ERICSSON

Commands: mp through n

COMMAND DESCRIPTION

12/190 82-CRA 119 1170/1-V1 Uen J

Contents

1	**Command Descriptions**	**1**
1.1	mp endpoint-discriminator	1
1.2	mpls	2
1.3	mpls igp-shortcut	3
1.4	mpls to qos	4
1.5	mpls traffic-engineering	6
1.6	mpls tunnel-shortcut	7
1.7	mpls use-ethernet	8
1.8	mpls use-ip	9
1.9	mp mrru	11
1.10	mrinfo	12
1.11	mrouter	13
1.12	mtrace	14
1.13	mtu (atm)	17
1.14	mtu (card)	19
1.15	mtu (channel)	20
1.16	mtu (port)	22
1.17	mtu (tunnel)	24
1.18	multicast adjust-qos-rate	25
1.19	multicast adjust-qos-rate delay-interval	27
1.20	multicast destination	28
1.21	multicast maximum-bandwidth	29
1.22	multicast output	32
1.23	multicast rate-limit	33
1.24	multi-paths	34
1.25	nak-on-subnet-deletion	37
1.26	national	38
1.27	native-vlan-tag	39
1.28	nat enhanced password	41
1.29	nat logging-profile	42
1.30	nat policy	43
1.31	nat policy-name	44

1.32 nbns 45
1.33 nd profile 46
1.34 neighbor 48
1.35 neighbor (BFD) 49
1.36 neighbor (BGP) 50
1.37 neighbor (OSPF) 51
1.38 neighbor mac-flush 52
1.39 neighbor password 53
1.40 neighbor profile 55
1.41 neighbor targeted 56
1.42 neighbor (VPLS) 57
1.43 net 58
1.44 netop 59
1.45 network 60
1.46 network-type 62
1.47 next-hop 63
1.48 next-hop-on-lsp 65
1.49 next-hop-self 66
1.50 nexthop triggered 68
1.51 nexthop triggered delay 69
1.52 nexthop triggered holdtime 71
1.53 next-hop-unchanged 73
1.54 no debug all 73
1.55 nonstop-routing 75
1.56 notify 76
1.57 ns-retry-interval 77
1.58 nssa-range 78
1.59 ntp-broadcast 80
1.60 ntp-mode 81
1.61 num-queues 82

Glossary **85**

1 Command Descriptions

Commands starting with “mp” through commands starting with “n” 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 mp endpoint-discriminator

`mp endpoint-discriminator` {**`hostname`** | **`ip`** | **`user-defined`** ***`text`***}

`{no | default} mp endpoint-discriminator`

1.1.1 Purpose

Specifies the type of endpoint discriminator to be used for negotiation for a Multilink Point-to-Point Protocol (MLPPP) bundle.

1.1.2 Command Mode

Link group configuration

1.1.3 Syntax Description

`hostname`	Specifies the system hostname of the router.
`ip`	Specifies the IP address assigned to the interface to which you bind the MLPPP bundle.
`user-defined` ***`text`***	User-defined endpoint discriminator. The ***`text`*** argument is a string of up to 20 characters.

1.1.4 Default

The endpoint discriminator is the system hostname.

1.1.5 Usage Guidelines

Use the **mp endpoint-discriminator** command to specify the endpoint discriminator to be used for negotiation for an MLPPP bundle. The endpoint discriminator identifies peers to the system and distinguishes peers from one another in the system. This identification ensures that the correct links are bundled together in the same MLPPP bundle.

Note: This command is applicable only to an MLPPP bundle.

Use the **no** or **default** form of this command to return the endpoint discriminator identification to the system hostname.

1.1.6 Examples

The following example shows how to specify the endpoint discriminator as the IP address of the interface to which the MLPPP bundle will be bound:

```
[local]Redback(config)#link-group lg-multi mp
[local]Redback(config-link-group)#mp endpoint-discriminator ip
[local]Redback(config-link-group)#exit
```

1.2 mpls

mpls {**encrypted 1** | **password**} ***password***

no mpls

1.2.1 Purpose

Enables Multiprotocol Label Switching (MPLS) features and functions.

1.2.2 Command Mode

Software license configuration

1.2.3 Syntax Description

encrypted1	Specifies that the password that follows is encrypted.
password	Specifies that the password that follows is not encrypted.
password	Paid license password that is required to enable MPLS features and functions. The ***password*** argument is unique for MPLS and is provided at the time the software license is paid. Optional only when using the **no** form.

1.2.4 Default

MPLS features and functions are disabled.

1.2.5 Usage Guidelines

Use the **mpls** command to enable MPLS features and functions. You can specify the ***password*** argument in either encrypted or unencrypted form. Neither form displays by the **show configuration** ***command*** command (in any mode). For more information on the **show configuration** command, see *Using the CLI*.

Use the **no** form of this command to disable MPLS features and functions. A password is not required if you are disabling the license for MPLS features and functions; it is ignored if entered.

1.2.6 Examples

The following example licenses MPLS. The password is in an unencrypted form:

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

1.3 mpls igp-shortcut

mpls igp-shortcut

no mpls igp-shortcut

1.3.1 Purpose

Configures Interior Gateway Protocol (IGP) shortcuts that allow Open Shortest Path First (OSPF) to use a Multiprotocol Label Switching (MPLS) label-switched path (LSP) as a next hop as if it were a logical interface from the ingress routing device to the egress routing device.

1.3.2 Command Mode

OSPF router configuration

1.3.3 Syntax Description

This command has no keywords or arguments.

1.3.4 Default

The use of MPLS LSPs as next hops is disabled.

1.3.5 Usage Guidelines

Use the **mpls igp-shortcut** command to configure IGP shortcuts that allow OSPF to use an MPLS LSP as a next hop as if it were a logical interface from the ingress routing device to the egress routing device. In order for shortcuts to work, you must also configure the **igp-shortcut** command in RSVP router configuration or RSVP LSP router configuration mode

Use the **no** form of this command to disable the use of MPLS LSPs as next hops.

1.3.6 Examples

The following example enables the use of MPLS LSPs as intra-area next hops:

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

1.4 mpls to qos

mpls {***exp-value*** | **all**} **to qos** ***pd-value***

default mpls {***exp-value*** | **all**}

1.4.1 Purpose

Translates Multiprotocol Label Switching (MPLS) experimental (EXP) values to packet descriptor (PD) quality of service (QoS) values on ingress.

1.4.2 Command Mode

Class map configuration

1.4.3 Syntax Description

exp-value	An integer from 0 (lowest priority) to 7 (highest priority) representing the contents of the three EXP bits in the MPLS label header.
all	Maps all valid values for the source value to the specified target value. Any existing configuration for the classification map is overridden.
pd-value	An integer from 0 to 63 (6 bits), with the packet priority encoded in 3 higher-order bits and the packet drop precedence in the 3 lower-order bits. You can enter the value in decimal or hexadecimal format, for example **16** or **0x10**. You can also enter a standard Differentiated Services Code Point (DSCP) marking label. The scale used by this command for packet priority, from 0 (lowest priority) to 7 (highest priority), is the relative inverse of the scale used by the **mark priority** command. For details on this command, see *Configuring Rate-Limiting and Class-Limiting*.

1.4.4 Default

None

1.4.5 Usage Guidelines

Use the **mpls to qos** command to define ingress mappings from MPLS EXP values to PD QoS values.

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

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

1.4.6 Examples

The following example defines the classification map **exp-to-pd** to determine initial MPLS values on ingress, defines the default mapping schema using **7P1D** values, then maps MPLS EXP value **1** to the PD value **0x24:**

```
[local]Redback(config)#qos class-map exp-to-pd mpls in

[local]Redback(config-class-map)#mapping-schema 7P1D

[local]Redback(config-class-map)#mpls 1 to qos 0x24
```

1.5 mpls traffic-engineering

`mpls traffic-engineering`

1.5.1 Purpose

Enables Open Shortest Path First (OSPF) advertisement of traffic engineering metrics.

1.5.2 Command Mode

OSPF router configuration

1.5.3 Syntax Description

This command has no keywords or arguments.

1.5.4 Default

The use of Multiprotocol Label Switching (MPLS) traffic engineering is disabled.

1.5.5 Usage Guidelines

Use the **`mpls traffic engineering`** command to cause OSPF to advertise traffic engineering metrics for OSPF interfaces.

1.5.6 Examples

The following example enables the use of MPLS traffic engineering:

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

[local]Redback(config-ospf)#mpls traffic-engineering
```

1.6 mpls tunnel-shortcut

mpls tunnel-shortcut

no mpls tunnel-shortcut

1.6.1 Purpose

Enables the use of Multiprotocol Label Switching .(MPLS) label-switched paths (LSPs) for tunneling the Label Distribution Protocol (LDP) over Resource Reservation Protocol (RSVP).

1.6.2 Command Mode

OSPF router configuration

1.6.3 Syntax Description

This command has no keywords or arguments.

1.6.4 Default

The use of MPLS LSPs for tunneling is disabled.

1.6.5 Usage Guidelines

Use the **mpls tunnel-shortcut** command to enable the use of MPLS LSPs for tunneling LDP over RSVP. To enable LDP over RSVP, you must configure the **mpls tunnel-shortcut** command and configure the **tunnel-shortcut** command in both RSVP router configuration mode (or RSVP LSP configuration mode) and LDP router configuration mode for all targeted LDP neighbors or for a specific targeted LDP neighbor (**neighbor** ***address*** **targeted tunnel-shortcut**).

Use the **no** form of this command to disable the use of MPLS LSPs for tunneling LDP over RSVP.

1.6.6 Examples

The following example enables the use of MPLS LSPs for tunneling LDP over RSVP:

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

[local]Redback(config-ospf)#mpls tunnel-shortcut
```

1.7 mpls use-ethernet

mpls {***exp-value*** | **all**} **use-ethernet** [***class-map-name***]

{**no** | **default**} **mpls** {***exp-value*** | **all**}

1.7.1 Purpose

On incoming packets, maps Ethernet 802.1p values to packet descriptor (PD) values with the specified EXP value, instead of directly using the Multiprotocol Label Switching (MPLS) experimental (EXP) values.

1.7.2 Command Mode

class map configuration

1.7.3 Syntax Description

exp-value	An integer from 0 (lowest priority) to 7 (highest priority) representing the contents of the 3 EXP bits in the MPLS label header.
all	Maps all valid values for the source value to the specified target value. Any existing configuration for the classification map is overridden.
use-ethernet	Enables a secondary mapping lookup using the packet's 802.1p bits as input. If no classification map is specified for the secondary lookup, the default 8P0D 802.1p-to-PD mapping is used.
class-map-name	Optional. Name of the secondary classification map.

1.7.4 Default

Ingress MPLS classification map entries use the 8P0D EXP-to-PD mapping, where the EXP value is copied to the PD QoS priority field. The PD drop-precedence field is set to zero.

1.7.5 Usage Guidelines

Use the **mpls use-ethernet** command to determine initial PD values by mapping Ethernet 802.1p values rather than directly mapping from MPLS EXP values for received MPLS packets with the specified EXP value. If a received packet with the specified EXP value does not include an Ethernet header, the SmartEdge router uses the default mapping instead of the specified mapping.

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

If you specify the optional ***class-map-name*** construct, the resulting mapping uses the specified 802.1p-to-PD classification map. The secondary classification map must have a value of *Ethernet* for the ***marking-type*** argument and a value of *in* for the mapping direction. If you do not specify a secondary classification map, the default mapping is used.

Use the **no** or **default** form of this command to revert one or all map entries to either the default 8P0D or mapping schema values, if a mapping schema has been specified.

1.8 mpls use-ip

mpls {***exp-value*** | **all**} **use-ip** [***class-map-name***]

default mpls {***exp-value*** | **all**}

1.8.1 Purpose

On incoming packets, maps Differentiated Services Code Point (DSCP) values to internal packet descriptor (PD) values, rather than using Multiprotocol Label Switching (MPLS) experimental (EXP) values.

1.8.2 Command Mode

class map configuration

1.8.3 Syntax Description

exp-value	An integer from 0 (lowest priority) to 7 (highest priority) representing the contents of the 3 EXP bits in the MPLS label header.
all	Maps all valid values for the source value to the specified target value. Any existing configuration for the classification map is overridden.
class-map-name	Optional. Name of the secondary classification map.

1.8.4 Default

None

1.8.5 Usage Guidelines

Use the **mpls use-ip** command to determine PD values by mapping DSCP values rather than MPLS EXP values on ingress for IP packets.

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

If you specify the optional ***class-map-name*** argument, the resulting mapping uses the specified DSCP-to-PD classification map. The secondary classification map must have a value of *ip* for the ***marking-type*** argument, and a value of *in* for the mapping direction. If you do not specify a secondary classification map, the default mapping is used.

