has the lowest starting VLAN-id of the VLANs supported by the transport circuit.

- Use the following criteria to determine whether to classify a local MEP as **`up`** or **`down:`**

  – A down MEP processes CFM PDUs received from the wire side and drops CFM PDUs received from the relay side.

  – An up MEP drops CFM PDUs received from the wire side and processes CFM PDUs received from the relay side.

- Use the **`mep-remotelist`** command to configure remote MEPs in the MA.

1.94.2 Command Mode

MA configuration

1.94.3 Syntax Description

mep-id	One of the MEPIDs defined by the **mep-remotelist** command. MEP IDs must be an integer in the range of 1 to 65535.
circuit	***slot/port*** **[*:ch:sub*]** Specifies the Ethernet circuit or port, to which the MEP binds.
link-group	**lg {*link-group-name* | id *link-group-id*}** Specifies the link group to which the MEP binds.
vlan	**vlan-id *vlan-id*** Specifies the Virtual LAN (VLAN) to which the MEP binds. The ***vlan-id*** argument is one of the following constructs: • ***pvc-vlan-id*** — VLAN tag value of a PVC (outer VLAN tag). • ***tunl-vlan-id:pvc-vlan-id*** — VLAN tag value for the 802.1Q 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. The ***vlan-id*** argument must also specify a PVC configured in the link group or port specified by the ***link-group*** or ***circuit*** arguments.

transport	**transport {*range* | any}** Specifies the transport-enabled VLAN to which the MEP binds. The ***range*** argument must also specify a transport-enabled PVC or PVCs configured in the link group or port to which the MEP is bound, and is one of the following constructs: • ***pvc-vlan-id***—VLAN tag value of a PVC (outer VLAN tag). • **any**—The entire range PVCs (outer VLAN tags). • ***pvc-vlan-id-first - pvc-vlan-id-last***—A range of PVCs (outer VLAN tags). • ***tunl-vlan-id:pvc-vlan-id***—VLAN tag value for the 802.1Q tunnel followed by the VLAN tag value for the PVC within the tunnel. • ***tunl-vlan-id:pvc-vlan-id-first - pvc-vlan-id -last***—A range of PVCs (inner VLAN tags) within an 802.1Q tunnel (outer VLAN tag). • ***tunl-vlan-id*:any**—All PVCs within the specified 802.1Q tunnel (outer VLAN tag).
direction	**direction up**—Specifies that the local MEP resides in a bridge that transmits CFM messages towards, and receives them from, the direction of the bridge relay. In other words for the current MA, incoming CFM messages pass through the bridge to reach the MEP bridge interface, and outgoing CFM pass through the bridge to reach other maintenance points in the MA. **direction down**—Specifies that the local MEP resides in a bridge that transmits CFM messages towards, and receives them from, the direction of the physical medium. In other words for the current MA, incoming and outgoing CFM messages reach the MEP bridge interface directly through the physical media and do not pass through the bridge.

1.94.4 Default

The default direction is up.

1.94.5 Examples

In the following example, MEPIDs **31** is associated with the Ethernet port 1 in slot 5 (**5/1**). This MEP is a local MEP in the **sbc.com** MA:

```
[local]Redback(config)#ethernet-cfm instance-1
[local]Redback(config-ether-cfm)#level 4
[local]Redback(config-ether-cfm)#domain-name sbc.com
[local]Redback(config-ether-cfm)#disable-linktrace
[local]Redback(config-ether-cfm)#group-mac 01:01:01:01:01:01
[local]Redback(config-ether-cfm)#maintenance-association bayarea
[local]Redback(config-ether-cfm-ma)#ccm
[local]Redback(config-ether-cfm-ma-ccm)#frame-loss 10
[local]Redback(config-ether-cfm-ma-ccm)#std-interval 10ms
[local]Redback(config-ether-cfm-ma-ccm)#exit
[local]Redback(config-ether-cfm-ma)#mep-local 31 4/2 direction up
```

1.95 mep-remotelist

mep-remotelist *id-first* [**through** *id-last*]

{**no** | **default**} *id-first* [**through** *id-last*]

1.95.1 Purpose

Creates a sequence of IDs to be used to identify the remote maintenance association endpoints (MEPs) belonging to the current maintenance association (MA).

1.95.2 Command Mode

MA configuration

1.95.3 Syntax Description

id-first	The first maintenance association endpoint ID (MEPID) assigned to the remote MEPs in the MA. All maintenance points in the MD must be integers in the range of 1 to 8191 and must be unique within the MA.
through *id-last*	Specifies the last MEPID assigned to the remote MEPs in the MA.

1.95.4 Default

No MEPIDs.

1.95.5 Usage Guidelines

Use this command to create a sequence MEIDs to be used to identify the remote MEPs belonging to the current MA. MEP IDs must be an integer in the range of 1 to 65535.

All local MEPs in the MA should be bound to Ethernet ports or interfaces to Ethernet circuits using the **`mep-local`** command.

The following illustration shows the role that MEPs play in transmitting and terminating continuity check messages (CCMs). Although the drawing shows only one MEP transmitting CCM PDUs in the MA, all MEPs do this at regular intervals. See the **`ccm`** command for further information:

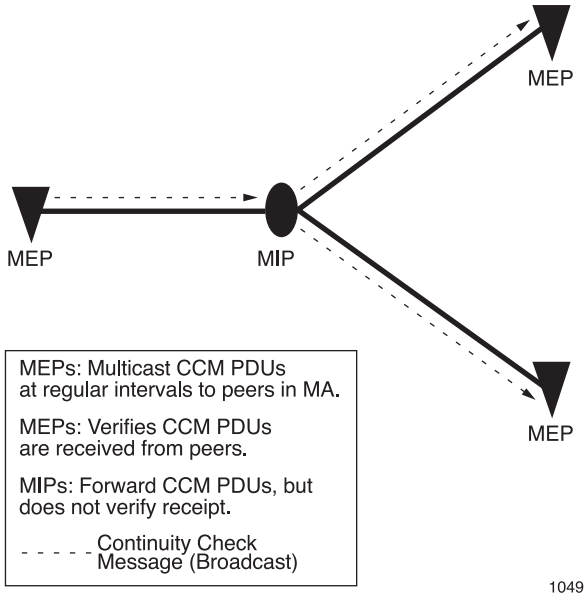


Figure 2 MEP Roles

1.95.6 Examples

The following example shows how to use this command to create the remote MEPIDs **301**, **302**, and **303 bayarea** MA:

```
[local]Redback(config)#ethernet-cfm instance-1
[local]Redback(config-ether-cfm)#level 4
[local]Redback(config-ether-cfm)#domain-name sbc.com
[local]Redback(config-ether-cfm)#disable-linktrace
[local]Redback(config-ether-cfm)#group-mac 01:01:01:01:01:01
[local]Redback(config-ether-cfm)#maintenance-association bayarea
[local]Redback(config-ether-cfm-ma)#ccm
[local]Redback(config-ether-cfm-ma-ccm)#frame-loss 10
[local]Redback(config-ether-cfm-ma-ccm)#std-interval 10ms
[local]Redback(config-ether-cfm-ma-ccm)#exit
[local]Redback(config-ether-cfm-ma)#mep-local 31 4/2 direction up
[local]Redback(config-ether-cfm-ma)#mep-remotelist 301 through 303
```

1.96 mesh-group

mesh-group ***group-name peer-addr***

no mesh-group ***group-name peer-addr***

1.96.1 Purpose

Configures a Multicast Source Discovery Protocol (MSDP) peer to be a member of a mesh group.

1.96.2 Command Mode

MSDP router configuration

1.96.3 Syntax Description

group-name	Mesh group name.
peer-addr	IP address of the peer to be added to the mesh group.

1.96.4 Default

None

1.96.5 Usage Guidelines

Use the **mesh-group** command to configure an MSDP peer to be a member of a mesh group.

Use the **no** form of this command to remove an MSDP peer's membership from a mesh group.

