Commands: g through io

COMMAND DESCRIPTION

Copyright

Disclaimer

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

Trademark List

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

Contents

1 Command Descriptions

Commands starting with “g” through commands starting with “io” 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 giaddr

```
giaddr ip-addr
```

```
no giaddr
```

1.1.1 Purpose

Sets the IP address used as the giaddr in DHCP packets that the SmartEdge router relays to the external DHCP server.

1.1.2 Command Mode

DHCP proxy configuration

1.1.3 Syntax Description

ip-addr	IP address

1.1.4 Default

If this command is not entered, the SmartEdge router uses the primary IP address of the multibind interface as the giaddr.

1.1.5 Usage Guidelines

Use the **giaddr** command to set the IP address used as the giaddr in DHCP packets that the SmartEdge router relays to the external DHCP server:

- The giaddr used by the DHCP proxy must be unique on each backup and active chassis in the Inter-Chasssis Redundancy (ICR) setup.
- The ***ip-addr*** value must be one of the addresses in the subnet configured for the multibind interface.

1.1.6 Examples

The following example illustrates the use of this command:

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

[local]Redback(config-if)#ip address 50.0.0.1/16

[local]Redback(config-if)#ip address 50.0.0.2 application

[local]Redback(config-if)#dhcp proxy 48000

[local]Redback(config-dhcp-giaddr)#giaddr 50.0.0.2
```

1.2 graceful-restart (BGP)

```
graceful-restart

no graceful-restart
```

1.2.1 Purpose

Enables graceful restart for a BGP routing instance.

1.2.2 Command Mode

BGP router configuration

1.2.3 Syntax Description

This command has no keywords or arguments

1.2.4 Default

Graceful restart is enabled on all BGP routing instances.

1.2.5 Usage Guidelines

Use the **graceful-restart** command to enable graceful restart for a BGP routing instance.

Keep the following in mind when configuring graceful restart for a BGP routing instance:

- Graceful restart is always enabled on all BGP routing instances.
- Graceful restart is supported for all IPv4 and IPv6 address families. You must use the send label command to enable the negotiation of IPv4 and IPv6 labeled address families.
- When an iBGP peer restarts, the restarting and helper peers exchange graceful restart capabilities. In addition, all iBGP peers within the same domain exchange their graceful restart capabilities, including the list of IP address families with routes that can be gracefully restarted. The helper router helps restart only those iBGP peers that have the same address-family capabilities.

A BGP speaker advertises its graceful restart capabilities to its peers.

Use the **no** form of this command to disable graceful restart for a BGP routing instance.

1.2.6 Examples

1.2.6.1 Disable Graceful Restart for a BGP Instance

The following example shows how to disable graceful restart on a BGP instance:

```
[local]Redback #configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#no graceful restart
```

1.2.6.2 Enable Graceful Restart for a BGP Instance

The following example shows how to enable graceful restart on a BGP instance that has graceful restart disabled:

```
[local]Redback #configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#graceful restart
```

1.3 graceful-restart (IS-IS)

graceful-restart ***interval***

no graceful-restart ***interval***

1.3.1 Purpose

Enables graceful restart for an Intermediate System-to-Intermediate System (IS-IS) instance. When an IS-IS instance is restarted, it attempts to restart gracefully, consistent with RFC 5306, *Restart Signaling for IS-IS*.

1.3.2 Command Mode

IS-IS router configuration

1.3.3 Syntax Description

interval	Optional. Grace period, in seconds. During this time, the IS-IS instance attempts to restart gracefully. The range of values is 10 to 900; the default value is 120.

1.3.4 Default

Graceful restart is enabled.

1.3.5 Usage Guidelines

Use the **graceful-restart** command to enable an IS-IS instance to attempt to restart gracefully after a planned or unplanned restart (crash). This implies that the forwarding state will be maintained while IS-IS reestablishes its neighbor adjacencies and recalculates its routes. It also implies that the IS-IS instance advertises its intent to restart gracefully to its neighbors. The IS-IS instance discontinues graceful restart when all of its prior IS-IS adjacencies have been established, or when the grace period expires.

Note: Helper mode is automatically enabled when you enable graceful restart for an IS-IS instance. An IS-IS instance enters into helper mode when it receives a restart request from a restarting IS-IS instance. The IS-IS instance exits helper mode when it receives a restarting-clear message from the restarting IS-IS instance.

IS-IS graceful restart must be enabled on the designated intermediate system (DIS) to be effective. If graceful restart is not enabled on the DIS, graceful restart does not work for any other routers on a LAN.

Graceful restart is enabled on IS-IS instances by default. Use the **no** form of this command to disable graceful restart.

1.3.6 Examples

The following example shows how to enable an IS-IS instance to restart gracefully, and discontinues graceful restart when it determines graceful restart has been completed successfully, or when the grace period of 60 seconds has expired:

```
[local]Redback(config-ctx)#router isis is1

[local]Redback(config-isis)#graceful-restart 60
```

1.4 graceful-restart (LDP)

graceful-restart [**reconnect-time** ***interval***] [**recovery-time** ***interval***]

no graceful-restart

1.4.1 Purpose

Enables a label-switched router (LSR) to restart its Label Distribution Protocol (LDP) component while preserving its Multiprotocol Label Switching (MPLS) forwarding state during restart.

1.4.2 Command Mode

LDP router configuration

1.4.3 Syntax Description

reconnect-time ***interval***	Optional. Reconnect time. Specifies the time interval (in seconds) that the remote LDP peer must wait for the local LDP peer to reconnect after the remote peer detects the LDP communication failure. The range of values for the ***interval*** argument is 1 to 3,600; the default value is 120.
recovery-time ***interval***	Optional. Recovery time. Specifies the time interval (in seconds) that the remote LDP peer preserves its MPLS forwarding state after receiving the initialization message (init msg) from the restarted local LDP peer. The recovery time is sent in the initialization message by the restarting LDP peer. The range of values for the ***interval*** argument is 1 to 3,600; the default value is 120.

1.4.4 Default

Graceful restart is enabled.

1.4.5 Usage Guidelines

Use the **graceful-restart** command to enable an LSR to restart its LDP component while preserving its MPLS forwarding state during restart.

After an LSR restarts its control plane, it starts an internal recovery timer and continues to forward traffic using the preserved MPLS forwarding state entries. Before the recovery timer expires, the LSR creates local label bindings by following the normal LDP procedure. When the recovery timer expires, the MPLS forwarding entries that are not refreshed from the LDP peer are deleted and the refreshed ones are preserved without any disruption to the forwarding path.

Use the **no** form of this command to disable the graceful restart capability.

1.4.6 Examples

The following example shows how to enable an LSR to restart its LDP component while preserving its MPLS forwarding component during restart and configure the reconnect and recovery times to 60 seconds each:

```
[local]Redback(config-ldp)#graceful-restart reconnect-time 60 recovery-time 60
```

1.5 graceful-restart (OSPF)

graceful-restart [*interval* | **helper** [**strict-checking**]]

no graceful-restart [*interval* | **helper** [**strict-checking**]]

1.5.1 Purpose

Enables graceful restart for the Open Shortest Path First (OSPF) or OSPF Version 3 (OSPFv3) instance. When the OSPF or OSPFv3 instance is restarted, it attempts to restart gracefully, consistent with RFC 3623, ***Graceful OSPF Restart*** and RFC 5187, ***OSPFv3 Graceful Restart***.

1.5.2 Command Mode

- OSPF router configuration
- OSPF3 router configuration

1.5.3 Syntax Description

interval	Optional. Grace period, in seconds. During this time, the OSPF or OSPFv3 instance attempts to restart gracefully. The range of values is 10 to 900; the default value is 120.
helper	Optional. Enables OSPF helper mode.
strict-checking	Optional. Disables OSPF helper mode on a link-state advertisement (LSA) change.

1.5.4 Default

Graceful restart is disabled. OSPF helper mode is enabled, with the strict checking option disabled.

1.5.5 Usage Guidelines

Use the **graceful-restart** command to enable an OSPF or OSPFv3 instance to attempt to restart gracefully after a planned or unplanned restart (crash). This implies that the forwarding state will be maintained while OSPF or OSPFv3 reestablishes its neighbor adjacencies and recalculate its routes. It also implies that the OSPF or OSPFv3 instance will advertise its intent to restart gracefully to its neighbors. The OSPF or OSPFv3 instance will discontinue graceful restart when all of its prior OSPF or OSPFv3 adjacencies have been established or when the grace period expires.

Use the **no** form of this command to disable graceful restart.

1.5.6 Examples

The following example shows how to enable an OSPF instance to restart gracefully, and discontinues graceful restart when it determines graceful restart has been completed successfully, or when the grace period of **60** seconds has expired:

```
[local]Redback(config-ospf)#graceful-restart 60
```

1.6 graceful-restart (RSVP)

In RSVP router configuration mode:

graceful-restart [**helper** | **restart-time** *interval* | **recovery-time** *interval* | **maximum_helper_recovery-time** *interval* | **maximum_helper_restart-time** *interval*]

no graceful-restart [**helper** | **restart-time** | **recovery-time** | **maximum_helper_recovery-time** *interval* | **maximum_helper_restart-time** *interval*]

default graceful-restart [**helper** | **restart-time** | **recovery-time**]

In RSVP interface configuration mode:

graceful-restart [restart-time *interval* | **recovery-time** *interval*]

no graceful-restart [restart-time | **recovery-time**]

default graceful-restart [restart-time | **recovery-time**]

1.6.1 Purpose

Enables graceful restart for the Resource Reservation Protocol (RSVP) instance.

1.6.2 Command Mode

- RSVP router configuration
- RSVP interface configuration

1.6.3 Syntax Description

`helper`	Optional. Enables RSVP helper mode.
`restart-time` *`interval`*	Optional. Restart time. Specifies the time interval (in seconds) that the remote RSVP peer must wait to receive an RSVP Hello message after the remote peer detects an RSVP communication failure. The range of values for the *`interval`* argument is 10 to 1800; the default value is 30.
`recovery-time` *`interval`*	Optional. Recovery time. Specifies the time interval (in seconds) that the remote RSVP peer preserves its LSPs after receiving the hello message (init msg) from the restarted local RSVP peer. The recovery time is sent in the hello message by the restarting RSVP peer. The range of values for the *`interval`* argument is 20 to 3600; the default value is 60.
`maximum_helper_recovery-time` *`interval`*	Optional. Specifies the maximum time interval (in seconds) that the RSVP instance retains information about the state of a neighbor after a graceful restart. When the helper recovery timer expires, the status information for the neighbor expires and is no longer retained. The range of values for the *`interval`* argument is 20 to 3600.
`maximum_helper_restart-time` *`interval`*	Optional. Specifies the maximum time interval (in seconds) that the RSVP instance waits for a neighbor to come up after a graceful restart before considering the neighbor to be down. When the helper restart timer expires, the LSPs between the SmartEdge router and the restarting neighbor are no longer retained. The range of values for the *`interval`* argument is 10 to 1800.

1.6.4 Default

Graceful restart is disabled.

1.6.5 Usage Guidelines

Use the `graceful-restart` command to enable an RSVP instance to attempt to restart gracefully after a planned or unplanned restart (crash). This implies that the forwarding state is maintained while RSVP reestablishes its neighbor adjacencies and rediscovers label-switched path (LSP) soft state. It also implies that the RSVP instance advertises its intent to restart gracefully to its neighbors.

RSVP graceful restart relies on RSVP Hello messages to determine if a neighbor is down, and if it should initiate graceful restart procedures. Use the **`hello interval`** and **`hello keep-multiplier`** commands in RSVP interface configuration mode to enable and configure RSVP Hello messages.

Use the **`restart-time`** *`interval`* and **`recovery-time`** *`interval`* options to configure more time than the default to allow the routing information for LSPs to be saved after a nbr (neighbor) restart has been detected depending on the system configuration. For example, more than 30 seconds can be needed if OSPF is also enabled.

When the interval is configured globally by entering the **`graceful-restart`** [**`restart-time`** *`interval`* | **`recovery-time`** *`interval`*] command in the router RSVP configuration mode, the interval applies to all RSVP interfaces. When the interval is configured under a specific interface by entering the **`graceful-restart`** [**`restart-time`** *`interval`* | **`recovery-time`** *`interval`*] command in the RSVP interface configuration mode, the interval applies only to that specific RSVP interface.

Note: The interval configured in the RSVP interface configuration mode takes precedence over the interval configured globally if the interval is configured both ways.

When the helper restart and recovery timers are not configured, the intervals used to preserve LSPs during a graceful restart are determined by Hello messages sent from the neighbor. When the helper restart and recovery timers are configured, the local timer values are compared with the timer values advertised by a neighbor. If the neighbor advertises restart and recovery timer values that are different from the locally configured maximum helper restart and recovery timer values, the smaller timer values take precedence. If you do not configure the maximum helper restart and recovery timers on the SmartEdge router, the router uses the restart and recovery timer values advertised by the neighbor. This behavior ensures that the LSPs are preserved for the length of time expected by the neighbor, reducing the risk of traffic loss during graceful restart.

If the maximum helper timer values are not configured, the SmartEdge router uses the timer values advertised by the neighbors in hello messages.

Note: You must enable RSVP helper mode before configuring the helper restart and recovery timers. If graceful restart helper mode is disabled, any helper mode restart and recovery timer configuration is not applied.

If the received maximum helper restart and recovery timer values are different from the configured maximum helper restart and recovery values, the greater maximum helper timer values take precedence.

Use the **`no`** form of the **`graceful-restart`** command to disable graceful restart for an RSVP instance.

Use the **`show rsvp neighbor`** command to display RSVP graceful restart information.

1.6.6 Examples

The following example shows how to enable an RSVP instance to restart gracefully:

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

[local]Redback(config-rsvp)#graceful-restart
```

The following example shows how to enable an RSVP instance to restart gracefully after 50 seconds:

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

[local]Redback(config-rsvp)#graceful-restart restart-time 50
```

The following examples shows how to enable an RSVP interface to restart gracefully after 1000 seconds:

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

[local]Redback(config-rsvp)#interface rsvp50

[local]Redback(config-rsvp-if)#graceful-restart restart-time 1000
```

