ERICSSON

Commands: pp through q

COMMAND DESCRIPTION

14/190 82-CRA 119 1170/1-V1 Uen L

Contents

1 Command Descriptions

Commands starting with “pp” through commands starting “q” 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 ppp delay lcp-confreq

`ppp delay lcp-confreq` ***`value`***

`default delay lcp-confreq`

1.1.1 Purpose

Sets the delay between sending a Point-to-Point Protocol over Ethernet (PPPoE) Active Discovery Session (PADS) packet and a Link Control Protocol (LCP) Configuration Request packet if the Point-to-Point Protocol (PPP) peer has not started the LCP.

1.1.2 Command Mode

global configuration

1.1.3 Syntax Description

`value`	Time, in seconds, that the LCP negotiation request is delayed. The range of values is 1 to 30 seconds; the default value is 3 seconds.

1.1.4 Default

The default value for the LCP negotiation request time delay is 3 seconds.

1.1.5 Usage Guidelines

Use the **ppp delay lcp-confreq** command to delay sending the PPP LCP Configuration Request to the peer after sending the PPPoE PADS packet. If the SmartEdge OS receives the LCP Configuration Request of the PPP peer before this delay is satisfied, the SmartEdge OS sends its own LCP Configuration Request immediately.

Note: This command is valid only with PPPoE sessions.

The default form of this command sets the delay to 3 seconds when the SmartEdge router sends the LCP Configuration Request.

1.1.6 Examples

The following example shows how to set the delay to 5 seconds:

```
[local]Redback(config)#ppp delay lcp-confreq 5
```

1.2 ppp ipcp disconnect invalid-ip-address

ppp ipcp disconnect invalid-ip-address

1.2.1 Purpose

Sends a Point-to-Point Protocol (PPP) termination request to subscribers when they do not negotiate a valid IP address during the PPP Internet Protocol Control Protocol (IPCP) negotiation process.

1.2.2 Command Mode

- global configuration

1.2.3 Syntax Description

This command has no keywords or arguments.

1.2.4 Default

None.

1.2.5 Usage Guidelines

Use the **ppp ipcp disconnect invalid-ip-address** command to send a PPP termination request to subscribers when they do not negotiate a valid IP address during the IPCP negotiation process.

1.2.6 Examples

The following example shows how to enable the PPP termination request feature:

```
[local]Redback(config)#ppp ipcp disconnect invalid-ip-address
```

1.3 ppp ipcp negotiate netmask

[no] **ppp ipcp negotiate netmask**

1.3.1 Purpose

Enable IPCP to reserve IP addresses or subnet ranges and install subnet routes for subscribers using RADIUS.

1.3.2 Command Mode

Global configuration

1.3.3 Syntax Description

This command has no keywords or arguments.

1.3.4 Default

For subscribers that have a valid /32 netmask configured, IPCP reserves one IP address for the subscriber and installs only the host /32 route. The SmartEdge OS rejects IPCP netmask option requests received from the CPE client.

1.3.5 Usage Guidelines

To enable IPCP netmask negotiation, use the **ppp ipcp negotiate netmask** command in combination with the **aaa provision route** command and optional **use-framed-route** keyword. To reserve one IP address and install the subnet route, include the keyword. To reserve an entire subnet range and install the subnet route, do not include the keyword.

1.3.6 Examples

The following example reserves an entire subnet range for the subscriber (assuming that the subscriber has a valid /32 netmask configured) and installs the subnet route in the RIB:

```
[local]Redback(config)#ppp ipcp negotiate netmask
[local]Redback(config)#context PPP
[local]Redback(config-ctx)#aaa provision route ip-netmask encapsulation pppoe
```

1.4 ppp ipcp peer-address

ppp ipcp peer-address ***ip-address***

1.4.1 Purpose

Configures a static IP address that the SmartEdge system can provide to the static point-to-point protocol (PPP) peer devices during the establishment of PPP links.

1.4.2 Command Mode

Interface configuration

1.4.3 Syntax Description

ip-address	The static IP address provided to the static PPP peer devices during the establishment of PPP links. ***ip-address*** should belong to the same subnet as the interface.

1.4.4 Default

No IP address is provided to the PPP peer device.

1.4.5 Usage Guidelines

Use the **ppp ipcp peer-address** command to configure a static IP address that the SmartEdge system can provide to the PPP peer devices during the establishment of PPP links.

Note: The peer ip-address assignment is only for PPP links (not for PPP subscriber sessions) and is applicable to only T1 cards; such as the Channelized-DS3 card.

1.4.6 Examples

The following example illustrates how the IP address offered in the IPCP phase of PPP negotiations is configured for an interface:

```
[local]Redback(config)#context blue
[local]Redback(config-ctx)#interface yellow
[local]Redback(config-if)#ip address 10.0.0.1/24
[local]Redback(config-if)#ppp ipcp peer-address 10.0.0.2
```

1.5 ppp keepalive

The first time you run this command in a context, the command syntax is:

ppp keepalive check-interval {**minutes** | **seconds**} ***time***

After you specify the check interval for a context, the command syntax is:

ppp keepalive {[**data-check**] [**response-timeout** ***seconds***] [**retries** ***retry-num***]}

no ppp keepalive [**check-interval**] [**data-check**]

default ppp keepalive {**response-timeout** | **retries**}

1.5.1 Purpose

Enables Point-to-Point Protocol (PPP) keepalive checks and specifies PPP timing attributes.

1.5.2 Command Mode

- context configuration

1.5.3 Syntax Description

check-interval	Sets the time interval between PPP keepalive checks. Optional after you have specified the initial check interval.
minutes	Specifies that the unit of measure for the ***time*** argument is minutes.
seconds	Specifies that the unit of measure for the ***time*** argument is seconds.
time	Time, in either minutes or seconds (depending on the preceding keyword), between keepalive checks.
data-check	Optional. Specifies that after the PPP keepalive check interval timer expires and before a Link Control Protocol (LCP) echo request message is sent, a check is performed to determine if data has been received on the circuit since the last check interval timer expiration.
response-timeout ***seconds***	Optional. Amount of time the system is to wait for a response to an LCP echo request message before incrementing the PPP keepalive retries counter. The range of values is 3 to 60 seconds; the default value is 10.
retries ***retry-num***	Optional. Number of times the system is to retry an unsuccessful PPP keepalive check. The range of values is 2 to 10; the default value is 2.

1.5.4 Default

Keepalive checks are not enabled, except in the case of circuits using PPP over Ethernet (PPPoE), for which the period between keepalive checks is 5 minutes (300 seconds).

1.5.5 Usage Guidelines

Use the **ppp keepalive** command to enable PPP keepalive checks and specify PPP timing attributes. The command keywords work together to configure when and how keepalives are sent, and what action is taken as a result of the response, or lack of response.

Keepalive checks are LCP echo request messages sent over PPP sessions in the context to detect abnormal session disconnects that the system would not otherwise know about. The **check-interval** keyword must be entered before the other command keywords are available.

The **check-interval** keyword sets the time between LCP echo requests, in either minutes or seconds. When this time expires, an LCP echo request is sent to the PPP peer and a response timer is started. The length of the response timer is determined by the value of the **response-timeout** ***seconds*** construct. If a valid LCP echo is received before the response timer expires, the response timer is canceled, and the check interval timer is reset.

If the response timer expires without a valid LCP echo being received, an optional check, specified by the **data-check** keyword, is performed to see if any data has been received on the circuit since the LCP echo request was sent. Only valid PPP packets are considered data. If data has been received since the LCP echo request was sent, the check interval timer is reset. If no data has been received, the retry counter is incremented and another LCP echo request message is sent. When the configured number of retries has been reached, set by the value of the **retries** ***retry-num*** construct, without a valid echo or data being received, the session is considered to be no longer alive and is torn down.

The **data-check** keyword specifies that after the check interval timer expires and before an LCP echo request message is sent, a check is performed to determine if data has been received on the circuit since the last check interval timer expiration. If data has been received, the check interval timer is simply reset, skipping the LCP echo request message altogether. This option is recommended when it is preferred to limit the overhead for PPP keepalive processing. The tradeoff is that using the **data-check** keyword to determine that a session is no longer active can take longer than using the PPP keepalive feature without the **data-check** keyword. For an example illustrating this tradeoff, see *PPP Keepalive Checks* in *PPP Keepalive Checks*.

Although the default period between keepalive checks for PPPoE circuits is 5 minutes (300 seconds) if keepalive checks are not enabled, PPPoE circuits take on the configured period between checks when keepalive checks are enabled.

Use the **no** form of this command without options to disable all command options.

Note: The **no ppp keepalive data-check** form is available only if you have previously specified the check interval.

Note: Entering the **no ppp keepalive check-interval** command does not disable the keepalive feature on active sessions. Because it is a context configuration mode command, applying to all PPP sessions in the context, the command takes effect when the last active session is torn down.

Use the **default** form of this command to specify the default value for the response timer or the number of retries.

1.5.6 Examples

The following example shows how to enable the PPP keepalive feature, sets the length of the response timer and the number of retries, and specifies the data check option to minimize LCP echo traffic:

```
[local]Redback(config-ctx)#ppp keepalive check-interval seconds 500
[local]Redback(config-ctx)#ppp keepalive data-check response-timeout 30 retries 3
```

1.6 ppp mru

ppp mru ***mru***

no ppp mru

1.6.1 Purpose and Usage Guidelines

If the Point-to-Point Protocol (PPP) peer does not negotiate its MRU, this command sets the maximum receive unit (MRU) on all PPP encapsulated dot1Q PVCs associated with the current dot1q profile.

If a PPPoE session is using a dot1Q profile with a configured PPP MRU, the value configured in the profile overrides that specific PPPoE session.

When the PPP client does not negotiate a MRU, the router applies a default MRU of 1492 bytes for the client. This command allows you to set a higher MRU than the default.

The **no** form of this command restores the default behavior.

1.6.2 Command Mode

dot1Q profile configuration

1.6.3 Syntax Description

mru	Maximum receive unit in bytes. The range of values is 256 to 12800.

1.6.4 Default

When a PPP peer does not negotiate its MRU, the default MRU is 1492 bytes.

1.6.5 Examples

The following example shows how to set the PPP MRU to **1600** bytes:

```
[local]rock1200(config-dot1q-profile)#ppp mru 1600
```

1.7 ppp mtu

ppp mtu ***mtu***

1.7.1 Purpose

Sets the maximum transmission unit (MTU) used by Point-to-Point Protocol (PPP) for a subscriber's circuit.

1.7.2 Command Mode

- subscriber configuration

1.7.3 Syntax Description

mtu	Maximum transmission unit in bytes. The range of values is 256 to 12800.

1.7.4 Default

None

1.7.5 Usage Guidelines

Use the **ppp mtu** command to set the MTU used by PPP for a subscriber circuit. The effect of this command is strictly local to the SmartEdge router, and therefore, does not force the router to negotiate a particular PPP MRU.

Use the **ppp mtu** command to lower the size of data packets being sent over that subscriber link from the MRU value that has been negotiated between the SmartEdge router and the PPP client. You cannot make the size any larger than the negotiated MRU. If an MRU value lower than the value of the ***mtu*** argument in the **ppp mtu** command has been negotiated, the MRU value takes precedence and the **ppp mtu** command setting is ignored.

On a normal Ethernet interface, the standard MTU is 1500. For Point-to-Point Protocol over Ethernet (PPPoE) implementation, the negotiated MTU uses the physical interface, minus eight bytes as the default.

1.7.6 Examples

The following example shows how to set the PPP MTU to **768** bytes:

```
[local]Redback(config-sub)#ppp mtu 768
```

1.8 ppp multilink

ppp multilink

no ppp multilink

1.8.1 Purpose

Enables Multilink Point-to-Point Protocol (MLPPP) for subscriber sessions on PPP-encapsulated Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs), PPPoE over Ethernet (PPPoE)-encapsulated 802.1Q PVCs, 802.1Q tunnels, untagged Ethernet traffic, and Layer 2 Tunneling Protocol (L2TP) tunnels.