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

1.8.6 Examples

The following example defines the classification map **dscp-to-pd** to determine initial quality of service (QoS) PD values on ingress, and specifies **7P1D** encoding as a default mapping schema. It then overrides the default **7P1D** values for EXP value **1** with PD value **0x24**, and specifies the IP header DSCP value to determine the initial QoS PD value for packets received with EXP value **3**. The secondary classification map **exp-to-dscp** is used for translation:

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

1.9 mp mrru

mp mrru ***value***

{no | default} mp mrru

1.9.1 Purpose

Sets the size of the maximum received reconstructed unit (MRRU) to be used to negotiate a Multilink Point-to-Point Protocol (MLPPP) bundle.

1.9.2 Command Mode

link group configuration

1.9.3 Syntax Description

value	Optional. The MRRU size for the MLPPP bundle. The range of values is 256 to 128000.

1.9.4 Default

If no MRRU is specified, 1524 is the maximum size that can be negotiated.

1.9.5 Usage Guidelines

Use the **mp mrru** command to set the MRRU to be used to negotiate an MLPPP bundle. The SmartEdge router uses this value when calculating the maximum receive unit (MRU) or MRRU value to send in the Link Control Protocol (LCP) Configure Request to the peer.

MRRU configuration is supported for static MLPPP links only; it is not supported for subscriber links.

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

1.9.6 Examples

The following example shows how to specify the endpoint discriminator as the IP address of the interface to which the MLPPP bundle is bound:

```
[local]Redback(config)#link-group lg-multi mp
[local]Redback(config-link-group)#mp mrru 4470
[local]Redback(config-link-group)#exit
```

1.10 mrinfo

mrinfo ***target-mrouter-addr***

1.10.1 Purpose

Queries a neighboring multicast router to determine which routers are peers of the local router.

1.10.2 Command Mode

exec

1.10.3 Syntax Description

target-mrouter-addr	IP address of the target neighboring multicast router.

1.10.4 Default

None

1.10.5 Usage Guidelines

Use the **mrinfo** command to query a neighboring multicast router to determine which routers are peers of the local router. This command sends a query to a target multicast router and displays the response containing information about the target's neighboring routers.

1.10.6 Examples

The following example queries a target multicast router, **10.3.1.3**, and displays information about the target's neighboring routers:

```
[local]Redback>mrinfo 10.3.1.3

10.3.1.3 (10.3.1.3) [version 21.3,mtrace]:
  10.4.1.3 -> 10.4.1.2 (10.4.1.2) [1/0/pim/querier]
  10.5.1.3 -> 10.5.1.4 (10.5.1.4) [1/0/pim]
```

1.11 mrouter

mrouter [**static**]

no mrouter

1.11.1 Purpose

Enables multicast router monitoring for circuits attached to the specified IGMP snooping profile.

1.11.2 Command Mode

IGMP snooping profile configuration

1.11.3 Syntax Description

static	Configures all circuits attached to the specified IGMP snooping profile to be static multicast router circuits.

1.11.4 Default

IGMP router monitoring is enabled on every circuit.

1.11.5 Usage Guidelines

Use the **mrouter** command to enable multicast router monitoring for all circuits attached to a specified IGMP snooping profile. All circuits attached to the IGMP snooping profile assume the multicast routing setting specified in the profile.

Use the **no** form of this command to disable the multicast router monitoring for all circuits attached to the specified IGMP snooping profile.

If you do not include the optional **static** keyword with the **mrouter** command, IGMP packets are monitored on the circuits. If IGMP queries are received by an associated circuit, that circuit is declared to be a multicast routing circuit.

By default, every circuit is enabled for monitoring of IGMP packets. This behavior can be overwritten by configuring a bridge profile with the mrouter setting disabled or set to **static**.

1.11.6 Examples

The following example shows how to enable IGMP router monitoring on every circuit attached to an IGMP snooping profile called `p1`:

```
[local]router#configure

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

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

The following example shows how to configure all circuits attached to an IGMP snooping profile called `sanjose1` to be static multicast router circuits:

```
[local]router#configure

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

[local]router(config-igmp-snooping-profile)#mrouter static
```

The following example shows how to disable multicast router discovery on all circuits attached to an IGMP snooping profile called `milpitas1`:

```
[local]router#configure

[local]router(config)#igmp snooping profile milpitas1

[local]router(config-igmp-snooping-profile)#no mrouter
```

1.12 mtrace

mtrace {***src-addr*** | ***src-name***} [**gateway** {***gateway-addr*** | ***gateway-name***}] [**group** {***group-addr*** | ***group-name***}] [**hops** ***hop-count***] [**interval**

trace-interval] [**local_addr** ***if-addr***] [**loop**] [**multicast**] [**no-router-alert**] [**numerical**] [**query** ***query-count***] [**receiver** {***rec-addr*** | ***rec-name***}] [**response** {***host-addr*** | ***hostname***}] [**short_form**] [**ttl** ***ttl***] [**unicast**] [**verbose**] [**wait** ***wait-interval***]

1.12.1 Purpose

Traces the path from a source to a destination branch on a multicast distribution tree.

1.12.2 Command Mode

exec

1.12.3 Syntax Description

src-addr	IP address of the source to end the process of tracing the path.
src-name	Name of the source to end the process of tracing the path.
gateway	Optional. Specifies the last hop router of the multicast receiver.
gateway-addr	IP address of the last hop router of the multicast receiver.
gateway-name	Name of the last hop router of the multicast receiver.
group	Optional. Specifies the group for which the path tracing is performed.
group-addr	IP address of the group for which the path tracing performed.
group-name	Name of the group for which the path tracing is performed.
hops ***hop-count***	Optional. Maximum number of hops that can be traced.
interval ***trace-interval***	Optional. Interval, in seconds, between statistics gathering traces.
local_addr ***if-addr***	Optional. IP address of the local interface used for sourcing the query.
loop	Optional. Loops indefinitely printing statistics.
multicast	Optional. Specifies that responses are always requested using multicast routing.
no-router-alert	Optional. Sends request without router alert IP option.
numerical	Optional. Specifies that hop addresses be printed in dotted decimal format only.
query ***query-count***	Optional. Maximum number of query attempts.

receiver	Optional. Specifies a receiver to begin the process of tracing the path.
rec-addr	IP address of receiver to begin the process of tracing the path.
rec-name	Name of receiver to begin the process of tracing the path.
response	Optional. Specifies a host to receive the path tracing responses.
host-addr	IP address of the host to receive the path tracing responses.
hostname	Name of host to receive the path tracing responses.
short_form	Optional. Enables short form output, and no statistics are displayed.
ttl ***ttl***	Optional. Time-to-live (TTL) value for multicast trace queries and responses. The range of values is 1 to 255; the default value is 5.
unicast	Optional. Specifies that responses are always requested using unicast routing.
verbose	Optional. Enables verbose mode.
wait ***wait-interval***	Optional. Interval, in seconds, to wait for a trace response.

1.12.4 Default

None

1.12.5 Usage Guidelines

Use the **mtrace** command to trace the path from a source to a destination branch on a multicast distribution tree. The trace query is passed hop by hop along the direction from the receiver to the source, collecting each hop's IP address, packet counts, and routing error codes. At the end of this path, a response to returned to the response IP address.

If the command is issued without specifying any trace query parameters, it interactively prompts for the parameters.

1.12.6 Examples

The following example displays the short form results of tracing a path from the source IP address, **11.1.1.21**, to the multicast receiver's last hop router IP address, **10.4.1.2**, using the Internet Group Management Protocol (IGMP) group with the IP address, **224.121.121.1:**

```
[local]Redback>mtrace 11.1.1.21 group 224.121.121.1 gate
way 10.4.1.2 short_form

Mtrace from 11.1.1.21 to 10.4.1.2 via group 224.121.121.1
Querying full reverse path... * switching to hop-by-hop:
  0  ? (10.4.1.2)
 -1  ? (10.4.1.2)  PIM  threshold 0  Reached RP/Core
 -2  * * ? (10.2.1.1)  PIM  threshold 0
 -3  ? (11.1.1.21)
Round trip time 15 ms; total ttl of 1 required.
```

The following example displays detailed results of tracing a path from the source IP address, **11.1.1.21**, to the multicast receiver's last hop router IP address, **10.4.1.2**, using the IGMP group with the IP address, **224.121.121.1:**

```
[local]Redback>mtrace 11.1.1.21 group 224.121.121.1 gateway 10.4.1.2

Mtrace from 11.1.1.21 to 10.4.1.2 via group 224.121.121.1
Querying full reverse path... * switching to hop-by-hop:
  0  ? (10.4.1.2)
 -1  ? (10.4.1.2)  PIM  threshold 0  Reached RP/Core
 -2  * * ? (10.2.1.1)  PIM  threshold 0
 -3  ? (11.1.1.21)
Round trip time 17 ms; total ttl of 1 required.

Waiting to accumulate statistics...Results after 10 seconds:

 Source         Response Dest     Overall       Packet Statistics For
Traffic From
11.1.1.21        10.3.1.3         Packet      11.1.1.21 To 224.121.121.1
     v        __/  rtt   17 ms     Rate       Lost/Sent = Pct  Rate
0.0.0.0          (null)
     v     ^      ttl    2     ^    0 pps        0/0    = --    0 pps
11.1.1.1
10.2.1.1         ?
     v     ^      ttl    2                      0/0    = --    0 pps
10.2.1.2
10.4.1.2         ?              Reached RP/Core
     v      \__   ttl    3                      ?/0            0 pps?
10.4.1.2         10.3.1.3
  Receiver       Query Source
```

1.13 mtu (atm)

mtu ***size***

default mtu

1.13.1 Purpose

Specifies the maximum transmission unit (MTU) size of the payload without fragmentation for an Asynchronous Transfer Mode (ATM) OC port.

1.13.2 Command Mode

ATM OC configuration

1.13.3 Syntax Description

size	MTU payload size in bytes. The range of values is 256 to 12,800 bytes.

1.13.4 Default

4470 bytes

1.13.5 Usage Guidelines

Use the **mtu** command to specify the MTU size of the payload without fragmentation for an ATM port.

Note: The MTU size for an ATM port is the size of the IP packet to be segmented into ATM cells.

The Layer 2 headers are automatically added to the payload size and do not cause fragmentation; you do not include them when selecting the value of the ***size*** argument. You can also specify the MTU size at the interface level; the MTU size used is the minimum of the two values.

Note: If you change the MTU value for a Point-to-Point Protocol (PPP)-encapsulated channel or port that you have already configured and enabled with the **no** form of the **shutdown** command in the appropriate configuration mode, the change does not take effect until you shut down the channel or port, and then reenable it.

Use the **default** form of this command to specify the default MTU payload size.

1.13.6 Examples

The following example shows how to specify a MTU payload size of `1000` bytes:

```
[local]Redback(config)#port atm 4/1
[local]Redback(config-atm-oc)#mtu 1000
```

1.14 mtu (card)

mtu ***size***

{**no** | **default**} **mtu**

1.14.1 Purpose

Specifies the maximum transmission unit (MTU) size of the payload without fragmentation for all Fast Ethernet (FE) ports on the Fast Ethernet-Gigabit Ethernet (FE-GE) traffic card.

1.14.2 Command Mode

card configuration

1.14.3 Syntax Description

size	MTU payload size in bytes. The range of values is 256 to 9600 bytes. The default value is 1500 bytes.

1.14.4 Default

The default MTU payload size is 1500 bytes.

1.14.5 Usage Guidelines

Use the **mtu** command to specify the MTU size of the payload without fragmentation for an all FE ports on the FE-GE traffic card.

The Layer 2 headers are automatically added to the payload size and do not cause fragmentation; you do not include them when selecting the value of the ***size*** argument.

Note: You can also specify the MTU size at the interface level; the MTU size used is the minimum of the two values.

Configuring ATM, Ethernet, and POS Ports also describes this command for all types of Ethernet and Gigabit Ethernet ports.

You can override the MTU setting for individual FE ports by using this command in port configuration mode.

Use the **no** or **default** form of this command to specify the default MTU payload size.

Warning!

Risk of data loss for IPv6 data packets created by a traffic card. IPv6 data packets created on a traffic card are fragmented based on the MTU set on the egress port. In the current release of the SmartEdge OS any ICMPv6 ‘‘Packet too big’’ message sent from any IPv6 router on the data path to the traffic card that created an IPv6 data packet if the fragment size exceeds the PMTU of the data path is ignored. As a result, the data packet traffic is dropped. (ICMPv6 "Packet too big" messages sent from any traffic card or IPv6 router on the data path to the control or ASE card that created an IPv6 control packet if the fragment size exceeds the PMTU are acted upon.)

To avoid this risk, ensure that the MTU set on the traffic card with the **mtu** command in card or port configuration mode is set to be less than the PMTU of the data path. If a network-wide PMTU policy is used, set matching port-level MTU and network-wide PMTU values.

1.14.6 Examples

The following example shows how to specify an MTU payload size of `9600` bytes for the FE ports on the FE-GE traffic card in slot `4`:

```
[local]Redback(config)#card fege-60-2-port 4
[local]Redback(config-card)#mtu 9600
```

1.15 mtu (channel)

mtu ***size***

default fault mtu

1.15.1 Purpose

Specifies the maximum transmission unit (MTU) payload size of the packet without fragmentation for a DS-3 channel or port, E1 channel or port, DS-1 channel on a channelized DS-3 channel or port, or DS-0 channel group on a channelized E1 channel or port.

1.15.2 Command Mode

- DS-0 group configuration
- DS-1 configuration

- DS-3 configuration
- E1 configuration

1.15.3 Syntax Description

size	MTU payload size of the packet in bytes. The range of values is 256 to 12,800. The default depends on the type of channel or port; see Table 1.

1.15.4 Default

The default MTU payload size depends on the type of channel or port; for more information see Table 1.

1.15.5 Usage Guidelines

Use the **mtu** command to specify the MTU payload size of the packet without fragmentation for a clear-channel DS-3 channel or port, E3 port, E1 channel or port, a DS-1 channel on a channelized DS-3 channel or port, or a DS-0 channel group on a channelized E1 channel or port.

Table 1 lists the range of values and default for each type of channel or port.

Table 1 Values for the MTU Payload Size Argument

Channel or Port Type	Range of Values (Bytes)	Default (Bytes)
E1	256 to 12,800	1,500
DS-3	256 to 12,800	4,470
DS-1	256 to 12,800	1,500
DS-0 channel group	256 to 12,800	1,500

The Layer 2 headers are automatically added to the payload size and do not cause fragmentation; you do not include them when selecting the value of the ***size*** argument.

Note: You can also specify the MTU size at the interface level; the MTU size used is the minimum of the two values.

Note: If you change the MTU value for a Point-to-Point Protocol (PPP)-encapsulated channel or port that you have already configured and enabled with the **no** form of the **shutdown** command in the appropriate configuration mode, the change does not take effect until you shut down the channel or port and then reenable it.

This command is also described in *Configuring ATM, Ethernet, and POS Ports* for Asynchronous Transfer Mode (ATM) OC, ATM DS-3, Ethernet, and Packet over SONET/SDH (POS) ports.

Use the **default** form of this command to specify the default value of the MTU payload size of the packet.

1.15.6 Examples

The following example shows how to specify the MTU payload size of the packet to be **2000** on clear-channel DS-3 port **1:**

```
[local]Redback(config)#port ds3 3/1
[local]Redback(config-ds3)#mtu 2000
```

1.16 mtu (port)

mtu ***size***

default mtu

1.16.1 Purpose

Specifies the maximum transmission unit (MTU) size of the payload without fragmentation for an Ethernet or Gigabit Ethernet port, or a Packet over SONET/SDH (POS) port.

1.16.2 Command Mode

port configuration

1.16.3 Syntax Description

size	MTU payload size in bytes. The range of values and the default value depends on the type of port. See Table 2.

1.16.4 Default

The default MTU payload size depends on the type of port; see Table 2.

1.16.5 Usage Guidelines

Use the **mtu** command to specify the MTU size of the payload without fragmentation for an Ethernet, or Gigabit Ethernet, or POS port.

Table 2 lists the range of values and default for each type of port.

Table 2 Values for MTU Payload Size Argument

Port Type	Range of Values (Bytes)	Default (Bytes)
Ethernet	• 256 to 2000—Ports on any Ethernet traffic card(1) • 256 to 9600—Ports on an FE-GE traffic card(2)	1500
Gigabit Ethernet	256 to 9198	1500
POS	256 to 12800	4470

(1) FE ports on an FE-GE traffic card support guaranteed lossless flow control for MTUs up to 2000 bytes.
(2) FE ports on an FE-GE traffic card support guaranteed lossless flow control for MTUs up to 9600 bytes if the ports are explicitly configured for lossless flow control.

The Layer 2 headers are automatically added to the payload size and do not cause fragmentation; you do not include them when selecting the value of the ***size*** argument. You can also specify the MTU size at the interface level; the MTU size used is the minimum of the two values.

Note: If you have specified an MTU for all FE ports on an FE-GE traffic card (by using this command in card configuration mode), entering this command in port configuration mode overrides that MTU for this port only.

Note: If you change the MTU value for a Point-to-Point Protocol (PPP)-encapsulated channel or port that you have already configured and enabled with the **no** form of the **shutdown** command in the appropriate configuration mode, the change does not take effect until you shut down the channel or port, and then reenable it.

Use the **default** form of this command to specify the default MTU payload size.

Warning!

Risk of data loss for IPv6 data packets created by a traffic card. IPv6 data packets created on a traffic card are fragmented based on the MTU set on the egress port. In the current release of the SmartEdge OS any ICMPv6 ‘‘Packet too big’’ message sent from any IPv6 router on the data path to the traffic card that created an IPv6 data packet if the fragment size exceeds the PMTU of the data path is ignored. As a result, the data packet traffic is dropped. (ICMPv6 "Packet too big" messages sent from any traffic card or IPv6 router on the data path to the control or ASE card that created an IPv6 control packet if the fragment size exceeds the PMTU are acted upon.)

To avoid this risk, ensure that the MTU set on the traffic card with the **mtu** command in port configuration mode is set to be less than the PMTU of the data path. If a network-wide PMTU policy is used, set matching port-level MTU and network-wide PMTU values.

1.16.6 Examples

The following example shows how to specify a MTU payload size of **1000** bytes for Ethernet port **1** in slot **4:**

```
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#mtu 1000
```

In this example, the Layer 2 headers for an Ethernet port include an 18-byte Ethernet header, a 4-byte 802.1Q header, and up to four 4-byte Multi Protocol Label Switching (MPLS) labels, for a total of 38 bytes. Thus, in this example, the actual maximum packet size without fragmentation is 1038 bytes.

1.17 mtu (tunnel)

mtu ***bytes***

{no | default} mtu

1.17.1 Purpose

Sets the maximum transmission unit (MTU) size for packets sent in a tunnel.

1.17.2 Command Mode

tunnel configuration

1.17.3 Syntax Description

bytes	MTU size in bytes. The range of values is 256 to 16384.

1.17.4 Default

MTU for the interface to which the tunnel is bound.

1.17.5 Usage Guidelines

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

A tunnel uses the MTU size for the interface to which you have bound it with the **bind interface** command (in tunnel configuration mode), 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** or **default** form of this command to delete the configured MTU and use the interface MTU.

1.17.6 Examples

The following example shows how to set the maximum IP packet size for the **DenverTnl** to **1024** bytes:

```
[local]Redback(config)#tunnel ipv6v4 DenverTnl
[local]Redback(config-tunnel)#mtu 1024
```

1.18 multicast adjust-qos-rate

multicast adjust-qos-rate {**metering** | **queuing**} [**minimum-rate** ***kbps***]

no multicast adjust-qos-rate {**metering** | **queuing**}

1.18.1 Purpose

Sets the QoS adjustment rate on metering and queuing bindings.

1.18.2 Command Mode

IGMP service profile configuration

1.18.3 Syntax Description

metering	Applies the adjusted QoS rate on metering bindings.
queuing	Applies the adjusted QoS rate on queuing bindings.
minimum-rate *kbps*	Minimum rate, in kbps, to be set aside for a given binding to avoid starving unicast traffic. The range is 64 to 9999999. The default minimum rate is 64 kbps.

1.18.4 Default

QoS rate adjustment is not applied to metering or queuing bindings.

1.18.5 Usage Guidelines

Use the **multicast adjust-qos-rate** command to adjust the QoS binding rate for metering or queuing bindings.

Within a given IGMP service profile, up to two instances of this command may be configured: one for metering and one for queuing. If the **queuing** keyword is used, the SmartEdge router adjusts the rate on the PWFQ Layer 2 node on the circuit on which the IGMP joins are received. If no Layer 2 node is found on that circuit, the SmartEdge router does not make any QoS adjustments and logs a message to this effect.

When making adjustments to metering, if both metering and shaping rates are in effect, the adjustments occur independently.

The **minimum-rate** option allows you to specify a minimum amount of bandwidth that cannot be eliminated by QoS adjustment. This option allows you to ensure that an incorrect IGMP state (for example, a missed leave message) does not starve delay-sensitive traffic (such as voice traffic) on the PPPoE session. If rate adjustment causes the enforced rate to reach this minimum rate, the SmartEdge router logs a message.

Use the **no** form of this command to disable the QoS rate adjustment on metering or queuing bindings.

1.18.6 Examples

The following example sets the minimum rate for QoS adjustment to 1200 kbps for metering bindings and 1000 kbps for queuing bindings in the IGMP service profile **profile1** in context **ContextA**:

```
[local]Redback(config)#context ContextA
[local]Redback(config-ctx)#igmp service-profile profile1
[local]Redback(config-igmp-service-profile)#multicast adjust-qos-rate metering minimum-rate 1200
[local]Redback(config-igmp-service-profile)#multicast adjust-qos-rate queuing minimum-rate 1000
```

1.19 multicast adjust-qos-rate delay-interval

multicast adjust-qos-rate delay-interval *seconds*

{**no** | **default**} **multicast adjust-qos-rate delay-interval**

1.19.1 Purpose

Sets a time interval after which QoS rate adjustment is to be applied.

1.19.2 Command Mode

IGMP service profile configuration

1.19.3 Syntax Description

seconds	The interval, in seconds, after which QoS rate adjustment is to be applied. The range is 1 to 10. The default is 5.

1.19.4 Default

QoS rate adjustment is applied after a 5-second delay.

1.19.5 Usage Guidelines

Use the **multicast adjust-qos-rate delay-interval** command to specify the delay between the time a subscriber leaves a multicast channel and the time when a corresponding QoS rate adjustment is removed from the subscriber circuit.

Suppressing rate adjustments after IGMP leaves helps control churn in cases of aggressive bandwidth changes.

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

1.19.6 Examples

The following example sets the delay interval to 8 seconds in the IGMP service profile **profile1** in context **ContextA**:

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

[local]Redback(config-ctx)#igmp service-profile profile1

[local]Redback(config-igmp-service-profile)#multicast adjust-qos-rate delay-interv
```

1.20 multicast destination

multicast destination [*if-name ctx-name* [**group-list** *acl-name*]]

no multicast destination

1.20.1 Purpose

Enables the forwarding of multicast data for Internet Group Management Protocol (IGMP) messages received on the Point-to-Point Protocol over Ethernet (PPPoE) subscriber circuits on an out-of-band (separated from the PPPoE circuit) IP over Ethernet (IPoE) interface.

1.20.2 Command Mode

IGMP service profile configuration

1.20.3 Syntax Description

if-name	Optional. Multicast-enabled interface name.
ctx-name	Optional. Context name in which the multicast-enabled interface resides.
group-list *acl-name*	Optional. Name of the access control list (ACL) used to filter IGMP control messages.

1.20.4 Default

Forwarding multicast data on an out-of-band IPoE interface is disabled.

1.20.5 Usage Guidelines

Use the **multicast destination** command to enable the forwarding of multicast data for IGMP messages received on the PPPoE subscriber circuits on an out-of-band IPoE interface.

The IGMP service profile must be bound to a subscriber record through a configuration or a Remote Authentication Dial-In User Service (RADIUS) attribute.

Note: For the **multicast destination** command to work properly, the out-of-band IPoE interface on which the multicast data is to be forwarded must be multicast-enabled; use the **multicast output** command (in interface configuration mode) to enable the out-of-band IPoE interface to forward multicast data.

Use the **no** form of this command to disable the forwarding of multicast data for IGMP messages received on the PPPoE subscriber circuits on an out-of-band IPoE interface.