The following example shows how to enable RSVP graceful restart helper mode, and configure the helper recovery time to 200 seconds and the helper restart time to 100 seconds:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#graceful-restart helper
[local]Redback(config-rsvp)#graceful-restart
maximum_helper_recovery-time 200
[local]Redback(config-rsvp)#graceful-restart
maximum_helper_restart-time 100
```

1.7 gre

gre key ***key-id***

1.7.1 Purpose

Specifies a key ID in the GRE tunnel. Each key ID creates a circuit (tunnel channel) in the GRE tunnel.

1.7.2 Command Mode

Tunnel configuration

1.7.3 Syntax Description

key ***key-id***	Specifies a key ID in the current GRE tunnel.

1.7.4 Default

Tunnel circuit 0.

1.7.5 Usage Guidelines

Use the **gre** command with the **key** keyword to specify a key ID in the GRE tunnel. Each key ID creates a circuit (tunnel channel) in the GRE tunnel. This command enters the GRE key configuration mode, where the tunnel circuits can be bound to interfaces and the other attributes of the tunnel circuits can be specified.

1.7.6 Examples

The following example shows the **crypto-map** command:

```
[local]Redback(config)#tunnel gre blue-tunnel

[local]Redback(config-tunnel)#gre key 5
```

1.8 gre mtu

```
gre mtu bytes

no gre mtu
```

1.8.1 Purpose

Sets the Maximum Transmission Unit (MTU) for packets sent on GRE tunnels.

1.8.2 Command Mode

Dynamic Tunnel Profile configuration

1.8.3 Syntax Description

bytes	MTU size in bytes. The range of values is 256 through 1468 bytes.

1.8.4 Default

1468 bytes

1.8.5 Usage Guidelines

Use the **gre mtu** command to set the MTU for packets sent in GRE tunnels. If an IP packet exceeds the MTU, the system fragments that packet.

A tunnel uses the MTU size for the interface to which the tunnel is bound to compute the tunnel MTU size, unless you explicitly configure the MTU using this command. After you configure an MTU for the tunnel, the system determines the effective MTU by comparing the configured MTU with the interface MTU and selecting the lesser of the two values.

Use the **no** form of this command to delete the configured MTU and use the interface MTU.

1.8.6 Examples

The following example shows how to set the maximum IP packet size for GRE tunnels for `prof1 to 1200 bytes`:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#dynamic-tunnel-profile prof1
[local]Redback(config-mip-dyn-tun1-profile)#gre mtu 1200
[local]Redback(config-mip-dyn-tun1-profile)#end
```

1.9 group

group *port-group-num* **ports** *port-num1. . . [port-numN]*

no group *port-group-num*

1.9.1 Purpose

Defines a specific port group.

1.9.2 Command Mode

Port group map configuration

1.9.3 Syntax Description

port-group-num	Number to be assigned to a port group. The range of values for the *port-group-num* argument depends on the type of card. See Table 1 for more information.
ports *port-num1* . . . [*port-numN*]	Specifies the port numbers to be mapped to the port group. The number of ports allowed for each port group depends on the type of card. See Table 1 for more information.

1.9.4 Default

None

1.9.5 Usage Guidelines

Use the **group** command to define a specific port group. Each port must be included in one and only one port group.

Table 1 lists the port group number range and the maximum number of ports per group for each supported line card.

Table 1 Port Group Range and Maximum Number of Ports per Group

Line Card	Port Group Number Range	Maximum Number of Ports per Group
fege-60-2-port	1 to 6	16
ge3-4-port	1 to 4	4
ge-10-port	1 to 5	5
ge-20-port	1 to 5	5
ge-5-port	1 to 5	5

Use the **no** form of this command to remove a port group configuration.

1.9.6 Examples

The following example shows how to enter the port group map configuration mode and define five port groups. Each specified port group has two ports mapped to it:

```
[local]Redback(config)#qos port-map portmap7 card-type ge-10-port
[local]Redback(config-port-group-map)#group 1 ports 1 6
[local]Redback(config-port-group-map)#group 2 ports 2 7
[local]Redback(config-port-group-map)#group 3 ports 3 8
[local]Redback(config-port-group-map)#group 4 ports 4 9
[local]Redback(config-port-group-map)#group 5 ports 5 10
```

1.10 group-mac

`group-mac` ***`group-address`***

{**`no`** | **`default`**} **`group-mac`**

1.10.1 Purpose

Sets the multicast MAC address of the link-trace message (LTM) PDUs in the current maintenance domain (MD).

1.10.2 Command Mode

CFM configuration

1.10.3 Syntax Description

`group-address`	The multicast MAC address for LTM

1.10.4 Default

01:80:C2:00:00:3y, where y is the MD level of the current MD.

1.10.5 Usage Guidelines

Use the **`group-mac`** command to set the multicast MAC for the LTM PDUs in the current MD.

Use the **`ethernet-cfm linktrace`** command to trace the links from a particular circuit interface to a destination MAC address.

1.10.6 Examples

In the following example, the **group-mac** command changes the default LTM broadcast address in the **sbc** MD from the default to **01:01:01:01:01:01:**

```
[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
```

1.11 group-mac-address

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

no group-mac-address

1.11.1 Purpose

Sets the group MAC address for the bridge.

1.11.2 Command Mode

Spanning-tree configuration

1.11.3 Syntax Description

mac-addr	Group MAC address in the dotted hexadecimal format ***hh:hh:hh:hh:hh:hh***.

1.11.4 Default

The default group MAC address is 01.80.C2.00.00.00.

1.11.5 Usage Guidelines

Use the **group-mac-address** command to set the group MAC address for the bridge.

Use the **spanning tree profile** command (in port configuration mode and dot1q PVC configuration mode) to assign which circuits send and listen for BPDUs using the group MAC address. All other circuits in the bridge send BPDUs to the standard MAC address.

The **l2protocol-tunnel** command controls the Layer 2 Protocol tunnel attribute in the spanning-tree profile that determines whether the assigned circuit uses the group MAC address or the standard MAC address.

1.11.6 Examples

The following example illustrates the creation of the spanning-tree profile womp and setting its l2protocol-tunnel attribute to enable the associated ports to send BPDUs through the Layer 2 Protocol tunnel.

The **spanning-tree profile** command (port configuration mode) then assigns the spanning-tree profile to an Ethernet port.

In the last part of the configuration, the **group-mac-address** command (in bridge configuration mode) specifies the destination MAC address for BPDUs sent through the Layer 2 Protocol tunnel:

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

[local]Redback(config-stp-prof)#l2protocol-tunnel

[local]Redback(config-stp-prof)#exit

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

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

[local]Redback(config-ctx)#bridge isp3

[local]Redback(config-bridge)#description Bridge for all traffic to ISP3

[local]Redback(config-bridge)#aging-time 18000

[local]Redback(config-bridge)#spanning-tree

[local]Redback(config-bridge-stp)#group-mac-address 01.80.C2.00.00.02
```

1.12 header format

header format *format-string* [*OS-variable*] [*OS-variable*] ...

no header format

1.12.1 Purpose

Specifies lines of informative text that are inserted at the beginning of each bulk statistics (bulkstats) collection file for this policy.

1.12.2 Command Mode

bulkstats configuration

1.12.3 Syntax Description

format-string	Table 2 describes the format strings, used to format the header line. Format strings can contain anything or nothing as a label for an SmartEdge operating system variable. They follow the C programming language printf() function syntax and must be enclosed in quotation marks.
OS-variable	Optional. SmartEdge operating system variable. Table 3 describes the supported variables.

1.12.4 Default

No header lines are included in any bulkstats collection file for any policy.

1.12.5 Usage Guidelines

Use the **header format** command to specify lines of informative text (headers) at the beginning of each bulkstats collection file for this policy. Lines added by using this command are inserted in each file in the order in which they are configured. You can specify at most 10 headers for a policy.

Table 2 describes the supported format strings.

Table 2 Format String Special Character Descriptions

Format String	Description
\n	Creates a new line
%s	Represents a character string
%d	Represents an integer in decimal (base 10)
%u	Represents an unsigned integer in decimal (base 10)
%x	Represents an integer in hexadecimal format (base 16)
%%	Represents a single % character

Table 3 describes the SmartEdge operating system variables that you can use to format the headers in each bulkstats collection file.

Table 3 Variables for the header format Command

Variable	Description	Type
chassis_type	Type of chassis	String
context	Context name	String
date	Today's date in ***YYYYMMDD*** format	String
epochtime	Time of day in epoch format (seconds since January 1, 1970)	Integer
hostname	Hostname as specified in the configuration file	String
policy	Bulkstats policy name	String
sysuptime	System uptime in seconds.	Integer
timeofday	Time of day in ***HHMMSS*** format (using a 24-hour clock)	String

Each header definition must be unique. If a new header line is configured so that it exactly matches an existing header line, the new header is ignored.

Use the **no** form of this command to delete all bulkstats header specifications for each bulkstats file. After you use this command, you must redefine all headers. Use a text editor for minor editing of the headers rather than editing them with the **header format** command.

1.12.6 Examples

The following example inserts a line of text about the date that data is collected in each bulkstats collection file for the policy, **bulk**, in the **local** context:

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

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


[local]Redback(config-bulkstats)#header format "Data collected on
%s for %s policy in %s context" date policy context
```

The previous line puts the following line in the collection file:

```
Data collected on 20030530 for bulk policy in local context
```

1.13 hello holdtime

hello holdtime ***seconds***

default fault hello holdtime

1.13.1 Purpose

Changes the time for which a Label Distribution Protocol (LDP) link Hello adjacency is maintained in the absence of link Hello messages from the LDP neighbor.

1.13.2 Command Mode

LDP router configuration

1.13.3 Syntax Description

seconds	Number of seconds after which, if LDP link hello messages from the LDP neighbor is not received, the LDP adjacency is deleted. The range of values is 15 to 3,600.

1.13.4 Default

The default LDP link Hello holdtime is 15 seconds.

1.13.5 Usage Guidelines

Use the `hello holdtime` command to change the time for which an LDP link Hello adjacency is maintained in the absence of link Hello messages from the LDP neighbor.

LDP neighbors periodically exchange Hello messages to maintain their adjacencies. The Hello holdtime determines the time after which, if LDP messages from the LDP neighbor are not received, the LDP hello adjacency is deleted. When the last LDP adjacency to a LDP neighbor is deleted, the LDP session to that LDP neighbor is torn down.

For LDP neighbors to negotiate a Hello hold time, each LDP neighbor includes a proposed Hello holdtime in their transmitted Hello message. The negotiated Hello holdtime used between the two neighbors is the lesser of the two proposed values.

The locally configured link Hello hold time as specified in the `hello holdtime` command is included in the link Hello messages sent to immediate LDP neighbors. The negotiated hold time used to time out a link Hello adjacency is the lesser of the time value specified in `hello holdtime`” command and the hello holdtime received in link hello messages from the LDP neighbor of the adjacency.

Use the **`default`** form of this command to return to the default value of 15 seconds.

1.13.6 Examples

The following example shows how to configure the LDP hold time to be **45** seconds:

```
[local]Redback(config-ctx)#router ldp
[local]Redback(config-ldp)#hello holdtime 45
```

1.14 hello interval (IS-IS)

`hello interval` {*`seconds`*[**`level-1`** | **`level-2`**] | {**`adaptive-millisecond`** | **`millisecond`**} *`milliseconds`*}

`no hello interval`

1.14.1 Purpose

Modifies the interval at which Intermediate System-to-Intermediate System (IS-IS) Hello packets are sent on the interface.

1.14.2 Command Mode

IS-IS interface configuration

1.14.3 Syntax Description

`seconds`	Amount of time, in seconds, after which Hello packets are sent on the interface. The range of values is 1 to 65,535; the default value is 10.
`level-1`	Optional. Configures the Hello interval for IS-IS level 1 independently.
`level-2`	Optional. Configures the Hello interval for IS-IS level 2 independently.
`adaptive-millisecond`	Configures the Hello interval in the sub-second mode, and allows the Hello hold time to be adaptively adjusted when the link or network is under flapping or is unstable.

`millisecond`	Configures the Hello interval in the sub-second mode.
`milliseconds`	Amount of time, in 100 millisecond increments, after which Hello packets are sent on the interface. The range of values is 200 to 800 milliseconds.

1.14.4 Default

Hello packets are sent on the interface every 10 seconds. When you enter this command without specifying either IS-IS level 1 or level 2 routing, Hello packets are sent at the same rate for both levels.

1.14.5 Usage Guidelines

Use the **`hello interval`** command to modify the interval at which IS-IS Hello packets are sent on the interface.

A shorter interval allows faster convergence; however, it increases bandwidth and CPU usage, and might add to instability in the network. In addition to saving bandwidth and CPU usage, a longer interval, especially when used in conjunction with a higher Hello multiplier can increase overall network stability. To modify the Hello multiplier, use the Hello multiplier command in IS-IS interface configuration mode.

You can configure the Hello interval independently for level 1 and level 2, except on serial point-to-point (P2P) interfaces. Tuning the Hello interval and Hello multiplier on P2P interfaces is more useful than on LAN interfaces.

Use the **`millisecond`** or **`adaptive-millisecond`** keyword to specify the sub-second IS-IS Hello interval. The minimum hold time, which is limited by IS-IS protocol, is one second. The hold time advertised by the Hello packets is the product of the Hello interval and the Hello multiplier rounded up to the nearest second. If the adaptive millisecond is configured on the interface, then the hold time can adaptively increase under the condition of adjacency flapping or network instability. The adaptive Hello hold time advertised by the Hello packets is double the regular hold time if the adjacencies over the interface has bounced three times in a 180-second period, and is limited by the hold time of 16 seconds.

The adaptive hold time can be reset to the original hold time value by issuing the **`clear isis adaptive-holdtime`** command in exec mode on the interface.

Caution!

Risk of data loss. Under link flapping, network churn, or heavy traffic congestion can cause Hello packet transmission or processing to be delayed, or packets to be dropped. Setting the Hello hold time too low can cause IS-IS adjacencies to flap, which can cause network instability. To reduce the risk, use the **`millisecond`** or **`adaptive-millisecond`** keyword only on some point-to-multipoint interfaces, where the fast detection of lost adjacencies is required. If you use the **`adaptive-millisecond`** keyword, and if the network churns cause IS-IS adjacencies to flap because the hold time is too small, the hold time on the interface is adaptively backed off to a safer region, to avoid network instability.