1.8.2 Command Mode

- global configuration

1.8.3 Syntax Description

This command has no keywords or arguments.

1.8.4 Default

Multilink PPP (MLPPP) is disabled for subscriber sessions on PPP-encapsulated ATM PVCs, PPPoE-encapsulated 802.1Q PVCs and tunnels, untagged Ethernet traffic, and L2TP tunnels.

1.8.5 Usage Guidelines

Use the **ppp multilink** command to enable MLPPP for subscriber sessions on ATM PVCs, PPPoE-encapsulated 802.1Q PVCs and tunnels, untagged Ethernet traffic, and L2TP tunnels.

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

1.8.6 Examples

The following example shows how to enable MLPPP:

```
[local]Redback(config)#ppp multilink
```

1.9 ppp multilink lfi

ppp multilink lfi fragment-threshold *value* [priority-threshold *value*]

no ppp multilink lfi

1.9.1 Purpose

Enables Multilink PPP (MLPPP) Link Fragmentation and Interleaving (LFI) within the specified priority or fragmentation threshold value for subscriber sessions on PPP-encapsulated Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs), PPP over Ethernet (PPPoE)-encapsulated 802.1Q PVCs and tunnels, untagged Ethernet traffic, and Layer 2 Tunneling Protocol (L2TP) tunnels.

1.9.2 Command Mode

global configuration

1.9.3 Syntax Description

fragment-threshold *value*	Fragmentation on outgoing traffic. The range of values is 258 to 16,320; the default value is 0.
priority-threshold *value*	Optional. Multiprotocol encapsulation priority level. The range of values is 0 to 7; the default value is 0.

1.9.4 Default

The default does not enable LFI priority and fragmentation thresholds for subscriber sessions on PPP-encapsulated ATM PVCs, PPPoE-encapsulated 802.1Q PVCs and tunnels, untagged Ethernet traffic, and L2TP tunnels.

1.9.5 Usage Guidelines

Use the **ppp multilink lfi** command to enable PPP LFI with the specified priority or fragmentation threshold values for subscriber sessions on PPP-encapsulated ATM PVCs, PPPoE-encapsulated 802.1Q PVCs and tunnels, untagged Ethernet traffic, and L2TP tunnels.

Use the fragment-threshold ***value*** construct to set the fragmentation threshold on outgoing traffic. The range of values is 258 to 16,320. The threshold size is not to exceed the value specified by the user, but does not necessarily need to be the same as the fragment threshold. The default value is 0, with no packets becoming fragmented.

Use the optional priority-threshold ***value*** construct to define the multiprotocol encapsulation priority level. The packet is encapsulated only if it is of lower or equal priority than the configured threshold. If the packet is not multiprotocol encapsulated, it is not fragmented, regardless of the size. All packets are multiprotocol encapsulated if their priority is lower than or equal to the threshold. The default value of 0 results in all packets being multiprotocol encapsulated.

This command only applies to MLPPP created by the ppp multilink command.

Use the **no** form of this command to disable LFI priority and fragmentation thresholds.

1.9.6 Examples

The following example shows how to enable PPP LFI with a specified fragmentation threshold value of **258**:

```
[local]Redback(config)#ppp multilink lfi fragment-threshold 258
```

The following example shows how to enable PPP LFI with a specified priority threshold value of **7**:

```
[local]Redback(config)#ppp multilink lfi priority-threshold 7
```

1.10 pppoe always-send-padt

pppoe always-send-padt

{**no** | **default**} **pppoe always-send-padt**

1.10.1 Purpose

Configures a Point-to-Point Protocol (PPP)-encapsulated (PPPoE) option that terminates the PPPoE session by sending a PPPoE Active Discovery Terminate (PADT) packet after the PPP session is terminated.

1.10.2 Command Mode

global configuration

1.10.3 Syntax Description

This command has no keywords or arguments.

1.10.4 Default

The PPPoE option does not terminate the PPPoE session when the PPP session is terminated

1.10.5 Usage Guidelines

Use the **pppoe always-send-padt** command to configure a PPPoE option that terminates the PPPoE session after a PPP session is terminated.

Use this command if the PPPoE client requires explicit termination of the PPPoE session.

The PPPoE option is a global and will be applied to all PPPoE sessions that are currently established and for all future sessions.

Use the **no** or **default** form of this command to disable the PPPoE option that terminates the PPPoE session once the PPP session has terminated.

1.10.6 Examples

The following example shows how to configure the PPPoE option to terminate the PPPoE session after the PPP session has terminated:

```
[local]Redback(config)#pppoe always-send-padt
[local]Redback(config)#end
```

1.11 pppoe circuit padi per-mac

pppoe circuit padi per-mac count ***padi-num*** **allow-time** ***allow-interval*** **drop-time** ***drop-interval***

{**no** | **default**} **pppoe circuit padi per-mac**

1.11.1 Purpose

Limits the number of Point-to-Point Protocol over Ethernet Active Discovery Initialization (PADI) messages that the system accepts in a specified interval for each medium access control (MAC) address.

1.11.2 Command Mode

- global configuration

1.11.3 Syntax Description

count ***padi-num***	Number of PADI messages allowed per MAC address on each circuit during the specified interval. The range of values is 1 to 255.
allow-time ***allow-interval***	Interval, in seconds, during which the system counts PADI messages. The range of values is 1 to 127.
drop-time ***drop-interval***	Number of seconds during which PADI messages are dropped, if the allowed number of PADI messages was exceeded in the previous interval. The range of values is 1 to 127.

1.11.4 Default

The SmartEdge router does not limit the outstanding PADI message that the router accepts in a specified interval for each MAC address.

1.11.5 Usage Guidelines

Use the **pppoe circuit padi per-mac** command to limit the number of PPPoE PADI messages that the system accepts in an interval for each MAC address.

Note: The SmartEdge router can accept many PADI messages simultaneously from the same MAC address, but it processes only one at any given time.

This command applies only to PPPoE-encapsulated circuits on the following traffic cards:

- All Ethernet and Gigabit Ethernet cards
- All ATM cards

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

1.11.6 Examples

The following example shows how to accept 150 PADI messages per MAC address in every 2-second interval. If more than 150 PADI messages are received during the interval, all PADI messages are dropped for 3 seconds following the interval. Following that, 150 PADI messages are allowed per MAC address for the next 2-second interval:

```
[local]Redback(config)#pppoe circuit padi per-mac count 150 allow-time 2 drop-time 3
```

1.12 pppoe circuit padr per-mac

pppoe circuit padr per-mac count ***padr-num*** **allow-time** ***allow-interval*** **drop-time** ***drop-interval***

{**no** | **default**} **pppoe circuit padr per-mac**

1.12.1 Purpose

Limits the number of Point-to-Point Protocol over Ethernet Active Discovery Request (PADR) messages that the system accepts in a specified interval for each medium access control (MAC) address.

1.12.2 Command Mode

- global configuration

1.12.3 Syntax Description

count ***padr-num***	Number of PADR messages allowed per MAC address on each circuit during the specified interval. The range of values is 1 to 255; the default value is 1.
allow-time ***allow-interval***	Interval, in seconds, during which the system counts PADR messages. The range of values is 1 to 127; the default value is 1.
drop-time ***drop-interval***	Number of seconds during which PADR messages are dropped, if the allowed number of PADR messages was exceeded in the previous interval. The range of values is 1 to 127; the default value is 1.

1.12.4 Default

The PPPoE session limits the outstanding PADR message count to 1 for each MAC address until it receives a PPPoE Active Discovery Session (PADS) reply for that session.

1.12.5 Usage Guidelines

Use the **pppoe circuit padr per-mac** command to limit the number of PPPoE PADR messages that the system accepts in an interval for each MAC address.

Note: The SmartEdge router can accept many PADR messages simultaneously from the same MAC address, but it processes only one at any given time.

This command applies only to PPPoE-encapsulated circuits on the following traffic cards:

- All Ethernet and Gigabit Ethernet cards
- All ATM cards

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

1.12.6 Examples

The following example shows how to accept 200 PADR messages per MAC address in every 2-second interval. If more than 200 PADR messages are received during the interval, all PADR messages are dropped for 3 seconds following the interval. Following that, 200 PADR messages are allowed per MAC address for the next 2-second interval:

```
[local]Redback(config)#pppoe circuit padr per-mac count 200 allow-time 2 drop-time 3
```

1.13 pppoe client route

pppoe client route ***ip-addr netmask metric***

no pppoe client route ***ip-addr netmask metric***

1.13.1 Purpose

Configures routes to be installed on the subscriber's PC when multiple Point-to-Point Protocol over Ethernet (PPPoE) sessions exist.

1.13.2 Command Mode

- subscriber configuration

1.13.3 Syntax Description

ip-addr	IP address of the destination host.
netmask	Network mask for the route entry.
metric	Cost (number of hops) to this destination.

1.13.4 Default

Routes are not sent to the subscriber's PPPoE client.

1.13.5 Usage Guidelines

Use the **pppoe client route** command to configure the SmartEdge router to provide different routes for different PPPoE sessions. For each PPPoE session, a route is sent in a PPPoE Active Discovery Network (PADN) message, and installed on the subscriber's PC. In this way, subscribers are enabled with seamless client route provisioning on a per-PPPoE session basis. The subscriber's PC client must support PADN. If the PPPoE client ignores the routes, they have no effect.

As an example of this feature, one PPPoE session could provide Internet connectivity, while another session connects corporate headquarters to a remote office site. Routes to the business site might be of a very different nature than the routes that provide access to the Internet.

Use the **no** form of this command to remove the specified route from the configuration.

1.13.6 Examples

The following example shows how to specify that a route at **200.1.1.0 255.255.255.0** is to be used for concurrent multiple PPPoE sessions. This route has a metric, or hop count, of **1**:

```
[local]Redback(config-sub)#pppoe client route 200.1.1.0 255.255.255.0 1
```

1.14 pppoe motm

pppoe motm *text*

no pppoe motm

1.14.1 Purpose

Creates and enables the sending of a message of the minute (MOTM) to a subscriber when logging on.

1.14.2 Command Mode

subscriber configuration

1.14.3 Syntax Description

text	Text of the MOTM to be sent to a newly authenticated subscriber. The maximum length of an MOTM is 256 characters. Only one MOTM can be active at a time.

1.14.4 Default

None

1.14.5 Usage Guidelines

Use the **pppoe motm** command to create and enable the sending of a message to the subscriber when logging on. You can use this command to send any information of general use to subscribers; for example, information about system downtime.

Note: A newly created MOTM overwrites an existing MOTM.

Use the **no** form of this command to delete the MOTM so that the message is no longer sent to the subscriber after logging on.

1.14.6 Examples

The following example establishes an MOTM:

```
[local]Redback(config-sub)#pppoe motm Network will be down for
maintenance from 0100-0400 Saturday.
```

The following example deletes the active MOTM:

```
[local]Redback(config-sub)#no pppoe motm
```

1.15 pppoe pado delay

pppoe pado delay ***delay-value***

no pppoe pado delay

1.15.1 Purpose

Sets the Point-to-Point Protocol over Ethernet Active Discovery Offer (PADO) delay timer to the specified number of seconds.

1.15.2 Command Mode

- dot1q profile configuration

1.15.3 Syntax Description

delay-value	Delay value, in seconds. The range of values is 1 to 3.

1.15.4 Default

No PPPoE PADO delay value is set.

1.15.5 Usage Guidelines

Use the **pppoe pado delay** command to set the PPPoE PADO delay timer to the specified value, in number of seconds.