1.96.6 Examples

The following example configures the MSDP peer with the IP address, **10.10.10.1**, to be a member of the mesh group, **foo:**

```
[local]Redback(config-ctx)#router msdp
[local]Redback(config-msdp)#mesh-group foo 10.10.10.1
```

1.97 message

message ***string***

no message

1.97.1 Purpose

Configures a message to display to the subscriber while the subscriber HTTP session is redirected to a preconfigured URL.

1.97.2 Command Mode

HTTP redirect profile configuration

1.97.3 Syntax Description

string	Optional. Printable ASCII characters string with up to 255 bytes and enclosed in quotation marks (" "). Specifies the message to display while redirecting the subscriber HTTP session to a preconfigured URL.

1.97.4 Default

A generic hardcoded message is used when redirecting the HTTP traffic.

1.97.5 Usage Guidelines

Use the **message** command to configure a message to display to the subscriber while the subscriber HTTP session is redirected to a preconfigured URL.

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

1.97.6 Examples

The following example shows how to configure an HTTP redirect message for the HTTP-redirect profile `ericsson:`

```
[local]Redback(config)#http-redirect profile ericsson
[local]Redback(config-hr-profile)#message "Please wait while you are redirected to the portal server. "
```

1.98 message-reordering

message-reordering message-queue ***queue-size***

{**no** | **default**} **message-reordering**

1.98.1 Purpose

Queues incoming out-of-order L2TP packets until the expected next sequence packet is received.

1.98.2 Command Mode

L2TP-peer configuration

1.98.3 Syntax Description

message-queue ***queue-size***	Whichever is smaller, ***queue-size*** argument or this command, or the L2TP received window, specifies the maximum number of L2TP packets that can be queued.

1.98.4 Default

Incoming out-of-order packets are dropped.

1.98.5 Usage Guidelines

Use the **message-reordering** command to queue incoming out-of-order L2TP packets until the expected next sequence packet is received. When the expected next sequence is received, the packets in the queue are forwarded and the queue is emptied.

The maximum value allowed for ***queue-size*** is 32. The effective queue size is the value specified by this command or the value specified for the received-window (**tunnel-window** command), whichever is smaller.

1.98.6 Examples

The following example shows the configuration of a context for LDP router operation with equal-cost multipath (ECMP). Since ECMP can cause L2TP packets to be received out-of-order, the L2TP-peer of a SmartEdge router is configured for message-reordering:

```
[local]lac1.net#config
[local]lac1.net(config)#context local
[local]lac1.net(config-ctx)#router ldp
[local]lac1.net(config-ldp)#ecmp-transit
!
[local]Redback#config
[local]Redback(config)#context local
[local]Redback(config-ctx)#l2tp-peer name lac1.net media udp-ip remote ip 10.5.5.5
[local]Redback(config-l2tp)#max-tunnels 2
[local]Redback(config-l2tp)#message-reodering message-queue 16
```

1.99 metric

metric ***metric*** [**level-1** | **level-2**]

{**no** | **default**} **metric**

1.99.1 Purpose

Configures the IS-IS interface metric for a specific address family.

1.99.2 Command Mode

IS-IS address family configuration

1.99.3 Syntax Description

metric	Metric used for calculating the Shortest Path First (SPF). The range of values is 1 to 63 for narrow-style metrics, and 0 to 16,777,215 for wide-style metrics; the default value is 10.
level-1	Optional. Configures the metric for IS-IS level 1 routing independently.
level-2	Optional. Configures the metric for IS-IS level 2 routing independently.

1.99.4 Default

The default metric value is 10.

1.99.5 Usage Guidelines

Use the **metric** command to configure the IS-IS interface metric for a specific address family.

Metric values are determined by circuit distance, load-sharing requirements, and other traffic engineering factors.

Use the **no** form of this command to remove the address family-specific IS-IS interface metric configuration. Use the **default** form of this command to return the metric configuration to the default value of 10.

1.99.6 Examples

This example shows how to assign the following IS-IS metrics to the **fa4/1** interface:

- For the IPv4 unicast address family, a metric value of **1234** for **level 2** routing.
- For the IPv6 unicast address family, a metric value of 123456 for all levels of routing.

```
[local]Redback(config-ctx)#router isis ip-backbone
[local]Redback(config-isis)#interface fa4/1
[local]Redback(config-isis-if)#address-family ipv4 unicast
[local]Redback(config-isis-if-af)#metric 1234 level-2
[local]Redback(config-isis-if-af)#exit
Transaction Committed
[local]Redback(config-isis-if)#address-family ipv6 unicast
[local]Redback(config-isis-if-af)#metric 123456
[local]Redback(config-isis-if-af)#exit
Transaction Committed
```

1.100 metric-style

metric-style [**narrow** | **transition** | **wide**] [**level-1** | **level-2**]

no metric-style

1.100.1 Purpose

Allows the advertisement of short or wide metrics and migration of existing traditional Intermediate System-to-Intermediate-System (IS-IS) networks into the new scheme for each level.

1.100.2 Command Mode

IS-IS router configuration

1.100.3 Syntax Description

narrow	Optional. Allows advertisement of metrics with values in the range from 0 to 63. If enabled on a level, no device operating in wide mode can be present in the same area. All metrics from redistributed and calculated routing information is clipped to a maximum of 63.
transition	Optional. Allows advertisement of metrics with values in the range from 0 to 63. Higher metrics can be specified and redistributed, but are only used when the metric style is changed to wide mode. Devices with narrow or wide mode enabled can be present in the same area.
wide	Optional. Allows advertisement of metrics longer than 63. If enabled on a level, no device operating in narrow mode can be present in the same area.
level-1	Optional. Sets the metric style independently for level 1. If wide metric style is enabled, routes can be advertised from the level 2 area into the level 1 area, and level 1 devices can select the best level 2 device for each destination. If narrow mode is enabled, level 1 devices must forward traffic to the closest level 2 device.
level-2	Optional. Sets the metric style independently for level 2.

1.100.4 Default

For IS-IS levels 1 and 2, the SmartEdge router uses the wide metric for IP version 4 (IPv4) and IP version 6 (IPv6) routing.

1.100.5 Usage Guidelines

Use the **metric-style** command to allow the advertisement of short or wide metrics and migration of existing traditional IS-IS networks into the new scheme for each level. Implementation of this command adheres to the IETF draft-ietf-isis-traffic-02.txt document, ***IS-IS Extensions for Traffic Engineering***.

You can enable the wide-style metric when traffic engineering capabilities or metrics longer than 63 are preferred. Other than any devices in transition mode, all devices in the area must apply the same metric style, otherwise the IP topology becomes partitioned.

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

1.100.6 Examples

The following example shows how to set the metric style to **transition** for **level-1** routing:

```
[local]Redback(config-ctx)#router isis isis01
[local]Redback(config-isis)#metric-style transition level-1
```

1.101 mic

mic ***mic-num*** {**atm-oc3-2-port** | **fe-12-port** | **ge-2-port**}

no mic ***mic-num*** {**atm-oc3-2-port** | **fe-12-port** | **ge-2-port**}

1.101.1 Purpose

Specifies the media interface card (MIC) type for the specified slot before the MIC is inserted into the SmartEdge 100 chassis and accesses MIC configuration mode.

1.101.2 Command Mode

Card configuration

1.101.3 Syntax Description

mic-num	MIC to be configured. The range of values is 1 to 2. MIC 1 is associated with ports 2/3 to 2/14. MIC 2 is associated with ports 2/15 to 2/26.
atm-oc3-2-port	Configures the specified MIC as an Asynchronous Transfer Mode (ATM) OC-3c/STM-1c MIC, with a maximum of 2 ports.
fe-12-port	Configures the specified MIC as a Fast Ethernet (FE) MIC, with a maximum of 12 ports.
ge-2-port	Configures the specified MIC as a Gigabit Ethernet (GE) MIC, with a maximum of 2 ports.

1.101.4 Default

No MICs are configured.

1.101.5 Usage Guidelines

Use the **mic** command to specify the MIC type for the specified slot before the MIC is inserted into the SmartEdge 100 chassis. You cannot configure any ports on a MIC that is not yet physically present in the router until you enter this command.

If you have already installed a MIC in the SmartEdge 100 chassis, you can configure its ports without first entering this command. The SmartEdge OS automatically detects the MIC when you enter the **port ethernet** or the **port atm** command (in global configuration mode).