Use the **`no`** form of this command to restore the default Hello packet interval.

1.14.6 Examples

The following example shows how to configure the **fa4/1** interface to send Hello packets every **20** seconds for IS-IS **level-2** routing:

```
[local]Redback(config-ctx)#router isis ip-backbone
[local]Redback(config-isis)#interface fa4/1
[local]Redback(config-isis-if)#hello interval 20 level-2
```

1.15 hello interval (LDP)

`hello interval` ***`seconds`***

`default fault hello interval`

1.15.1 Purpose

Configures the interval between consecutive Label Distribution Protocol (LDP) link Hello messages used in basic LDP discovery.

1.15.2 Command Mode

LDP router configuration

1.15.3 Syntax Description

seconds	Number of seconds between consecutive LDP link Hello messages. The range of values is 5 to 1,200.

1.15.4 Default

The default LDP link Hello interval is five seconds.

1.15.5 Usage Guidelines

Use the **hello interval** command to configure the interval between consecutive LDP link Hello messages used in basic LDP discovery.

If the Hello interval is explicitly configured, then the specified value is used to control the link Hello interval regardless of the link Hello hold time; however, if the Hello interval is not explicitly configured, the Hello interval used is the negotiated LDP link Hello hold time divided by three. The negotiated LDP link Hello holdtime is the lesser of the received LDP link Hello hold time and the locally configured LDP link Hello hold time.

Use the **hello holdtime** command in LDP router configuration mode to change the locally configured LDP link Hello hold time.

Use the **targeted-hello interval** command in LDP router configuration mode to change the locally configured LDP targeted hello interval.

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

1.15.6 Examples

The following example illustrates the configuration of an LDP link Hello interval of **10** seconds:

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

[local]Redback(config-ldp)#hello interval 10
```

1.16 hello-interval (OSPF)

hello-interval *interval*

{**no** | **default**} **hello-interval**

1.16.1 Purpose

Configures the interval at which Open Shortest Path First (OSPF) or OSPF Version 3 (OSPFv3) Hello packets are sent out through the specified interface, sham link, or virtual link.

1.16.2 Command Mode

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

1.16.3 Syntax Description

interval	Interval, in seconds, between Hello packets. The range of values is 1 to 65,535; the default value is 10. This value must be the same for all devices that attempt to establish adjacencies over a shared subnet.

1.16.4 Default

The default interval between Hello packets is 10 seconds for broadcast and point-to-point (P2P) interfaces, and 30 seconds for point-to-multipoint (P2MP) and nonbroadcast multiaccess (NBMA) networks.

1.16.5 Usage Guidelines

Use the **hello-interval** command to configure the interval at which OSPF or OSPFv3 Hello packets are sent out through the specified interface, sham link, or virtual link.

Hello packets are sent at a fixed interval on all interfaces, sham links, and virtual links to establish and maintain neighbor relationships. This interval must be the same on all OSPF or OSPFv3 routers on an IP subnet. The smaller the Hello interval, the faster topological changes are detected; however, a smaller interval results in additional traffic.

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

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

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

Use the **no** or **default** form of this command to return the interval to its default setting of 10 seconds.

1.16.6 Examples

The following example sets the interval between Hello packets to **12** seconds:

```
[local]Redback(config-ospf-if)#hello-interval 12
```

1.17 hello interval (RSVP)

hello interval ***interval***

{no | default} hello interval

1.17.1 Purpose

Enables Resource Reservation Protocol (RSVP) Hello messages for an interface and specifies the interval at which the messages are sent.

1.17.2 Command Mode

RSVP interface configuration

1.17.3 Syntax Description

interval	Amount of time, in seconds, between consecutive RSVP Hello messages. The range of values is 1 to 60.

1.17.4 Default

RSVP Hello messages are disabled.

1.17.5 Usage Guidelines

Use the **hello interval** command to enable RSVP Hello messages for an interface and specify the interval at which the messages are sent.

RSVP Hello messages allow the router to detect the loss of RSVP peer adjacencies, such as when a neighboring router restarts or the link fails. At regular intervals, RSVP Hello messages containing a HELLO REQUEST object are sent to all adjacent RSVP neighbors. Neighbors receiving the Hello message generate and send an RSVP Hello message containing a HELLO ACK object, which acknowledges that it received the original RSVP Hello message. If a router stops receiving the RSVP Hello message acknowledgements, then it declares that the peer adjacency is down.

Note: RSVP Hello messages must be enabled on the interface and the neighbor to which it connects for RSVP graceful restart to function properly.

Use the **`hello keep-multiplier`** command to configure the number of lost (unacknowledged) RSVP Hello messages that can be missed by a neighbor before it declares that the peer adjacency is down.

Use the **`no`** or **`default`** form of this command to disable the sending of RSVP Hello messages.

1.17.6 Examples

The following example shows how to configure the **test12** interface to send RSVP Hello messages at intervals of **10** seconds:

```
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#interface test12
[local]Redback(config-rsvp-if)#hello interval 10
```

1.18 hello-interval (spanning-tree)

`hello-interval` *`sec`*

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

1.18.1 Purpose

Sets the interval between the sending of bridge protocol data units (BPDUs).

1.18.2 Command Mode

Spanning-tree configuration

1.18.3 Syntax Description

sec	Interval between BPDUs in seconds. The Hello interval is either 1 or 2 seconds and must be in whole seconds.

1.18.4 Default

The default Hello interval is 2 seconds.

1.18.5 Usage Guidelines

Use the **hello-interval** command to set the interval between sending BPDUs, that is, Spanning Tree Protocol Hello packets. This command applies when the current bridge is the root bridge.

1.18.6 Examples

The following example shows how to set the forward delay, maximum 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
```

1.19 hello keep-multiplier

```
hello keep-multiplier multiplier

default hello keep-multiplier
```

1.19.1 Purpose

Configures the number of lost (unacknowledged) Resource Reservation Protocol (RSVP) Hello messages that can be missed by a neighbor before it declares that the peer adjacency is down.

1.19.2 Command Mode

RSVP interface configuration

1.19.3 Syntax Description

multiplier	Number of RSVP Hello messages a neighbor can miss before it declares that the peer adjacency is down. The range of values is 3 to 255.

1.19.4 Default

The default keep multiplier value is 3 messages.

1.19.5 Usage Guidelines

Use the **hello keep-multiplier** command to configure the number of lost (unacknowledged) RSVP Hello messages that can be missed by a neighbor before it declares that the peer adjacency is down.

The hello keep multiplier value is used to calculate the Hello time to die (TTD) interval. The Hello TTD interval is a fixed time interval, after which the RSVP neighbor is taken down if no RSVP hello reply is received.

The Hello TTD interval for RSVP is calculated using the following formula:

(hello keep-multiplier x 2 + 1) x hello interval

Use the **default** form of this command to return to the default RSVP Hello keep multiplier value of 3.

1.19.6 Examples

The following example specifies that **15** RSVP Hello messages can be missed (unacknowledged) by a neighbor before it declares the RSVP peer adjacency down:

```
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#interface rsvp05
[local]Redback(config-rsvp-if)#hello keep-multiplier 15
```

1.20 hello multiplier

hello multiplier ***multiplier*** [**level-1** | **level-2**]

```
no hello multiplier
```

1.20.1 Purpose

Determines how many Intermediate System-to-Intermediate System (IS-IS) Hello packets can be missed by a neighbor before the SmartEdge router declares that the adjacency is down.

1.20.2 Command Mode

IS-IS interface configuration

1.20.3 Syntax Description

`multiplier`	Number of IS-IS Hello packets a neighbor can miss. The range of values is 3 to 1,000; the default value is 3.
`level-1`	Optional. Configures the Hello multiplier independently for level 1 adjacencies independently.
`level-2`	Optional. Configures the Hello multiplier independently for level 2 adjacencies independently.

1.20.4 Default

The Hello multiplier is 3. When you enter this command without specifying either IS-IS level 1 or level 2 routing, the Hello multiplier value is the same for both levels.

1.20.5 Usage Guidelines

Use the **`hello multiplier`** command to determine how many IS-IS Hello packets can be missed by a neighbor before the SmartEdge router declares that the adjacency is down.

The advertised hold time in IS-IS Hello packets is the value of the *`multiplier`* argument multiplied by the value of the *`seconds`* argument set through the **`hello interval`** command (in IS-IS interface configuration mode). The advertised holdtime is also known as the IS-IS router dead interval.

The Hello multiplier can be configured independently for level 1 and level 2, except on serial point-to-point interfaces. The **`level-1`** and **`level-2`** keywords are used on multiaccess networks or LAN interfaces. The Hello multiplier and the Hello interval can be different between different devices in one area.

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

1.20.6 Examples

The following example shows how to configure the neighbor to determine that an adjacency has gone down after **5** Hello packets are missed:

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

[local]Redback(config-isis)#interface fa4/1

[local]Redback(config-isis-if)#hello multiplier 5 level-2
```

1.21 hello padding

hello padding {**always** | **first-only** | **never**}

no hello padding

1.21.1 Purpose

Configures the size of Intermediate System-to-Intermediate System (IS-IS) Hello packets sent on the interface.

1.21.2 Command Mode

IS-IS interface configuration

1.21.3 Syntax Description

always	Specifies that Hello packets should always be padded up to a maximum transmission unit (MTU) size. This is the default behavior.
first-only	Specifies that only the initial Hello packets are padded up to the MTU size.
never	Specifies that Hello packets are not padded to an MTU size.

1.21.4 Default

By default, first-only Hello packets are padded up to the MTU size.

1.21.5 Usage Guidelines

Use the **`hello padding`** command to configure the size of IS-IS Hello packets sent on the interface.

Use the **`always`** keyword if permanent checking of an MTU size in both directions is preferred and bandwidth is not important. Use the **`first-only`** keyword to balance between ensuring MTU integrity and saving bandwidth. Use the **`never`** keyword to allow for maximum bandwidth efficiency with no MTU integrity protection.

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

1.21.6 Examples

The following example shows how to pad Hello packets up to the MTU size until the adjacency is established in both directions:

```
[local]Redback(config-ctx)#router isis ip-backbone
[local]Redback(config-isis)#interface fa4/1
[local]Redback(config-isis-if)#hello padding first-only
```

1.22 hello-timer

`hello-timer` *`interval`*

{**`no`** | **`default`**} **`hello-timer`**

1.22.1 Purpose

Specifies the amount of time that the SmartEdge router waits before sending a Hello control message to a Layer 2 Tunneling Protocol (L2TP) peer if there has been no control message activity between the peers.

1.22.2 Command Mode

L2TP peer configuration

1.22.3 Syntax Description

`interva l`	Amount of time in seconds that the SmartEdge router waits before sending an L2TP Hello packet. The range of values is 0 to 3,600; the default value is 300.

1.22.4 Default

The SmartEdge router waits 300 seconds before sending an L2TP Hello packet.

1.22.5 Usage Guidelines

Use the **`hello-timer`** command to specify the amount of time that the SmartEdge router waits before sending a Hello control message to an L2TP peer if there has been no control message activity between the peers. The Hello control message is used as a keepalivemechanism to determine if a link has failed between the L2TP access concentrator (LAC) and L2TP network server (LNS).

Note: We do not recommend that you change the value of the ***`interval`*** argument from the default unless you are specifically requested to do so by a technical support representative.

Use the **`no`** or **`default`** form of this command to set the value of the ***`interval`*** argument to the default of 300 seconds.

1.22.6 Examples

The following example shows how to set the amount of time that the SmartEdge router waits before sending a Hello control message to an L2TP peer to **120** seconds (two minutes):

```
[local]Redback(config-l2tp)#hello-timer 120
```

1.23 help

`help`

1.23.1 Purpose

Describes how to use the question mark (**`?`**) command to display help about available commands or command options.

1.23.2 Command Mode

All modes

1.23.3 Syntax Description

This command has no keywords or arguments.

1.23.4 Default

None

1.23.5 Usage Guidelines

Use the **help** command to display a brief description of the **?** command. You can enter this command in any mode. The output describes full help, which you use to identify all possible arguments for a command or command keyword, and partial help, which you use to identify how to complete a command keyword.

1.23.6 Examples

The following example displays the output from the **help** command:

```
[local]Redback>help


Help may be requested at any point in a command by entering

a question mark '?'.  If nothing matches, the help list will

be empty and you must backup until entering a '?' shows the

available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a

   command argument (e.g. 'show ?') and describes each possible

   argument.

2. Partial help is provided when an abbreviated argument is entered

   and you want to know what arguments match the input

   (e.g. 'show pr?'.)
```

1.24 high-circuit-count

high-circuit-count

no high-circuit-count

1.24.1 Purpose

Increases the maximum number of circuits on the 1-port 10 gigabit Ethernet card (10ge-1-port) to 32,000.

1.24.2 Command Mode

Card configuration

1.24.3 Syntax Description

This command has no keywords or arguments.

1.24.4 Default

The maximum number of circuits is 16,000.

1.24.5 Usage Guidelines

Use the **`high-circuit-count`** command to increase the maximum number of circuits on the 1-port 10 gigabit Ethernet card to 32,000.

Note: Entering or leaving the high-circuit-count mode of operation causes the card to reload. Performance of the card might be reduced in high-circuit-count mode.

1.25 hold-time

`hold-time` ***`seconds`***

{**`no`** | **`default`**} **`hold-time`**

1.25.1 Purpose

Specifies the number of seconds for the router to wait before it brings down a dynamic tunnel that has no active bindings or visitors.

1.25.2 Command Mode

dynamic tunnel profile configuration

1.25.3 Syntax Description

seconds	Number of seconds for the router chassis to wait before it brings down a dynamic tunnel that has no active bindings or visitors. The range of values is 0 through 3600 seconds.

1.25.4 Default

30 seconds

1.25.5 Usage Guidelines

Use the **hold-time** command to specify the number of seconds for the SmartEdge router to wait before it brings down a dynamic tunnel that has no active bindings or visitors.

Use the **no** or **default** form of this command to restore the setting to its default value of 30 seconds.

1.25.6 Examples

The following example shows how to set the device to wait to `10` seconds before it brings down a dynamic tunnel that has no active bindings or visitors for profile `prof1`:

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

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

[local]Redback(config-mip)#dynamic-tunnel-profile prof1

[local]Redback(config-mip-dyn-tun1-profile)#hold-time 10

[local]Redback(config-mip-dyn-tun1-profile)#end
```

1.26 home-agent

home-agent

no home-agent

1.26.1 Purpose

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

1.26.2 Command Mode

- Mobile IP configuration

1.26.3 Syntax Description

This command has no keywords or arguments.