Note: All PVCs with the PPPoE encapsulation type that are bound to the 802.1Q profile inherit the PPPoE PADO delay value. After you delete an 802.1Q profile, all PPPoE PVCs that refer to this profile no longer have PPPoE PADO delay timer values specified.

Use the **no** form of this command to delete the PPPoE PADO delay timer value.

1.15.6 Examples

The following example shows how to set the 802.1Q **blue** profile to have a PADO delay time of 3 seconds:

```
[local]Redback(config)#dot1q profile blue
[local]Redback(config-dot1q-profile)#pppoe pado delay 3
```

1.16 pppoe service-name accept-all

pppoe service-name accept-all

no pppoe service-name accept-all

1.16.1 Purpose

Enables the SmartEdge router to accept any service name tag that is included in a Point-to-Point Protocol over Ethernet (PPPoE) Active Discovery Initiation (PADI) or PPPoE Active Discovery Request (PADR) message and include it among the advertised services in a PPP Active Discovery Offer (PADO) or PPPoE Active Discovery Session (PADS) message, respectively.

1.16.2 Command Mode

- global configuration

1.16.3 Syntax Description

This command has no keywords or arguments.

1.16.4 Default

The SmartEdge router accepts and advertises only those services (domains) that have been configured through the SmartEdge router.

1.16.5 Usage Guidelines

Use the **pppoe service-name accept-all** command to enable the SmartEdge router to accept any service name tag that is included in a PPPoE PADI message, and include it among the advertised services in PPP PADO messages. It also accepts any service name tag that is included in a PPPoE PADR message and includes it in a PPPoE PADS message.

Use the **no** form of this command to disable the acceptance and advertisement of service name tags that are not configured through the SmartEdge router.

1.16.6 Examples

The following example shows how to enable the acceptance of all service names that might be included in PADI or PADR messages:

```
[local]Redback(config)#pppoe service-name accept-all
```

1.17 pppoe services

pppoe services {**all-domains** | **marked-domains**}

{**no** | **default**} **pppoe services**

1.17.1 Purpose

Specifies which domains (services) are advertised to Point-to-Point Protocol over Ethernet (PPPoE) clients.

1.17.2 Command Mode

global configuration

1.17.3 Syntax Description

all-domains	Specifies that all domains are advertised.
marked-domains	Specifies that only domains that have the **advertise** keyword as part of their definition are advertised.

1.17.4 Default

No domains are advertised to PPPoE clients.

1.17.5 Usage Guidelines

Use the **pppoe services** command to specify which domains (services) are advertised to PPPoE clients and make public the services that the SmartEdge router provides.

Note: Domain names, not context names, are advertised during the PPPoE discovery protocol.

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

1.17.6 Examples

The following example shows how to enable the advertisement of marked domains to PPPoE clients:

```
[local]Redback(config)#pppoe services marked-domains
```

1.18 pppoe tag

pppoe tag {ac-cookie | ac-name *string*}

no pppoe tag ac-cookie

default pppoe tag {ac-cookie | ac-name}

1.18.1 Purpose

Replaces the default access concentrator (AC)-Name PPPoE tag value with the specified string or enables AC-Cookie tag support.

1.18.2 Command Mode

global configuration

1.18.3 Syntax Description

ac-cookie	Enables AC-Cookie tag support.
ac-name *string*	Alphanumeric string to replace the default value for the AC-Name PPPoE tag.

1.18.4 Default

The SmartEdge router uses an automatically generated (and guaranteed to be unique) value for the AC-Name PPPoE tag and AC-cookie tag support is disabled.

1.18.5 Usage Guidelines

RFC 2516, *Transmitting PPP Over Ethernet*, specifies that the AC-Name PPPoE tag sent in PPPoE Active Discovery Offer (PADO) messages must have a unique value. The SmartEdge router ensures that this value is unique by creating it from a combination of the backplane serial number and the hostname of the AC device sending the PADO message. When it is preferred to override this default, use this command to establish an alternate value for the AC-Name tag. After you change the default, the SmartEdge router can no longer guarantee that the value is unique.

SmartEdge router also supports the AC-Cookie tag described in RFC 2516 to allow the AC to uniquely regenerate the tag value based on the PADR source address. Using this feature, the AC can ensure that the PADI source address is indeed reachable and can then limit concurrent sessions for that address.

Use the **no** or **default** form of this command to return the AC-Name value to the automatically generated default name or to disable AC-Cookie tag support.

1.18.6 Examples

The following example replaces the AC-Name PPPoE tag with **fortune-1**:

```
[local]Redback(config)#pppoe tag ac-name fortune-1
```

1.19 pppoe url

pppoe url *url*

no pppoe url

1.19.1 Purpose

Sets the subscriber's Point-to-Point Protocol over Ethernet (PPPoE) client to automatically point the web browser to a specified URL as soon as the session is established.

1.19.2 Command Mode

subscriber configuration

1.19.3 Syntax Description

url	URL to which the subscriber's browser is pointed after the subscriber's PPP session is established. For special-character sequences that can be used in the url argument, see Table 1.

1.19.4 Default

None

1.19.5 Usage Guidelines

Use the **pppoe url** command to set the subscriber's PPPoE client to point the subscriber's browser to a specific location after the subscriber's PPP session is established.

This command can be configured in each subscriber record, in a named subscriber profile, or in the subscriber default profile.

The ***url*** argument is a standard URL that can contain the special-character sequences listed in Table 1.

Table 1 Special-Character Sequences

Character Sequence	Expands to:
%U	The entire subscriber name used in PPP authentication.
%u	The user portion of the subscriber name used in PPP authentication. This is the portion of the subscriber name that precedes the first @ or other divider character. If there is no divider character, then %u expands to the entire subscriber name.
%d	The domain portion of the subscriber name used in PPP authentication. This is the portion of the subscriber name that follows the first @ or other divider character. If there is no divider character, %d expands to a zero length string.
%D	The name of the context to which the subscriber was authenticated. This may be different than the domain portion of the subscriber name.
%%	Single % character.

The SmartEdge router expands these sequences prior to inclusion in a PPP Active Discovery Message (PADM) and can be used to personalize the URL to the subscriber.

Use the **no** form of this command to remove the URL association from the subscriber record.

1.19.6 Examples

For a subscriber **joe** in the **local** context, the following example allows a PADM containing the URL **http://www.loe.com/members/joe@local** to be sent to the PPPoE client when the PPP session is established:

```
[local]Redback(config-ctx)#subscriber name joe
[local]Redback(config-sub)#pppoe url http://www.loe.com/members/%U
```

For every subscriber to which the subscriber default value is applied, the following example sends a PADM containing **http://www.loe.com/members/*name*** to the PPPoE client when the PPP session is established:

```
[local]Redback(config-ctx)#subscriber default
[local]Redback(config-sub)#pppoe url http://www.loe.com/members/%u
```

1.20 ppp our-options mru

ppp our-options mru initial ***initial-mru*** **maximum** ***max-mru***

default ppp our-options mru

1.20.1 Purpose

Specifies the range for the maximum receive unit (MRU) with which the SmartEdge router negotiates Link Control Protocol (LCP) option values for the SmartEdge router end of the Point-to-Point Protocol (PPP) session.

1.20.2 Command Mode

- global configuration

1.20.3 Syntax Description

initial ***initial-mru***	MRU value at which negotiation begins. The range of values is 256 to 12,800; the default value is 1,500 for PPP circuits, and 1,492 for PPP over Ethernet (PPPoE) circuits.
maximum ***max-mru***	Maximum MRU value that the SmartEdge router can negotiate. The range of values is 256 to 12,800; the default value is 12,800.

1.20.4 Default

If you do not use this command, the SmartEdge router uses the default values described in the Syntax Description section of this command.

1.20.5 Usage Guidelines

Use the **ppp our-options mru** command to specify the range for the MRU with which the SmartEdge router negotiates LCP option values for the SmartEdge router end of PPP sessions.

Currently, the options available are the initial and maximum MRU values. When these values are specified, the SmartEdge router begins negotiation for its MRU at the value of the ***initial-mru*** argument, and does not exceed the value of the ***max-mru*** argument. The resulting size guidelines are reflected in all packets sent to the SmartEdge router by the remote peer.

If, after 10 attempts, an agreement with the peer can not be reached as to a local MRU between the configured initial and maximum values, the SmartEdge router establishes the PPP session without negotiating the local MRU. In that case, the SmartEdge router uses an MRU of 1,500 for PPP circuits and 1,492 for PPPoE circuits.

Note: This command affects only subscriber sessions.

Use the **default** form of this command to return the LCP options for MRU to their default values.

1.20.6 Examples

The following example shows how to set the local initial and maximum MRU values:

```
[local]Redback(config)#ppp our-options mru initial 1800 maximum 11000
```

1.21 ppp our-options multilink

ppp our-options multilink endpoint-discriminator [***addr***]

{**no** | **default**} **ppp our-options multilink endpoint-discrimina tor**

1.21.1 Purpose

Specifies the address for the SmartEdge router end of multilink Point-to-Point Protocol (MLPPP) bundles.

1.21.2 Command Mode

- global configuration

1.21.3 Syntax Description

endpoint-discriminator	Specifies the endpoint discriminator for the SmartEdge router end of MLPPP bundles.
addr	Optional. Address, either IP or medium access control (MAC), for the SmartEdge router, according to one of the constructs or keywords listed in Table 2.

1.21.4 Default

If you do not use this command, the SmartEdge router uses the hostname and IP address of the SmartEdge router.

1.21.5 Usage Guidelines

Use the **ppp our-options multilink** command to specify the address for the SmartEdge router end of MLPPP bundles. This command is not available until you have enabled MLPPP using the **ppp multilink** command (in global configuration mode).

Note: This command only applies to MLPPP bundles created by the ppp multilink command; namely, it applies to MLPPP bundles on Point-to-Point Protocol (PPP)-encapsulated Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs), PPP over Ethernet (PPPoE)-encapsulated 802.1Q PVCs and tunnels, untagged Ethernet traffic, and Layer 2 Tunneling Protocol (L2TP) tunnels.

Table 2 lists the address types and their constructs for the ***addr*** argument.

Table 2 Address Types

addr Argument	Description
class-1 ***text***	Locally assigned address consisting of up to 20 characters.
class-2 ***ip-addr***	IP address.
class-3 ***mac-addr***	MAC address.
class-5 ***text***	Public-switched network directory number consisting of up to 15 characters.
local-ip-address	IP address of the Ethernet management port on the controller card.
local-mac-address	MAC address of the SmartEdge router; this is the default address.

Use the **no** or **default** form of this command to specify the local MAC address of the SmartEdge router.

1.21.6 Examples

The following example shows how to specify the IP address of the Ethernet management port on the controller card as the endpoint discriminator:

```
[local]Redback(config)#ppp our-options multilink endpoint-discriminator local-ip-address
```

1.22 ppp peer-options mru

ppp peer-options mru minimum *min-mru* maximum *max-mru*

default ppp peer-options mru

1.22.1 Purpose

Specifies the range for the maximum receive unit (MRU) with which the SmartEdge router negotiates Link Control Protocol (LCP) option values for the remote end of the Point-to-Point Protocol (PPP) session.

1.22.2 Command Mode

global configuration

1.22.3 Syntax Description

minimum *min-mru*	Minimum MRU value for the remote peer. The range of values is 128 to 16,384; the default value is 128.
maximum *max-mru*	Maximum MRU value for the remote peer. The range of values is 128 to 16,384; the default value is 16,384.

1.22.4 Default

The SmartEdge router negotiates LCP options with the default values.

1.22.5 Usage Guidelines

Use the **ppp peer-options mru** command to specify the range for the MRU with which the SmartEdge router negotiates LCP option values for the remote end of PPP sessions.

Note: The use of this command can alter the values negotiated during LCP, but it does not force any options to be negotiated or prevent any options from being negotiated. For MRU (the only option supported at the moment), it controls the SmartEdge end of the MRU negotiation if the remote peer is willing to negotiate MRU.