Note: The native ports on the SmartEdge 100 router (2/1 and 2/2) are not associated with a MIC; you configure them without entering this command.

The MIC type that you specify with this command must match the type of the installed MIC. A mismatch between the installed type and the specified keyword causes the system to display the **mic mismatch** error message.

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

1.101.6 Examples

The following example shows how to configure MIC number 1 as an FE MIC:

```
[local]Redback(config-card)#mic 1 fe-12-port
```

The following example shows how to configure MIC number 2 as a GE MIC:

```
[local]Redback(config-card)#mic 2 ge-2-port
```

1.102 minimum-bandwidth

minimum-bandwidth *number* [**kbps** | **mbps** | **gbps**]

no bandwidth

1.102.1 Purpose

Configures the minimum bandwidth requirement for a label-switched path (LSP) to be applied as a constraint during Constrained Shortest Path First (CSPF) calculation.

1.102.2 Command Mode

Constraint configuration

1.102.3 Syntax Description

number	Minimum bandwidth for an LSP. If no unit is specified, the value is in bytes per second. The range of values is 1 to 4294967295.
kbps	Optional. Specifies that the minimum bandwidth requirement for an LSP is in kilobytes per second.
mbps	Optional. Specifies that the minimum bandwidth requirement for an LSP is in megabytes per second.
gbps	Optional. Specifies that the minimum bandwidth requirement for an LSP is in gigabytes per second.

1.102.4 Default

An LSP has no minimum bandwidth requirement.

1.102.5 Usage Guidelines

Use the **minimum-bandwidth** command to configure the minimum bandwidth requirement for an LSP to be applied as a constraint during CSPF calculation.

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

1.102.6 Examples

The following example shows how to configure the minimum interface bandwidth required for an LSP to `3 megabytes per second:`

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#constraint constraint
[local]Redback(config-rsvp-constr)#minimum-bandwidth 3 mbps
```

1.103 minimum-links

minimum-links ***min-active***

{**no** | **default**} **minimum-links** [***min-active***]

1.103.1 Purpose

Specifies the minimum number of active links that a link group must have for that link group to be in an up state.

1.103.2 Command Mode

Link group configuration

1.103.3 Syntax Description

min-active	Minimum number of active links that a link group must have for the link group to be in an up state. The range of values is 1 to 8 for an access link group and 1 to 255 for any other type of link group. The default value is 1 for any type of link group.

1.103.4 Default

The minimum number of active links is one for an access link group and eight for any other type of link group.

1.103.5 Usage Guidelines

Use the **minimum-links** command to specify the minimum number of active links that a link group must have for that link group to be in an up state.

You cannot specify a value for the ***min-active*** argument that is greater than the value you have specified for the ***max-active*** argument with the **maximum-links** command (in link group configuration mode).

If the number of active links falls below the number specified by the ***min-active*** argument, the system considers the link group to be down. One active link is needed to keep the link group in an up state.

An active (or working) link is defined as having an associated port, channel, or PVC in an up state. This command is typically used to specify when a link group is no longer considered viable after member links shut down. Whenever fewer than the specified number of links are working, the link group itself reverts to the down state and no longer forwards any traffic, even on the links that are working. As a result, the link group no longer appears in the routing table.

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

1.103.6 Examples

The following example shows how to configure the **lg-ether** link group with a minimum of **2** working links:

```
[local]Redback(config)#link-group lg-ether ether
[local]Redback(config-link-group)#minimum-links 2
```

1.104 minimum receive-interval

minimum receive-interval *interval*

{**no** | **default**} **minimum receive-interval**

1.104.1 Purpose

Specifies the minimum required interval, in milliseconds, between received Bidirectional Forwarding Detection (BFD) control packets that the system is capable of supporting.

1.104.2 Command Mode

- BFD interface configuration
- BFD neighbor configuration

1.104.3 Syntax Description

interval	Minimum required receive interval value. The range of values, in milliseconds, is 10 to 60000; the default value is 1000.

1.104.4 Default

The default minimum receive interval is 1,000 ms (1 second).

1.104.5 Usage Guidelines

Use the **minimum receive-interval** command to specify the minimum required interval, in milliseconds, between received BFD control packets that the system is capable of supporting.

Use the **no** or **default** form of this command to return the minimum required receive interval to 1,000 ms.

1.104.6 Examples

The following example shows how to set the minimum required receive interval on the interface, **to_foo**, to **30** ms:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bfd
[local]Redback(config-bfd)#interface to_foo
[local]Redback(config-bfd-if)#minimum receive-interval 30
[local]Redback(config-bfd-if)#
```

1.105 minimum transmit-interval

minimum transmit-interval *interval*

{**no** | **default**} **minimum transmit-interval**

1.105.1 Purpose

Specifies the minimum desired transmit interval, in milliseconds, used by the local system when transmitting Bidirectional Forwarding Detection (BFD) control packets.

1.105.2 Command Mode

- BFD interface configuration
- BFD neighbor configuration

1.105.3 Syntax Description

interval	Minimum desired transmit interval value. The range of values, in milliseconds, is 10 to 60,000; the default value is 1,000.

1.105.4 Default

The default minimum desired transmit interval is 1,000 ms (1 second).

1.105.5 Usage Guidelines

Use the **minimum transmit-interval** command to specify the minimum desired transmit interval, in milliseconds, used by the local system when transmitting BFD control packets.

Use the **no** or **default** form of this command to return the minimum desired transmit interval to 1,000 ms.

1.105.6 Examples

The following example shows how to set the minimum desired transmit interval on the interface, **to_foo**, to **30** ms:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bfd
[local]Redback(config-bfd)#interface to_foo
[local]Redback(config-bfd-if)#minimum transmit-interval 30
[local]Redback(config-bfd-if)#
```

1.106 min-wait

min-wait ***interval***

{**no** | **default**} **min-wait** ***interval***

1.106.1 Purpose

Configures the interval, in seconds, to wait before forwarding requests to the Dynamic Host Configuration Protocol (DHCP) server.

1.106.2 Command Mode

DHCP relay server configuration

1.106.3 Syntax Description

interval	Wait interval in seconds. The range of values is 0 to 60.

1.106.4 Default

The default wait interval is 0 seconds.

1.106.5 Usage Guidelines

Use the **min-wait** command to configure the interval, in seconds, to wait before forwarding requests to the DHCP server.

Use the **no** or **default** form of this command to return to the default DHCP relay server minimum wait interval of 0 seconds.

1.106.6 Examples

The following example shows how to configure a wait interval of **45** seconds for DHCP relay server, **10.30.40.50:**