1.26.4 Default

No HA instances are created.

1.26.5 Usage Guidelines

Use the **home-agent** command to create or select an HA instance in this context and access HA configuration mode.

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

1.26.6 Examples

The following example shows how to create an HA instance in the `ha context`:

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

1.27 home-agent-peer

home-agent-peer ***ip-addr***

no home-agent-peer ***ip-addr***

1.27.1 Purpose

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

1.27.2 Command Mode

- FA configuration

1.27.3 Syntax Description

ip-addr	IP address for this HA peer.

1.27.4 Default

No HA peers are created.

1.27.5 Usage Guidelines

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

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

1.27.6 Examples

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

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

1.28 hop-limit (CSPF)

hop-limit *number*

no hop-limit

1.28.1 Purpose

For Constrained Shortest Path First (CSPF), specifies the maximum number of routers that the label-switched path (LSP) can traverse, including the ingress and egress routers.

1.28.2 Command Mode

Constraint configuration

1.28.3 Syntax Description

number	Maximum number of routers the LSP can traverse. The range of values is 2 to 255.

1.28.4 Default

The default hop limit is 255.

1.28.5 Usage Guidelines

For CSPF, use the **hop-limit** command to specify the maximum number of routers that the LSP can traverse, including the ingress and egress routers.

Use the **no hop-limit** form of this command to disable the hop limit.

1.28.6 Examples

The following example shows how to configure the maximum number of routers that the LSP can traverse to 10:

```
[local]Redback#configure

[local]Redback(config)#context local

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

[local]Redback(config-rsvp)#constraint constraint1

[local]Redback(config-rsvp-constr)#hop-limit 10
```

1.29 hop-limit (ND)

`hop-limit` ***`number`***

`no hop-limit`

1.29.1 Purpose

Configures the hop limit (the maximum number of routers that IPv6 traffic can traverse) advertised in Neighbor Discovery (ND) Router Advertisement (RA) messages.

1.29.2 Command Mode

- ND router configuration
- ND router interface configuration

1.29.3 Syntax Description

`number`	Number of hops advertised in ND RA messages that are sent by the router or a particular interface. The range of values is 0 to 255. A value of 0 means no hop limit is specified.

1.29.4 Default

The default hop limit is 64.

1.29.5 Usage Guidelines

Use the **`hop-limit`** command to configure the hop limit (the maximum number of routers that IPv6 traffic can traverse) advertised in ND RA messages.

In ND router configuration mode, this command configures the hop limit advertised in ND RA messages that are sent by all interfaces configured under ND router configuration mode.

In ND router interface configuration mode, this command configures the hop limit advertised in ND RA messages sent by a particular interface.

Use the **`no hop-limit`** command to return the hop limit advertised in ND RA messages to a default value of 64 hops.

1.29.6 Examples

The following example illustrates the configuration of a 10-hop limit advertisement in ND RA messages sent by the router:

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#router nd
[local]Redback(config-nd)#hop-limit 10
```

The following example shows how to configure the hop limit advertised by a particular interface in ND RA messages to be `0` so that the hop limit is not specified by the interface :

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface int1
[local]Redback(config-nd-if)#hop-limit 0
```

1.30 http-redirect profile

http-redirect profile {**default** | ***prof-name***} **[ipv6 url] [temporary]**

no http-redirect profile {**default** | ***prof-name***} **[temporary]**

1.30.1 Purpose

In context configuration mode, configures an HTTP redirect profile and enters HTTP redirect profile configuration mode.

In subscriber configuration mode, applies an HTTP redirect profile to a subscriber record, a named subscriber profile, or the default subscriber profile.

1.30.2 Command Mode

- Context configuration
- Subscriber configuration

1.30.3 Syntax Description

default	Specifies the default HTTP redirect profile name.
prof-name	Specifies the HTTP redirect profile name.

ipv6 url	Optional. Specifies the IPv6 redirect url. Both IPv4 and IPv6 traffic can use the same profile.
temporary	Optional. Specifies that the HTTP redirect profile to apply to the subscriber profile is temporary. After the HTTP redirect is processed, the HTTP redirect profile is removed from the subscriber profile.

1.30.4 Default

An HTTP redirect profile is not preconfigured.

1.30.5 Usage Guidelines

Use the **http-redirect profile** command in context configuration mode to configure an HTTP redirect profile and to enter HTTP redirect profile configuration mode. To specify the default HTTP redirect profile, use the keyword **default**.

Note: A shared key is configured in the default HTTP redirect profile. This key is used to encrypt identity attributes associated with a redirected subscriber HTTP session, if VSA 165 is configured in RADIUS.

Use the **http-redirect profile** command in subscriber configuration mode to apply an HTTP redirect profile to a subscriber record, a named subscriber profile, or the default subscriber profile. To specify that the HTTP redirect profile applied to a subscriber profile istemporary, use the keyword **temporary**.

Use the **no** form of this command to do the following:

- In context configuration mode, delete an HTTP redirect profile.
- In subscriber configuration mode, remove an HTTP redirect profile from a subscriber record, a named subscriber profile, or the default subscriber profile.

1.30.6 Examples

The following example configures the HTTP profile, **Redirect**, and enters HTTP redirect profile configuration mode:

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

[local]Redback(config-ctx)#http-redirect profile Redirect

[local]Redback(config-hr-profile)#
```

The following example applies the HTTP profile, **Redirect**, to the **default** subscriber record in the **local** context:

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

[local]Redback(config-sub)#http-redirect profile Redirect
```

The following example shows how to configure the HTTP redirect profile, **Redirect**, to be a temporary HTTP redirect policy, and to apply it to the **default** subscriber record in the **local** context:

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

[local]Redback(config-sub)#http-redirect profile Redirect temporary
```

1.31 http-redirect server

```
http-redirect server

no http-redirect server
```

1.31.1 Purpose

Enables an HTTP server on the controller card and accesses HTTP redirect server configuration mode.

1.31.2 Command Mode

Global configuration

1.31.3 Syntax Description

This command has no keywords or arguments.

1.31.4 Default

The HTTP server is disabled on the controller card.

1.31.5 Usage Guidelines

Use the `http-redirect server` command to enable an HTTP server on the controller card and access HTTP redirect server configuration mode.

Use the **no** form of this command to disable the HTTP server on the controller card.

1.31.6 Examples

The following example enables the HTTP server on the controller card and enters HTTP redirect server configuration mode:

```
[local]Redback(config)#http-redirect server

[local]Redback(config-hr-server)#
```

1.32 icmp-notification

icmp-notification

no icmp-notification

1.32.1 Purpose

Sends ICMP administratively prohibited messages to the sender when the NAT translation cannot be created due to resource or administrative constraints.

1.32.2 Command Mode

- NAT policy configuration
- NAT policy class configuration

1.32.3 Syntax Description

This command has no keywords or arguments.

1.32.4 Default

By default, for all carrier-grade NAT policies, an ICMP destination unreachable message is sent with a code of 13 (Communication administratively prohibited) to the sender when the NAT translation cannot be created.

1.32.5 Usage Guidelines

Use the **icmp-notification** command to send ICMP messages to a sender when the NAT translation cannot be created.

Use the **`no`** form of this command to disable ICMP messages.

1.32.6 Examples

```
[local]Redback(config)#context nat-context
[local]Redback(config-ctx)#nat ?
  logging-profile  Configure NAT logging profile
  policy           Configure NAT policy
[local]Redback(config-ctx)#nat policy nat-policy enhanced
[local]Redback(config-policy-nat)#icmp-notification
```

1.33 idle-character

`idle-character {flags | marks}`

`default idle-character`

1.33.1 Purpose

Specifies the idle character to be sent between packets on a DS-0 channel group, a DS-1 channel, a clear-channel DS-3 channel or port, an E3 port, or an E1 channel or port.

1.33.2 Command Mode

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

1.33.3 Syntax Description

`flags`	Specifies High-Level Data Link Control (HDLC) flag (0x7E) characters to be sent between packets; this is the default.
`marks`	Specifies mark (0xFF) characters to be sent between packets.

1.33.4 Default

The default value is the HDLC flag character.

1.33.5 Usage Guidelines

Use the **idle-character** command to specify the idle character to be sent between packets on a DS-0 channel group, a DS-1 channel, a DS-3 channel or port, or an E1 channel or port.

Use the **default** form of this command to set the idle character to the HDLC flag character.

Note: Some systems interpret the mark character as an abort signal; therefore, the HDLC flag character is preferred.

1.33.6 Examples

The following example shows how to specify the HDLC flag as the idle character on DS-3 channel **1** on port **1** of the channelized OC-12 traffic card in slot **3:**

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

[local]Redback(config-ds3)#idle-character marks
```

1.34 idle-down

idle-down ***seconds***

{**no** | **default**} **idle-down**

1.34.1 Purpose

Enables a watchdog timer to delete any inactive Asynchronous Transfer Mode (ATM) or 802.1Q permanent virtual circuit (PVC) in a range of on-demand PVCs.

1.34.2 Command Mode

- ATM PVC configuration

1.34.3 Syntax Description

seconds	Time (in seconds) to wait before deleting an inactive on-demand 802.1Q or ATM PVC. The range of values is 0 to 86,400; the default value is 0. An inactive on-demand PVC is a circuit in which no active subscriber sessions are present.

1.34.4 Default

The watchdog timer is disabled; inactive 802.1Q or ATM PVCs are not deleted.

1.34.5 Usage Guidelines

Use the **idle-down** command to enable a watchdog timer to delete any inactive ATM or802.1Q PVC in a range of on-demand PVCs. A PVC is inactive if there are no connected subscriber sessions on it.

Note: The inactive circuit is deleted only from memory and becomes dormant (returns to listening mode).

Note: This command is not supported for on-demand ATM PVCs that you have configured with multiprotocol encapsulation.

If the timer is set and a subscriber session is initiated before the timer expires, the timer is cancelled.

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

1.34.6 Examples

The following example shows how to set a watchdog timer to **1** minute for a range of on-demand ATM PVCs on an ATM OC port:

```
[local]Redback(config)#port atm 3/3
[local]Redback(config-atm-oc)#atm pvc on-demand 10:32 through 10:63 profile adam encapsulation pppoe
[local]Redback(config-atm-pvc)#idle-down 60
```

1.35 idle-pattern

idle-pattern ***pattern***

default idle-pattern

1.35.1 Purpose

Configures the idle-pattern settings of a CESoPSN interworking function (IWF).

1.35.2 Command Mode

CESoPSN or SAToP Config Modes.

1.35.3 Syntax Description

pattern	This 8-bit pattern determines the value to be played when CE bound packets have over/underflow the jitter buffer, or are missing for any reason.The range is 0x00 to 0xff; the default pattern is 0x54 for E1 and 0x3f for T1.

1.35.4 Default

Default pattern is 0x54 for E1 and 0x3f for T1.

1.35.5 Usage Guidelines

This is user defined pattern that will be played on the TDM channel.

1.35.6 Examples

The following example shows how to configure the idle-pattern on a CES IWF:

```
[local]Redback(config)#port ds0s 1/1:1:1:1
[local]Redback(config-ds0-ces)#timeslot 16
[local]Redback(config-ds0-ces)#l2vpn local
[local]Redback(config-ds0-ces)#cesopsn
[local]Redback(config-ds0-cesopsn)#end-to-end-delay latency 4 jitter 160 outage-criteria 1 10
[local]Redback(config-ds0-cesopsn)#idle-pattern 0x3f
```

1.36 igmp access-group

igmp access-group *acl-name*

no igmp access-group *acl-name*

1.36.1 Purpose

Configures Internet Group Management Protocol (IGMP) membership on an interface.

1.36.2 Command Mode

Interface configuration

1.36.3 Syntax Description

acl-name	Name of the access control list (ACL) used to filter IGMP membership.

1.36.4 Default

None

1.36.5 Usage Guidelines

Use the **`igmp access-group`** command to configure IGMP membership on an interface.

Note: Only multicast groups permitted by the ACL are accepted on the interface.

Use the **`no`** form of this command to remove the ACL filter, and allow all groups to have access on an interface.

1.36.6 Examples

The following example configures IGMP membership using the ACL **igmp_mem03:**

```
[local]Redback(config-ctx)#interface enet01
[local]Redback(config-if)#igmp access-group igmp_mem03
```

1.37 igmp group-bandwidth

`igmp group-bandwidth` *`rate`* **`group-list`** *`acl-name`* [**`qos-adjust`** [**`average-packet-size`** *`bytes`*] [**`no-oif`**]]

`no igmp group-bandwidth` *`rate`* **`group-list`** *`acl-name`* [**`qos-adjust`** [**`average-packet-size`**] [**`no-oif`**]]

1.37.1 Purpose

Configures the estimated bandwidth required by each of the specified multicast groups.

1.37.2 Command Mode

Context configuration

1.37.3 Syntax Description

`rate`	Estimated rate in kbps of network bandwidth required to transport each group. The range is 1 to 65,535.
`group-list` *`acl-name`*	Access control list (ACL) name used to specify the criteria to be used to match IGMP join requests received by the SmartEdge router to the multicast group and bandwidth.
`qos-adjust`	Optional. Indicates that QoS adjustment is to be applied to circuits configured with the **`multicast adjust-qos-rate`** command in its IGMP profile when they join matching IGMP groups.
`average-packet-size` *`bytes`*	Optional. Specifies the average size, in bytes, of packets belonging to matching multicast groups. This value is used to help calculate QoS adjustments to the PWFQ scheduling rate for remote multicast replication (RMR) when a QoS overhead profile is in effect on the circuit. If this parameter is not specified, a default packet size of 1,500 bytes applies. This option is only applicable and configurable if the **`qos-adjust`** keyword is specified.
`no-oif`	Optional. Indicates that, for the groups in the group list, outgoing interface (OIF) creation on the SmartEdge router in response to an IGMP join is suppressed. When the OIF creation is suppressed, multicast traffic for the group cannot transit through the SmartEdge router. This option is only applicable and configurable if the **`qos-adjust`** keyword is specified.