Currently, the options available are the minimum and maximum MRU values. When these values are specified, the SmartEdge router negotiates the remote peer's MRU value to be at least the value specified by the ***min-mru*** argument, and not greater than the value specified by the ***max-mru*** argument. The resulting size guidelines are reflected in all packets that the SmartEdge router sends to the remote peer.

If, after 10 attempts, the SmartEdge router has not reached an agreement with the peer regarding the value of the peer's MRU between the specified minimum and maximum values, the SmartEdge router establishes the PPP session without negotiating the peer's MRU. In that case, the SmartEdge router uses the standard MRU of 1,500 for PPP circuits, and 1,492 for PPP over Ethernet (PPPoE) circuits.

Note: This command affects only subscriber sessions.

Use the **`default`** form of this command to return the options to their default values.

1.22.6 Examples

The following example shows how to set the peer's minimum and maximum MRU values:

```
[local]Redback(config)#ppp peer-options mru minimum 200 maximum 2000
```

1.23 ppp pppoe-large-mru

ppp pppoe-large-mru

no ppp pppoe-large-mru

1.23.1 Purpose

Enables the negotiation (as described in RFC 4638) of a maximum receive unit (MRU) larger than 1492 bytes for Point-to-Point Protocol over Ethernet (PPPoE) circuits.

1.23.2 Command Mode

global configuration

1.23.3 Syntax Description

This command has no keywords or arguments.

1.23.4 Default

MRU negotiation is disabled.

1.23.5 Usage Guidelines

Use the **ppp pppoe-large-mru** command to enable the negotiation (as described in RFC 4638) of an MRU larger than 1492 bytes for PPPoE circuits. If the SmartEdge router is configured with this command, an MRU larger than 1492 bytes is allowed only when the PPPoE PPP-Max-Payload tag is received from the client and the client initiates MRU negotiation.

The MRU negotiation is decided in described in RFC 4638. These negotiations are based on the PPPoE PPP-Max-Payload tag value received, and the subscribers and ports MTU value.

Use the **no** form of this command to disable MRU negotiation. When MRU negotiation is disabled, the MRU is set to 1,492 bytes.

1.23.6 Examples

The following example shows how to enable MRU negotiation:

```
[local]Redback(config)#ppp pppoe-large-mru
```

1.24 ppp validate pppoe-source-mac

ppp validate pppoe-source-mac

no ppp validate pppoe-source-mac

1.24.1 Purpose

Instructs the system to validate that the source MAC address of the request matches the MAC address stored in the requestor's profile.

1.24.2 Command Mode

- global configuration

1.24.3 Syntax Description

This command has no keywords or arguments.

1.24.4 Default

Validation of PPPoE source MAC address is disabled.

1.24.5 Usage Guidelines

Use the **validate pppoe-source-mac** command to instruct the system to validate that the source MAC address of the request matches the MAC address stored in the requestor's profile.

Use the **no** form of this command to disable validation of the PPPoE source MAC address.

1.24.6 Examples

The following example shows how to enable validation of the requestor's MAC address:

```
[local]Redback(config)#ppp validate pppoe-source-mac
```

1.25 preempt

preempt [hold-time *interval*]

{**no** | **default**} **preempt [hold-time *interval*]**

1.25.1 Purpose

Enables a higher priority Virtual Router Redundancy Protocol (VRRP) backup router to preempt a lower priority VRRP master.

1.25.2 Command Mode

VRRP configuration

1.25.3 Syntax Description

hold-time *interval*	Specifies a hold time, in seconds, for which a higher-priority VRRP backup router must wait before preempting a lower-priority VRRP master. This construct is supported on backup (non-owner) VRRP routers only.

1.25.4 Default

Preemption is enabled.

1.25.5 Usage Guidelines

Use the **preempt** command to enable a VRRP backup router that has a higher priority to preempt a lower priority VRRP master. Use the optional **hold-time *interval*** construct to specify a hold time, in seconds, for which a higher-priority VRRP backup router must wait before preempting a lower-priority VRRP master. Configure the preemption hold time when you want the higher-priority server to wait before trying to preempt the current master while the system completely converges.

When preemption is disabled, a higher priority VRRP backup router does not preempt a lower priority VRRP master.

Note: Preemption can only be disabled for VRRP backup routers; VRRP owner routers always have preemption enabled.

The master VRRP router can never be preempted by another router, and it always advertises a VRRP priority of 255. The priority of 255 is reserved for the master VRRP router. If a failure occurs in the master VRRP router, a backup router takes over until the master VRRP router comes back up. In such cases,

the master VRRP router immediately preempts the backup router; a preempt hold time is ignored if it is configured on the master VRRP router.

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

1.25.6 Examples

The following example disables preemption on the VRRP backup router with virtual ID **23**:

```
[local]Redback(config-if)#vrrp 23 backup
[local]Redback(config-vrrp)#no preempt
[local]Redback(config-vrrp)#
```

1.26 preferred-lifetime

preferred-lifetime ***preferred-lifetime***

{**no** | **default**} ***preferred-lifetime***

When entered in Neighbor Discovery (ND) profile configuration mode, the syntax is:

preferred-lifetime {***preferred-lifetime*** | **infinite**}

default ***preferred-lifetime***

1.26.1 Purpose

Specifies the preferred lifetime for one or more IPv6 prefixes advertised in a Router Advertisement (RA) message.

1.26.2 Command Mode

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

1.26.3 Syntax Description

preferred-lifetime	Optional in the ND profile configuration mode. Value for the preferred lifetime, in seconds. The range of values is 0 to 4,294,967,295; the default value is infinite.
infinite	Optional. Only applicable to the ND profile configuration mode. Sets the value of the preferred lifetime to the lifetime of the subscriber circuit.

1.26.4 Default

The preferred lifetime is infinite by default.

1.26.5 Usage Guidelines

Use the **preferred-lifetime** command to specify the preferred lifetime for one or more IPv6 prefixes advertised in an RA message. This value is the length of time in seconds that the IPv6 address generated from an IPv6 prefix remains preferred. In ND profile configuration mode, this command specifies

the value for the subscribers using the specified ND profile. In ND router configuration mode, this command specifies the global value for all interfaces; in ND router interface mode, it specifies the value for the specified 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 in the ND router configuration or ND router interface modes.

In the ND profile configuration mode, use the **default** form of this command to specify the default value.

1.26.6 Examples

The following example specifies a preferred lifetime of **86400** seconds (24 hours) for the ND profile **ndprofile7**:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#nd profile ndprofile7
[local]Redback(config-nd-profile)#preferred-lifetime 86400
```

The following example specifies a preferred lifetime of **43200** seconds (12 hours) for all interfaces for this ND router:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router nd
[local]Redback(config-nd-if)#preferred-lifetime 43200
```

The following example specifies a preferred lifetime of **2880** seconds (48 minutes) for the **int1** ND router interface, 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)#preferred-lifetime 2880
```

1.27 preferred-nhop

preferred-nhop ***ip-address***

{**no** | **default**} **preferred-nhop** ***ip-address***

1.27.1 Purpose

Configures the preferred next-hop attribute in the VPLS profile for a VPLS neighbor.

1.27.2 Command Mode

VPLS profile neighbor configuration

1.27.3 Syntax Description

ip-address	Specifies the IP address of the preferred next-hop router.

1.27.4 Default

No preferred next hop is configured.

1.27.5 Usage Guidelines

Use the **preferred-nhop** command to configure the preferred next-hop attribute in the VPLS profile for a VPLS neighbor. This attribute dictates that packets are forwarded to the specified next hop as long as that next hop is available. Specifying a preferred next hop prevents the router from performing ARP if the preferred next hop is available.

Use the **no** or **default** form of this command to remove a specified next hop from a VPLS profile.

1.27.6 Examples

The following example configure the preferred next-hop attribute in the VPLS profile for the VPLS neighbor with the IP address 1.2.3.4. In this example, the preferred next hop is the router with the IP address `2.2.3.4`:

```
[local]Redback(config)#vpls profile vpls-prof1
[local]Redback(config-vpls-profile)#neighbor 1.2.3.4
[local]Redback(config-vpls-profile-neighbor)#preferred-nhop 2.2.3.4
```

1.28 prefix

prefix ***ipv6-prefix/length*** [**no-autoconfig**] [**no-onlink**] [**preferred-lifetime** ***preferred-lifetime***] [**valid-lifetime** ***valid-lifetime***]

{**no** | **default**} **prefix** ***ipv6-prefix/length***

1.28.1 Purpose

Configures a prefix to be advertised for this Neighbor Discovery (ND) router interface.

1.28.2 Command Mode

- ND router interface configuration

1.28.3 Syntax Description

ipv6-prefix	Prefix for the IPv6 address for this ND router interface in the format ***A:B:C:D:E:F:G:H***.
length	Number of prefix bits. The range of values is 0 to 128.
no-autoconfig	Optional. Sets the autonomous address configuration flag to not use this prefix for automatic configuration; this is the default.
no-onlink	Optional. Sets the on-link flag to not use this prefix for on-link determination; this is the default.
preferred-lifetime ***preferred-lifetime***	Optional. Preferred lifetime for this prefix (in seconds). The range of values is 0 to 4,294,967,295; the default value is 604,800 seconds (7 days).
valid-lifetime ***valid-lifetime***	Optional. Valid lifetime for this prefix (in seconds). The range of values is 0 to 4,294,967,295; the default value is 2,592,000 seconds (30 days).

1.28.4 Default

No prefix is configured for any ND router interface.

1.28.5 Usage Guidelines

Use the **prefix** command to configure a prefix to be advertised for this ND router interface. Enter this command multiple times to configure more than one prefix.

Use the optional keywords and constructs to define the fields in the Prefix Information option for this prefix:

- **no-autoconfig**—Sets the autonomous address configuration flag in the Prefix Information option to FALSE.

- **no-onlink**—Sets the on-link flag to FALSE.
- **preferred-lifetime**—Specifies the value for the Preferred Lifetime field.
- **valid-lifetime**—Specifies the value for the Valid Lifetime field.

The values for the **preferred-lifetime** ***preferred-lifetime*** and **valid-lifetime** ***valid-lifetime*** constructs override the values for the interface that you specified with the **preferred-lifetime** and **valid-lifetime** commands (in ND router interface configuration mode).

Use the **no** or **default** form of this command to delete the specified prefix from this interface configuration.

1.28.6 Examples

The following example configures the **5555:bbbb::22/64** prefix 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)#prefix 5555:bbbb::22/64 no-autoconfig
 no-onlink preferred-lifetime 360 valid-lifetime 360
```

1.29 prefix duid

prefix ***ipv6-prefix*** **duid** ***colon-delimited-hex-string*** [**iaid** ***hex-string***]

{**no** | **default**} **prefix** ***ipv6-prefix*** **duid** ***colon-delimited-hex-string*** [**iaid** ***hex-string***

1.29.1 Purpose

For a DHCPv6 server, statically maps a specified IPv6 prefix to a DHCPv6 Unique Identifier (DUID) and, optionally, an Identity Association Identifier (IAID).

1.29.2 Command Mode

DHCPv6 server policy configuration

1.29.3 Syntax Description

ipv6-prefix	Configures an IPv6 prefix for a DUID and, optionally, an IAID.
colon-delimited-hex-string	Specifies a client DUID; replace ***hex-string*** with a colon-delimited hexadecimal number.
hex-string	Optional. Specifies a IAID for the DHCPv6 server or subnet; replace ***hex-string*** with a hexadecimal number preceded by 0x (not case-sensitive).

1.29.4 Default

No DUID or IAID is configured for a static DHCPv6 delegated prefix.

1.29.5 Usage Guidelines

Use the **prefix duid** command on a DHCPv6 server to statically map a specified IPv6 prefix to a DUID and, optionally, IAID tuple. If a match occurs, the matching prefixes are added to the list of prefixes that can be assigned to the subscriber. If you do not configure an IAID for the prefix attribute, only the DUIDs must match for the client to receive that IPv6 prefix from the server.