```
[local]Redback(config-ctx)#dhcp relay server 10.30.40.50
[local]Redback(config-dhcp-relay)#min-wait 45
[local]Redback(config-dhcp-relay)#
```

1.107 mip

mip ***mip-id*** {***circuit*** | ***link-group***} [***vlan*** | ***transport***]

{**no** | **default**} **mip** ***mip-id*** {***circuit*** | ***link-group***} [***vlan*** | ***transport***]

1.107.1 Purpose and Usage Guidelines

Creates a maintenance association intermediate point (MIP) bound to a specified Ethernet link group, circuit, transport circuit, or port in the current maintenance domain (MD).

You create a MIP for the following reasons:

- To make the circuit interface or port visible to loopback tests; that is, make the MIP respond to loopback message PDUs (LBM PDUs).
- Optionally, to make the circuit interface or port visible to link-trace reports; that is, make the MIP respond to link-trace message PDUs (LTM PDUs).

Note: When bound to a transport circuit, a MEP or MIP is matched to the circuit that best matches the VLANs configured under it.

When a VLAN range is configured on a transport circuit on which an MP (MEP or MIP) is already configured, the existing MP configuration on that circuit is deleted and remapped to the new transport circuit. CCMs are sent out on the new circuit instead of the previously associated transport circuit.

When multiple MPs qualify for the same transport circuit, the MP with the lowest starting VLAN-ID valid within the range of VLANs supported under the transport circuit is mapped to the circuit regardless of whether or not the transport circuit is already associated to an MP at the same level. If the transport circuit was associated with another MP, the new MP (with the lowest starting VLAN-ID) replaces the old one, and the old MP is best matched to another transport circuit if present on the SmartEdge router .

On deletion of a best matched circuit on which MP is configured, the MP is remapped to the next transport circuit that supports the VLANs configured under the MP. Similarly, on deletion of an MP, the circuit associated with the MP is best matched to any other MP which has the lowest starting VLAN-ID of the VLANs supported by the transport circuit.

1.107.2 Command Mode

CFM configuration

1.107.3 Syntax Description

mip-id	The ID assigned to the MIP in the MD. An integer in the range of 1 to 8191 and must be unique within the MD.
circuit	***slot/port*** **[***:ch:sub***]** Specifies the Ethernet circuit or port, to which the MIP binds.
link-group	**lg {***link-group-name* | **id** *link-group-id***}** Specifies the link group to which the MIP binds.

vlan	**vlan-id** ***vlan-id*** Specifies the Virtual LAN (VLAN) to which the MIP binds. The ***vlan-id*** argument is one of the following constructs: • ***pvc-vlan-id*** — VLAN tag value of a PVC (outer VLAN tag). • ***tunl-vlan-id:pvc-vlan-id*** — VLAN tag value for the 802.1Q 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. The ***vlan-id*** argument must also specify a PVC configured in the link group or port specified by the ***link-group*** or ***circuit*** arguments.
transport	**transport** {***range*** | **any**} Specifies the transport-enabled VLAN to which the MIP binds. The ***range*** argument must also specify a transport-enabled PVC or PVCs configured in the link group or port to which the MIP is bound. The possible values for the ***range*** argument follow: • ***pvc-vlan-id*** — VLAN tag value of a PVC (outer VLAN tag). • **any** — The entire range PVCs (outer VLAN tags). • ***pvc-vlan-id-first - pvc-vlan-id-last*** — A range of PVCs (outer VLAN tags). • ***tunl-vlan-id:pvc-vlan-id*** — VLAN tag value for the 802.1Q tunnel followed by the VLAN tag value for the PVC within the tunnel. • ***tunl-vlan-id:pvc-vlan-id-first - pvc-vlan-id-last*** — A range of PVCs (inner VLAN tags) within an 802.1Q tunnel (outer VLAN tag). • ***tunl-vlan-id*****:any** — All PVCs within the specified 802.1Q tunnel (outer VLAN tag).

1.107.4 Default

None

1.107.5 Examples

In the following example, the **mip** command binds a MIP (in the **redback.com** MD) to the physical Ethernet port at slot 4/port 2:

```
[local]Redback(config)#ethernet-cfm instance-1
[local]Redback(config-ether-cfm)#level 4
[local]Redback(config-ether-cfm)#domain-name sbc.com
[local]Redback(config-ether-cfm)#disable-linktrace
[local]Redback(config-ether-cfm)#group-mac 01:01:01:01:01:01
[local]Redback(config-ether-cfm)#maintenance-association bayarea
[local]Redback(config-ether-cfm-ma)#ccm
[local]Redback(config-ether-cfm-ma-ccm)#frame-loss 10
[local]Redback(config-ether-cfm-ma-ccm)#std-interval 10ms
[local]Redback(config-ether-cfm-ma-ccm)#exit
[local]Redback(config-ether-cfm-ma)#mep-local 31 4/2 direction up
[local]Redback(config-ether-cfm-ma)#mep-remotelist 301 through 303
!
[local]Redback(config)#ethernet-cfm instance-2
[local]Redback(config-ether-cfm)#level 5
[local]Redback(config-ether-cfm)#domain-name redback.com
[local]Redback(config-ether-cfm)#mip 31 4/2
```

1.108 mirror destination

mirror destination *dest-name* {**all** | **dropped** | **forwarded**} [**ip-datagrams** | **l2-frames**] [**header-only**] [**sampling** *interval*]

no mirror destination

1.108.1 Purpose

Enables the mirroring of packets to an output destination.

1.108.2 Command Mode

- Forward policy configuration
- Policy group class configuration

1.108.3 Syntax Description

dest-name	Output destination name for mirrored traffic.
all	For Layer 2 Circuits: Ignored. All traffic is mirrored when **forward policy dest in** is applied. Only the forwarded traffic is mirrored when **forward policy dest out** is applied. For Layer 3 Circuits: Mirrors all traffic.
dropped	For Layer 2 Circuits: Unsupported and rejected by the command line interface. For Layer 3 Circuits: Mirrors only dropped packets. Packets dropped by IP checksums or by access control lists (ACLs) are not mirrored.
forwarded	For Layer 2 Circuits: Unsupported and rejected by the command line interface when **forward policy dest in** is applied. Only the forwarded traffic is mirrored when **forward policy dest out** is applied. For Layer 3 Circuits: Mirrors only forwarded packets.
ip-datagrams	For Layer 2 Circuits: Optional (this is the default). Mirrors only IP packets. Mirrors IP datagrams of IP packets and omits the Layer 2 headers. Only IP datagram type data is included. If the mirror destination is a GRE tunnel, **ip-datagrams** must be selected. For Layer 3 Circuits: Optional (this is the default). Mirrors only IP packets. Mirrors IP datagrams of IP packets and omits the Layer 2 headers. Only IP datagram type data is included.
l2-frames	For Layer 2 Circuits: Optional. Mirrors both IP and non-IP packets, including Layer 2 frame data with the MAC address and ethertype from the Layer 2 headers, from the packets on the Layer 2 attachment circuit specified in the configuration. All packets are mirrored when **forward policy dest in** is applied. Only the forwarded packets are mirrored when **forward policy dest out** is applied. If **l2-frames** is selected, the mirror destination must support Layer 2 mirroring. PPA2-based Ethernet cards support Layer 2 mirroring. For Layer 3 Circuits: Unsupported and ignored.

header-only	For Layer 2 Circuits: Unsupported and ignored. For Layer 3 Circuits: Optional. Mirrors only packet IP headers.
sampling *interval*	For Layer 2 Circuits: Optional. Configures a sampling interval. If this parameter is specified, traffic is mirrored on a periodic rather than continuous basis. The sampling interval is specified in milliseconds and determines the minimum amount of time that must pass after a packet is mirrored before a subsequent packet on the circuit is mirrored rather than ignored. For Layer 3 Circuits: Optional. Configures a sampling interval. If this parameter is specified, traffic is mirrored on a periodic rather than continuous basis. The sampling interval is specified in milliseconds and determines the minimum amount of time that must pass after a packet is mirrored before a subsequent packet on the circuit is mirrored rather than ignored.

1.108.4 Default

Packets are not mirrored.

1.108.5 Usage Guidelines

Use the **mirror destination** command to enable the mirroring of packets to an output destination. The destination name is the one that you specified for the circuit using the **forward output** command (in ATM PVC, Frame Relay PVC, tunnel, or port configuration mode). This command is used to capture traffic for troubleshooting and/or security.

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

Use the **no** form of this command to disable the mirroring of packets to an output destination.

Use the **l2-frames** keyword to mirror Layer 2 frame data, including MAC and PPP headers, from traffic on Layer 2 circuits (a circuit is a Layer 2 circuit if it is bound to a bridge/VPLS, XC, or L2VPN and a circuit is a Layer 3 circuit if it is bound to an IP interface).

When **l2-frames** is configured, the MAC and Ethertype data are preserved in the mirrored data; however, the original VLAN tags are overwritten by the mirror destination VLAN tags. Use the MAC address, session ID, or IP addresses to

identify mirrored traffic streams because the original VLAN tags from the data are not preserved in the mirrored data.

The **show configuration** and **show configuration forward** command display `l2-frames` when **l2-frames** mirroring is configured.

The **show forward policy** *pol-name* command displays `l2-frames` when **l2-frames** mirroring is configured.

Note: Configurations that include the **mirror destination** command generated by the SmartEdge router, Release 6.1.4.2 and higher are not backward compatible with older releases (6.1.4.1 and earlier) even if **ip-datagrams** is not specified in the configuration because the default **ip-datagrams** command is automatically added to the **show configuration** output.

1.108.6 Examples

The following example shows how to configure a policy, **MirrorPolicy**, which mirrors dropped packets every 3 seconds (**3000** milliseconds) to the output destination, **DroppedTraffic:**