1.20.6 Examples

The following example enables the **to_dslam5** interface on the **local** context to forward multicast data, and configures the **foo** IGMP service profile to enable the forwarding of multicast data received on a PPPoE subscriber circuit on the **to_dslam5** interface:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface to_dslam5
[local]Redback(config-if)#multicast output
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#igmp service-profile foo
[local]Redback(config-igmp-service-profile)#multicast destination to_dslam5
```

1.21 multicast maximum-bandwidth

multicast maximum-bandwidth *rate*[**percent**]

no multicast

1.21.1 Purpose

Specifies a maximum allowed rate for an 802.1Q PVC.

1.21.2 Command Mode

dot1q PVC configuration

1.21.3 Syntax Description

rate	The maximum allowed bandwidth, specified either as an absolute bandwidth in Mbps or as a percentage using the **percent** keyword. If specified as a percentage, the range is 0 to 125; if a higher rate is configured, it is reset to 125. If the ***percent*** argument is not specified, the ***rate*** argument is interpreted as an absolute bandwidth.
percent	Optional. The ***rate*** argument is interpreted as a percentage of the maximum rate already configured for the 802.1Q PVC using the **qos rate maximum** command.

1.21.4 Default

No maximum rate is applied to 802.1Q PVCs.

1.21.5 Usage Guidelines

Use the **multicast maximum-bandwidth** command to control the multicast bandwidth allowed on an 802.1Q PVC.

This feature can be used to implement Call Admission Control (CAC) at the service virtual local area network (S-VLAN) level; for example enforcing bandwidth ceilings for Internet Group Management Protocol (IGMP) traffic replicating Point to Point Protocol over Ethernet (PPPoE) subscribers. When this feature is enabled, the system monitors the 802.1Q PVC (including its child circuits or subscriber circuits) to ensure that the sum of IGMP Join requests on the PVC does not exceed the specified limit. If a Join is received that would cause the configured limit to be exceeded and a child circuit with lower priority exists on the PVC, the lower priority group is dropped to reclaim the bandwidth and the event is logged; otherwise, the request to join the new group is rejected, the event is logged, and statistics are incremented.

The rate can be either an absolute value or a percentage of a quality of service (QoS) maximum rate limit set using the **qos rate** command with the **maximum** keyword.

The highest allowed percentage is 125%. If the percentage option is specified but a QoS maximum rate limit has not been configured, then bandwidth control

is not applied. If the percentage option is specified and QoS maximum rate limit configuration is later deleted, bandwidth control is not applied. If the allowable bandwidth limit is reduced by changing configuration, existing groups are dropped and new channels are not admitted until bandwidth usage is within the new limits.

Use the **no** form of this command to remove the multicast maximum rate limitation on an 802.1Q PVC.

S-VLAN CAC can be used together with per-port CAC. When used together, bandwidth limits are applied hierarchically: S-VLAN bandwidth limits are applied first, followed by port bandwidth limits if the call has not been rejected.

This feature is supported for clientless IP service selection (CLIPS) and PPPoE subscribers. It is also supported for IP over Ethernet (IPoE) VLANs created using the **bind interface** and **bind subscriber** commands. This feature can be used with hitless link aggregation groups (LAGs) and economical access LAGs.

If you are using this feature, consider the following limitations:

- If maximum bandwidth is configured for 802.1Q PVCs with multiencapsulation, only CLIPS and PPPoE subscribers are supported.
- This feature is not supported for Layer 2 Tunneling Protocol Network Server (LNS) subscribers.
- This feature is not supported for 802.1Q PVCs in an 802.1Q tunnel (Q-in-Q or "double-tagged" PVCs).
- This feature is not supported with non-access type LAGs.
- CAC through IGMP is not supported if the multicast source is in front of the SmartEdge router or if local Remote Multicast Replication (RMR) is enabled on the system (that is, if subscribers are receiving traffic through replication at the access node).

If the total volume of downstream traffic to be forwarded on the S-VLAN exceeds its capacity, congestion may occur. In this case, traffic is discarded according to the scheduling parameters configured for the PVC and port. Discarded traffic could include multicast traffic admitted by this feature. This can occur for several reasons:

- IGMP maximum bandwidth has been specified as a percentage value greater than 100% on the port (using the **igmp max-bandwidth** command).
- The maximum bandwidth specified in this command is greater than the maximum QoS scheduling rate configured for the PVC.
- Insufficient bandwidth has been reserved on the PVC for non-multicast traffic.

- There is overall congestion at the port level preventing the PVC from achieving its maximum scheduling rate.
- CAC through IGMP is not supported if the multicast source is in front of the SmartEdge router or if local Remote Multicast Replication (RMR) is enabled on the system (that is, if subscribers are receiving traffic through replication at the access node).

1.22 multicast output

multicast output [**accept-unknown-mac**]

{**no** | **default**} **multicast output** [**accept-unknown-mac**]

1.22.1 Purpose

Enables an interface to forward multicast data, and to send and receive Internet Group Management Protocol (IGMP) control messages.

1.22.2 Command Mode

interface configuration

1.22.3 Syntax Description

accept-unknown-mac	Optional. Accepts IGMP control packets with unknown Medium Access Control (MAC) addresses.

1.22.4 Default

No interface is enabled for multicast data.

1.22.5 Usage Guidelines

Use the **multicast output** command to enable an interface to forward multicast data, and to send and receive IGMP control messages.

An IP over Ethernet (IPoE) circuit, on a Gigabit Ethernet port or an 802.1Q permanent virtual circuit (PVC) configured on it, must be configured on the interface to carry the multicast services. The MAC addresses received from IGMP control packets on the IPoE circuit are compared to the subscriber's MAC address received on the corresponding Point-to-Point Protocol over Ethernet (PPPoE) circuit. By default, if the MAC addresses do not match, the IGMP control packet is dropped. Use the **accept-unknown-mac** keyword to

accept IGMP control packets that have MAC addresses that do not match the subscriber's MAC address.

Note: The **multicast output** command only enables an interface for multicast services; the **multicast destination** command (in IGMP service profile configuration mode) must also be configured to enable the forwarding of multicast data for IGMP messages received on the PPPoE subscriber circuits on the multicast-enabled interface. A single multicast-enabled interface carry multicast data for multiple IGMP service profiles with configured multicast destinations.

Use the **no** form of this command to disable an interface from forwarding multicast data, and from sending and receiving IGMP control messages.

Use the **default** form of this command to disable the acceptance of IGMP control packets with unknown MAC addresses on an interface where the **accept-unknown-mac** keyword is configured.

1.22.6 Examples

The following example enables the **to_dslam5** interface on the **local** context to forward multicast data, and configures the **foo** IGMP service profile to enable the forwarding of multicast data received on a PPPoE subscriber circuit on the **to_dslam5** interface:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface to_dslam5
[local]Redback(config-if)#multicast output accept-unknown-mac
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#igmp service-profile foo
[local]Redback(config-igmp-service-profile)#multicast destination to_dslam5
```

1.23 multicast rate-limit

multicast rate-limit *kbps* **burst-size** *bytes*

no multicast rate-limit

1.23.1 Purpose

Sets the rate and burst tolerance for multicast traffic on any port, circuit, or Virtual Private LAN Services (VPLS) pseudowire circuit to which you assign this bridge profile.

1.23.2 Command Mode

bridge profile configuration

1.23.3 Syntax Description

kbps	Rate in kilobits per second. The range of values is 5 to 1,000,000.
burst-size ***bytes***	Burst tolerance in bytes. The range of values is 1 to 12,000,000.

1.23.4 Default

No rate limiting is imposed on multicast traffic on any port, circuit, or VPLS pseudowire circuit to which you assign this bridge profile.

1.23.5 Usage Guidelines

Use the **multicast rate-limit** command to set the rate and burst tolerance for multicast traffic on any port, circuit, or VPLS pseudowire circuit to which this profile is assigned. For more information about VPLS pseudowire circuits, see *Configuring VPLS*.

Use the **no** form of this command to remove any rate limiting for multicast traffic.

1.23.6 Examples

The following example shows how to create the **prof-isp1** bridge profile and rate limits the multicast traffic to **6000000** kbps and the burst size to **10000** bytes:

```
[local]Redback(config)#bridge profile prof-isp1
[local]Redback(confg-bridge-profile)#multicast rate-limit 600000 burst-size 10000
```

1.24 multi-paths

multi-paths {**external** ***path-num*** [**internal** ***path-num***] | **internal** ***path-num*** [**external** ***path-num***] | **eibgp** ***path-num***}

{no | default} multi-paths {external *path-num* [internal *path-num*] | internal *path-num* [external *path-num*] | eibgp}

1.24.1 Purpose

Configures the Border Gateway Protocol (BGP) routing process to install multiple best equal-cost paths in the routing table for load-balancing traffic to BGP destinations.

1.24.2 Command Mode

BGP router configuration

1.24.3 Syntax Description

external ***path-num***	External BGP (eBGP) equal-cost paths. The ***path-num*** argument specifies the maximum number of equal-cost eBGP best paths a BGP route can have. The range of values is 1 to 8; the default value is 1.
internal ***path-num***	Internal BGP (iBGP) equal-cost paths. The ***path-num*** argument specifies the maximum number of equal-cost iBGP best paths a BGP route can have. The range of values is 1 to 8; the default value is 1.
eibgp ***path-num***	Configures multipath load balancing using both eBGP and iBGP paths in a BGP/Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN). This keyword is not supported for IPv6 traffic. This option is available only in a VPN context. If this option is configured, only one eBGP path is allowed, and the number of allowed iBGP equal cost paths is equal to the **eibgp** ***path-num*** minus 1. For example, if you configure **eibgp 7**, there are six iBGP paths and one eBGP path. The range of values for ***path-num*** is 1 to 8; the default value is 0.

1.24.4 Default

BGP multipath capabilities are disabled.

1.24.5 Usage Guidelines

Use the **multi-paths** command to configure the BGP routing process to install multiple best equal-cost paths in the routing table for load-balancing

traffic to BGP destinations. Equal-cost means that each path has the same weight, local preference, AS path length, origin type, IGP metric, and Multi-Exit Discriminator (MED) attributes if the MED values are learned from the same AS. If one of these attributes is different, the path is not considered to be an equal-cost path.

Use the **external** keyword to balance loads among equal-cost paths from different eBGP neighbors. Use the **internal** keyword to balance loads among equal-cost paths from different iBGP neighbors.

With the exception of eiBGP VPN contexts, BGP either installs all iBGP equal-cost best paths or all eBGP equal-cost best paths, depending on whether the best path that is advertised to the BGP peers is an eBGP path or an iBGP path. Paths learned from BGP confederation peers are considered as iBGP paths. Although multiple paths are installed, only one path (the best path available) is advertised at a time.

Note: When eiBGP is configured, the IGP metric is not considered in equal-cost path calculations.

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

1.24.6 Examples

The following example load balances outgoing traffic packets between either **2** eBGP paths or **5** iBGP paths:

```
[local]Redback(config)#router bgp 64001
[local]Redback(config-bgp)#multi-paths external 2 internal 5
```

The following example configures multipath load balancing in a VPN context among **1** eBGP and up to **6** iBGP equal cost paths:

```
[local]Redback#config
[local]Redback(config)#context vpn1 vpn-rd
[local]Redback(config)#router bgp vpn
[local]Redback(config-bgp)#multi-paths eibgp 7
[local]Redback(config-bgp)#
```

1.25 nak-on-subnet-deletion

nak-on-subnet-deletion

{**no** | **nak-on-subnet-deletion**

1.25.1 Purpose

Instead of dropping a request, when a subnet or range is deleted, responds with a DHCP NAK for lease renewal requests for IP addresses.

1.25.2 Command Mode

DHCP server configuration

1.25.3 Syntax Description

This command has no keywords or arguments.

1.25.4 Default

This functionality is disabled. Lease renewal requests for IP addresses on a deleted subnet or range are dropped.

1.25.5 Usage Guidelines

Use the **nak-on-subnet-deletion** command to make the DHCP server to NAK lease renewal requests for IP addresses on a deleted subnet or range. This will trigger the DHCP clients to reinitiate the discovery process to get a new IP address. When this feature is disabled, renewal requests for IP addresses on a deleted subnet or range will be dropped by the DHCP server. In this case, the DHCP clients will continue to use their IP addresses until the lease expires. Use the **no** form of this command to delete nak-on-subnet-deletion from DHCP server configuration.