Note: The number of prefixes that can be assigned to a subscriber is limited by the Delegated-Max-Prefix value. If the number of matching prefixes is greater than the Delegated-Max-Prefix value, the router arbitrarily chooses which prefixes are assigned to the subscriber.

Consider the following when configuring statically mapped DHCPv6 PD prefixes:

- Statically mapped prefixes must not fall within the prefix range of any prefix pools configured on the system.
- Statically mapped prefixes are included in the Delegated-Max-Prefix value.

Use the **no** form of this command to remove a static DHCPv6 delegated prefix for DUID from a DHCPv6 server configuration.

1.29.6 Examples

The following example configures the static prefix **2:2:db8::c/64** for the DUID **00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2** and the IAID **0xfedcba98**:

```
[local]Redback(config-ctx)#dhcpv6 server
[local]Redback(config-dhcpv6-server)#prefix 2:2:db8::c/64 duid 00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2 iaid
```

1.30 prefix lifetime

prefix lifetime {**preferred** ***seconds*** **valid** ***seconds*** | **infinite**}

no prefix lifetime

1.30.1 Purpose

In a DHCPv6 server policy, configures the length of time the subscriber router is allowed to use the delegated IPv6 prefix and the number of seconds a client can use a given DHCPv6 address.

1.30.2 Command Mode

DHCPv6 server policy configuration

DHCPv6 server subnet configuration

1.30.3 Syntax Description

preferred ***seconds***	Number of seconds the IPv6 addresses using the delegated IPv6 prefix are preferred. Range is from 600 through 4,294,967,294 seconds.
valid ***seconds***	Number of seconds a delegated IPv6 prefix is valid and can be used by a client. Range is from 600 through 4,294,967,294 seconds.
infinite	Configures both the preferred and valid lifetimes to be infinite.

1.30.4 Default

The default value is infinite.

1.30.5 Usage Guidelines

Use the **prefix lifetime** command to configure the length of time the subscriber router is allowed to use the delegated IPv6 prefix and the number of seconds a client can use a given DHCPv6 address.

Use the **no** version of this command to return to the DHCPv6 server policy prefix lifetime attribute to the default configuration.

1.30.6 Examples

The following example configures the preferred and valid lifetime attributes in a DHCPv6 server policy to be 3600 seconds and 7200 seconds.

```
[local]BRAS(config-ctx)#dhcpv6 server
[local]Redback(config-dhcpv6-server)#prefix lifetime preferred 3600 valid 7200
```

The following example configures the preferred and valid lifetime attributes in a DHCPv6 server policy to be infinite:

```
[local]BRAS(config-ctx)#dhcpv6 server
[local]Redback(config-dhcpv6-server)#prefix lifetime infinite
```

1.31 prefix-list

prefix-list *pl-name* {**in** | **out**}

no prefix-list *pl-name* {**in** | **out**}

1.31.1 Purpose

Filters Border Gateway Protocol (BGP) routes from or to the neighbor address family or peer group address family.

1.31.2 Command Mode

- BGP neighbor address family configuration
- BGP peer group address family configuration

1.31.3 Syntax Description

pl-name	Name of the prefix list.
in	Applies the prefix list to incoming updates from the neighbor.
out	Applies the prefix list to outgoing updates to the neighbor. This keyword can only be applied in BGP neighbor address family configuration mode.

1.31.4 Default

There are no preconfigured prefix lists.

1.31.5 Usage Guidelines

Use the **prefix-list** command to filter BGP routes from or to the neighbor address family or peer group address family. Use this command in conjunction with the **ip prefix-list** command in context configuration mode, which creates the conditions of the filter.

Use the **in** keyword to filter incoming BGP routes from the specified neighbor or peer. Use the **out** keyword to filter outgoing BGP routes to the specified neighbor.

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

Currently, prefix list changes automatically take effect, and issuing the **clear bgp neighbor** *ip-addr* **soft** [**in** | **out**] command in exec mode to update a prefix list can cause updates to be unnecessarily sent; therefore, it is not recommended.

To aggregate multiple policy changes, such as the prefix list, the operating system performs the automatic update 15 seconds after any routing policy has changed.

Note: If the remote peer does not support the BGP route refresh capability, an inbound policy change for the peer will result in an automatic hard reset of the session.

Use the **no** form of this command to remove the application of a prefix list.

1.31.6 Examples

The following example denies incoming unicast BGP routes **10.0.0.0/8** (and more-specific routes) from the unicast neighbor at IP address **102.210.210.1**. Outgoing multicast BGP routes **204.16.16.0/24** can be sent to the multicast neighbor at IP address **68.68.68.68**:

```
[local]Redback(config-ctx)#ip prefix-list prefix-101
[local]Redback(config-prefix-list)#deny 10.0.0.0/8 le 32
[local]Redback(config-prefix-list)#permit 0.0.0.0/0 le 32
[local]Redback(config-prefix-list)#exit
[local]Redback(config-ctx)#ip prefix-list prefix-202
[local]Redback(config-prefix-list)#permit 204.16.16.0/24
.
.
.
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#neighbor 102.210.210.1 external
[local]Redback(config-bgp-neighbor)#remote-as 200
[local]Redback(config-bgp-neighbor)#address-family ipv4 unicast
[local]Redback(config-bgp-peer-af)#prefix-list prefix-101 in
[local]Redback(config-bgp-peer-af)#exit
[local]Redback(config-bgp-neighbor)#exit
[local]Redback(config-bgp)#neighbor 68.68.68.68 external
[local]Redback(config-bgp-neighbor)#remote-as 300
[local]Redback(config-bgp-neighbor)#address-family ipv4 multicast
[local]Redback(config-bgp-peer-af)#prefix-list prefix-202 out
```

1.32 priority (IGMP)

priority *priority*

no priority

1.32.1 Purpose

Configures the priority of the interface when the maximum bandwidth in the service profile has been exhausted.

1.32.2 Command Mode

IGMP service profile configuration

1.32.3 Syntax Description

priority	Priority setting for the interface. The range of values is 0 to 10.

1.32.4 Default

The interface has no priority setting.

1.32.5 Usage Guidelines

Use the **priority** command to configure the priority of the interface when the maximum bandwidth in the service profile has been exhausted.

When the addition of a new group would cause the maximum bandwidth, as specified by the **igmp maximum-bandwidth** command, to be exceeded on the port, the router searches for subscribers joined on the same port with a lower priority. The router drops the lower priority subscribers and reclaims their bandwidth until it gets enough bandwidth to service the higher priority subscriber. If it cannot reclaim enough bandwidth the new group join will be dropped.

Use the **no** form of this command to delete the priority setting for the interface.

1.32.6 Examples

The following example configures a priority of **8** for the interface:

```
[local]Redback(config-ctx)#igmp service-profile bar
[local]Redback(config-igmp-service-profile)#priority 8
```

1.33 priority (IS-IS)

priority *priority* [**level-1** | **level-2**]

no priority

1.33.1 Purpose

Configures the Intermediate System-to-Intermediate System (IS-IS) designated router priority setting for the specified LAN interface.

1.33.2 Command Mode

IS-IS interface configuration

1.33.3 Syntax Description

priority	Priority setting. The range of values is 0 to 127; the default value is 64. Higher numbers signify a higher priority.
level-1	Optional. Sets the priority for IS-IS level 1 routing independently.
level-2	Optional. Sets the priority for IS-IS level 2 routing independently.

1.33.4 Default

The priority setting is 64.

1.33.5 Usage Guidelines

Use the **priority** command to configure the IS-IS designated router priority setting for the specified LAN interface.

A priority value determines which router on a network is the first router chosen for sending and receiving traffic. The priority value is advertised in Hello packets. The router with the highest priority becomes the Designated Intermediate System (DIS).

In IS-IS, there is no backup designated router. If a router is set to priority 0, it has a smaller chance of becoming the DIS, but it may not be prevented from becoming the DIS. When a router with a higher priority becomes available on the network, it takes over as the current DIS. In the case of equal priorities, the highest medium access control (MAC) address breaks the tie.

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

1.33.6 Examples

The following example sets the priority for the **fa4/1** interface to **80**, making it more likely to become the DIS for IS-IS **level-1** routing:

```
[local]Redback(config-ctx)#router isis ip-backbone
[local]Redback(config-isis)#interface fa4/1
[local]Redback(config-isis-if)#priority 80 level-1
```

1.34 priority (loop-detection)

priority *level*

no priority

1.34.1 Purpose

Sets the priority of loop-prevention blocking on the assigned circuit.

1.34.2 Command Mode

- loop-detection profile configuration

1.34.3 Syntax Description

level	Priority of loop-prevention blocking on the assigned circuit (0 to 5).

1.34.4 Default

0 (never blocked)

1.34.5 Usage Guidelines

Use the **priority** command to set the priority of loop-prevention blocking on the assigned circuit. The default is 0 (unblockable). Except for circuits with priority 0, circuits with higher priority are blocked before circuits with lower priority. Circuits with priority 0 are never blocked.

Use the **no** form of this command to return the priority of loop-detection of the assigned circuit to its default.

1.34.6 Examples

The following example creates the bridge profile, **plow**, and sets the loop-detection priority for circuits associated with that bridge profile to the value **2**:

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

1.35 priority (maintenance-association)

priority ***priority***

no priority

1.35.1 Purpose

Sets the 802.1p priority level for CFM message CCM, ETH-LB, and ETH-LT frames. CCMs, ETH-LB, and ETH-LT frames are priority agnostic; no errors are flagged on priority mismatch. Upon a mismatch between the frames received and the priority configured, the priority of the incoming LB/LT/LM frames is used. The configured priority is used for the OAM traffic initiated from the MEP and the incoming priority of the LB/LT/LM frames is used to respond back to those OAM frames.

1.35.2 Command Mode

- CFM Maintenance Association (MA) configuration

1.35.3 Syntax Description

priority	Sets the 802.1p priority level of CCM, Ethernet loopback (ETH-LB), and Ethernet linktrace (ETH-LT) frames. The range is 0 to 7 ; the default value is 6.

1.35.4 Default

6

1.35.5 Usage Guidelines

Use the **priority** command to set the CFM message priority for CCM, ETH-LB, and ETH-LT frames.

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

1.35.6 Examples

The following example shows how to the CFM message 802.1p priority level of the MA "bayarea" to 4.

```
[local]Redback(config-ether-cfm)#maintenance-association bayarea
[local]Redback(config-ether-cfm)#priority 4
```

1.36 priority (RSVP)

priority ***setup-priority*** [***hold-priority***]

no priority

1.36.1 Purpose

For Constrained Shortest Path First (CSPF), specifies the preemptive characteristics of the label-switched path (LSP).

1.36.2 Command Mode

- RSVP constraint configuration

1.36.3 Syntax Description

setup-priority	Setup priority. The range of values is 0 to 7, where the lower the number, the greater the priority.
hold-priority	Optional. Hold priority. The range of values is 0 to 7, where the lower the number, the greater the priority.

1.36.4 Default

Setup priority is 7. Hold priority is 0.

1.36.5 Usage Guidelines

For CSPF, specifies the preemptive characteristics of the LSP. The setup priority specifies whether a new LSP can preempt an existing LSP. The hold priority determines whether the LSP can preserve its session reservation after being established. If the setup priority of the new LSP has a higher priority (a lower number) than the hold priority of an existing LSP, and resource contention exists between two LSPs, they preempt each other forever because neither LSP can preserve its session reservation. The system prevents you from configuring the hold priority to a higher priority (lower number) than the setup priority.

Note: You typically configure the setup priority and hold priority to the same value.