1.37.4 Default

By default, the OIF state creation on the SmartEdge router in response to an IGMP join is not suppressed.

1.37.5 Usage Guidelines

Use the **`igmp group-bandwidth`** command to configure the estimated network bandwidth required by multicast groups that match the criteria specified in the referenced ACL. In conjunction with the **`igmp maximum-bandwidth`** command, this command is used to limit the maximum amount of port bandwidth that can be used for multicast traffic. Alternately, if the optional **`qos-adjust`** keyword is specified, you can use this command to effect QoS adjustments for RMR. See *QoS Adjustments for RMR* for more information.

Before configuring the estimated group bandwidth, you should know the sending rate on each group.

Note: You can use inbound rate limiting to ensure that the estimated bandwidth of the groups is not exceeded.

When you use the `qos-adjust` keyword, you can configure the `no-oif` keyword to suppress the creation of OIF. If you do not configure the `no-oif` keyword, an OIF is created for the multicast route, allowing the multicast traffic to transit through the SmartEdge router.

Use the `no` form of this command to delete a group bandwidth profile or to restore the default behavior for an option.

1.37.6 Examples

The following example shows how to configure an estimated bandwidth rate of **512** Kbps for each group matching the ACL **grp936**:

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

[local]Redback(config-ctx)#igmp group-bandwidth 512 group-list grp936
```

The following example shows how to configure an estimated bandwidth rate of **1000** kbps for each group matching the ACL **grp7** and specify the QoS adjustment to be applied to circuits joining multicast groups matching the ACL **grp7**:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#igmp group-bandwidth 1000 group-list grp7 qos-adjust
```

1.38 igmp join-group

`igmp join-group` ***`group-addr`***

`no igmp join-group` ***`group-addr`***

1.38.1 Purpose

Configures a router to join a multicast group.

1.38.2 Command Mode

Interface configuration

1.38.3 Syntax Description

group-addr	Multicast group IP address.

1.38.4 Default

None

1.38.5 Usage Guidelines

Use the **igmp join-group** command to configure a router to join a multicast group on the interface.

Use the **no** form of this command to remove a router from a multicast group.

Caution!

Risk of reduced router performance. If local joins are configured, packets are punted from the Packet Processing ASIC (PPA) to the controller card. To reduce the risk, ensure that data is not sent at high rates for local joins.

1.38.6 Examples

The following example configures a router to join multicast group **224.1.1.1:**

```
[local]Redback(config-ctx)#interface enet01
[local]Redback(config-if)#igmp join-group 224.1.1.1
```

1.39 igmp last-member-query-interval

igmp last-member-query-interval ***interval***

{**no** | **default**} **igmp last-member-query-interval** ***interval***

1.39.1 Purpose

Configures the interval at which the router sends Internet Group Management Protocol (IGMP) group-specific host query messages.

1.39.2 Command Mode

Interface configuration

1.39.3 Syntax Description

`interval`	Interval, in milliseconds, at which IGMP group-specific host query messages are sent.

1.39.4 Default

The default last member query interval is 1,000 milliseconds (1 second).

1.39.5 Usage Guidelines

Use the **`igmp last-member-query-interval`** command to configure the interval at which the router sends IGMP group-specific host query messages.

Use the **`no`** or **`default`** form of this command to set the interval to the default value of 1,000 milliseconds.

1.39.6 Examples

The following example sets the last member query interval to **2500** milliseconds (2.5 seconds):

```
[local]Redback(config-ctx)#interface enet01
[local]Redback(config-if)#igmp last-member-query-interval 2500
```

1.40 igmp maximum-bandwidth

`igmp maximum-bandwidth` *`rate`* [**`percent`**]

`no igmp maximum-bandwidth`

1.40.1 Purpose

Configures the total maximum bandwidth allowed for multicast data traffic on a port or channel.

1.40.2 Command Mode

- ATM configuration

- AU-3 configuration
- port configuration
- STM-1 configuration

1.40.3 Syntax Description

rate	Maximum rate in Kbps when the **percent** keyword is not specified. When the **percent** keyword is specified, the *rate* value is taken as a percentage of the port bandwidth, and not a rate in Kbps.
percent	Optional. Specifies that the *rate* value is taken as a percentage of the port bandwidth, and not a rate in Kbps.

1.40.4 Default

None

1.40.5 Usage Guidelines

Use the **igmp maximum-bandwidth** command to configure the total maximum bandwidth allowed for multicast data traffic on a port or channel.

Note: If the addition of a new group would cause the bandwidth usage on this port to exceed the maximum bandwidth, and if a subscriber with a lower priority exists on this port, the lower priority group is dropped to reclaim the bandwidth; otherwise, the new group is dropped.

Use the **no** form of this command to remove maximum bandwidth restrictions a the port or channel.

1.40.6 Examples

The following example configures a maximum bandwidth of **300** Kbps for an Ethernet port in slot **7:**

```
[local]Redback(config)#port ethernet 7/1
[local]Redback(config-port)#igmp maximum-bandwidth 300
```

The following example configures a maximum bandwidth of **35** percent of an Ethernet port's maximum bandwidth:

```
[local]Redback(config)#port ethernet 7/1
[local]Redback(config-port)#igmp maximum-bandwidth 35 percent
```

1.41 igmp mtrace-prohibit

igmp mtrace-prohibit

1.41.1 Purpose

Ensures that all mtrace queries are received within the administratively scoped domain of the router.

1.41.2 Command Mode

Context configuration

1.41.3 Syntax Description

This command has no keywords or arguments.

1.41.4 Default

None

1.41.5 Usage Guidelines

Use the **igmp mtrace-prohibit** command to ensure that all mtrace queries are received within the administratively scoped domain of the router.

1.41.6 Examples

The following example ensures that all mtrace queries are received within the administratively scoped domain of the router:

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

1.42 igmp query-interval

igmp query-interval ***interval***

{**no** | **default**} **igmp query-interval** ***interval***

1.42.1 Purpose

Configures the interval at which the router sends Internet Group Management Protocol (IGMP) host query messages.

1.42.2 Command Mode

Interface configuration

1.42.3 Syntax Description

interval	Interval, in seconds, at which IGMP host query messages are sent.

1.42.4 Default

The default IGMP query interval is 60 seconds (1 minute).

1.42.5 Usage Guidelines

Use the **igmp query-interval** command to configure the interval at which the router sends IGMP host query messages. The multicast router sending the IGMP host query messages is the one on the subnet with the lowest IP address.

Use the **no** or **default** form of this command to set the interval to the default value of 60 seconds.

1.42.6 Examples

The following example sets the IGMP query interval to 120 seconds:

```
[local]Redback(config-ctx)#interface enet01
[local]Redback(config-if)#igmp query-interval 120
```

1.43 igmp query-max-response-time

igmp query-max-response-time *interval*

{**no** | **default**} **igmp query-max-response-time** *interval*

1.43.1 Purpose

Configures the maximum response time specified in Internet Group Management Protocol (IGMP) queries.

1.43.2 Command Mode

Interface configuration

1.43.3 Syntax Description

interval	Interval, in seconds, specified in IGMP queries.

1.43.4 Default

The default IGMP query-max-response-time is 10 seconds.

1.43.5 Usage Guidelines

Use the **igmp query-max-response-time** command to configure the maximum response time specified for IGMP queries.

Use the **no** or **default** form of this command to set the interval to the default value of 10 seconds.

1.43.6 Examples

The following example sets the maximum response time to **20** seconds:

```
[local]Redback(config-ctx)#interface enet01
[local]Redback(config-if)#igmp query-max-response-time 20
```

1.44 igmp query-solicitation

igmp query-solicitation

no igmp query-solicitation

1.44.1 Purpose

Enables and disables the generation of IGMP general query response messages on an interface.

1.44.2 Command Mode

interface configuration

1.44.3 Syntax Description

This command has no keywords or arguments.

1.44.4 Default

The sending of IGMP general query messages is disabled on an interface.

1.44.5 Usage Guidelines

Use the **`igmp query-solicitation`** command to enable the generation of IGMP general query response messages on an interface.

If query solicitation is enabled on a circuit, query solicitation messages are sent from a circuit when an STP-port-unblock event occurs, or the state of a circuit changes from down to up.

When an IGMP router receives a general leave message from a circuit, it responds with an IGMP general query that records topology changes.

Note: For IGMP query solicitation to work, you must enable IGMP query solicitation on both the bridge from which you want to forward query solicitation messages to the router, and on the interface over which IGMP query messages and general response messages are exchanged. Use the **`igmp query-solicitation`** command in IGMP snooping configuration mode to enable the generation of IGMP query solicitation messages by a bridge.

Use the **`no`** form of this command to disable the generation of IGMP general query response messages on an interface.

1.44.6 Examples

The following example shows how to enable the generation of IGMP general query response messages on an interface:

```
[local]Redback(config-ctx)#interface enet01
[local]Redback(config-if)#igmp query-solicitation
```

1.45 igmp robust

`igmp robust` ***`packet-number`***

{**`no`** | **`default`**} **`igmp robust`*****`packet-number`***

1.45.1 Purpose

Configures the Internet Group Management Protocol (IGMP) robustness variable.

1.45.2 Command Mode

Interface configuration

1.45.3 Syntax Description

packet-number	Robustness value. The range of values is 2 to 7; the default value is 2.

1.45.4 Default

The default robustness value is 2.

1.45.5 Usage Guidelines

Use the **igmp robust** command to configure the IGMP robustness value. The group membership interval, other querier present interval, startup query count, and last member query count are all determined by the robustness value.

Use the **no** or **default** form of this command to set the robustness to the default value of 2.

1.45.6 Examples

The following example configures the robustness variable to **4:**

```
[local]Redback(config-ctx)#interface enet01
[local]Redback(config-if)#igmp robust 4
```

1.46 igmp service-profile

igmp service-profile ***prof-name***

{**no** | **default**} **igmp service-profile** ***prof-name***

1.46.1 Purpose

In context configuration mode, creates a service profile and enters IGMP service profile configuration mode.

In interface configuration mode, enables the specified service profile on the interface.

1.46.2 Command Mode

- Context configuration
- Interface configuration

1.46.3 Syntax Description

prof-name	In context configuration mode, name of the service profile to be created. In interface configuration mode, name of an existing service profile to enable on the interface.

1.46.4 Default

None

1.46.5 Usage Guidelines

Use the **igmp service-profile** command in context configuration mode to create a service profile and enters IGMP service profile configuration mode.

Use the **igmp service-profile** in interface configuration mode to enable the specified service profile on the interface.

Use the **no** form of this command in context configuration mode to delete the specified service profile.

Use the **no** form of this command in interface configuration mode to disable the specified service profile on the interface.

The **no access-group** command does not offer an optional input for an ***acl-name***.

Use the **default** form of this command in context configuration mode to return all parameters in an existing IGMP service profile to their default settings.

Use the `default` form of this command in interface configuration mode to return all parameters in an existing IGMP service profile to their default settings for the specified interface only.

1.46.6 Examples

The following example creates a service profile, **pro332**, and enters IGMP service profile configuration mode:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#igmp service-profile pro332
[local]Redback(config-igmp-service-profile)#
```

The following example enables a service profile, **pro332**, on the interface, **foo:**

```
[local]Redback(config-ctx)#interface foo
[local]Redback(config-if)#igmp service-profile pro332
```

1.47 igmp snooping

`igmp snooping`

`no igmp snooping`

1.47.1 Purpose

Enables IGMP snooping on a particular bridge and enters IGMP snooping configuration mode for that bridge.

1.47.2 Command Mode

Bridge configuration

1.47.3 Syntax Description

This command has no keywords or arguments.

1.47.4 Default

IGMP snooping is disabled on the bridge.

1.47.5 Usage Guidelines

Use the **igmp snooping** command to enable IGMP snooping on a particular bridge and enter IGMP snooping configuration mode for that bridge. After you are in IGMP snooping configuration mode, you can modify the default IGMP snooping behavior for the bridge, if desired.

Use the **no** form of this command to disable IGMP snooping on a bridge.

1.47.6 Examples

The following example shows how to enable IGMP snooping on the bridge called ny1 and enter IGMP snooping configuration mode for that bridge:

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#bridge ny1
[local]Redback(config-bridge)#igmp snooping
[local]Redback(config-igmp-snooping)#
```

1.48 igmp snooping profile

igmp snooping profile ***profile-name***

no igmp snooping profile ***profile-name***

1.48.1 Purpose

In global configuration mode, creates an IGMP snooping profile and enters IGMP snooping profile configuration mode.

In bridge configuration mode, adds an IGMP snooping profile to a bridge profile.

1.48.2 Command Mode

- Global configuration
- Bridge profile configuration

1.48.3 Syntax Description

profile-name	Unique name that identifies the IGMP snooping profile.

1.48.4 Default

IGMP snooping is disabled on a bridge, and no IGMP snooping profiles are attached to a bridge profile.

1.48.5 Usage Guidelines

In global configuration mode, use the **`igmp snooping profile`** command to create an IGMP snooping profile and enter IGMP snooping profile configuration mode. After you are in IGMP snooping configuration mode, you can modify the default IGMP snooping profile parameters, if desired.

In bridge profile configuration mode, use the **`igmp snooping profile`** command to add an IGMP snooping profile to a bridge profile. After you add an IGMP snooping profile to a bridge profile, the settings in the IGMP snooping profile are applied to all circuits that belong to the bridge profile.

Use the **`no`** form of this command to remove an IGMP snooping profile from the router or from a bridge profile.

Note: When entered in IGMP snooping profile configuration mode, the **`no access-group`** command syntax does not include the optional ***`acl-name`*** argument because only one access group can be configured for an IGMP snooping profile.