1.25.6 Examples

The following example enables this feature:

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

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

[local]Redback(config-dhcp-server)#nak-on-subnet-deletion
```

1.26 national

national

{**no** | **default**} **national**

1.26.1 Purpose

Enables or disables the national bit (bit 12 of set 1) in the E3 frame.

1.26.2 Command Mode

E3 configuration

1.26.3 Syntax Description

This command has no keywords or arguments.

1.26.4 Default

The national bit is disabled

1.26.5 Usage Guidelines

Use the **national** command to enable the national bit (bit 12 of set 1) in the E3 frame.

You enable the national bit if the digital path crosses a geographical border and only if the port is configured with G.751 framing (the default).

Use either the **no** or **default** form of this command to disable the national bit.

1.26.6 Examples

The following example shows how to enable the national bit for the E3 port **1** on the clear-channel E3 traffic card in slot **4:**

```
[local]Redback(config)#port e3 4/1
[local]Redback(config-e3)#framing g751
[local]Redback(config-e3)#national
```

1.27 native-vlan-tag

native-vlan-tag *value*

no native-vlan-tag

1.27.1 Purpose

Configures a native virtual LAN (VLAN) tag for transporting untagged 802.1Q permanent virtual circuit (PVC) traffic across a pseudowire.

1.27.2 Command Mode

VPLS profile neighbor configuration

1.27.3 Syntax Description

value	Native VLAN tag value. The range of values is 1 to 4,095.

1.27.4 Default

The native VLAN tag is not configured.

1.27.5 Usage Guidelines

Use the **native-vlan-tag** command to configure a native VLAN tag for transporting untagged 802.1Q PVC traffic across a pseudowire.

The native VLAN tag value is configurable on the SmartEdge router to enable interoperability with the native VLAN tag used by other devices in the network.

When the native VLAN tag is configured for a pseudowire instance:

- All untagged ingress packets are prepended with the configured native VLAN tag.
- All ingress packets with a VLAN tag value of 0 have that tag value rewritten to the configured native VLAN tag value. The original dot1q bits are not preserved.
- At egress, when a packet is received over a pseudowire, the VLAN tag is removed if its value matches the native VLAN tag value associated with the pseudowire. If the pseudowire is configured with a different native VLAN tag value, or is not configured, then the packet retains its VLAN tag.

Note: Only one native VLAN tag per pseudowire is supported.

Use the **no** form of this command to remove the native VLAN tag configuration.

1.27.6 Examples

The following example configures a native VLAN tag with a tag value of **23:**

```
[local]Redback#config
[local]Redback(config)#vpls profile foo
[local]Redback(config-vpls-profile)#neighbor 10.10.10.1
[local]Redback(config-vpls-profile-neighbor)#native-vlan-tag 23
```

1.28 nat enhanced password

nat enhanced password ***nat_password***

1.28.1 Purpose

Enable enhanced NAT features, such as paired mode and logging. For a list of supported features, see *Configuring NAT Policies*

1.28.2 Command Mode

software license configuration.

1.28.3 Syntax Description

password	Specifies that the password follows is not encrypted.
nat_password	Paid license password that is required to enable NAT enhanced functions.

1.28.4 Default

No enhanced NAT software licensed features and functions are enabled.

1.28.5 Usage Guidelines

Use the **nat enhanced password** command to enable enhanced NAT features and functions. Enter this command in software license configuration mode.

Use the no or default form to disable software licensing and remove any licensing.

1.28.6 Example

The following example shows how to enable NAT enhanced software license features and access software license configuration mode.

```
[local]Redback#configure
Enter configuration commands, one per line, 'end' to exit
[local]Redback(config)#software license
[local]Redback(config-license)#nat ?
  enhanced  Configure NAT enhanced license
[local]Redback(config-license)#nat enhanced ?
  password  Enter password
[local]Redback(config-license)#nat enhanced password password
```

1.29 nat logging-profile

nat logging-profile ***profile***

no nat logging-profile ***profile***

1.29.1 Purpose

Configure an external collector to be used for capturing NAT log messages.

1.29.2 Command Mode

Context Configuration

1.29.3 Syntax Description

profile	Name of logging profile

1.29.4 Default

None.

1.29.5 Usage Guidelines

Use the **nat logging-profile** command to configure an external collector to be used for capturing NAT log messages..

Note: To create a NAT logging profile, you must enable the enhance CGNAT software license by using the **nat enhanced password** ***nat-password*** command.

For information about using an enhanced NAT policy with paired mode and logging, see *Configuring NAT Policies*.

1.29.6 Examples

The following examples shows how to create NAT logging profile

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

1.30 nat policy

nat policy *pol-name* [**enhanced** | **radius-guided**]

no nat policy *pol-name*

1.30.1 Command Mode

context configuration

1.30.2 Syntax Description

pol-name	NAT policy name.
enhanced	Optional. Specifies an enhanced NAT policy that supports paired-mode address translation, P2MP TCP transport (as well as the basic UDP), inbound refresh settings for UDP, port block configuration for IP ranges, and NAT logging profiles. Requires a paid license.
radius-guided	Optional. Specifies a Remote Authentication Dial-In User Service (RADIUS) guided policy and allows the policy to be modified by dynamic access control lists (ACLs).

1.30.3 Default

None

1.30.4 Usage Guidelines

Use the **nat policy** command to create a Network Address Translation (NAT) policy and enter NAT policy configuration mode.

You cannot remove a dynamic policy ACL from the policy after you have configured it, nor can you change the policy type from static to enhanced or RADIUS-guided. To remove a dynamic policy ACL or change its type, delete the policy and then recreate it as a static policy.

Use the **no** form of this command to remove the NAT policy.

1.30.5 Examples

The following example configures a NAT policy, `p2` that translates source addresses on packets received on the interface it is applied to:`pos2` :

```
[local]Redback(config-ctx)#nat policy p2
[local]Redback(config-policy-nat)#ip static in source 34.34.34.34 35.35.35.35
[local]Redback(config-policy-nat)#exit
[local]Redback(config-ctx)#interface pos2
[local]Redback(config-if)#ip nat p2
```

The following example configures an enhanced NAT policy with the following functions:

- The action for the default class is `drop`.
- Uses a previously configured ACL, `nat-acl`). For the named class `nat-class`, IP addresses assigned by NAT translations are from the pool, `nat-pool`, endpoint-independent filtering and inbound refresh is applied to UDP packets.

```
[local]Redback(config-ctx)#nat policy nat-policy-1 enhanced
[local]Redback(config-policy-nat)#drop
[local]Redback(config-policy-nat)#access-group nat-acl
[local]Redback(config-policy-acl)#class nat-class
[local]Redback(config-policy-acl-class)#pool nat-pool-1 nat-context
[local]Redback(config-policy-acl-class)#endpoint-independent filtering tcp
[local]Redback(config-policy-acl-class)#endpoint-independent filtering udp
[local]Redback(config-policy-acl-class)#inbound-refresh udp
```

1.31 nat policy-name

nat policy-name ***pol-name***

no nat policy-name ***pol-name***

1.31.1 Purpose

Attaches the specified Network Address Translation (NAT) policy name to the subscriber's circuit.

1.31.2 Command Mode

subscriber configuration

1.31.3 Syntax Description

pol-name	NAT policy name.

1.31.4 Default

None

1.31.5 Usage Guidelines

Use the **nat policy-name** command to attach the specified NAT policy to the subscriber's circuit.

Use the **no** form of this command to remove the NAT policy from the subscriber's circuit.

1.31.6 Examples

The following example attaches the NAT policy, **nat-pol-1**, to the circuit attached to the **nat-sub** subscriber's circuit:

```
[local]Redback(config-ctx)#subscriber name nat-sub
[local]Redback(config-sub)#nat policy-name nat-pol-1
```

1.32 nbns

nbns {**primary** | **secondary**} ***ip-addr***

no nbns {**primary** | **secondary**} ***ip-addr***

1.32.1 Purpose

Specifies the IP address of the primary or secondary NetBIOS Name Server (NBNS) in the subscriber record or profile.

1.32.2 Command Mode

subscriber configuration

1.32.3 Syntax Description

primary	Specifies that the IP address is for the primary NBNS.
secondary	Specifies that the IP address is for the secondary NBNS.
ip-addr	IP address of the primary or secondary NBNS.

1.32.4 Default

NBNS information is not provided to the subscriber.

1.32.5 Usage Guidelines

Use the **nbns** command to specify the IP address of the primary or secondary NBNS in the subscriber record or profile.

Note: This command does not instruct the SmartEdge router to use the specified name servers in any way for its own purposes. Rather, this information is passed to the subscriber using the Point-to-Point Protocol (PPP) negotiation. The subscriber uses NBNS to obtain IP addresses from NetBIOS names. These values are utilized using PPP when the remote peer requests this information (see RFC 1877, *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*). The SmartEdge router does not push this information to the remote peer.

Use the **no** form of this command to remove the IP address of the primary or secondary NBNS from the subscriber profile or record.

Note: The comparable commands to specify the IP addresses for a Domain Name System (DNS) server are described in *Configuring DNS*.

1.32.6 Examples

The following example specifies the primary address of the NBNS in the record for subscriber **SamQ:**

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

[local]Redback(config-sub)#nbns primary 10.1.1.20
```

1.33 nd profile

nd profile ***profile-name***

{**no**} **nd profile** ***profile-name***

1.33.1 Purpose

Configures a Neighbor Discovery (ND) profile and enters ND profile configuration mode.

1.33.2 Command Mode

Context configuration

1.33.3 Syntax Description

profile-name	ND profile name. Specify up to 39 ASCII characters.

1.33.4 Default

If an ND profile is not assigned to an IPV6 subscriber circuit, ND assigns a default ND profile (GLOBAL DEFAULT PROFILE) to the circuit. This profile consists of default values for each ND parameter.

Note: The default ND profile is included in the output display of the **`show nd profile`** command.

1.33.5 Usage Guidelines

Use the **`nd profile`** command to configure an ND profile or select an existing one for modification, and enter ND profile configuration mode. In ND profile configuration mode, you can configure the ND parameters to apply to the profile. After you create the profile, you can assign it to an IPV6 subscriber by specifying the profile name under the appropriate subscriber record using the **`ipv6 nd profile`** command. For more information about this configuration, see *Configuring ND*.

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

Note: If a profile is deleted, the subscribers using that profile are automatically reassigned to the default ND profile.

1.33.6 Examples

The following example shows how to configure an ND profile **ndprofile7**:

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

[local]Redback(config-ctx)#nd profile ndprofile7
```

1.34 neighbor

neighbor ***ipv6-addr mac-addr***

no neighbor ***ipv6-addr mac-addr***

1.34.1 Purpose

Specifies a static neighbor for this Neighbor Discovery (ND) router interface.

1.34.2 Command Mode

ND router interface configuration

1.34.3 Syntax Description

ipv6-addr	IPv6 address for this neighbor in the format ***A:B:C:D:E:F:G:H***.
mac-addr	Medium Access Control (MAC) address for this neighbor.

1.34.4 Default

No static neighbors are specified for any interface.

1.34.5 Usage Guidelines

Use the **neighbor** command to specify a static neighbor for this ND router interface. Enter this command multiple times to configure more than one neighbor.

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

1.34.6 Examples

The following example specifies a neighbor with IPv6 address, **2006::1/112**, and MAC address, **00:30:88:00:0a:30**, for 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)#neighbor 2006::1/112 00:30:88:00:0a:30
```

1.35 neighbor (BFD)

neighbor ***ip-addr***

no neighbor ***ip-addr***

1.35.1 Purpose

Creates a new Bidirectional Forwarding Detection (BFD) neighbor, or selects an existing one for modification, and enters BFD neighbor configuration mode.

1.35.2 Command Mode

BFD router configuration

1.35.3 Syntax Description

ip-addr	BFD neighbor IP address, in the form ***A.B.C.D***.

1.35.4 Default

No BFD neighbors are configured.

1.35.5 Usage Guidelines

Use the **neighbor** command to create a new BFD neighbor, or select an existing one for modification, and enter BFD neighbor configuration mode.

Use the **no** form of this command to delete a BFD neighbor configuration.