The following scenario illustrates what happens when two LSPs are configured with the same setup priority but with a lower hold priority, and resource contention exists between both LSPs. In this case, both LSP1 and LSP2 have a setup priority of `6 and a hold priority of 7:`

1. LSP1 establishes a tunnel.
2. LSP2 attempts to establish a tunnel, and contention exists for resources with LSP1.
3. LSP2 preempts (disassembles) LSP1 because its setup priority is higher than the hold priority.
4. LSP1 attempts to re-establishes its tunnel and succeeds by disassembling the LSP2 tunnel, because its setup priority is higher than the hold priority.
5. This process continues forever if the hold priorities continues to remain lower than the setup priorities and sufficient bandwidth is available for both LSPs.

Use the **no** form of this command to remove the tunnel priority.

1.36.6 Examples

The following example shows how to configure an LSP with a setup priority of `2` and a hold priority of `2`:

```
[local]Redback#configure
[local]Redback(config)#context sj1
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#constraint constraint1
[local]Redback(config-rsvp-constr)#priority 2 2
```

1.37 priority (spanning-tree)

priority ***level***

{**no** | **default**} **priority**

1.37.1 Purpose

Sets the priority of the bridge.

1.37.2 Command Mode

- spanning-tree configuration

1.37.3 Syntax Description

level	Priority of the bridge. The range of values is 0 to 61,440, in multiples of 4096.

1.37.4 Default

The default priority level is 32768.

1.37.5 Usage Guidelines

Use the **priority** command to set the priority of the bridge (0 to 61,440). The lower the priority of the bridge, the more likely it is to be elected as the root bridge.

In the Spanning Tree Protocol, the bridge identifier consists of the bridge MAC address and the bridge priority. These attributes can optionally be set by the **bridge-mac-address** command (in bridge configuration mode) and the **priority** command, respectively.

1.37.6 Examples

An example of the bridge priority follows:

```
[local]Redback(config-bridge-stp)#priority 8192
```

1.38 priority (VRRP)

priority ***priority***

no priority

1.38.1 Purpose

Configures the Virtual Router Redundancy Protocol (VRRP) election priority for the backup virtual router.

1.38.2 Command Mode

VRRP configuration

1.38.3 Syntax Description

priority	Priority setting for the backup virtual router. The range of values is 1 to 254.

1.38.4 Default

The priority is set to 100.

1.38.5 Usage Guidelines

Use the **priority** command to configure the VRRP priority for the backup virtual router. A backup router that has a higher priority value is preferred over a router that has a lower priority value.

Use the **no** form of this command to return the priority setting to its default value.

1.38.6 Examples

The following example configures VRRP backup routers for two separate routers, **Router_A** and **Router_B**, on the same LAN. Both VRRP backup routers have the same virtual ID, **2**. The VRRP backup router on **Router_B**, which has a priority of **200**, is preferred over the VRRP backup router on **Router_A**, which has a priority of **100**.

The configuration for **Router_A** is as follows:

```
[local]Router_A(config)#context local
[local]Router_A(config-ctx)#interface foo
[local]Router_A(config-if)#ip address 1.1.1.100/24 secondary
[local]Router_A(config-if)#vrrp 2 backup
[local]Router_A(config-vrrp)#virtual-address 1.1.1.111
[local]Router_A(config-vrrp)#priority 100
```

The configuration for **Router_B** is as follows:

```
[local]Router_B(config)#context local
[local]Router_B(config-ctx)#interface foo
[local]Router_B(config-if)#ip address 1.1.1.200/24 secondary
[local]Router_B(config-if)#vrrp 2 backup
[local]Router_B(config-vrrp)#virtual-address 1.1.1.111
[local]Router_B(config-vrrp)#priority 200
```

1.39 privilege

privilege ***mode*** [**inherit**] **level** ***level command***

{**no** | **default**} **privilege** ***mode command***

1.39.1 Purpose

Assigns a different privilege level to the specified command.

1.39.2 Command Mode

global configuration

1.39.3 Syntax Description

mode	Mode of the command.
inherit	Optional. Assigns the specified privilege level to all keywords that follow the last keyword specified in the ***command*** argument.
level ***level***	Minimum privilege level required to generate the specified command. The range of values is 0 to 15.
command	Command keyword (or keywords).

1.39.4 Default

For the default minimum privilege level, see the individual commands. In general, most exec mode commands require privilege level 3, and most configuration mode commands require privilege level 10.

1.39.5 Usage Guidelines

Use the **privilege** command to assign a different privilege level to a specific command or set of commands.

Use the **inherit** keyword to modify the privilege level of all commands that begin with one or more keywords within a particular mode. For example, to modify all commands that begin with the **snmp** keyword (**snmp server**, **snmp target**, and so on) in global configuration mode, specify **configuration** for the ***mode*** argument, the **inherit** keyword, and **snmp** for the ***command*** argument; the command appears as follows:

```
[local]Redback(config)#privilege config inherit snmp
```

If you are an administrator at privilege level 15, you can determine the privilege level of any given command by recursively applying the **enable** and **show ?** commands at level 15, level 14, level 13, and so on. Initially, all commands at privilege level 15 and lower are listed, then all commands at privilege level 14 and lower, and do on. Be aware that this method yields the current privilege levels, which could be different from the default privilege levels.

Use the **no** or **default** form of this command to return a command to the default privilege level.

1.39.6 Examples

The following example assigns the minimum privilege level to the **abort** and **commit** commands (in **exec** mode) to **15**:

```
[local]Redback(config)#privilege exec abort level 15
[local]Redback(config)#privilege exec commit level 15
```

The following example assigns the minimum privilege level, 12, to all global configuration mode commands that start with the **snmp** keyword:

```
[local]Redback(config)#privilege configuration inherit level 12 snmp
```

1.40 privilege max

privilege max *level*

default fault privilege max

1.40.1 Purpose

Specifies the maximum privilege level for the administrator.

1.40.2 Command Mode

administrator configuration

1.40.3 Syntax Description

level	Maximum privilege level for an administrator. The range of values is 0 to 15; the default value is 15.

1.40.4 Default

The maximum privilege level is 15.

1.40.5 Usage Guidelines

Use the **privilege max** command to specify the maximum privilege level for the administrator.

Using the **enable** command (in exec mode), an administrator can change the privilege level of the current exec session up to the maximum privilege level specified by this command for the administrator.

Use the **default** form of this command to return the maximum privilege level to the default value.

1.40.6 Examples

The following command configures administrator **fred** to a maximum privilege level of **13**:

```
[local]Redback(config-ctx)#administrator fred
[local]Redback(config-administrator)#privilege max 13
```

1.41 privilege start

privilege start *level*

default privilege start

1.41.1 Purpose

Specifies the initial privilege level for exec sessions initiated by an administrator.

1.41.2 Command Mode

administrator configuration

1.41.3 Syntax Description

level	Initial privilege level for exec sessions initiated by an administrator. The range of values is 0 to 15; the default value is 6.

1.41.4 Default

The initial privilege level is set to 6.

1.41.5 Usage Guidelines

Use the **privilege start** command to specify the initial privilege level for any exec session initiated by the administrator.

When an administrator logs on to the system, the exec session runs at the initial privilege level specified by this command for the administrator.

Use the **default** form of this command to return the initial privilege level for an administrator to the default value.

1.41.6 Examples

The following command configures administrator **fred** with an initial privilege level of **11**:

```
[local]Redback(config-ctx)#administrator fred
[local]Redback(config-administrator)#privilege start 11
```

1.42 probablecause

probablecause ***probable-cause-value***

no probablecause ***probable-cause-value***

1.42.1 Purpose

Identifies the probable cause of the event as defined by IANAItuProbableCause in IANA-ITU-ALARM-MIB.

1.42.2 Command Mode

- SNMP alarm model configuration

1.42.3 Syntax Description

probable-cause-value	Value from 1–1,024, based on IANA ITU ALARM-MIB. See Usage Guidelines for values for this argument

1.42.4 Default

None

1.42.5 Usage Guidelines

Identifies the probable cause of the event as defined by IANAItuProbableCause in ASNA-ITU-ALARM-MIB. The value identifies the event type. The following are possible values for the ***probable-cause-value*** argument:

1—aIS

2—callSetUpFailure

3—degradedSignal

4—farEndReceiverFailure

5—framingError

6—lossOfFrame

7—lossOfPointer

8—lossOfSignal

9—payloadTypeMismatch

10—transmissionError

11—remoteAlarmInterface

12—excessiveBER

13—pathTraceMismatch

14—unavailable

15—signalLabelMismatch

16—lossOfMultiFrame

17—receiveFailure

18—transmitFailure

19—modulationFailure

20—demodulationFailure

21—broadcastChannelFailure

22—connectionEstablishmentError

23—invalidMessageReceived

24—localNodeTransmissionError

25—remoteNodeTransmissionError

26—routingFailure

51—backplaneFailure

52—dataSetProblem

53—equipmentIdentifierDuplication

54—externalIFDeviceProblem

55—lineCardProblem

56—multiplexerProblem

57—nEIdentifierDuplication

58—powerProblem

59—processorProblem

60—protectionPathFailure

61—receiverFailure

62—replaceableUnitMissing

63—replaceableUnitTypeMismatch

64—synchronizationSourceMismatch

65—terminalProblem

66—timingProblem

67—transmitterFailure

68—trunkCardProblem

69—replaceableUnitProblem

70—realTimeClockFailure

71—antennaFailure

72—batteryChargingFailure

73—diskFailure

74—frequencyHoppingFailure

75—iODeviceError

76—lossOfSynchronisation

77—lossOfRedundancy

78—powerSupplyFailure

79—signalQualityEvaluationFailure

80—tranceiverFailure

81—protectionMechanismFailure

82—protectingResourceFailure

101—airCompressorFailure

102—airConditioningFailure

103—airDryerFailure

104—batteryDischarging

105—batteryFailure

106—commercialPowerFailure

107—coolingFanFailure

108—engineFailure

109—fireDetectorFailure

110—fuseFailure

111—generatorFailure

112—lowBatteryThreshold

113—pumpFailure

114—rectifierFailure

115—rectifierHighVoltage

116—rectifierLowFVoltage

117—ventilationsSystemFailure

118—enclosureDoorOpen

119—explosiveGas120—fire

121—flood

122—highHumidity

123—highTemperature

124—highWind

125—iceBuildUp

126—intrusionDetection

127—lowFuel

128—lowHumidity

129—lowCablePressure

130—lowTemperatue

131—lowWater

132—smoke

133—toxicGas

134—coolingSystemFailure

135—externalEquipmentFailure

136—externalPointFailure

151—storageCapacityProblem

152—memoryMismatch

153—corruptData

154—outOfCPUCycles

155—sfwrEnvironmentProblem

156—sfwrDownloadFailure

157—lossOfRealTimeI

158—applicationSubsystemFailure

159—configurationOrCustomisationError

160—databaseInconsistency

161—fileError

162—outOfMemory

163—softwareError

164—timeoutExpired

165—underlayingResourceUnavailable

166—versionMismatch

201—bandwidthReduced

202—congestion

203—excessiveErrorRate

204—excessiveResponseTime

205—excessiveRetransmissionRate

206—reducedLoggingCapability

207—systemResourcesOverload

500—adapterError

501—applicationSubsystemFailture

502—bandwidthReducedX733

503—callEstablishmentError

504—communicationsProtocolError

505—communicationsSubsystemFailure

506—configurationOrCustomizationError

507—congestionX733

508—coruptData

509—cpuCyclesLimitExceeded

510—dataSetOrModemError

511—degradedSignalX733

512—dteDceInterfaceError

513—enclosureDoorOpenX733

514—equipmentMalfunction

515—excessiveVibration

516—fileErrorX733

517—fireDetected

518—framingErrorX733

519—heatingVentCoolingSystemProblem

520—humidityUnacceptable

521—inputOutputDeviceError

522—inputDeviceError

523—lanError

524—leakDetected

525—localNodeTransmissionErrorX733

526—lossOfFrameX733

527—lossOfSignalX733

528—materialSupplyExhausted

529—multiplexerProblemX733

530—outOfMemoryX733

531—ouputDeviceError

532—performanceDegraded

533—powerProblems

534—pressureUnacceptable

535—processorProblems

536—pumpFailureX733

537—queueSizeExceeded

538—receiveFailureX733

539—receiverFailureX733

540—remoteNodeTransmissionErrorX733

541—resourceAtOrNearingCapacity

542—responseTimeExecessive

543—retransmissionRateExcessive

544—softwareErrorX733

545—softwareProgramAbnormallyTerminated

546—softwareProgramError

547—storageCapacityProblemX733

548—temperatureUnacceptable

549—thresholdCrossed

550—timingProblemX733

551—toxicLeakDetected

552—transmitFailureX733

553—transmiterFailure

554—underlyingResourceUnavailable

555—versionMismatchX733

600—authenticationFailure

601—breachOfConfidentiality

602—cableTamper

603—delayedInformation

604—denialOfService

605—duplicateInformation

606—informationMissing

607—informationModificationDetectede

608—informationOutOfSequence

609—keyExpired

610—nonRepudiationFailure

611—outOfHoursActivity

612—outOfServic

613—proceduralError

614—unauthorizedAccessAttempt

615—unexpectedInformation

1024—other

Use the **no** form of this command to remove the probable cause of the event.