1.48.6 Examples

The following example shows how to create an IGMP snooping profile called `p1` and enter IGMP snooping profile configuration mode:

```
[local]Redback #configure

[local]Redback(config)#igmp snooping profile p1

[local]Redback(config-igmp-snooping-profile)#
```

The following example shows how to add an IGMP snooping profile called `p1` to a bridge profile called `red-bridge1`:

```
[local]Router(config)#bridge profile red-bridge1

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

[local]Router(config-bridge-profile)#commit
```

1.49 igmp verify source subnet

`igmp verify source subnet`

{**`no`** | **`default`**} **`igmp verify source subnet`**

1.49.1 Purpose

Enables IGMP source subnet verification on an interface; the interface accepts only those packets with a matching source IP subnet.

1.49.2 Command Mode

Interface configuration

1.49.3 Syntax Description

This command has no keywords or arguments.

1.49.4 Default

IGMP source subnet verification is disabled; the interface accepts incoming packets from any source.

1.49.5 Usage Guidelines

Use the **`igmp verify source subnet`** command to enable IGMP source subnet verification on an interface; the interface accepts only those packets with a matching source IP subnet. Packets with a nonmatching source IP subnet are dropped.

Note: We recommend enabling IGMP source subnet verification on nonloopback IGMP interfaces; nonloopback IGMP interfaces should accept only those packets that have a source IP subnet that matches the IGMP interface IP subnet. Loopback IGMP interfaces can accept packets from any source.

Use the **`no`** or **`default`** form of this command to disable IGMP source subnet verification on an interface. When IGMP source subnet verification is disabled, the interface accepts incoming packets from any source.

1.49.6 Examples

The following example enables IGMP source subnet verification on the IGMP interface called `igmp-int1`:

```
[local]Redback(config-ctx)#interface igmp-int1
[local]Redback(config-if)#igmp verify source subnet
```

1.50 igmp version

igmp version {1 | 2 | 3}

no igmp version

1.50.1 Purpose

Configures the interface to operate in either Internet Group Management Protocol (IGMP) Version 1, Version 2, or Version 3 mode.

1.50.2 Command Mode

Interface configuration

1.50.3 Syntax Description

1	Configures the interface to operate in IGMP Version 1 mode.
2	Configures the interface to operate in IGMP Version 2 mode.
3	Configures the interface to operate in IGMP Version 3 mode.

1.50.4 Default

The default mode is IGMP Version 2.

1.50.5 Usage Guidelines

Use the **igmp version** command to configure the interface to operate in either IGMP Version 1, Version 2, or Version 3 mode.

Use the **no** form of this command to configure the interface to the default value.

1.50.6 Examples

The following example configures the interface to operate in **IGMP Version 2** mode:

```
[local]Redback(config-ctx)#interface enet01

[local]Redback(config-if)#igmp version 2
```

1.51 ignore

`ignore`

1.51.1 Purpose

Removes the application of the Network Address Translation (NAT) policy to configure the Network Address Translation (NAT) policy or its class to not translate the source IP address of all packets, or classes of packets, traveling across circuits attached to the interface or subscriber to which the NAT policy is applied.

1.51.2 Command Mode

- NAT policy configuration
- Policy group class configuration

1.51.3 Syntax Description

This command has no keywords or arguments.

1.51.4 Default

If no action is configured for the NAT policy, by default, packets are dropped.

1.51.5 Usage Guidelines

Use the **`ignore`** command to remove the application of the NAT policy to configure the Network Address Translation (NAT) policy or its class to not translate the source IP address of all packets, or classes of packets, traveling across circuits attached to the interface or subscriber to which the NAT policy is applied.

1.51.6 Examples

The following example configures the **NAT-2** policy and applies the **NAT-ACL-2** access control list (ACL) to it. Packets that are classified as **NAT-CLASS-2** are ignored; the policy will not be applied to these packets they are forwarded without translation of the source IP address. All other packets, except those defined in the static rule, are dropped.:

```
[local]Redback(config)#context CUSTOMER
[local]Redback(config-ctx)#nat policy NAT-2
[local]Redback(config-policy-nat)#ip static in source 10.0.0.1 171.71.71.1
[local]Redback(config-policy-nat)#access-group NAT-ACL-2
[local]Redback(config-policy-group)#class NAT-CLASS-2
[local]Redback(config-policy-group-class)#ignore
```

1.52 ignore config-seq-num

ignore config-seq-num

no ignore config-seq-num

1.52.1 Purpose

Ignores the change in the configuration sequence number specified in a Label Distribution Protocol (LDP) neighbor's Hello packets.

1.52.2 Command Mode

LDP router configuration

1.52.3 Syntax Description

This command has no keywords or arguments.

1.52.4 Default

The configuration sequence number is not ignored.

1.52.5 Usage Guidelines

Use the **ignore config-seq-num** command to ignore the change in the configuration sequence number specified in an LDP neighbor's hello packets. Normally, a SmartEdge® router will terminate the LDP session when a change in configuration sequence number is detected.

Use the **no** form of this command to acknowledge the change in the configuration sequence number specified in an LDP neighbor's Hello packets.

1.52.6 Examples

The following example causes the SmartEdge® router to ingore the configuration sequence number:

```
[local]Redback(config-ldp)#ignore config-seq-num
```

1.53 igp-shortcut

igp-shortcut

no igp-shortcut

1.53.1 Purpose

Enables Resource Reservation Protocol (RSVP) label-switched paths (LSPs) to serve as Interior Gateway Protocol (IGP) shortcuts to nodes in a network.

1.53.2 Command Mode

- RSVP router configuration
- RSVP LSP configuration

1.53.3 Syntax Description

This command has no keywords or arguments.

1.53.4 Default

IGP shortcuts are disabled.

1.53.5 Usage Guidelines

Use the **igp-shortcut** command to enable RSVP LSPs to serve as IGP shortcuts to nodes in a network. When RSVP LSPs are enabled to serve as IGP shortcuts, Open Shortest Path First (OSPF) can include the RSVP LSPs in its Shortest Path First (SPF) calculation when determining the shortest-path tree to all nodes in a network. In order for IGP shortcuts to work, you must also enable the **mpls igp-shortcut** command in OSPF router configuration mode.

When the **igp-shortcut** command in entered in RSVP router configuration mode, it enables all RSVP LSPs for the specified RSVP routing instance to serve as IPG shortcuts. When entered in RSVP LSP configuration mode, only the specified RSVP LSP is enabled to serve as an IGP shortcut.

For more information about IGP shortcuts, see RFC 3906, *Calculating Interior Gateway Protocol (IGP) Routes Over Traffic Engineering Tunnels*. The IGP shortcut implementation uses shortcuts locally and does not advertise these to its neighbors.

Use the **no** form of this command to disable RSVP LSPs from serving as IGP shortcuts.

1.53.6 Examples

The following example enables the RSVP LSP, **lspfoo**, to serve as an IGP shortcut:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#lsp lspfoo
[local]Redback(config-rsvp-lsp)#igp-shortcut
```

1.54 igp-synchronization timeout

igp-synchronization timeout ***seconds***

no igp-synchronization timeout ***seconds***

1.54.1 Purpose

Sets the maximum number of seconds Label Distribution Protocol (LDP) waits before notifying the Interior Gateway Protocol (IGP) that label exchange is completed, so that IGP can start advertising the normal metric for the link.

1.54.2 Command Mode

LDP router configuration

1.54.3 Syntax Description

timeout*seconds*	Optional. Sets the maximum interval, in seconds, that the LDP waits before notifying the IGP that label exchange is completed. When this interval expires, the IGP begins to advertise the regular metric for the link.

1.54.4 Default

None

1.54.5 Usage Guidelines

Use the **igp-synchronization timeout** command to set the maximum number of seconds Label Distribution Protocol (LDP) waits before notifying the Interior Gateway Protocol (IGP) that label exchange is completed, so that IGP can start advertising the normal metric for the link.

Note: LDP-IGP synchronization is supported in the local context only.

Use the **no** form of this command to remove the interval limitation.

1.54.6 Examples

The following example shows how to configure LDP to wait 100 seconds before notifying the IGP that label exchange is completed:

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

[local]Redback(config-ldp)#igp-synchronization timeout 100
```

1.55 import route-target

import route-target ***ext-com***

no import route-target ***ext-com***

1.55.1 Purpose

Creates a list of import route target extended communities for a specified virtual private network (VPN) context.

1.55.2 Command Mode

BGP address family configuration

1.55.3 Syntax Description

`ext-com`

Route target extended community value that is added to the import target list. The route target extended community value can be expressed in either of the following formats:

- *`asn`*`:`*`nnnn`*, where *`asn`* is the autonomous system number, *`nnnn`* is either a 32-bit integer or a 16-bit integer, depending on the size of the ASN. You can specify the ASN as either a two-byte (two-octet) or four-byte (four-octet) integer. A value of 65535 or lower is interpreted as a two-byte integer, unless you add an `L` suffix (for example, `125L`), in which case it is interpreted as a four-byte integer. A value larger than 65535 is always interpreted as a four-byte integer, and the `L` suffix is optional. If the ASN is two-bytes, then *`nnnn`* is a 32-bit integer. If the ASN is four-bytes, then *`nnnn`* is a 16-bit integer.
- *`ip-addr`*`:`*`nn`*, where *`ip-addr`* is the IP address in the form *`A.B.C.D`* and *`nn`* is a 16-bit integer.

1.55.4 Default

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

1.55.5 Usage Guidelines

Use the **`import route-target`** command to create a list of import route target extended communities for a specified VPN context. You can add multiple target communities on the same line, or you can issue the command multiple times with a single target as the parameter. BGP routes learned from other provider edge (PE) routers that carry a specific route target extended community are imported into all VPN contexts configured with that extended community as an import route target.

Import route targets are used to filter routes from other PE routers before importing the routes into a VPN context.

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

Use the **`no`** form of this command to remove a list of import route target extended communities for a specified VPN context.

1.55.6 Examples

The following example configures the two import route targets, **701:3** and **192.168.1.2:5:**

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

1.56 inactive-timeout

`inactive-timeout` *`timeout-value`*

`no inactive-timeout` *`timeout-value`*

1.56.1 Purpose

Configures the inactive timeout setting in seconds for the flows that use the specified profile .

1.56.2 Command Mode

Flow IP profile configuration

1.56.3 Syntax Description

`timeout-value`	Number of seconds after which a flow that does not have any current activity on it is considered complete (expired). A flow record is created and exported to the external collector. The range for the timeout value is 1-10 seconds.

1.56.4 Default

The default inactive timeout value is 5 seconds.

1.56.5 Usage Guidelines

Use the **`inactive-timeout`** command to configure the inactive timeout setting for the flows that use the specified profile, in seconds. Transient-state TCP inactive timeouts are 2 seconds (coming up) and 1 second (going down). Flows without current activity are considered expired and exported to an external collector.

1.56.6 Examples

The following example sets the timeout value for the inactive timeout to 10 seconds:

```
[local]Redback# configure
[local]Redback(config)# flow ip profile p1
[local]Redback(config-flow-ip-profile)# inactive-timeout 10
```

1.57 inbound-refresh udp

1.57.1 Purpose

Configures inbound refresh behavior for inbound UDP traffic.

1.57.2 Command Mode

- NAT policy configuration
- NAT policy class configuration

1.57.3 Syntax Description

udp	Specifies UDP traffic.

1.57.4 Default

Inbound refresh UDP is enabled.

1.57.5 Usage Guidelines

Use the **inbound-refresh udp** command to configure inbound refresh behavior for inbound UDP traffic. This can be useful for applications with no outgoing UDP traffic. You can apply inbound refresh settings at the class level, both for regular classes and the default class.

The **no inbound-refresh udp** command disables refreshing.

Note: To configure the **`no inbound-refresh udp`**, you must first configure a pool or a ignore action. The system does not allow you to configure inbound refresh for UDP in a class in the NAT policy with a drop action. If you do, the following error message appears:

```
"% not supported combination of commands in a NAT
policy/class"
```

1.57.6 Examples

The following example shows you how to configure the refresh behavior for inbound UDP traffic.

```
[local]rock1200(config)#context na-context
[local]rock1200(config-ctx)#nat policy nat-policy enhanced
[local]rock1200(config-policy-nat)#pool nat-pool nat-context
[local]rock1200(config-policy-nat)#inbound-refresh udp
```

1.58 ingress

`ingress` ***`ingress-addr`***

1.58.1 Purpose

Specifies the IP address of the ingress label-switched router (LSR) in a Resource Reservation Protocol (RSVP) label-switched path (LSP).

1.58.2 Command Mode

RSVP LSP configuration

1.58.3 Syntax Description

`ingress-addr`	IP address of the ingress LSR.

1.58.4 Default

None

1.58.5 Usage Guidelines

Use the **`ingress`** command to specify the IP address of the ingress LSR in an RSVP LSP. The ingress LSR is an edge LSR that forwards packets into a network, and is the first router in the chain of routers that constitute an LSP.

Note: An ingress IP address does not have to be specified for an RSVP LSP. If it is not specified, the IP address of the interface used to reach the egress IP address is used. If the interface changes, the ingress IP address will also change; however, if an ingress IP address is specified, then the specified address is always used.