1.35.6 Examples

The following example creates a new BFD neighbor, **10.10.10.1:**

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bfd
[local]Redback(config-bfd)#neighbor 10.10.10.1
[local]Redback(config-bfd-nbr)#
```

1.36 neighbor (BGP)

neighbor {*ip-addr* | *ipv6-addr*} {**external** | **internal**}

no neighbor *ip-addr* {**external** | **internal**}

1.36.1 Purpose

Configures a Border Gateway Protocol (BGP) neighbor and enters BGP neighbor or BGP VPN neighbor configuration mode.

1.36.2 Command Mode

router BGP router configuration

router BGP VPN configuration

1.36.3 Syntax Description

ip-addr	BGP neighbor IP address in the form ***A.B.C.D***.
ipv6-addr	BGP neighbor IP Version 6 (IPv6) address in the form ***A:B:C:D:E:F:G***.
external	Identifies the peer as an external BGP (eBGP) neighbor.
internal	Identifies the peer as an internal BGP (iBGP) neighbor.

1.36.4 Default

There are no preconfigured neighbors.

1.36.5 Usage Guidelines

Use the **neighbor** command to configure a BGP neighbor either for a BGP routing instance or for a BGP instance in a Virtual Private Network (VPN) context. Once specified, the system enters BGP neighbor or BGP VPN configuration mode, respectively.

If you enter the **external** keyword, you must also enable the **remote-as** command in BGP neighbor configuration mode. If you enter the **internal** keyword, the **remote-as** command is not needed.

When the **neighbor** command is issued, the address family for that neighbor defaults to unicast. For an IP Version 4 (IPv4) address family, you

can set the address family to multicast using the **multicast** option of the **address-family ipv4** command; alternatively, you can set the address family to multicast distribution tree (MDT) using the **address-family ipv4 mdt** command. Both of these commands are available in BGP neighbor and BGP VPN neighbor configuration mode.

Use the **no** form of this command to remove a configured BGP neighbor.

1.36.6 Examples

The following example configures an eBGP neighbor at IP address, **102.210.210.1**, and enters BGP neighbor configuration mode:

```
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#neighbor 102.210.210.1 external
[local]Redback(config-bgp-neighbor)#
```

The following example configures an iBGP neighbor at IPv6 address, **28FF:AA12:0DB8:85A3::2000**, and enters BGP neighbor configuration mode:

```
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#neighbor 28FF:AA12:0DB8:85A3::2000 internal
[local]Redback(config-bgp-neighbor)#
```

1.37 neighbor (OSPF)

neighbor{*ip-addr* | *ipv6-addr*} [**cost** *cost*] [**poll-interval** *interval*] [**router-priority** *priority*]

no neighbor {*ip-addr* | *ipv6-addr*} [**cost** *cost*] [**poll-interval** *interval*] [**router-priority** *priority*]

1.37.1 Purpose

Configures an Open Shortest Path First (OSPF) or OSPF Version 3 (OSPFv3) neighbor.

1.37.2 Command Mode

- OSPF interface configuration

- OSPF3 interface configuration

1.37.3 Syntax Description

ip-addr	OSPF neighbor IP address in the form ***A.B.C.D***.
ipv6-addr	OSPFv3 neighbor IP Version 6 (IPv6) address in the form ***A:B:C:D:E:F:G***.
cost ***cost***	Optional. Cost to reach the neighbor. This cost overrides the interface cost set through the **cost** command (in OSPF or OSPF3 interface configuration mode). The range of values is 1 to 65,535; the default value is 1.
poll-interval ***interval***	Optional. Interval, in seconds, at which the neighbor is polled when it is unreachable or down. The range of values is 1 to 65,535; the default value is 120.
router-priority ***priority***	Optional. Priority setting for the neighbor. The range of values is 0 to 255; the default value is 1.

1.37.4 Default

If a cost value is not specified, the value set through the **cost** command is used; otherwise, the cost is 1. The poll interval is 120 seconds; the router priority is 1.

1.37.5 Usage Guidelines

Use the **neighbor** command to configure an OSPF or OSPFv3 neighbor.

You can only use the **router-priority** ***priority*** construct for nonbroadcast multiaccess (NBMA) networks when designated and backup routers are elected.

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

1.37.6 Examples

The following example sets a cost of **10** for the neighbor at IP address **193.12.3.2:**

```
[local]Redback(config-ospf-if)#neighbor 193.12.3.2 cost 10
```

1.38 neighbor mac-flush

neighbor mac-flush

no neighbor mac-flush

1.38.1 Purpose

Sends a MAC withdrawal message to VPLS hub peers when the spoke pseudowire state on the PE-RS node changes to active state.

1.38.2 Command Mode

VPLS configuration

1.38.3 Syntax Description

This command has no keywords or arguments.

1.38.4 Default

A MAC withdrawal message is not sent to VPLS hub peers when the spoke pseudowire state on the PE-RS node changes to active state.

1.38.5 Usage Guidelines

Use the **neighbor mac-flush** command on the PE-RS node to send a MAC withdrawal message to VPLS hub peers when the spoke pseudowire state on the PE-RS node changes to active state. Enabling this option improves MAC forwarding convergence time.

Use the **no** form of this command to disable the sending of MAC withdrawal messages.

1.38.6 Examples

The following example sends MAC withdrawal message to VPLS hub peers when the pseudowire state changes to active state:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#bridge isp224-bridge
[local]Redback(config-bridge)#vpls
[local]Redback(config-vpls)#neighbor mac-flush
```

1.39 neighbor password

neighbor ***ip-addr*** **password** ***password***

no neighbor *ip-addr* **password**

1.39.1 Purpose

Assigns an encrypted Message Digest 5 (MD5) password to a Label Distribution Protocol (LDP) neighbor.

1.39.2 Command Mode

LDP router configuration

1.39.3 Syntax Description

ip-addr	Neighbor IP address in the form *A.B.C.D*.
password	Alphanumeric string consisting of up to 80 characters.

1.39.4 Default

MD5 password is disabled.

1.39.5 Usage Guidelines

Use the **neighbor password** command to assign an encrypted MD5 password to an LDP neighbor.

Note: For an LDP session to be established, the MD5 password must be the same on both the router and its neighbor.

Use the **no** form of this command to remove the password from an LDP neighbor.

1.39.6 Examples

The following example assigns the password, **secret**, to LDP neighbor, **10.1.1.1:**

```
[local]Redback(config-ctx)#router ldp
[local]Redback(config-ldp)#neighbor 10.1.1.1 password secret
```

1.40 neighbor profile

neighbor profile *prof-name*

no neighbor profile *prof-name*

1.40.1 Purpose

Creates an empty Access Node Control Protocol (ANCP) profile for an ANCP neighbor peer, and accesses ANCP neighbor configuration mode.

1.40.2 Command Mode

ANCP configuration

1.40.3 Syntax Description

prof-name	ANCP neighbor profile name.

1.40.4 Default

No ANCP neighbor profile exists.

1.40.5 Usage Guidelines

Use the **neighbor profile** command to create an ANCP neighbor profile and access ANCP neighbor configuration mode.

The SmartEdge router listens for incoming ANCP sessions, using the Transmission Control Protocol (TCP) local port that you have configured with the **tcp-port local** command (in ANCP configuration mode). When an ANCP session is received, its attributes must match the attributes you have configured for one of the ANCP neighbor profiles. This means that the session must match each attribute that you have configured for the profile. If an attribute is not configured, then any value for that attribute is accepted. For example, if the remote TCP port is not configured, then the incoming session can have any source port number, as long as the other items match. An empty neighbor profile with no attributes configured allows all incoming connections.

Use the **no** form of this command to delete this ANCP neighbor profile.

1.40.6 Examples

The following example creates the **ancp-profile** ANCP neighbor profile and accesses ANCP neighbor configuration mode:

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

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

1.41 neighbor targeted

neighbor *ip-addr* targeted

no neighbor *ip-addr* targeted

1.41.1 Purpose

Configures a remote Label Distribution Protocol (LDP) neighbor and enables extended LDP discovery of the specified neighbor.

1.41.2 Command Mode

LDP router configuration

1.41.3 Syntax Description

ip-addr	IP address of the remote LDP neighbor in the form ***A.B.C.D***.

1.41.4 Default

Extended LDP discovery is disabled.

1.41.5 Usage Guidelines

There are two types of LDP neighbor discovery mechanisms: basic LDP discovery and extended LDP discovery. Basic LDP discovery is used to discover immediate neighbors; extended LDP discovery is used to discover neighbors that can be multiple hops away.

There are two types of LDP Hello messages: link Hello messages and targeted Hello messages. Link Hello messages are multicast on an interface to immediate neighbors. Link Hello messages are used in basic LDP discovery. Targeted Hello messages are unicast directly to remote neighbors, and are used in extended LDP discovery. Two LDP speaking label-switched routers (LSRs) can form LDP adjacencies after discovering each other. LDP adjacencies discovered by link Hello messages are link Hello adjacencies. LDP adjacencies discovered by targeted Hello messages are targeted Hello adjacencies.

Use the **neighbor targeted** command to configure a remote LDP neighbor and enable extended LDP discovery of the specified neighbor. Targeted Hello messages can be transmitted or accepted to or from the specified neighbor.

Use the **no** form of this command to remove a configured remote LDP neighbor, and to disable extended LDP discovery of the specified neighbor.

1.41.6 Examples

The following example configures a remote neighbor of address **10.1.1.1**:

```
[local]Redback(config-ctx)#router ldp
[local]Redback(config-ldp)#neighbor 10.1.1.1 targeted
```

1.42 neighbor (VPLS)

neighbor ***ip-addr***

{**no** | **default**} **neighbor** ***ip-addr***

1.42.1 Purpose

Creates a new neighbor, or selects an existing one for modification, and enters Virtual Private LAN Services (VPLS) profile neighbor configuration mode.

1.42.2 Command Mode

VPLS profile configuration

1.42.3 Syntax Description

ip-addr	Neighbor IP address, in the form A.B.C.D.

1.42.4 Default

None

1.42.5 Usage Guidelines

Use the **neighbor** command to create a new neighbor, or select an existing one for modification, and enter VPLS profile neighbor configuration mode.

The neighbor is identified by the IP address of the remote provider edge (PE) device. It is used along with the pseudowire ID from the VPLS instance configuration to establish a pseudowire between the local and remote PE devices. Multiple peering sessions (created by VPLS profiles) can be established to the same PE device; different profiles can reference the same remote PE IP address.

Use the **no** or **default** form of this command to remove a configured neighbor.

1.42.6 Examples

The following example creates a new VPLS neighbor with the IP address, **10.10.10.1:**

```
[local]Redback#config

[local]Redback(config)#vpls profile foo

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

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

1.43 net

net*net*

no net*net*

1.43.1 Purpose

Configures a network entity title (NET) for the Intermediate System-to-Intermediate System (IS-IS) routing process.

1.43.2 Command Mode

IS-IS router configuration

1.43.3 Syntax Description

net	Area address and system ID for the IS-IS routing process. This argument can be either an address in hexadecimal-dotted byte format or a name.

1.43.4 Default

A NET is mandatory for IS-IS operation. If this option is not configured, the IS-IS instance is disabled.

1.43.5 Usage Guidelines

Use the **net** command to configure a NET for the IS-IS routing process.

Network entity titles can be anywhere between 8 and 20 bytes in length, and are provided in a hexadecimal-dotted byte format, such as 47.0005.80ff.e200.02aa.0a00.0002.00. The last byte, which is the Network Service Access Point (NSAP) n-selector, must be zero. The 6 bytes before the last byte indicate the system ID. This ID must be the same for all NETs configured for the system, and must be unique within the IS-IS domain. The bytes before that indicate an area ID, which is a variable from 1 to 13 bytes. Multiple areas can be specified in scenarios of area merges and the necessity of renumbering. The protocol will not form a level 1 adjacency between two devices if they have no areas in common.

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

1.43.6 Examples

The following example assigns a NET of **47.0001.0002.0002.0002.00** to the **ip-backbone** IS-IS instance:

```
[local]Redback(config-ctx)#router isis ip-backbone
[local]Redback(config-isis)#net 47.0001.0002.0002.0002.00
```

1.44 netop

netop

no netop

1.44.1 Purpose

Enables the NetOp™ daemon, which allows the SmartEdge router to communicate with the NetOp Element Management System (EMS) server, and enters NetOp configuration mode.

1.44.2 Command Mode

global configuration

1.44.3 Syntax Description

This command has no keywords or arguments.

1.44.4 Default

The NetOp daemon is disabled.

1.44.5 Usage Guidelines

Use the **netop** command to enable the NetOp daemon, which allows the SmartEdge router to communicate with the NetOp EMS server, and enter NetOp configuration mode.

Use the **no** form of this command to disable communication with the NetOp EMS server.

Note: You must configure the Simple Network Management Protocol (SNMP) community before you specify the version of the SNMP traps that the NetOp EMS server receives.

1.44.6 Examples

The following example enables the SmartEdge router to communicate with the NetOp EMS server and enters NetOp configuration mode:

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

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

1.45 network

network{*ip-addr/prefix-length* | *ipv6-addr/prefix-length*} [**route-map** *map-name*]

no network{*ip-addr/prefix-length* | *ipv6-addr/prefix-length*} [**route-map** *map-name*]

1.45.1 Purpose

Originates Border Gateway Protocol (BGP) routes that are advertised to peers for the BGP address family.

1.45.2 Command Mode

BGP address family configuration

1.45.3 Syntax Description

ip-addr/prefix-length	Specifies the IP address, in the form ***A.B.C.D***, and the prefix length, separated by the slash (**/**) character. The range of values for the ***prefix-length*** argument is 0 to 32.
ipv6-addr/prefix-length	Specifies the IP Version 6 (IPv6) address, in the form ***A:B:C:D:E:F:G:H***,and the prefix length, separated by the slash (**/**) character. The range of values for the ***prefix-length*** argument is 0 to 128.
route-map ***map-name***	Optional. Route map conditions to apply to the prefix.

1.45.4 Default

No routes are specified.

1.45.5 Usage Guidelines

Use the **network** command to originate BGP routes that are advertised to peers.

Use the **route-map** ***map-name*** construct to apply a route map to modify the BGP attributes of these routes. Routes specified in the **network** command must exist in the routing table to generate those routes into BGP.

Note: The **network** command is available in the local context only. You cannot configure the network statement inside an IP VPN.

Use the **no** form of this command to remove routes.

1.45.6 Examples

The following example advertises unicast route **120.34.56.0/24** to unicast BGP neighbors. Multicast route **40.0.0.0/8** is advertised to multicast BGP neighbors using a metric of 100. The two **ip route** commands in context configuration mode statically add these routes to the routing table:

```
[local]Redback(config-ctx)#ip route 40.0.0.0/8 null0
[local]Redback(config-ctx)#ip route 120.34.56.0/24 null0
[local]Redback(config-ctx)#route-map map1
[local]Redback(config-route-map)#set metric 100
[local]Redback(config-route-map)#exit
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#address-family ipv4 unicast
[local]Redback(config-bgp-af)#network 120.34.56.0/24
[local]Redback(config-bgp-af)#exit
[local]Redback(config-bgp)#address-family ipv4 multicast
[local]Redback(config-bgp-af)#network 40.0.0.0/8 route-map map1
```

1.46 network-type

network-type {**broadcast** | **non-broadcast** | **point-to-point** | **point-to-multipoint**}

no network-type

1.46.1 Purpose

Configures the Open Shortest Path First (OSPF) or OSPF Version 3 (OSPFv3) network type.

1.46.2 Command Mode

- OSPF interface configuration
- OSPF3 interface configuration

1.46.3 Syntax Description

broadcast	Specifies that the interface is attached to a broadcast network.
non-broadcast	Specifies that the interface is attached to a nonbroadcast network.
point-to-point	Specifies that the interface is attached to a point-to-point (P2P) network.
point-to-multipoint	Specifies that the interface is attached to a point-to-multipoint (P2MP) network.

1.46.4 Default

The media type determines the network type; for example, an Ethernet interface defaults to the broadcast type.

1.46.5 Usage Guidelines

Use the **network-type** command to configure the following types of OSPF or OSPF3 networks:

- Broadcast network—Broadcast networks support multiple routers and have the ability to address a single physical message to all attached routers.
- Nonbroadcast multiaccess (NBMA)—A nonbroadcast network, such as X.25, that simulates an OSPF or OSPFv3 broadcast network.
- P2P network—A P2P network joins a single pair of routers.
- P2MP network—Acts as though the nonbroadcast network is a collection of P2P links.

Use the **no** form of this command to return the network type to its default value.

1.46.6 Examples

The following example configures the network type as a broadcast network:

```
[local]Redback(config-ospf-if)#network-type broadcast
```

1.47 next-hop

next-hop ***next-hop-addr*** ***{*****loose** | **strict*****}***

no next-hop ***next-hop-addr***

1.47.1 Purpose

Configures a next-hop entry for a Resource Reservation Protocol (RSVP) explicit route, or for a static label-switched path (LSP).

1.47.2 Command Mode

- MPLS static LSP configuration
- RSVP explicit route configuration

1.47.3 Syntax Description

next-hop-addr	IP address of the next-hop label-switched router (LSR).
loose	Specifies that the next hop does not need to be directly connected to the previous node.
strict	Specifies that the next hop is directly connected to the previous node in the path.

1.47.4 Default

Strict

1.47.5 Usage Guidelines

Use the **next-hop** command to configure a next-hop entry for an RSVP explicit route, or for a static LSP.

Use the **no** form of this command to remove a next-hop entry from an RSVP explicit route. You cannot remove a next-hop entry from a static LSP.

1.47.6 Examples

The following example configures two next-hop entries for an RSVP explicit route:

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

The following example configures two next-hop entries for a static LSP:

```
[local]Redback(config-ctx)#router mpls-static
[local]Redback(config-mpls-static)#lsp 24
[local]Redback(config-mpls-static-lsp)#next-hop 20.20.20.10
[local]Redback(config-mpls-static-lsp)#next-hop 30.20.20.16
```

1.48 next-hop-on-lsp

next-hop-on-lsp

no next-hop-on-lsp

1.48.1 Purpose

Requires the next hop of a Border Gateway Protocol (BGP) Virtual Private Network (VPN) path to be reachable through a Multiprotocol Label Switching (MPLS) label-switched path (LSP) or a tunnel in order for a VPN route to be considered active.

1.48.2 Command Mode

BGP router configuration

1.48.3 Syntax Description

This command has no keywords or arguments.

1.48.4 Default

The next hop of a BGP VPN path must be reachable through an MPLS LSP or a tunnel in order for the VPN route to be considered active.

1.48.5 Usage Guidelines

Use the **next-hop-on-lsp** command to require the next hop of a BGP VPN path to be reachable through an MPLS LSP or a tunnel, in order for a VPN route to be considered active.

Use the **no** form of this command to enable a BGP VPN path to be considered active without requiring the next hop of a VPN path to be reachable through an MPLS LSP or a tunnel.

One common application for this command is configuring a BGP route reflector that is not part of an MPLS network, but is used to reflect BGP VPN routes to its clients within that MPLS network. In this configuration, the next hops of the VPN paths may not be reachable through an MPLS LSP or a tunnel from the route reflector's point of view. To solve the problem, use the **no** form of this command to disable the LSP or tunnel reachability check for the next hops, and therefore allow the BGP route reflector to correctly select the best paths and reflect the best paths to its clients.

1.48.6 Examples

The following example enables the sending of BGP VPN routes when the next hop is not resolved or reachable:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bgp
[local]Redback(config-bgp)#next-hop-on-lsp
[local]Redback(config-bgp)#
```

1.49 next-hop-self

next-hop-self

no next-hop-self

1.49.1 Purpose

Advertises the local peer address as the next-hop address for all external Border Gateway Protocol (eBGP) routes sent to the specified neighbor or peer group.

1.49.2 Command Mode

- BGP neighbor configuration

- BGP peer group configuration

1.49.3 Syntax Description

This command has no keywords or arguments.

1.49.4 Default

The command is disabled.

1.49.5 Usage Guidelines

Use the **next-hop-self** command to advertise the local peer address as the next-hop address for all eBGP routes sent to the specified BGP neighbor or peer group. This command disables the sending of third-party next-hop information to peers.

By default, when it receives BGP routes from an eBGP neighbor, the BGP routing process forwards eBGP routes to its internal BGP (iBGP) neighbors without changing the next-hop address; this is still the case if the eBGP neighbors are on the same subnet as the local BGP speaker.

When you enable the **next-hop-self** command, the BGP routing process changes the next-hop address, advertising the local peer address as the next-hop address for all received eBGP routes.

Use the **no** form of this command to restore the default behavior of sending third-party next-hop information to peers.

1.49.6 Examples

The following example ensures that all updates destined for the neighbor at IP address, **10.100.1.102**, advertise this SmartEdge router as the next hop:

```
[local]Redback(config-ctx)#router bgp 64001
[local]Redback(config-bgp)#neighbor 10.100.1.102 external
[local]Redback(config-bgp-neighbor)#remote-as 64001
[local]Redback(config-bgp-neighbor)#next-hop-self
```

The following example provides output from the **show bgp neighbor** command where the neighbor views the SmartEdge router as the next hop for all received routes:

```
[local]Redback>show bgp neighbor 10.100.1.102

BGP neighbor: 10.100.1.102, remote AS: 64001, internal link
Version: 4, router identifier: 10.100.1.102
State: Established for 00:41:01
.
.
.
Next hop set to self (next-hop-self)
.
.
.
Prefixes: advertised 99877, accepted 2, active 2
```

1.50 nexthop triggered

nexthop triggered

no nexthop triggered

1.50.1 Purpose

Enables the triggering of an immediate BGP best-path calculation on notification of a next-hop change by the RIB.

1.50.2 Command Mode

BGP address family configuration

1.50.3 Syntax Description

This command has no keywords or arguments.

1.50.4 Default

Next-hop triggering is disabled.

1.50.5 Usage Guidelines

Use the **nexthop triggered** command to the triggering of an immediate BGP best-path calculation on notification of a next-hop change by the RIB.

You must enter the **nexthop triggered** command separately for each BGP instance on which you want to enable next-hop triggering.

Note: The **nexthop triggered** command is supported for IPv4 BGP UNI address families only.

Use the **no** form of this command to disable next-hop triggering on a BGP instance.

1.50.6 Examples

The following example shows how to enable the triggering of an immediate BGP best-path calculation on notification of a next-hop change by the RIB:

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#address-family ipv4 vpn
[local]Redback(config-bgp-af)#nexthop triggered
```

1.51 nexthop triggered delay

nexthop triggered delay {**millisecond** *msec* | *seconds*}

no nexthop triggered delay {**millisecond** *msec* | *seconds*}

1.51.1 Purpose

Defines the delay, in milliseconds or seconds, before starting a best path calculation after a next-hop change.

1.51.2 Command Mode

BGP address family configuration

1.51.3 Syntax Description

millisecond ***msec***	Minimum number of milliseconds that must pass after a next-hop change before a best path calculation begins. Values range from 0 through 30,000 milliseconds. A value of 0 triggers an immediate best path calculation.
seconds	Minimum number of seconds that must pass after a next-hop change before a best path calculation begins. Values range from 0 through 30 seconds. A value of 0 triggers an immediate best path calculation.

1.51.4 Default

3 seconds or 3000 milliseconds

1.51.5 Usage Guidelines

Use the **nexthop triggered delay** command to configure the minimum number of milliseconds or seconds before a best path calculation begins following a next-hop change. This delay allows the accumulation of more than one next-hop change into a single best path calculation when multiple next-hop change events are expected in response to a network event.

Note: Next-hop-triggered BGP best-path calculation is not supported for the IPv4 multicast address family.

Use the **no** form of this command to return the router to the default setting in which next-hop scans occur every 3 seconds.

1.51.6 Examples

The following example configures a 20 second delay before starting a best path calculation after a next-hop change:

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#address-family ipv4 vpn
[local]Redback(config-bgp-af)#nexthop triggered delay 20
```

The following example configures a 40 millisecond delay before starting a best path calculation after a next-hop change:

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#address-family ipv4 vpn
[local]Redback(config-bgp-af)#nexthop triggered delay millisecond 40
```

1.52 nexthop triggered holdtime

nexthop triggered holdtime {**milliseconds** *msec* | *seconds*}
[**backoff milliseconds** *msec* | *seconds*]

no nexthop triggered holdtime

1.52.1 Purpose

Defines the minimum interval, in seconds or milliseconds, between two consecutive next-hop triggered best path calculations.

1.52.2 Command Mode

BGP address-family configuration

1.52.3 Syntax Description

seconds	Time, in seconds, between two consecutive next-hop triggered best path calculations. The range of values is 0 through 30 seconds; the default value is 3. A value of 0 allows a second next-hop triggered best path calculation immediately after the previous best path calculation.
millisecond *msec*	Time, in milliseconds, between two consecutive next-hop triggered best path calculations. The range of values is 0 through 30,000 milliseconds. A value of 0 allows a second next-hop triggered best path calculation immediately after the previous best path calculation.
backoff*seconds*	Optional. Time, in seconds, by which BGP increases the hold down time between two consecutive next-hop triggered best path calculations. The range of values is 0 through 30 seconds.
backoff millisecond *msec*	Optional. Time, in milliseconds, by which BGP increases the hold down time between two consecutive next-hop triggered best path calculations. The range of values is 0 through 30,000 milliseconds.

1.52.4 Default

holdtime ***seconds*** equals 3 seconds or 3000 milliseconds

1.52.5 Usage Guidelines

Use the **nexthop triggered holdtime** command to define the minimum interval between two consecutive next-hop triggered best path calculations.

You must enter the **nexthop triggered holdtime** command separately for each BGP instance for which you want to define the minimum interval between next-hop triggered best path calculations.

A hold time is not applicable across different hext-hop changes. In other words, a next-hop change for 10.12.13.14/32 followed by a next-hop change for 10.40.50.60/32 does not trigger a hold time. A next-hop change caused by an IGP route change and a next-hop change caused by an LSP route change will have individual hold times.

Note: The **nexthop triggered holdtime** command is not supported for IPv4 multicast address family.

Use the **no** form of this command to disable next-hop triggering on a BGP instance.

1.52.6 Examples

The following example configures a minimum interval of 15 seconds between two consecutive next-hop triggered best path calculations:

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#address-family ipv4 vpn
[local]Redback(config-bgp-af)#nexthop triggered holdtime 15
```

The following example configures a minimum interval of 40 milliseconds between two consecutive next-hop triggered best path calculations:

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#address-family ipv4 vpn
[local]Redback(config-bgp-af)#nexthop triggered holdtime 40
```

1.53 next-hop-unchanged

[no] **next-hop-unchanged**

1.53.1 Command Mode

BGP peer address-family configuration

1.53.2 Syntax Description

This command has no keywords or arguments.

1.53.3 Default

1.53.4 Usage Guidelines

Use the **next-hop-unchanged** command to enable the router to redistribute the iBGP path's nexthop unchanged to external neighbors. Enter the command in the local context as part of the eBGP neighbor address-family configurations.

Use the **no** form of the command to disable this functionality.

1.53.5 Examples

The following example enables the router to redistribute the iBGP path's nexthop unchanged for both IPv4 and IPv6 address-families to the neighbor at IP address, 2.2.2.2:

```
router bgp 400
  address-family ipv4 unicast
  address-family ipv4 vpn
  address-family ipv6 vpn
!
  neighbor 2.2.2.2 external
   ... (some configurations removed)
   address-family ipv4 unicast
   address-family ipv4 vpn
      next-hop-unchanged
   address-family ipv6 vpn
      next-hop-unchanged
```

1.54 no debug all

debug all

1.54.1 Purpose

Disables the generation of all debug message types supported by the SmartEdge router.

1.54.2 Command Mode

exec (10)

1.54.3 Syntax Description

This command has no keywords or arguments.

1.54.4 Default

Debugging is disabled.

1.54.5 Usage Guidelines

Use the **no debug all** command to disable the generation of all debug messages types supported by the SmartEdge router. The **no debug all** command displays the functions of the **debug** commands, which are listed in Table 3.

Table 3 Related Debug Commands

Feature	Command
General system processes	**debug rcm**, **debug snmp**, **debug ssh**
IP routing	**debug ip routing**, **debug isis all**, **debug ospf**, **debug policy general**, **debug rip**, **debug vrrp**
BGP routing	**debug bgp event**, **debug bgp listen**, **debug bgp message**, **debug bgp policy**, **debug bgp rib**, **debug bgp session-state**, **debug bgp update**
IP services	**debug arp**, **debug dhcp-relay**, **debug ip dns**, **debug nat**, **debug ntp**
Quality of service	**debug qos**
Access control lists	**debug cls**, **debug ip-access-list**
Authentication	**debug aaa**

1.54.6 Examples

The following example disables the generation of all debugging messages:

```
[local]Redback#no debug all
```

1.55 nonstop-routing

nonstop-routing

no nonstop-routing

1.55.1 Purpose

OSPF nonstop routing (NSR) maintains OSPF neighbor relationships and operations in steady state if the active XCRP Controller card fails and switches over to the standby XCRP Controller card. Consequently, other OSPF routers in the network do not detect the failure of the active XCRP Controller card, and the OSPF routing domain continues to operate in steady state. All other routing domains will be disrupted.

1.55.2 Command Mode

OSPF router configuration

1.55.3 Syntax Description

---	This command has no keywords or arguments.

1.55.4 Default

None

1.55.5 Usage Guidelines

Use the **nonstop-routing** command to maintain OSPF neighbor relationships and operations in steady state when the active XCRP Controller card fails and switches over to the standby XCRP Controller card. The OSPF routing domain continues to operate in steady state.

If both nonstop-routing and graceful-restart are configured, non-stop routing is used on XCRP Controller switchover. However, when OSPF restarts,

graceful-restart is used. Using NSR with fast-hello is discouraged. Some adjacencies might be terminated prematurely because of the fast-hello setup.

Use the **no** form of this command to disable NSR.

Note: Use the **show ospf** command on the standby XCRP Controller card to verify its availability for NSR support. You can also use other commands, such as **show ospf database**, **show ospf neighbor**, and **show osfp interface**, to verify active and standby XCRP Controller card synchronization.

1.55.6 Examples

The following example enables NSR.

```
[local]Redback#config
[local]Redback(config)#context 1
[local]Redback(config-ctx)#router osf 1
[local]Redback(config-ospf)#nonstop-routing
[local]Redback(config-ospf)#no nonstop-routing
```

1.56 notify

notify ***notify-oid***

no notify

1.56.1 Purpose

Identifies the name of the notification you want to use for the SNMP alarm model.

1.56.2 Command Mode

SNMP alarm model configuration

1.56.3 Syntax Description

notify-oid	Object identifier (OID) in words or numbers of the notification you are using for the SNMP alarm model.

1.56.4 Default

None

1.56.5 Usage Guidelines

Use the **notify** command to identify the name of the notification to use for the SNMP alarm model. Set the name by identifying the OID (in name or number) of the notification to configure.

Use the **no** form of this command to remove the name of the notification for this alarm model.

1.56.6 Examples

The following example shows how to name the **linkup** notification as the notification for this alarm model.

```
[local]jazz#config
[local]jazz(config)#snmp alarm model 1 state clear
[local]jazz(config-snmp-alarmmodel)#notify linkUp
[local]jazz(config-snmp-alarmmodel)#
```

1.57 ns-retry-interval

ns-retry-interval ***retrans-timer***

{**no** | **default**} **ns-retry-interval**

1.57.1 Purpose

Specifies the value for the Retrans Timer field.

1.57.2 Command Mode

- ND profile configuration
- ND router configuration
- ND router interface configuration

1.57.3 Syntax Description

retrans-timer	Value for the Retrans Timer field (in milliseconds). The range of values is 0 to 4294967295; the default value is 5,000.

1.57.4 Default

The default value for the Retrans Timer field is 5,000.

1.57.5 Usage Guidelines

Use the **ns-retry-interval** command to specify the value for the Retrans Timer field, which is the time between retransmitted Neighbor Solicitation (NS) messages. In ND profile configuration mode, this command specifies the value for the specified ND profile. In ND router configuration mode, this command specifies the global value for all interfaces; in ND router interface configuration mode, it specifies the value for this ND router interface. If specified, the setting for the interface overrides the global setting.

Use the **no** or **default** form of this command to specify the default value for the Retrans Timer field.

In the ND profile configuration mode, only the **default** form of this command is available to specify the default value for the Retrans Timer field. The **no** form of this command is not available.

1.57.6 Examples

The following example specifies **30** milliseconds for the Retrans Timer field for the ND profile **ndprofile7**:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#nd profile ndprofile7
[local]Redback(config-nd-profile)#ns-retry-interval 30
```

The following example specifies **100** milliseconds for the Retrans Timer field for the ND router:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router nd
[local]Redback(config-nd-if)#ns-retry-interval 100
```

The following example specifies **20** milliseconds for the Retrans Timer field for the ND router interface, **int1**, which overrides the global setting:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router nd
[local]Redback(config-nd)#interface int1
[local]Redback(config-nd-if)#ns-retry-interval 20
```

1.58 nssa-range

nssa-range*ip-addr* {*netmask*| */prefix-length*} [**not-advertise** | **tag** ***tag***]

no nssa-range*ip-addr* {***netmask***| ***/prefix-length***} [**not-advertise** | **tag** ***tag***]

1.58.1 Purpose

Summarizes not-so-stubby-area (NSSA) routes advertised by an area border router (ABR).

1.58.2 Command Mode

- OSPF area configuration
- OSPF3 area configuration

1.58.3 Syntax Description

ip-addr	IP address in the form ***A.B.C.D***.
netmask	Network mask in the form ***E.F.G.H***.
prefix-length	Prefix length. The range of values is 0 to 32.
not-advertise	Optional. Prevents all routes in the specified range from being advertised in inter-area route summarizations.
tag ***tag***	Optional. Route tag included in translated external route summarization Type 5 link-state advertisements (LSAs). An unsigned 32-bit integer, the range of values is 1 to 4,294,967,295; the default value is 0.

1.58.4 Default

Address ranges for NSSA route summarization are not specified.

1.58.5 Usage Guidelines

Use the **nssa-range** command to summarize NSSA routes advertised by an ABR. This command is used for NSSA-translated external route summarization and is only relevant when the router is configured as an ABR.

Use the optional **not-advertise** keyword to prevent the specified route from being advertised in translated external route summarizations.

Use the **no** form of this command to disable route summarization for a particular summary range. All individual routes contained in the summary range are advertised to other areas.

1.58.6 Examples

The following example sends routes that fall into the range **10.1.0.0 255.255.0.0** as a single autonomous system (AS) external advertisement:

```
[local]Redback(config-ospf-area)#nssa-range 10.1.0.0 255.255.0.0
```

1.59 ntp-broadcast

ntp-broadcast [*delay-num*]

{**no** | **default**} **ntp-broadcast [*delay-num*]**

1.59.1 Purpose

Enables an NTP server to broadcast time updates to all clients on a subnet.

1.59.2 Command Mode

interface configuration

1.59.3 Syntax Description

delay-num	Time delay for NTP broadcasts, in microseconds (ms); the valid range is 0 to 999,999. The default is 3000.

1.59.4 Default

The NTP server does not broadcast time updates.

1.59.5 Usage Guidelines

Use the **ntp-broadcast** command in interface mode to enable the NTP server for a context to broadcast time updates to NTP clients. The clients must be on the same subnet as the server. Add the **ntp-broadcast** command to the interface leading to the subnet; set the broadcast address to `255.255.255.255`.

Use the **no** form of the command to disable the NTP server from broadcasting time updates to its clients.

1.59.6 Examples

The following example enables NTP broadcast on the **ntp** interface in a context set up as an NTP server.

```
[local]Redback(config-ctx)#interface ntp
[local]Redback(config-if)#ntp-broadcast
```

1.60 ntp-mode

ntp-mode

1.60.1 Purpose

Enters NTP server configuration mode.

1.60.2 Command Mode

context configuration

1.60.3 Syntax Descriptions

This command has no keywords or arguments.

1.60.4 Default

None

1.60.5 Usage Guidelines

Use the **ntp-mode** command to enter NTP server configuration mode.

1.60.6 Examples

The following example changes the mode from context configuration to NTP server configuration mode:

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

1.61 num-queues

In MDRR and PWFQ policy configuration modes, the command syntax is:

num-queues {**1** | **2** | **4** | **8**}

{**no** | **default**} **num-queues**

In ATMWFQ policy and queue map configuration modes, the command syntax is:

num-queues {**2** | **4** | **8**}

{**no** | **default**} **num-queues**

1.61.1 Purpose

In ATMWFQ, MDRR, or PWFQ policy configuration mode, specifies the number of queues for the policy.

In queue map configuration mode, specifies the number of queues for the quality of service (QoS) queue map, and enters num-queues configuration mode.

1.61.2 Command Mode

- ATMWFQ policy configuration
- MDRR policy configuration
- PWFQ policy configuration
- queue map configuration

1.61.3 Syntax Description

1	Specifies that the policy has one queue.(1)
2	Specifies that the policy has two queues.(2)
4	Specifies that the policy has four queues.(1)
8	Specifies that the policy has eight queues.(1)

(1) In MDRR and PWFQ policy configuration modes
(2) In ATMWFQ and queue map configuration modes

1.61.4 Default

For queue maps, modified deficit round-robin (MDRR) and priority weighted fair queuing (PWFQ) policies, the default number of queues is 8. For Asynchronous Transfer Mode weighted fair queuing (ATMWFQ) policies, the default value is 4.

1.61.5 Usage Guidelines

Use the **num-queues** command in ATMWFQ policy, MDRR policy, or PWFQ policy configuration mode to specify the number of queues to be used for the policy.

Use the **num-queues** command in queue map configuration mode to specify number of queues for the queue map, and to enter num-queues configuration mode.

A queue map consists of three independent subprofiles—one each for num-queues equal to 2, 4, and 8. The only function of the **num-queues** command in the queue-map configuration context is to enter the configuration mode for one of the three subprofiles so the priority mapping settings for that num-queues value can be modified from the default (8). To modify the default number of queues to use for a circuit, configure the **num-queues** command of the queuing policy. This configuration then determines which of the num-queues-indexed subprofiles of the queue map is relevant for a circuit subject to the queuing policy in question.

Caution!

Risk of dropping packets. Modifying the parameters of an ATMWFQ policy will momentarily interrupt the traffic on all ATM permanent virtual circuits (PVCs) using the policy. To reduce the risk, use caution when modifying ATMWFQ policy parameters.

Caution!

Risk of traffic disruption. Modifying the parameters of an MDRR policy momentarily removes the rate applied to all 10GE circuits using the policy. The rate is restored as soon as the change is effective. To reduce the risk, use caution when modifying MDRR policy parameters.

Note: For information about the correlation between the number of queues configured on a particular traffic card type and the corresponding number of virtual circuits (VCs) allowed per port (and per traffic card), see *Configuring Contexts and Interfaces*.

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

1.61.6 Examples

The following example configures the PWFQ policy, **firstout**, to have **4** queues:

```
[local]Redback(config)#qos policy firstout pwfq
[local]Redback(config-policy-pwfq)#num-queues 4
```

Glossary

MLPPP
Multilink PPP. An extension to PPP that allows a router to use more than one physical link for communication.

MP
Multilink PPP or Merge Point.

Merge Point: The point at which traffic exits the tail end router of a bypass RSVP LSP.

MLPPP: An extension to PPP that allows a router to use more than one physical link for communication.

PWFQ
Priority weighted fair queuing.