1.42.6 Examples

The following example shows how to configure the probable cause for the alarm model event as thresholdCrossed (549).

```
[local]jazz#config
[local]jazz(config)#snmp alarm model 1 state clear
[local]jazz(config-snmp-alarmmodel)#probablecause 549
[local]jazz(config-snmp-alarmmodel)#exit
```

1.43 process coredump

process coredump {***proc-name*** | **-** ***proc-id***}

1.43.1 Purpose

Interrupts the specified process and saves the core dump file.

1.43.2 Command Mode

- exec (10)

1.43.3 Syntax Description

proc-name	Process name for which a core dump is to be generated. The value of the ***proc-name*** argument can be any one of the keywords listed in Table 3.
proc-id	Dash (-) followed by the process identification number (PID). The range of values is 1 to 65,535.

1.43.4 Default

None

1.43.5 Usage Guidelines

Use the **process coredump** command to interrupt a specified process and save the core dump file. You can specify the process either by its process name or PID.

Caution!

Risk of data loss. Generating a core dump interrupts the specified process for a brief period, the length of which depends on the size of the binary and the amount of memory used by the process, before the process is automatically restarted by the system. To reduce the risk, do not initiate a core dump while the system is experiencing heavy traffic.

Caution!

Risk of system crash. Allow sufficient time after entering the **process coredump** command to allow the SmartEdge router to stabilize. Monitor the SmartEdge router and wait for it to stabilize before entering the **process restart** command. Contact technical support before you start and restart multiple processes.

For an overview of core dumps, crash files, and a guide to their management, see *Performing Core Dump and Crash File Management Tasks* in *Managing Files* for additional information.

Note: We strongly recommend that you configure the system to upload crash files automatically to a remote File Transfer Protocol (FTP) server, using the **service upload-coredump** command (in global configuration mode). By configuring this service, you maximize the use of available disk space and improve system stability and performance. For more information about the **service upload-coredump** command (in global configuration mode), see the *Command List*.

Note: This command is used to provide troubleshooting information to the technical support group.

Table 3 lists the keywords for the processes supported by this command.

Table 3 Keywords for Processes

Keyword	Process
aaad	authentication, authorization, and accounting (AAA) process
arp	Address Resolution Protocol (ARP) process
atm	Asynchronous Transfer Mode (ATM) process
bgp	Border Gateway Protocol (BGP) process
bridge	bridge process
cfm	Ethernet 802.1PG-CFM process
clips	clientless IP service selection process
cls	Classifier Manager process
csm	Controller State Manager (CSM) process
cspf	Constrained Shortest Path First (CSPF) process
dhcp	Dynamic Host Configuration Protocol (DHCP) relay/proxy process

Keyword	Process
dhcpv6	DHCPv6 process
dhelperd	DHCP helper process
dhelper6d	DHCPv6 helper process
dlm	Download Manager (DLM) process
dns	Domain Name System (DNS) process
dot1q	802.1Q encapsulation process(1)
flowd	flow process(2)
fr	Frame Relay process (3)
fsd	File server process
fssbcsim	FSSB client simulator
gsmp	General Switch Management Protocol (GSMP) process
hr	HTTP redirect process
igmp	Internet Group Management Protocol (IGMP) process
ipfix	IPFIX Aggragation and Protocol process
isis	Intermediate System-to-Intermediate System (IS-IS) process
ism	Interface and Circuit State Manager (ISM) process
l2tp	Layer 2 Tunneling Protocol (L2TP) process
l4l7	L4L7 process
ldp	Label Distribution Protocol (LDP) process
lg	link group (LG) process
lm	Label Manager (LM) process
metad	META process
mgd	Media Gateway process
mgmd	Media Gateway Manager process
mip	Mobile IP process
mipsim	Mobile IP simulator process
mpls_static	Multiprotocol Label Switching (MPLS) static process
msdp	Multicast Source Discovery Protocol (MSDP) process
nat	IP Network Address Translation (NAT) process
nd	Neighbor Discovery (ND) process
netopd	NetOp process daemon
ntp	Network Time Protocol (NTP) process

Keyword	Process
odd	on-demand diagnostics (ODD) process
ospf	Open Shortest Path First (OSPF) protocol process
ospf3	OSPF Version 3 (OSPF3) protocol process
ped_parse	process execution descriptor (PED) parse process
pem	Port encapsulation module (PEM) process
pim	Protocol Independent Multicast (PIM) process
ppaslog	Packet Processing ASIC (PPA) syslog process
ppp	Point-to-Point Protocol (PPP) process
pppoe	PPP over Ethernet (PPPoE) process
qos	quality of service (QoS) process
rcm	Router Configuration Manager (RCM) process
rib	Routing Information Base (RIB) process
rip	Routing Information Protocol (RIP) process
rpm	Routing Policy Manager (RPM) process
rsvp	Resource Reservation Protocol Traffic Engineering (RSVP-TE) process
sctp	Stream Control Transmission Protocol (SCTP) process
shm_ribd	Shared Memory RIB process
snmp	Simple Network Management Protocol (SNMP) process
static	static routing process
stats	statistics process
sysmon	system monitor process
tunnel	tunnel management process
vrrp	Virtual Router Redundancy Protocol (VRRP) process
xcd	Cross-connect process daemon

(1) The SmartEdge 100 router does not support 802.1Q.
(2) Not all controller cards support flow.
(3) The SmartEdge 100 router does not support Frame Relay.

1.43.6 Examples

The following example initiates a core dump and creates a crash file for the BGP process:

```
[local]Redback#process coredump bgp
```

1.44 process restart

process restart *proc-name* [*delay*]

1.44.1 Purpose

Restarts a process that has been stopped.

1.44.2 Command Mode

- exec (10)

1.44.3 Syntax Description

proc-name	Process to be restarted. The value of the *proc-name* argument can be any one of the keywords listed inTable 4 .
delay	Optional. Delay, in seconds, before a process is restarted. The range of values is 0 to 4,294,967,295; the default value is 2.

1.44.4 Default

The default for the optional delay is two seconds.

1.44.5 Usage Guidelines

Use the **process restart** command to restart a process that has been stopped.

Table 4 lists the keywords for the processes supported by this command.

Table 4 Keywords for Processes

Keyword	Process
aaad	authentication, authorization, and accounting (AAA) process
arp	Address Resolution Protocol (ARP) process
atm	Asynchronous Transfer Mode (ATM) process
bgp	Border Gateway Protocol (BGP) process
bridge	bridge process
cfm	Ethernet 802.1PG-CFM process
clips	clientless IP service selection process
cls	Classifier Manager process

Keyword	Process
csm	Controller State Manager (CSM) process
cspf	Constrained Shortest Path First (CSPF) process
dhcp	Dynamic Host Configuration Protocol (DHCP) relay/proxy process
dhcpv6d	DHCPv6 process
dhelperd	DHCP helper daemon
dhelper6d	DHCPv6 helper daemon
dlm	Download Manager (DLM) process
dns	Domain Name System (DNS) process
dot1q	802.1Q encapsulation process(1)
flowd	flow process(2)
fr	Frame Relay process (3)
fsd	File server process
fssbcsim	FSSB client simulator process
gsmp	General Switch Management Protocol (GSMP) process
hr	HTTP redirect process
igmp	Internet Group Management Protocol (IGMP) process
ipfix	IPFIX aggregation and protocol process
isis	Intermediate System-to-Intermediate System (IS-IS) process
ism	Interface and Circuit State Manager (ISM) process
l2tp	Layer 2 Tunneling Protocol (L2TP) process
l4l7	L4L7 process
ldp	Label Distribution Protocol (LDP) process
lg	link group (LG) process
lm	Label Manager (LM) process
mcastmgr	Multicast manager process.
metad	META daemon process
mgd	Media Gateway daemon process
mgmd	Media Gateway manager process
mip	Mobile IP process
mipsim	Mobile IP simulator process
mpls_static	Multiprotocol Label Switching (MPLS) static process

Keyword	Process
msdp	Multicast Source Discovery Protocol (MSDP) process
nat	IP Network Address Translation (NAT) process
nd	Neighbor Discovery (ND) process
netopd	NetOp process daemon
ntp	Network Time Protocol (NTP) process
odd	on-demand diagnostics (ODD) process
ospf	Open Shortest Path First (OSPF) protocol process
ospf3	OSPF Version 3 (OSPF3) protocol process
ped_parse	process execution descriptor (PED) parse process
pem	Port encapsulation module (PEM) process
pim	Protocol Independent Multicast (PIM) process
ppaslog	Packet Processing ASIC (PPA) syslog process
ppp	Point-to-Point Protocol (PPP) process
pppoe	PPP over Ethernet (PPPoE) process
qos	quality of service (QoS) process
rcm	Router Configuration Manager (RCM) process
rib	Routing Information Base (RIB) process
rip	Routing Information Protocol (RIP) process
rpm	Routing Policy Manager (RPM) process
rsvp	Resource Reservation Protocol Traffic Engineering (RSVP-TE) process
sctp	Stream Control Transmission Protocol (SCTP) process
shm_ribd	Shared Memory RIB process
snmp	Simple Network Management Protocol (SNMP) process
static	static routing process
stats	statistics process
sysmon	system monitor process
tunnel	tunnel management process
vrrp	Virtual Router Redundancy Protocol (VRRP) process
xcd	cross-connect process daemon

(1) The SmartEdge 100 router does not support 802.1Q.
(2) Not all controller cards support flow.
(3) The SmartEdge 100 router does not support Frame Relay.

1.44.6 Examples

The following example restarts the BGP process after a five-minute delay (300 seconds):

```
[local]Redback#process restart bgp 300
```

1.45 process set

process set *proc-name* {**heart-beat** {**on** | **off**} | **kill-time** *seconds* | **max-crashes** *num-crashes* [**within** *seconds*] | **spawn-time** [*seconds*]}

1.45.1 Purpose

Sets process management parameters.