1.58.6 Examples

The following example configures the ingress IP address to 192.168.1.5 for the RSVP LSP, lsp01:

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

[local]Redback(config-rsvp)#lsp lsp01

[local]Redback(config-rsvp-lsp)#ingress 192.168.1.5
```

1.59 instant-leave

```
instant-leave

no instant-leave
```

1.59.1 Purpose

Enables Instant Leave on the interface.

1.59.2 Command Mode

IGMP service profile configuration

1.59.3 Syntax Description

This command has no keywords or arguments.

1.59.4 Default

Instant Leave is disabled.

1.59.5 Usage Guidelines

Use the **`instant-leave`** command to enable Instant Leave on the interface.

Instant Leave allows Internet Group Management Protocol (IGMP) to perform a 0-delay leave upon receiving an IGMP Version 2 (IGMPv2) leave message. If the router is an IGMP querier, it sends an IGMP last member query with a 100 ms last member query response time; however, the router does not wait for 100 ms before it prunes off the group. This allows channel surfing applications to function better.

Use the **no** form of this command to disable Instant Leave on the interface.

1.59.6 Examples

The following example enables Instant Leave on the service profile, **bar:**

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

1.60 interarea-distribute

interarea-distribute {**l1-to-l2** | **l2-to-l1**} [{**prefix-list** | ***ipv6-prefix-list***} ***pl-name***]

no interarea-distribute {**l1-to-l2** | **l2-to-l1**}

1.60.1 Purpose

Distributes routes from one level of an Intermediate System-to-Intermediate System (IS-IS) to another.

1.60.2 Command Mode

IS-IS address family configuration

1.60.3 Syntax Description

l1-to-l2	Distributes routes from level 1 into level 2. By default, level 1 routes are distributed into level 2.
l2-to-l1	Distributes routes from level 2 into level 1. By default, level 2 routes are not distributed into level 1.
prefix-list ***pl-name***	Optional. Name of an IP Version 4 (IPv4) prefix list to be applied.
ipv6-prefix-list ***pl-name***	Optional. Name of an IP Version 6 (IPv6) prefix list to be applied.

1.60.4 Default

Level 1 routes are distributed into level 2. Level 2 routes are not distributed into level 1.

1.60.5 Usage Guidelines

Use the **interarea-distribute** command to distribute routes from one level of IS-IS to another. This distribution is also known as route leaking. If scalability is a concern, you can apply a prefix list and its routing policies to limit the routes that are distributed from one level to another. Use the **ip prefix-list** command (in context configuration mode) to create a prefix list.

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

To distribute routes from level 2 to level 1, all devices inside level 1 must be able to calculate routes based on IS-IS-wide metrics.

Use the **no** form of this command to disable distribution of routes between IS-IS levels.

1.60.6 Examples

The following configuration distributes level 2 routes into level 1 if the routes match the IPv4 prefix list **sys2**, which permits routes that match **23.4.5.0** for prefix length **24** and above. No other routes are distributed into level 1:

```
[local]Redback(config-ctx)#router isis second_tag
[local]Redback(config-isis)#address-family ipv4 unicast
[local]Redback(config-isis-af)#interarea-distribute l2-to-l1 prefix-list sys2
[local]Redback(config-isis-af)#exit
[local]Redback(config-isis)#exit
[local]Redback(config-ctx)#ip prefix-list sys2 permit 23.4.5.0/24 ge 25
```

The following example shows how to configure level 2 routes into level 1 if the routes match the sys4 IPv6 prefix list, which permits routes that match `23.4.5.0` for prefix length `24` and higher. No other routes are distributed into level 1:

```
[local]Redback(config-ctx)#router isis second_tag
[local]Redback(config-isis)#address-family ipv6 unicast
[local]Redback(config-isis-af)#interarea-distribute l2-to-l1 ipv6-prefix-list sys4
[local]Redback(config-isis-af)#exit
[local]Redback(config-isis)#exit
[local]Redback(config-ctx)#ip prefix-list sys4 permit 23.4.5.0/24 ge 25
```

1.61 interface (ANCP)

interface ***if-name***

```
no interface
```

1.61.1 Purpose

Filters incoming new neighbor connections using the interface on which Access Node Control Protocol (ANCP) sessions are transmitted and received for this ANCP neighbor profile.

1.61.2 Command Mode

ANCP neighbor configuration

1.61.3 Syntax Description

`if-name`	Name of the interface; an alphanumeric string with up to 127 characters.

1.61.4 Default

ANCP sessions using this profile can arrive on any interface.

1.61.5 Usage Guidelines

Use the **`interface`** command to filter incoming new neighbor connections using the interface on which ANCP sessions are transmitted and received. The incoming session is matched against the circuit on which it is first connected.

ANCP sessions can arrive on any type of circuit that you have bound to this interface using the **`bind interface`** command (in various configuration modes). For information about the **`bind interface`** command, see the *Command List*.

All packets for ANCP sessions defined in this neighbor profile must arrive on this interface; otherwise, they are discarded.

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

1.61.6 Examples

The following example specifies the **ancp** interface for the circuit on which ANCP sessions are transmitted and received:

```
[local]Redback(config-ancp-neighbor)#interface ancp
```

1.62 interface (BFD)

`interface` {*`if-name`* | *`ip-addr`*}

`no interface` {*`if-name`* | *`ip-addr`*}

1.62.1 Purpose

Enables Bidirectional Forwarding Detection (BFD) on a named interface and enters BFD interface configuration mode.

1.62.2 Command Mode

BFD router configuration

1.62.3 Syntax Description

`if-name`	Interface name.
`ip-addr`	IP address of the interface, in the form *`A.B.C.D`*.

1.62.4 Default

None

1.62.5 Usage Guidelines

Use the **`interface`** command to enable BFD on a named interface and enter BFD interface configuration mode.

The interface must already be configured through the **`interface`** command (in context configuration mode) before BFD can be enabled on it. For more information about the **`interface`** command, see the *Command List*.

Note: If you are configuring BFD on a Resource Reservation Protocol (RSVP) label-switched path (LSP), you must first enable BFD on the RSVP client by entering the **`bfd`** command in RSVP router configuration mode. BFD does not work on RSVP links if it is not first enabled at RSVP level.

Use the **`no`** form of this command to disable BFD on the specified interface.

1.62.6 Examples

The following example enables BFD on the interface, **to_foo:**

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bfd
[local]Redback(config-bfd)#interface to_foo
[local]Redback(config-bfd-if)#
```

1.63 interface (context)

interface *if-name* [**bridge** | {**intercontext** *if-type grp-num*} | **ipsec** [**multibind**] | **loopback** | **multibind** [**lastresort**] | **p2p**]

no interface *if-name* [**bridge** | {**intercontext** *if-type grp-num*} | **ipsec** [**multibind**] | **loopback** | **multibind** [**lastresort**] | **p2p**]

1.63.1 Purpose

Creates a new interface, or selects an existing one for modification, and enters interface configuration mode.

1.63.2 Command Mode

Context configuration

1.63.3 Syntax Description

if-name	Name of the interface; an alphanumeric string with up to 127 characters.
bridge	Optional. Specifies that the interface is a bridged interface.
intercontext	Optional. Specifies that the interface is to link two or more contexts. Use an intercontext interface only for: • Intermediate System-to-Intermediate System (IS-IS) routing • Intercontext static routes • Interfacing to the default multicast domain tree (MDT) group in multicast virtual private networks (VPNs). If you provide an IP address to an intercontext interface, the netmask 255.255.255.255 is not allowed.
if-type	Optional. Type of intercontext interface, according to the following keywords: • **lan**—Specifies a point-to-multipoint (LAN) interface. • **p2p**—Specifies a point-to-point interface.

grp-num	Optional. Intercontext group number; the range of values is 1 to 1,023.
ipsec	Optional. Specifies that the interface is an IPsec interface.
loopback	Optional. Specifies that the interface is a loopback interface.
multibind	Optional. Enables the interface to have multiple circuits bound to it.
lastresort	Optional. Specifies that this multibind interface, called a last-resort interface, is used for any subscriber circuit that attempts to come up and cannot bind to any other interface.
p2p	Optional. When binding to a LAN circuit, indicates to routing protocols, such as IS-IS or Open Shortest Path First (OSPF), that the circuit should be treated as a point-to-point interface from an Interior Gateway Protocol (IGP) perspective.

1.63.4 Default

None

1.63.5 Usage Guidelines

Use the **interface** command to create a new interface, or select an existing one for modification, and enter interface configuration mode. Optionally, you can specify the interface as an intercontext interface or a loopback interface, or enable the interface to have multiple circuits bound to it.

You must bind a port or circuit to an interface (other than a bridged or loopback interface) for data to flow across the interface.

For an IPsec multibind interface, the interface is always unnumbered. Most of the operations listed for the **interface** command are not supported when you configure **interface ipsec multibind**. If a routing protocol is enabled over an IPsec multibind interface, then all tunnels bound to a multibind interface will run the same routing protocol. Static routes cannot be configured to use the IPsec multibind interface.

When there are only two routers over the LAN media, you can configure the interface as a point-to-point interface from a routing protocol perspective by using the **p2p** keyword. For more detailed information, see the Internet Draft, *draft-ietf-isis-igp-p2p-over-lan-03. txt*.

Use the **bind interface** command (in link configuration mode) to bind a port or circuit to a previously created interface in the specified context. Both the interface and the specified context must exist before you enter the **bind interface** command. If either is missing, an error message displays. For more information about this command, see the *Command List*.

Use the **`bridge`** command (in interface configuration mode) to associates the bridge with the interface or subscriber. For more information on this command, see the *Command List*.

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

Caution!

Risk of data loss. Deleting an interface removes all bindings to the interface. To reduce the risk, do not delete an interface, unless you are certain it is no longer needed.

Note: To enable OSPF routing on an interface, see *Configuring OSPF*.

1.63.6 Examples

The following example configures an interface, **enet1:**

```
[local]Redback(config-ctx)#interface enet1
[local]Redback(config-if)#ip address 10.1.1.1 255.255.255.0
```

The following example configures a loopback interface, **local-loopback**, for the local context:

```
[local]Redback(config-ctx)#interface local-loopback loopback
[local]Redback(config-if)#ip address 10.1.1.1/32
```

The following example configures three intercontext interfaces in three different contexts all with group **10:**

```
[local]Redback(config-config)#context isp1
[local]Redback(config-ctx)#interface isp1-lan intercontext lan 10
[local]Redback(config-if)#ip address 10.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#exit
!Configure the second interface
[local]Redback(config-config)#context isp2
[local]Redback(config-ctx)#interface isp2-lan intercontext lan 10
[local]Redback(config-if)#ip address 10.1.1.2/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#exit
!Configure the third interface
[local]Redback(config-config)#context isp3
[local]Redback(config-ctx)#interface isp3-lan intercontext lan 10
[local]Redback(config-if)#ip address 10.1.1.3/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#exit
```

The following example deletes the **atm3** interface:

```
[local]Redback(config-ctx)#no interface atm3
```

The following example configures a last-resort interface and borrows an IP address for it from the **enet1** interface:

```
[local]Redback(config-ctx)#interface last multibind lastresort
[local]Redback(config-if)#ip unnumbered enet1
```

The following example configures a bridged interface and binds it to an existing bridge group, **isp1:**

```
[local]Redback(config-config)#context bridge
[local]Redback(config-ctx)#interface if-isp1 bridge
[local]Redback(config-if)#bridge name isp1
```

The following example configures an IPsec multibind interface:

```
[local]ipsec-se1(config)#context ctx-1
[local]ipsec-se1(config-ctx)#interface ipsec_mb_se_1 ipsec multibind
```

1.64 interface-cost

interface-cost *cost*

{**no** | **default**} **interface-cost**

1.64.1 Purpose

Modifies the cost associated with the specified Routing Information Protocol (RIP) or RIP next generation (RIPng) interface.

1.64.2 Command Mode

- RIP interface configuration
- RIPng interface configuration

1.64.3 Syntax Description

cost	Interface cost. The range of values is 1 to 16; the default value is 1.

1.64.4 Default

The RIP interface cost is 1.

1.64.5 Usage Guidelines

Use the **interface-cost** command to modify the cost associated with the specified RIP or RIPng interface. RIP or RIPng uses the cost as a metric for route selection. The lower its cost, the more likely an interface is selected to forward traffic.

Note: This command does not apply to loopback interfaces.

Use the no or **default** form of this command to return the cost to the default value of 1.

1.64.6 Examples

The following example assigns a cost of **5** to the **fe01** interface:

```
[local]Redback(config-ctx)#router rip rip002
[local]Redback(config-rip)#interface fe01
[local]Redback(config-rip-if)#interface-cost 5
```

1.65 interface (BGP neighbor fast reset)

interface ***if-name***

no interface ***if-name***

1.65.1 Purpose

Designates an interface to be used as an alternative BGP best path if the BGP best path interface fails.

1.65.2 Command Mode

BGP neighbor fast-reset configuration mode

1.65.3 Syntax Description

if-name	Name of the interface to be used as an alternative BGP best path if the BGP best path interface fails.

1.65.4 Default

No alternative BGP best path interface is configured.

1.65.5 Usage Guidelines

Use the **`interface`** command to designate an interface to be used as an alternative BGP best path if the BGP best path interface fails. When one interface fails in a multihop BGP session, BGP immediately withdraws the failed route and resets the BGP session to use an alternative path as soon as one of the interfaces connecting to the peer fails.

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

- You can enable fast reset on a group of up to 10 interfaces. BGP selects the best path from the active interfaces in this group. Each time a new interface is configured, the peer session is checked to ensure the best path available is being used.
- When the best path interface fails, BGP withdraws its session with the failed interface and starts a new BGP session with the next best path interface. The BGP session with the failed interface remains down until the failed interface becomes active again or is removed from the configuration.
- If all of the available interfaces configured for fast reset fail, the BGP session fails and does not become active until at last one of the interfaces configured for fast reset is active.
- Peer configuration overrides peer group configuration. For example, if you configure use the **`fast reset`** command in router BGP mode to enable BGP fast reset on a router that belongs to a peer group that has BGP fast reset is disabled (in BGP neighbor configuration mode), the peer

group configuration takes precedence and BGP fast reset is disabled on the router.

Use the **no** form of this command remove an alternative BGP best path interface configuration.

1.65.6 Examples

The following example designate the interface lo1 to be used as an alternative BGP best path if the BGP best path interface fails:

```
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#neighbor 1.1.1.1 internal
[local]Redback(config-bgp)#fast-reset 1000
[local]Redback(config-nbr-fast-reset)#interface lo1
```

1.66 interface (IS-IS)

interface ***if-name***

no interface ***if-name***

1.66.1 Purpose

Enables Intermediate System-to-Intermediate System (IS-IS) routing on the interface and enters IS-IS interface configuration mode.

1.66.2 Command Mode

IS-IS router configuration

1.66.3 Syntax Description

if-name	Name of the interface on which IS-IS is to be enabled.

1.66.4 Default

None

1.66.5 Usage Guidelines

Use the **interface** command to enable IS-IS routing on the interface and enter IS-IS interface configuration mode. To activate IS-IS on the interface, you must also assign a network entity title (NET) through the **net** command in IS-IS router configuration mode and bind the interface to a valid, activated port using the **bind interface** command in port configuration mode. For information on the **bind interface** command, *Command List*.

Note: Only one IS-IS instance can be running on an interface.

Use the **no** form of this command to disable IS-IS routing on the interface.