```
[local]Redback#config
[local]Redback(config)#forward policy MirrorPolicy
[local]Redback(config-policy-frwd)#mirror destination DroppedTraffic dropped sampling 3000
```

1.109 mkdir

mkdir *url*

1.109.1 Purpose

Creates a new directory on a local file system.

1.109.2 Command Mode

Exec (10)

1.109.3 Syntax Description

url	URL of the directory to be created.

1.109.4 Default

None

1.109.5 Usage Guidelines

Use the **mkdir** command to create a new directory on the local file system.

When specifying a directory on the local file system, the URL takes 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. If you do not specify the ***directory*** argument, the default value is the current directory. Directories can be nested. The value for the ***filename*** argument can be up to 256 characters in length.

1.109.6 Examples

The following example shows how to create a new top-level directory, **backups**, on the flash file system:

```
[local]Redback#mkdir /flash/backups
```

1.110 modify ip access-list

modify ip access-list ***acl-name*** **condition** ***cond-id*** {**permit** | **deny**}

1.110.1 Purpose

Modifies in real time the action for the specified condition referenced by statements in the IP access control list (ACL), without requiring reconfiguration of the IP ACL.

1.110.2 Command Mode

Exec

1.110.3 Syntax Description

acl-name	Name of the ACL to be modified.
condition ***cond-id***	ACL condition ID in integer or IP address format. The ID range of values is 1 to 4294967295.

permit	Applies a permit action.
deny	Applies a deny action.

1.110.4 Default

None

1.110.5 Usage Guidelines

Use the **modify ip access-list** command to modify in real time the action for the specified condition referenced by statements in the IP ACL, without requiring reconfiguration of the IP ACL.

Note: If the specified condition ID is already configured (using the **condition** command in access control list configuration mode), the **modify ip access-list** command is ignored. If a condition ID is configured using the **condition** command and the changes are saved, any condition ID that may be currently applied using the **modify ip access-list** command at runtime is immediately overwritten.

For information about the **condition** and **ip access-list** commands in context configuration mode, see the *Command List*.

1.110.6 Examples

With the following configuration, using the **modify ip access-list list_cond condition 200 deny** command changes the action of the ACL condition **200** in statement **20** in the IP ACL **list_cond** from **permit** to **deny**. However, using the **modify ip access-list list_cond condition 100 permit** command does not affect the **deny** action of the ACL condition **100** because it has already been configured:

```
[local]Redback(config-ctx)#ip access-list list_cond
[local]Redback(config-access-list)#condition 100 time-range
[local]Redback(config-acl-condition)#absolute start 2005:01:01:01:00 end 2006:01:01:01:01 permit
[local]Redback(config-acl-condition)#exit
[local]Redback(config-access-list)#seq 10 deny tcp any any eq 80 cond 100
[local]Redback(config-access-list)#seq 20 permit tcp any any eq 81 cond 200
```

1.111 modify policy access-list

modify policy access-list *acl-name* **condition** *cond-id* **class** *class-name*

1.111.1 Purpose

Modifies in real time the action for the specified condition referenced by statements in the policy access control list (ACL), without requiring reconfiguration of the policy ACL.

1.111.2 Command Mode

Exec

1.111.3 Syntax Description

acl-name	Name of the ACL to be modified.
condition ***cond-id***	ACL condition ID in integer or IP address format. The ID range of values is 1 to 4294967295.
class ***class-name***	Class name applied to statements in the policy ACL.

1.111.4 Default

None

1.111.5 Usage Guidelines

Use the **modify policy access-list** command to modify in real time the action for the specified condition referenced by statements in the policy ACL, without requiring reconfiguration of the policy ACL.

Note: If the specified condition ID is already configured (using the **condition** command in access control list configuration mode), the **modify policy access-list** command is ignored. If a condition ID is configured using the **condition** command and the changes are saved, any condition ID that may be currently applied using the **modify policy access-list** command at runtime is immediately overwritten.

1.111.6 Examples

With the following configuration, using the **modify policy access-list list_cond condition 200 deny** command will change the action of the ACL condition, **200**, in statement **20** in the IP ACL, **list_cond**, from **permit** to **deny**. However, using the **modify policy access-list list_cond condition 100 permit** command will not affect the **deny** action of the ACL condition, **100**, because it has already been configured:

```
[local]Redback(config-ctx)#policy access-list list_cond
[local]Redback(config-access-list)#condition 100 time-range
[local]Redback(config-acl-condition)#absolute start 2005:01:01:01:00 end 2006:01:01:01:01 permit
[local]Redback(config-acl-condition)#exit
[local]Redback(config-access-list)#seq 10 deny tcp any any eq 80 cond 100
[local]Redback(config-access-list)#seq 20 permit tcp any any eq 81 cond 200
```

1.112 monitor duration

monitor duration ***seconds***

no monitor duration

1.112.1 Purpose

Sets the duration of the system monitoring process.

1.112.2 Command Mode

Global configuration

1.112.3 Syntax Description

seconds	Amount of time, in seconds, that system monitoring lasts. The range of values is 1 to 65535; the default value is 600.

1.112.4 Default

The default duration of system monitoring is 600 seconds, or 10 minutes.

1.112.5 Usage Guidelines

Use the **monitor duration** command to set the duration of the monitoring process, enabled through any of the **monitor** commands (available in exec mode). For additional information, see the *Command List*.

Use the **no** form of this command to set the monitor duration to its default value of 600 seconds.

1.112.6 Examples

The following example shows how to set the monitor duration to **3600** seconds, or 60 minutes:

```
[local]Redback(config)#monitor duration 3600
```

1.113 monitor ip

monitor ip route summary

1.113.1 Purpose

Monitors the current status of IP processes and provides continuous updates to the status.

1.113.2 Command Mode

Exec

1.113.3 Syntax Description

route	Specifies that Routing Information Base (RIB) information is to be monitored.
summary	Specifies that summaries of all routes are to be provided.

1.113.4 Default

None

1.113.5 Usage Guidelines

Use the **monitor ip** command to monitor the current status of IP processes and to provide periodic updates on status changes.

Press **Ctrl+C** to exit monitoring mode.

1.113.6 Examples

The following example shows how to enable monitoring of the RIB process and provides status for the process:

```
[local]Redback>monitor ip route summary
Rt Tbl Version:      765133, Nh Tbl Version: 19580
FIB Rt Tbl Version:  765133
Route Source                 Tot-Routes     Act-Routes  Max Ever Reached

Connected                             5              5               5
Static                                3              3               3
Isis-Level 1                         34             30              76
Isis-Level 2                         17             17              59
Ospf-IntraArea                        7              3               7
IBGP                              19122          19122           20293
EBGP                              82165          82165          101511

% enter ctrl-C to exit monitor mode, monitor duration(sec): 600    (00:00:10)
```

1.114 monitor isis adjacency

monitor isis [**multicast**] **adjacency** [**detail**]

1.114.1 Purpose

Displays continuously updated information about Intermediate System-to-Intermediate System (IS-IS) neighbors.

1.114.2 Command Mode

Exec

1.114.3 Syntax Description

multicast	Optional. Displays IS-IS multicast topology.
detail	Optional. Displays additional information about IS-IS neighbors.

1.114.4 Default

Provides summary information if no options are specified. Updates occur every 2 seconds.

1.114.5 Usage Guidelines

Use the **monitor isis adjacency** command to continuously display updated information about IS-IS neighbors. This information is automatically updated every 2 seconds. Monitoring continues for the number of seconds specified in the **monitor duration** command. The default duration is 600 seconds. For information on the **monitor duration** command, see the *Command List*.

Press **Ctrl+C** to stop displaying information.

Table 16 describes the output fields for the **monitor isis adjacency** command.

Table 16 Field Descriptions for the monitor isis adjacency Command

Field	Description
SystemId	ID of an IS-IS in an area.
Interface	Interface advertising the IS-IS.
L	Level 1 routing only (1), level 2 routing only (2), or levels 1 and 2 (3) routing.
MT	Multi-topology. Indicates whether each IS-IS instance performs unicast (U), multicast (M), or unicast and multicast (UM) topology-based routing. Displays no value when the default routing topology, unicast, is used.
State	IS-IS adjacency state.
Holdtime	Amount of time, in seconds, before an adjacency timeout occurs.
SNPA	Subnetwork Point of Attachment (SNPA) or the data-link address of the remote system.
Uptime	Amount of time that the adjacency has been up.

1.114.6 Examples

The following example displays output from the **monitor isis adjacency** command:

```
[local]Redback>monitor isis adjacency

IS-IS Adjacency:
SystemId    Interface  L MT   State  Holdtime  SNPA            Uptime
a3-ngp      1/1        1      Up     25        0010.7bcc.4b7e  00:01:11
a4-ngp      2/1        2      Up     27        0010.7bcc.4b7e  00:04:33
a5-ngp      3/1        1      Up     29        0050.732e.afd8  00:02:03

Total IS-IS Adjacencies:   3
```

The following example displays output from the **monitor isis adjacency detail** command:

```
[local]Redback>monitor isis adjacency detail

IS-IS Adjacency:
SystemId   Interface  L MT   State  Holdtime  SNPA           Uptime
a3-ngp     1/1        1      Up     25        0010.7bcc.4b7e  00:09:10
  Area Address(es): 49.0002  49.0003
  IP Address(es): 192.168.1.5*
a4-ngp     1/1        1      Up     28        0010.7bcc.4b7e  00:12:32
  Area Address(es): 49.0002
  IP Address(es): 192.168.1.5*
a6-ngp     2/1        1      Up     28        0050.732e.afd8  00:10:02
  Area Address(es): 49.0002  49.0003
  IP Address(es): 192.168.1.6*

Total IS-IS Adjacencies:    3
```

1.115 monitor isis interfaces

monitor isis [**multicast**] **interfaces** [*if-name*] [**detail**]

1.115.1 Purpose

Displays continuously updated information about Intermediate System-to-Intermediate System (IS-IS) interfaces.

1.115.2 Command Mode

Exec

1.115.3 Syntax Description

multicast	Optional. Displays IS-IS multicast topology.
if-name	Optional. Interface name. Displays information only for the specified interface.
detail	Optional. Displays detailed IS-IS interface information.

1.115.4 Default

Provides summary information if no options are specified. Updates occur every 2 seconds.

1.115.5 Usage Guidelines

Use the **monitor isis interfaces** command to display continuously updated information about interfaces configured with IS-IS. This information is automatically updated every 2 seconds. Monitoring continues for the number of seconds specified in the **monitor duration** command. The default duration is 600 seconds. For information on the **monitor duration** command, see the *Command List*.

Press **Ctrl+C** to stop displaying information.

Table 17 describes the output fields for the **monitor isis interface** command.

Table 17 Field Descriptions for the monitor isis interface Command

Field	Description
Interface	Interface advertising the IS-IS.
L	Level 1 routing only (1), level 2 routing only (2), or levels 1 and 2 (3) routing.
MT	Multi-topology. Indicates whether each IS-IS instance performs unicast (U), multicast (M), or unicast and multicast (UM) topology-based routing. Displays no value when the default routing topology, unicast, is used.
State	IS-IS adjacency state.
Level-1-DR	IS-IS level 1 designated router (DR) for the interface.
Level-2-DR	IS-IS level 1 designated router (DR) for the interface.
Metric	Routing metric. A value inside the brackets is a multicast metric, and a value without brackets, or outside the brackets, is a unicast metric.

1.115.6 Examples

The following example displays output from the **monitor isis interfaces** command:

```
[local]Redback>monitor isis interfaces
IS-IS interface(s) for tag A2-wtn:
Interface    L  MT   State  Level-1-DR        Level-2-DR        Metric
1/1          3  UM   Up     a2-wtn.01         a2-wtn.01         10
2/1          3  UM   Up     A1-WTN-3600.02    A1-WTN-3600.02    12[10]
3/1          3  UM   Down   a2-wtn.03         a2-wtn.03         12[10]
4/1          3  UM   Up     a2-wtn.03         a2-wtn.03         27[10]
```

The following example displays output from the **monitor isis interfaces detail** command:

```
[local]Redback>monitor isis interfaces detail
IS-IS interface(s) for tag test:
Redback
Up, Level: 3, Ckt Id: 6, lan, ucast-mcast, IP address: 10.53.36.107/21, Grid:0x10000001
 Level  Adjs Priority  Hello  Hold  Auth Blocked  Metric
 1      0    64        5      24                  10
 1      0    64        3      24                  10
gre0
Up, Level: 3, Ckt Id: 6, lan, ucast-mcast, IP address: 10.53.36.107/21, Grid:0x10000001
 Level  Adjs Priority  Hello  Hold  Auth Blocked  Metric
 1      0    64        7      30                  27
 1      0    64        3      30                  27

Total IS-IS Interface(s):   2
```

1.116 monitor isis statistics

monitor isis [**multicast**] **statistics** [**detail**]

1.116.1 Purpose

Displays continuously updated information about Intermediate System-to-Intermediate System (IS-IS) traffic statistics.

1.116.2 Command Mode

Exec

1.116.3 Syntax Description

multicast	Optional. Displays IS-IS multicast topology.
detail	Optional. Displays detailed IS-IS traffic statistics.

1.116.4 Default

Provides summary information if no options are specified. Updates occur every 2 seconds.

1.116.5 Usage Guidelines

Use the **monitor isis statistics** command to display continuously updated information about IS-IS traffic statistics. This information is automatically updated every 2 seconds. Monitoring continues for the number of seconds specified in the **monitor duration** command. The default duration is 600 seconds. For information on the **monitor duration** command, see the *Command List*.

Press **Ctrl+C** to stop displaying information.

1.116.6 Examples

The following example displays output from the **monitor isis statistics** command:

```
[local]Redback>monitor isis statistics

IS-IS Router tag A2-wtn:
System Id: a2-wtn               Type: Level-1   SPF runs: 299
PDU Type      Received      Processed    Drops       Sent
LSP           2290          2290         0           2515
IIH           91580         91580        0           52756
CSNP          18701         18701        0           17916
PSNP          6             6            0           4
                                Type: Level-2    SPF runs: 366
PDU Type      Received      Processed    Drops       Sent
LSP           5362          5360         2           4502
IIH           91580         91580        0           52787
CSNP          18709         18708        1           17904
PSNP          3             3            0           3
Total         115654        228228       3           75196

Unknown Packets Received: 1
Total Received: 228232; Total Sent: 148387
```

The following example displays output from the **monitor isis statistics detail** command:

```
[local]Redback>monitor isis statistics detail

IS-IS Router tag A2-wtn:
System Id: a2-wtn                Type: Level-1   SPF runs: 299
PDU Type       Received       Processed     Drops        Sent
LSP            2290           2290          0            2515
IIH            91580          91580         0            52756
CSNP           18701          18701         0            17916
PSNP           6              6             0            4
                                  Type: Level-2    SPF runs: 366
PDU Type       Received       Processed     Drops        Sent
LSP            5362           5360          2            4502
IIH            91580          91580         0            52787
CSNP           18709          18708         1            17904
PSNP           3              3             0            3
Total          115654         228228        3            75196

isis kernel stats:
        228272 packets received
        148400 packets sent
        0 incoming packets dropped
        0 packets with bad outgoing interface
```

1.117 monitor ospf interface

monitor ospf interface

1.117.1 Purpose

Displays continuously updated information about Open Shortest Path First (OSPF) interfaces.

1.117.2 Command Mode

Exec

1.117.3 Syntax Description

This command has no keywords or arguments.

1.117.4 Default

Updates occur every 2 seconds.

1.117.5 Usage Guidelines

Use the **monitor ospf interface** command to display continuously updated information about OSPF interfaces. This information is automatically updated every 2 seconds.

Press **Ctrl**+**C** to stop displaying information.

1.117.6 Examples

The following example displays output from the **monitor ospf interface** command:

```
[local]Redback>monitor ospf interface


--- OSPF Interfaces for Instance 64001/Router ID 10.100.1.5 ---

ddr             Len  Network Type    Cost    Priority State    Area

0.100.11.10     29   broadcast       1       1        DR       0.0.0.0

0.100.11.27     29   broadcast       1       1        BDR      0.0.0.11

0.100.11.49     29   broadcast       1       1        BDR      0.0.0.11
```

1.118 monitor ospf neighbor

monitor ospf neighbor

1.118.1 Purpose

Displays continuously updated information about Open Shortest First Path (OSPF) neighbors.

1.118.2 Command Mode

Exec

1.118.3 Syntax Description

This command has no keywords or arguments.

1.118.4 Default

Updates occur every 2 seconds.

1.118.5 Usage Guidelines

Use the **monitor ospf neighbor** command to display continuously updated information about OSPF neighbors. This information is automatically updated every 2 seconds.

Press **Ctrl**+**C** to stop displaying information.

1.118.6 Examples

The following example displays output from the **monitor ospf neighbor** command:

```
[local]Redback>monitor ospf neighbor

--- OSPF Neighbors for Instance 64001/Router ID 10.100.1.5 ---


NeighborID      NeighborAddress Pri State    DR-State IntfAddress     TimeLeft
10.100.1.1      10.100.11.9     1   Full     BDR      10.100.11.10    30
10.100.1.3      10.100.11.25    1   Full     DR       10.100.11.27    38
10.100.1.102    10.100.11.50    1   Full     DR       10.100.11.49    35
```

1.119 monitor ospf spf last

monitor ospf spf last

1.119.1 Purpose

Displays continuously updated information about the most recent Open Shortest Path First (OSPF) Shortest Path First (SPF) calculation.

1.119.2 Command Mode

Exec

1.119.3 Syntax Description

This command has no keywords or arguments.

1.119.4 Default

Updates occur every 2 seconds.

1.119.5 Usage Guidelines

Use the **monitor ospf spf last** command to display continuously updated information about the most recent OSPF SPF calculation. This information is automatically updated every 2 seconds.

Press **Ctrl+C** to stop displaying information.

1.119.6 Examples

The following example displays output from the **monitor ospf spf last** command:

```
[local]Redback>monitor ospf spf last

--- Most Recent OSPF SPF Route Calculation ---

When (elapsed)  Instance/Area          Phase     Duration
00:20:23        64001/N/A              External  < 10 ms
00:20:23        64001/0.0.0.0          Summary   < 10 ms
00:20:23        64001/0.0.0.0          Intra     < 10 ms
00:20:23        64001/0.0.0.11         Intra     < 10 ms
```

1.120 monitor ospf statistics

monitor ospf statistics [*instance-id*] [**interface** {*ip-addr* | *if-name*} | **neighbor** *ip-addr* [**interface** {*ip-addr* | *if-name*}]]

1.120.1 Purpose

Displays continuously updated information about Open Shortest Path First (OSPF) statistics.

1.120.2 Command Mode

Exec

1.120.3 Syntax Description

instance-id	Optional. OSPF instance ID. Monitors statistics for the specified OSPF instance. The range of values is 1 to 65,535.
interface ***ip-addr***	Optional. Interface IP address. Monitors statistics on the specified interface. When used with the **neighbor** ***ip-addr*** construct, monitors statistics on the specified interface for the neighbor.
interface ***if-name***	Optional. Interface name. Monitors statistics on the specified interface. When used with the **neighbor** ***ip-addr*** construct, monitors statistics on the specified interface for the neighbor.
neighbor ***ip-addr***	Optional. Neighbor IP address. Monitors statistics for the specified neighbor.

1.120.4 Default

Provides summary information if no options are specified. Updates occur every 2 seconds.

1.120.5 Usage Guidelines

Use the **monitor ospf statistics** command to display continuously updated information about OSPF statistics. This information is automatically updated every 2 seconds.

Press **Ctrl**+**C** to stop displaying information.

1.120.6 Examples

The following example displays output from the **monitor ospf statistics** command:

```
[local]Redback>monitor ospf statistics

--- OSPF Statistics for Instance 64001 ---

x flood queue length   : 3           Interval            : 5d 16:49:59
As received            : 6705        LSAs sent           : 6513
As changes received    : 536
Packet Retransmissions : 63          LSA Retransmissions : 105
Minutes downloaded     : 78          Routes deleted      : 62
Download Errors        : 0           RIB IPC messages    : 88

            Hello    DD       LSR      LSU      ACK
      Sent  147867   99       23       3917     3065
      Recv  143087   80       28       3290     2913
```

1.121 monitor port

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

monitor port {**counters** [**persistent**] | **traffic**} ***slot***[**/***port*]

1.121.1 Purpose

Monitors the current status of one or more ports or channels and provides continuous updates to the status.

1.121.2 Command Mode

Exec

1.121.3 Syntax Description

counters	Displays port counters.
persistent	Optional. If omitted, displays values since the counters were last cleared or the card was last reloaded. If specified, displays values since the system was last reloaded.
traffic	Displays values for traffic.
slot	Chassis slot number of the traffic card for which monitoring is requested.
port	Optional. Port number for which monitoring is requested. If omitted, monitors all ports on the specified traffic card.

1.121.4 Default

None

1.121.5 Usage Guidelines

Use the **monitor port** command to monitor the current status of one or more ports or channels and to provide periodic updates on status changes.

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

Note:

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

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

Press **Ctrl+C** to exit monitoring mode.

1.121.6 Examples

The following example shows how to monitor the port counters for an Ethernet port:

```
[local]Redback>monitor port counters 5/1
This may adversely impact system performance
% enter ctrl-C to exit monitor mode, monitor duration(sec): 600 (00:00:02)
Port            Type                    Pkts/Bytes Sent  Pkts/Bytes Received
5/1             ethernet                              3                    0
                                                    126                    0
```

The following example shows how to monitor the port traffic for an Ethernet port:

```
[local]Redback>monitor port traffic 5/1
This may adversely impact system performance
% enter ctrl-C to exit monitor mode, monitor duration(sec): 600 (00:00:00)
Port            Type                        Output pps/bps        Input pps/bps
5/1             ethernet                                 0                    0
```

1.122 monitor process

monitor process[*proc-name*] [{**crash-info** | **detail**}]

1.122.1 Purpose

Monitors the current status of a specified category of processes, and provides continuous updates to the status.

1.122.2 Command Mode

Exec

1.122.3 Syntax Description

proc-name	Optional. Process that you want to monitor. The value of the ***proc-name*** argument can be any one of the keywords listed in Table 18.
crash-info	Optional. Specifies that process crash information is to be monitored.
detail	Optional. Specifies that detailed process information is to be displayed.

1.122.4 Default

Monitors all processes and displays summary information if no optional keywords are specified.

1.122.5 Usage Guidelines

Use the **monitor process** command to monitor the current status of system processes and to provide periodic updates on status changes.

Table 18 lists the keywords for the processes supported by this command.

Table 18 Keywords for Processes

Keyword	Process
aaad	Authentication, authorization, and accounting (AAA) process
arp	Address Resolution Protocol (ARP) process
atm	Asynchronous Transfer Mode (ATM) process
bgp	Border Gateway Protocol (BGP) process
bridge	Bridge process
cfm	Ethernet 802.1ag CFM process
clips	Clientless IP service selection process
cls	Classifier Manager process
cpustats	Display CPU statistics
csm	Controller State Manager (CSM) process
dhcp	Dynamic Host Configuration Protocol (DHCP) relay/proxy process
dhcpv6	DHCPv6 process
dhelperd	DHCP helper daemon
dhelperd6	DHCPv6 helper daemon
dlm	Download Manager (DLM) process
dns	Domain Name System (DNS) process
dot1q	802.1Q encapsulation process(1)
flowd	Flow process(2)
fr	Frame Relay process (3)
fsd	File Server manager
fssbcsim	FSSB Client simulator
gsmp	General Switch Management Protocol (GSMP) process
hr	HTTP redirect process
igmp	Internet Group Management Protocol (IGMP) process
isis	Intermediate System-to-Intermediate System (IS-IS) process
ism	Interface and Circuit State Manager (ISM) process
l2tp	Layer 2 Tunneling Protocol (L2TP) process
l4l7	L4L7 process
ldp	Label Distribution Protocol (LDP) process
lg	Link group (LG) process
lm	Label Manager (LM) process

Table 18 Keywords for Processes

Keyword	Process
metad	META process
mgd	Media Gateway process
mgmd	Media Gateway Manager process
mip	Mobile IP process
mipsim	Mobile IP Simulator process
mpls_static	Multiprotocol Label Switching (MPLS) static process
msdp	Multicast Source Discovery Protocol (MSDP) process
nat	IP Network Address Translation (NAT) process
nd	Neighbor discovery (ND) process
netopd	NetOp™ process daemon
ntp	Network Time Protocol (NTP) process
odd	On-demand diagnostics (ODD) process
ospf	Open Shortest Path First (OSPF) protocol process
ospf3	OSPF Version 3 (OSPF3) protocol process
ped_parse	Process execution descriptor (PED) parse process
pem	Port encapsulation module (PEM) process
pim	Protocol Independent Multicast (PIM) process
ppaslog	Packet Processing ASIC (PPA) syslog process
ppp	Point-to-Point Protocol (PPP) process
pppoe	PPP over Ethernet (PPPoE) process
qos	Quality of service (QoS) process
rcm	Router Configuration Manager (RCM) process
rib	Routing Information Base (RIB) process
rip	Routing Information Protocol (RIP) process
rpm	Router Policy Manager (RPM) process
rsvp	Resource Reservation Protocol Traffic Engineering (RSVP-TE) process
sctp	SCTP process
shm_ribd	Shared Memory RIB process
snmp	Simple Network Management Protocol (SNMP) process
static	Static routing process
stats	Statistics process

Table 18 Keywords for Processes

Keyword	Process
sysmon	System monitor process
tunnel	Tunnel management process
vrrp	Virtual Router Redundancy Protocol (VRRP) process
xcd	Cross-connect process daemon

(1) The SmartEdge 100 router does not support 802.1Q.
(2) Not all controller cards support flow.
(3) The SmartEdge 100 router does not support Frame Relay.

Updates occur every two seconds. Monitoring continues for the number of seconds specified by the **monitor duration** command (in global configuration mode). The default duration is 600 seconds.

Use the **monitor process** command without any keywords to monitor all system processes, or use the appropriate keyword to monitor a specific category of processes.

Press **Ctrl+C** to exit monitoring mode.

1.122.6 Examples

The following example shows how to enable monitoring of the RIP process and provide status for the process:

```
[local]Redback>monitor process rip
% enter ctrl-C to exit monitor mode, monitor duration(sec): 5600 (00:00:08)

NAME          PID    SPAWN      MEMORY  TIME         %CPU   STATE
rip           12652      1      576K    00:00:00.02  0.00%  run
```

1.123 more

more ***url***

1.123.1 Purpose

Displays the contents of a file on the local file system, one page at a time.

1.123.2 Command Mode

Exec

1.123.3 Syntax Description

url	URL of the file to be displayed.

1.123.4 Default

None

1.123.5 Usage Guidelines

Use the **more** command to display the contents of a file on the local file system, one page at a time.

At the end of each page, the SmartEdge router prints “--More--” to indicate the presence of more output. You can use a subset of the commands available in the UNIX **more(1)** command, such as pressing **Space** to show the next page of output, pressing **Enter** to show one additional line of output, or typing **q**, to end the display.

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

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

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

1.123.6 Examples

The following example displays the contents of the file, **/flash/redback.cfg**. At the prompt, the user ends the display by entering **q:**

```
[local]Redback>more /flash/redback.cfg
```

```
context local
!
 interface 1/1
  ip address 10.5.1.2/16
  ip router isis tag
!
 interface 2/1
  ip address 10.7.1.1/16
  ip router isis tag
--More--q
[local]Redback#
```

1.124 mount /md

mount /md

1.124.1 Purpose

Mounts a mass-storage device that has been inserted in the external slot of a controller card.

1.124.2 Command Mode

Exec (10)

1.124.3 Syntax Description

This command has no keywords or arguments.

1.124.4 Default

None

1.124.5 Usage Guidelines

Use the **mount /md** command to mount a mass-storage device. You must enter this command from the command-line interface (CLI) that is running on the controller card with the device to be mounted.

When you insert a mass-storage device into the external slot of a controller card, the system mounts it for you; you do not need to enter this command. However, if the **show disk** command (in any mode) indicates that the device is not mounted, you can enter this command to mount it. Failure to mount a mass-storage device is also recorded in the log messages.

The following guidelines apply to file management for mass-storage devices:

- The contents of the mass-storage devices installed in the active and standby controller cards are not synchronized. Any files written to a device are not automatically written to the device installed on the other controller card; however, you can copy the files manually. You can perform the copy only when you are connected to the CLI running on the controller card to which you want to copy the files.
- After you have unmounted a mass-storage device installed on a controller card, any files written to /md from the CLI running on that controller are stored on the NetBSD compact-flash card in its /md directory. After a device is mounted, either by the system or by using this command, those files are no longer accessible, and, because they are not automatically written to the device, you must copy them manually to the device.

To transfer the files written to the /md directory on the NetBSD compact-flash card while the mass-storage device was unmounted, perform the following steps:

1. Before you mount the mass-storage device (or insert it in the external slot on the controller card), create a temporary directory in the local file system on the NetBSD compact-flash card for the files you need to transfer; for example:

```
[local]Redback#mkdir /flash/temp
```

2. Transfer the files from the /md directory to the directory you have created; for example:

```
[local]Redback#copy /md/newconfig.cfg /flash/temp/newconfig.cfg
```

3. Delete the files in the /md directory to recover the file space; for example:

```
[local]Redback#delete /md/newconfig.cfg
```

4. Insert the device in the external slot on the controller card and check its status; for example:

```
[local]Redback#show disk

Filesystem  512-blocks     Used    Avail Capacity  Mounted on

NetBSD          362526   133210   211188    38%    /

Microdrive     1021244    54118   916062     5%    /md
```

5. If the status does not indicate that the device was mounted, mount the device; for example:

```
[local]Redback#mount /md
```

6. Transfer the files from the temporary directory you created on the internal compact-flash card to a directory on the device; for example:

```
[local]Redback#copy /flash/temp/newconfig.cfg /md/myconfg/newconfig.cfg
```

7. Delete the files and the temporary directory to recover the file space; for example:

```
[local]Redback#delete /flash/temp/newconfig.cfg

[local]Redback#rmdir /flash/temp
```

To transfer the files to the mass-storage device on the other controller card, perform the following steps:

1. Connect to the CLI running on the other controller card; for example, to the standby controller card.

2. Transfer the files; for example:

```
[local]standby#copy mate /md/myconfg/newconfig.cfg
/md/myconfg/newconfig.cfg
```

1.124.6 Examples

The following example shows how to mount the mass-storage device installed in the active controller card:

```
[local]Redback#mount /md
```

1.125 move-frequency

move-frequency ***moves-per-sec***

no move-frequency

1.125.1 Purpose

Sets the threshold above which a bridging loop is declared.

1.125.2 Command Mode

Loop-detection configuration

1.125.3 Syntax Description

moves-per-sec	Moves per second. The range of values is 0 to 65535, where 0 specifies no limit is placed on the move frequency.

1.125.4 Default

0 (blocking is never applied)

1.125.5 Usage Guidelines

Use the **move-frequency** command to set the threshold above which a bridging loop is declared; that is, when the frequency threshold (MAC moves per second) is reached or exceeded, the loop-detection process blocks circuits that have been designated as available until the loop is no longer observed.

The **priority** command specifies order in which circuits are available for blocking.

Use the **no** form of this command to return the move-frequency to its default.

1.125.6 Examples

The following examples shows how to set the move frequency threshold .

```
[local]Redback(config)#context ink
[local]Redback(config-ctx)#bridge lbdl
[local]Redback(config-bridge)#loop-detection
[local]Redback(config-ld)#move-frequency 20000
```