1.66.6 Examples

The following example enables the IS-IS instance, **ip-backbone**, on the **fa4/1** interface. A NET of **49.003.0003.0003.0003.00** is assigned to the instance and the **fa4/1** interface is bound to an Ethernet port in the **local** context:

```
[local]Redback(config-ctx)#router isis ip-backbone
[local]Redback(config-isis)#net 49.0003.0003.0003.0003.00
[local]Redback(config-isis)#interface fa4/1
[local]Redback(config-isis-if)#exit
[local]Redback(config-isis)#exit
[local]Redback(config-ctx)#exit
[local]Redback(config)#port ethernet 7/1
[local]Redback(config-port)#bind interface fa4/1 local
```

1.67 interface (LDP)

interface ***if-name***

no interface ***if-name***

1.67.1 Purpose

Enables the Label Distribution Protocol (LDP) on an interface so that the interface can be used to exchange Hello messages with neighbors and to establish a label-switched path (LSP).

1.67.2 Command Mode

LDP router configuration

1.67.3 Syntax Description

if-name	Name of the interface; an alphanumeric string.

1.67.4 Default

Disabled

1.67.5 Usage Guidelines

Use the interface command to enable LDP on an interface so that the interface can be used to exchange Hello messages with neighbors and to establish an LSP.

Note: You must also enable Multiprotocol Label Switching (MPLS) on the interface for the LSP to be established properly. You may also need to enable an Interior Gateway Protocol (IGP), such Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF).

Use the **no** form of this command to disable LDP on the interface.

1.67.6 Examples

The following example enables an LDP, OSPF, and MPLS routing instance for the **local** context, and enables LDP, OSPF, and MPLS on the interface, **backbone1:**

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface backbone1
[local]Redback(config-if)#ip address 10.1.2.3 255.255.255.0
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#router ospf 1
[local]Redback(config-ospf)#area 1
[local]Redback(config-ospf-area)#interface backbone1
[local]Redback(config-ospf-interface)#exit
[local]Redback(config-ospf-area)#exit
[local]Redback(config-ospf)#exit
[local]Redback(config-ctx)#router mpls 1
[local]Redback(config-mpls)#interface backbone1
[local]Redback(config-mpls-if)#exit
[local]Redback(config-mpls)#exit
[local]Redback(config-ctx)#router ldp
[local]Redback(config-ldp)#interface backbone1
```

1.68 interface (mobile IP)

interface ***if-name***

no interface ***if-name***

1.68.1 Purpose

Selects an existing interface, enables it for Mobile IP services, and accesses Mobile IP interface configuration mode.

1.68.2 Command Mode

Mobile IP configuration

1.68.3 Syntax Description

if-name	Name of an existing interface.

1.68.4 Default

None

1.68.5 Usage Guidelines

Use the **interface** command to select an existing interface, enable it for Mobile IP services, and access Mobile IP interface configuration mode. Use this command to specify the interfaces supporting IPv4 Mobility as defined in RFC 3344, *IP Mobility Support for IPv4*.

Use the **no** form of this command to disable the interface for Mobile IP services.

1.68.6 Examples

The following example shows how to create the **mn-access** interface in the **fa** context, select it, and access Mobile IP interface configuration mode:

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

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

[local]Redback(config-if)#exit

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

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

[local]Redback(config-if)#exit

[local]Redback(config-if)#ip address 10.1.1.1/16
```

1.69 interface (MPLS and RSVP)

```
interface if-name
```

```
no interface if-name
```

1.69.1 Purpose

When entered in MPLS router configuration, enables Multiprotocol Label Switching (MPLS) routing on an interface.

When entered in MPLS static router configuration, enables static MPLS routing on an interface, and enters MPLS static interface configuration mode.

When entered in RSVP router configuration mode, enables Resource Reservation Protocol (RSVP) routing on an interface and enters RSVP interface configuration mode.

When entered in RSVP tracking object configuration mode, adds the specified interface to the tracking object.

1.69.2 Command Mode

- MPLS router configuration
- MPLS static router configuration
- RSVP router configuration
- RSVP tracking object configuration mode

1.69.3 Syntax Description

if-name	Name of the interface; an alphanumeric string.

1.69.4 Default

None

1.69.5 Usage Guidelines

Use the **interface** command in MPLS router configuration to enable MPLS routing on an interface.

Use the **interface** command in MPLS static router configuration to enable static MPLS routing on an interface, and enter MPLS static interface configuration mode.

Use the **`interface`** command in RSVP router configuration mode to enable RSVP routing on an interface, and enter RSVP interface configuration mode.

Note: If an RSVP interface is not created, RSVP packets cannot be received, and the label-switched path (LSP) setup will fail.

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

1.69.6 Examples

The following example shows how to enable MPLS routing on the **mpls22** interface:

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

[local]Redback(config-mpls)#interface mpls22

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

The following example shows how to enable static MPLS routing on the **statmpls** interface and enter MPLS static interface configuration mode:

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

[local]Redback(config-mpls)#interface statmpls

[local]Redback(config-mpls-static-if)#
```

The following example shows how to enable RSVP routing on the **rsvp05** interface and enter RSVP interface configuration mode:

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

[local]Redback(config-rsvp)#interface rsvp05

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

1.70 interface (ND)

```
interface if-name [disable-on-address-collision]

no interface if-name
```

1.70.1 Purpose

Selects the interface to be configured for the Neighbor Discovery (ND) protocol and accesses ND router interface configuration mode.

1.70.2 Command Mode

ND router configuration

1.70.3 Syntax Description

if-name	Name of the ND router interface.
disable-on-address-collision	Optional. Shuts down the interface if an IP address collision occurs. The default is not to shut down the interface.

1.70.4 Default

None

1.70.5 Usage Guidelines

Use the **interface** command to select the interface to be configured for the ND router protocol and access ND router interface configuration mode.

You must have already created the interface with the **interface** command (in context configuration mode). You must also have assigned an IPv6 IP address to it with the **ipv6 address** command (in interface configuration mode).

The interface inherits the default ND parameters and any global ND parameters that you have configured for the ND router. To configure an ND parameter specific to this interface, enter the appropriate command in ND router interface configuration mode.

Use the **disable-on-address-collision** keyword to shut down the interface if an IP address collision occurs. The system brings up the interface after the collision is no longer detected.

Use the **no** form of this command to delete the ND router configuration for the specified interface.

1.70.6 Examples

The following example shows how to select the **int1** ND router interface:

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

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

[local]Redback(config-nd)#interface int1

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

1.71 interface (OSPF)

interface {*if-name* | *ip-addr*}

no interface {*if-name* | *ip-addr*}

1.71.1 Purpose

In OPSF area configuration mode, enables Open Shortest Path First (OSPF) routing on a specified interface and enters OSPF interface configuration mode.

In OPSF3 area configuration mode, enables OSPF Version 3 (OSPFv3) routing on a specified interface and enters OSPF3 interface configuration mode.

1.71.2 Command Mode

- OSPF area configuration
- OSPF3 area configuration

1.71.3 Syntax Description

if-name	Interface name.
ip-addr	IP address of the interface.

1.71.4 Default

None

1.71.5 Usage Guidelines

Use the **interface** command (in OSPF area configuration mode) to enable OSPF routing on a specified interface, and to enter OSPF interface configuration mode.

Use the **interface** command (in OSPF3 area configuration mode) to enable OSPFv3 routing on a specified interface, and to enter OSPF3 interface configuration mode.

OSPF or OSPFv3 routing must be enabled on at least one interface. That interface must already be configured through the **interface** command (in context configuration mode).

An OSPF or OSPFv3 interface can connect to the following:

- Broadcast network—Supports more than two attached routers and have the ability to address a single physical message to all attached routers.
- Point-to-point (P2P) network—Joins a single pair of routers.
- Nonbroadcast multi-access (NBMA)—a network topology supporting a full mesh of routers; however, there is no capability for sending a single message to all routers.
- Point-to-multipoint (P2MP) network—Acts as though the nonbroadcast network is a collection of P2P links.
- Loopback interface—An interface that is not bound to any circuit.

Use the **no** form of this command to disable OSPF routing on the specified interface.

Caution!

Risk of lost or down OSPF or OSPFv3 interfaces. If an interface is configured using an IP address and that IP address is deleted, the corresponding OSPF or OSPFv3 interface is deleted. If an interface is configured using an interface name and that interface name is deleted, the corresponding OSPF or OSPFv3 interface is deleted. However, if an interface is configured using an interface name and its primary IP address is changed, the OSPF or OSPFv3 interface continues normal operation using the new primary IP address. If an OSPF or OSPFv3 interface is configured using an interface name and its primary address is deleted, the OSPF or OSPFv3 interface is forced to the down state. To reduce the risk, avoid deleting an OSPF or OSPFv3 interface's IP address.

1.71.6 Examples

The following example shows how to enable OSPF routing on the interface at IP address, **192.30.200.10:**

```
[local]Redback(config-ospf-area)#interface 192.30.200.10
[local]Redback(config-ospf-if)#
```

1.72 interface (RIP)

`interface` ***`if-name`***

`no interface` ***`if-name`***

1.72.1 Purpose

In RIP router configuration mode, enables the specified interface to receive and send Routing Information Protocol (RIP) packets for the specified RIP instance, and enters RIP interface configuration mode.

In RIPng router configuration mode, enables the specified interface to receive and send RIP next generation (RIPng) packets for the specified RIPng instance, and enters RIPng interface configuration mode.

1.72.2 Command Mode

- RIPng router configuration
- RIP router configuration

1.72.3 Syntax Description

`if-name`	Name of the interface on which RIP or RIPng is to be enabled.

1.72.4 Default

RIP or RIPng are disabled on an interface.

1.72.5 Usage Guidelines

Use the **`interface`** command (in RIP router configuration mode) to enable the specified interface to receive and send RIP packets for the specified RIP instance, and enter RIP interface configuration mode.

Use the **interface** command (in RIPng router configuration mode) to enable the specified interface to receive and send RIPng packets for the specified RIPng instance, and enter RIPng interface configuration mode.

To enable an interface to send, but not receive RIP or RIPng packets, use the **no listen** command in RIP or RIPng interface configuration mode. To enable an interface to receive, but not send RIP or RIPng packets, use the **no supply** command in RIP or RIPng interface configuration mode.

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

1.72.6 Examples

The following example shows how to enable the **fe0** interface to receive and send RIP packets for the **rip001** instance:

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

[local]Redback(config-rip)#interface fe0

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

1.73 interface (RSVP object tracking)

interface*if-name*

no interface *if-name*

1.73.1 Purpose

Adds an interface to a tracking object.

1.73.2 Command Mode

RSVP tracking object configuration mode

1.73.3 Syntax Description

if-name	Name of the interface, in the format of an alphanumeric string, you want to add to the tracking object.

1.73.4 Default

None

1.73.5 Usage Guidelines

Use the **interface** command in RSVP tracking object configuration mode to add an interface to a tracking object.

Note: The maximum number of interfaces that can be tracked by a single object is ten.

Use the **no** form of this command to remove an interface from an RSVP tracking object.

1.73.6 Examples

The following example shows how to add interfaces `1`, `2`, and `3` to an RSVP tracking object called `san-jose-1`:

```
[local]Redback#configure

[local]Redback(config)#context local

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

[local]Redback(config-rsvp)#track san-jose-1

[local]Redback(config-rsvp-track_obj)#interface 1

[local]Redback(config-rsvp-track_obj)#interface 2

[local]Redback(config-rsvp-track_obj)#interface 3

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

[local]Redback(config-mpls)#interface mpls22

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

1.74 interval

interval ***interval-secs***

no interval

1.74.1 Purpose

Configures the amount of time over which MAC moves frequency is averaged.

1.74.2 Command Mode

Loop-detection configuration

1.74.3 Syntax Description

interval-secs	The amount of time over which MAC moves frequency is averaged can be set from 1 to 255 seconds.

1.74.4 Default

The default interval is 5 seconds.

1.74.5 Usage Guidelines

Use the **interval** command to configure the amount of time over which MAC moves frequency is averaged. Increasing the time interval reduces the sensitivity of this method to spikes, but also increases the response time.

1.74.6 Examples

The following example shows how to enable the MAC moves loop detection process and set the amount of time over which the frequency of MAC moves is averaged:

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

[local]Redback(config-ctx)#bridge lbdl

[local]Redback(config-bridge)#loop-detection

[local]Redback(config-ld)#interval 10
```

1.75 interval (malicious traffic)

interval ***interval-seconds***

{**no** | **default**} **interval**

1.75.1 Purpose

Configures the time interval between reports of malicious-traffic counters.

1.75.2 Command Mode

malicious-traffic alarms configuration mode

1.75.3 Syntax Description

interval-seconds	Number of seconds between malicious-traffic counter reports. The range is 60 to 3600.

1.75.4 Default

The default interval value is 60 seconds.

1.75.5 Usage Guidelines

Use the **interval** command to configure the time interval between reports of malicious-traffic counters. The SmartEdge OS compares the new counters to the old counters from the previous interval and generates alarms according to the configured thresholds.

Use the **no** form of this command to disable or remove the interval. Use the **default** form of this command to return to the default value of 60 seconds.

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

1.75.6 Examples

The following example shows how to configure the an interval of 700 seconds between malicious-traffic counter reports:

```
[local]Redback(config-malicious-traffic)#alarms
[local]Redback(config-malicious-traffic-alarms)#interval 700
```

1.76 invert-data

invert-data

{**no** | **default**} **invert-data**

1.76.1 Purpose

Inverts the polarity of all bits in the DS-0 channel group, DS-1, or E1 data stream.

1.76.2 Command Mode

- DS-0 group configuration
- DS-1 configuration
- E1 configuration

1.76.3 Syntax Description

This command has no keywords or arguments.

1.76.4 Default

The default value is no inversion.

1.76.5 Usage Guidelines

Use the **`invert-data`** command to invert the polarity of all bits in the DS-0 channel group, DS-1, or E1 data stream.

Use the **`no`** or **`default`** form of this command to return the bits in the data stream to the original polarity.

1.76.6 Examples

The following example shows how to invert the polarity of all bits in the data stream on DS-1 channel **1** on DS-3 channel **1** on port **1** of the channelized OC-12 traffic card in slot **3:**

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

[local]Redback(config-ds1)#invert-data
```