1.45.2 Command Mode

- exec (10)

1.45.3 Syntax Description

proc-name	Process for which you are setting management parameters. The value of the *proc-name* argument can be any one of the keywords listed inTable 5 .
heart-beat	Specifies that a heartbeat setting follows.
on	Turns the process heartbeat on.
off	Turns the process heartbeat off.
kill-time *seconds*	Number of seconds from issuing the **process set** command after which the Process Manager (PM) kills the specified process. The range of values is 1 to 429,496,729.
max-crashes *num-crashes*	Maximum number of crashes allowed within the time interval specified by the **within** *seconds* construct. The range of values is 0 to 10; the default value is 5.
within *seconds*	Optional. Number of seconds within which the maximum number of crashes is allowed. If not specified, the system uses the default value of 86,400 (24 hours).
spawn-time	Specifies that a spawn time setting follows. If used without the optional *seconds* argument, sets the spawn time to the default value of two seconds.
seconds	Optional with the **spawn-time** keyword. Number of seconds delay between the crash of a process and the subsequent spawn by the PM. The range of values is 1 to 300; the default value is 2.

1.45.4 Default

The heartbeat is on; the maximum number of crashes allowed is five per process within a 24 hour period; the spawn time is two seconds.

1.45.5 Usage Guidelines

Use the **process set** command to set process management parameters including whether the heartbeat is turned on or off, the kill time, the maximum number of crashes allowed within a configurable period of time, and the amount of time between the crash of a process and the subsequent spawn by the PM (spawn time).

Table 5 lists the keywords for the processes supported by this command.

Table 5 Keywords for Processes

Keyword	Process
aaad	authentication, authorization, and accounting (AAA) process
arp	Address Resolution Protocol (ARP) process
atm	Asynchronous Transfer Mode (ATM) process
bgp	Border Gateway Protocol (BGP) process
bridge	bridge process
cfm	Ethernet 802.1pg-CFM process
clips	clientless IP service selection process
cls	Classifier Manager process
csm	Controller State Manager (CSM) process
cspf	Constrained Shortest Path First (CSPF) process
dhcp	Dynamic Host Configuration Protocol (DHCP) relay/proxy process
dhcpv6d	DHCPv6 process
dhelperd	DHCP helper daemon
dhelper6d	DHCPv6 helper daemon
dlm	Download Manager (DLM) process
dns	Domain Name System (DNS) process
dot1q	802.1Q encapsulation process(1)
flowd	flow process(2)
fr	Frame Relay process (3)
fsd	File server process
fssbcsim	FSSB client simulator
gsmp	General Switch Management Protocol (GSMP) process
hr	HTTP redirect process
igmp	Internet Group Management Protocol (IGMP) process

Keyword	Process
ipfix	IPFIX aggregation and protocol process
isis	Intermediate System-to-Intermediate System (IS-IS) process
ism	Interface and Circuit State Manager (ISM) process
l2tp	Layer 2 Tunneling Protocol (L2TP) process
l4l7	L4L7 process
ldp	Label Distribution Protocol (LDP) process
lg	link group (LG) process
lm	Label Manager (LM) process
mcastmgr	Multicast manager process.
metad	META process
mgd	Media Gateway daemon process
mgmd	Media Gateway manager process
mip	Mobile IP process
mipsim	Mobile IP simulator process
mpls_static	Multiprotocol Label Switching (MPLS) static process
msdp	Multicast Source Discovery Protocol (MSDP) process
nat	IP Network Address Translation (NAT) process
nd	Neighbor Discovery (ND) process
netopd	NetOp process daemon
ntp	Network Time Protocol (NTP) process
odd	on-demand diagnostics (ODD) process
ospf	Open Shortest Path First (OSPF) protocol process
ospf3	OSPF Version 3 (OSPF3) protocol process
ped_parse	process execution descriptor (PED) parse process
pem	Port encapsulation module (PEM) process
pim	Protocol Independent Multicast (PIM) process
ppaslog	Packet Processing ASIC (PPA) syslog process
ppp	Point-to-Point Protocol (PPP) process
pppoe	PPP over Ethernet (PPPoE) process
qos	quality of service (QoS) process
rcm	Router Configuration Manager (RCM) process

Keyword	Process
rib	Routing Information Base (RIB) process
rip	Routing Information Protocol (RIP) process
rpm	Routing Policy Manager (RPM) process
rsvp	Resource Reservation Protocol Traffic Engineering (RSVP-TE) process
sctp	Stream Control Transmission Protocol (SCTP) process
shm_ribd	Shared Memory RIB process
snmp	Simple Network Management Protocol (SNMP) process
static	static routing process
stats	statistics process
sysmon	system monitor process
tunnel	tunnel management process
vrrp	Virtual Router Redundancy Protocol (VRRP) process
xcd	cross-connect process daemon

(1) The SmartEdge 100 router does not support 802.1Q.
(2) Not all controller cards support flow.
(3) The SmartEdge 100 router does not support Frame Relay.

The heartbeat is a message that each process sends to the PM to identify itself as an active process. If the heartbeat ceases, the PM considers the process a candidate for automatic restart. It can be useful for debugging processes to turn the heartbeat off so that a hung process is not restarted automatically by the PM.

1.45.6 Examples

The following example sets process management parameters for the BGP process:

```
[local]Redback#process set bgp kill-time 100
[local]Redback#process set bgp max-crashes 3 within 43200
[local]Redback#process set bgp spawn-time 10
```

1.46 process start

process start *proc-name*

1.46.1 Purpose

Instructs the Process Manager (PM) to start the specified process.

1.46.2 Command Mode

- exec (10)

1.46.3 Syntax Description

proc-name	Process to be started. The value of the ***proc-name*** argument can be any one of the keywords listed in Table 6.

1.46.4 Default

None

1.46.5 Usage Guidelines

Use the **process start** command to instruct the PM to start the specified process.

Caution!

Risk of system crash. If more than one process has been stopped, you must restart each process individually, monitoring the SmartEdge router and waiting for it to stabilize before trying to restart the stopped process. Contact technical support before stopping and restarting multiple processes.

Table 6 lists the keywords for the processes supported by this command.

Table 6 Keywords for Processes

Keyword	Process
aaad	authentication, authorization, and accounting (AAA) process
arp	Address Resolution Protocol (ARP) process

Keyword	Process
atm	Asynchronous Transfer Mode (ATM) process
bgp	Border Gateway Protocol (BGP) process
bridge	bridge process
cfm	Ethernet 802.1pg-CFM process
clips	clientless IP service selection process
cls	Classifier Manager process
csm	Controller State Manager (CSM) process
cspf	Constrained Shortest Path First (CSPF) process
dhcp	Dynamic Host Configuration Protocol (DHCP) relay/proxy process
dhcpv6d	DHCPv6 process
dhelperd	DHCP helper daemon
dhelper6d	DHCPv6 helper daemon
dlm	Download Manager (DLM) process
dns	Domain Name System (DNS) process
dot1q	802.1Q encapsulation process(1)
flowd	flow process(2)
fr	Frame Relay process (3)
fsd	File server process
fssbcsim	FSSB client simulator
gsmp	General Switch Management Protocol (GSMP) process
hr	HTTP redirect process
igmp	Internet Group Management Protocol (IGMP) process
ipfix	IPFIX aggregation and protocol process
isis	Intermediate System-to-Intermediate System (IS-IS) process
ism	Interface and Circuit State Manager (ISM) process
l2tp	Layer 2 Tunneling Protocol (L2TP) process
l4l7	L4L7 process
ldp	Label Distribution Protocol (LDP) process
lg	link group (LG) process
lm	Label Manager (LM) process
metad	META process

Keyword	Process
mcastmgr	Multicast manager process.
mgd	Media Gateway process
mgmd	Media Gateway manager process
mip	Mobile IP process
mipsim	Mobile IP simulator process
mpls_static	Multiprotocol Label Switching (MPLS) static process
msdp	Multicast Source Discovery Protocol (MSDP) process
nat	IP Network Address Translation (NAT) process
nd	Neighbor Discovery (ND) process
netopd	NetOp process daemon
ntp	Network Time Protocol (NTP) process
odd	on-demand diagnostics (ODD) process
ospf	Open Shortest Path First (OSPF) protocol process
ospf3	OSPF Version 3 (OSPF3) protocol process
ped_parse	process execution descriptor (PED) parse process
pem	Port encapsulation module (PEM) process
pim	Protocol Independent Multicast (PIM) process
ppaslog	Packet Processing ASIC (PPA) syslog process
ppp	Point-to-Point Protocol (PPP) process
pppoe	PPP over Ethernet (PPPoE) process
qos	quality of service (QoS) process
rcm	Router Configuration Manager (RCM) process
rib	Routing Information Base (RIB) process
rip	Routing Information Protocol (RIP) process
rpm	Routing Policy Manager (RPM) process
rsvp	Resource Reservation Protocol Traffic Engineering (RSVP-TE) process
sctp	Stream Control Transmission Protocol (SCTP) process
snmp	Simple Network Management Protocol (SNMP) process
static	static routing process
stats	statistics process
sysmon	system monitor process

Keyword	Process
tunnel	tunnel management process
vrrp	Virtual Router Redundancy Protocol (VRRP) process
xcd	cross-connect process daemon

(1) The SmartEdge 100 router does not support 802.1Q.
(2) Not all controller cards support flow.
(3) The SmartEdge 100 router does not support Frame Relay.

1.46.6 Examples

The following example starts the BGP process:

```
[local]Redback#process start bgp
```

1.47 process stop

process stop ***proc-name***

1.47.1 Purpose

Stops the specified process.

1.47.2 Command Mode

exec (10)

1.47.3 Syntax Description

proc-name	Process to be stopped. The value of the ***proc-name*** argument can be any one of the keywords listed in Table 7.

1.47.4 Default

None

1.47.5 Usage Guidelines

Use the **process stop** command to the specified process.

Table 7 lists the keywords for the processes supported by this command.

Table 7 Keywords for Processes

Keyword	Process
aaad	authentication, authorization, and accounting (AAA) process
arp	Address Resolution Protocol (ARP) process
atm	Asynchronous Transfer Mode (ATM) process
bgp	Border Gateway Protocol (BGP) process
bridge	bridge process
cfm	Ethernet 802.1pg-CFM process
clips	clientless IP service selection process
cls	Classifier Manager process
csm	Controller State Manager (CSM) process
cspf	Constrained Shortest Path First (CSPF) process

Keyword	Process
dhcp	Dynamic Host Configuration Protocol (DHCP) relay/proxy process
dhcpv6d	DHCPv6 process
dhelperd	DHCP helper daemon
dhelper6d	DHCPv6 helper daemon
dlm	Download Manager (DLM) process
dns	Domain Name System (DNS) process
dot1q	802.1Q encapsulation process(1)
flowd	flow process(2)
fr	Frame Relay process (3)
fsd	File server process
fssbcsim	FSSB client simulator process
gsmp	General Switch Management Protocol (GSMP) process
hr	HTTP redirect process
igmp	Internet Group Management Protocol (IGMP) process
ipfix	IPFIX aggregation and protocol process
isis	Intermediate System-to-Intermediate System (IS-IS) process
ism	Interface and Circuit State Manager (ISM) process
l2tp	Layer 2 Tunneling Protocol (L2TP) process
l4l7	L4L7 process
ldp	Label Distribution Protocol (LDP) process
lg	link group (LG) process
lm	Label Manager (LM) process
metad	META process
mcastmgr	Multicast manager process.
mgd	Media Gateway daemon
mgmd	Media Gateway manager process
mip	Mobile IP process
mipsim	Mobile IP simulator process
mpls_static	Multiprotocol Label Switching (MPLS) static process
msdp	Multicast Source Discovery Protocol (MSDP) process
nat	IP Network Address Translation (NAT) process

Keyword	Process
nd	Neighbor Discovery (ND) process
netopd	NetOp process daemon
ntp	Network Time Protocol (NTP) process
odd	on-demand diagnostics (ODD) process
ospf	Open Shortest Path First (OSPF) protocol process
ospf3	OSPF Version 3 (OSPF3) protocol process
ped_parse	process execution descriptor (PED) parse process
pem	Port encapsulation module (PEM) process
pim	Protocol Independent Multicast (PIM) process
ppaslog	Packet Processing ASIC (PPA) syslog process
ppp	Point-to-Point Protocol (PPP) process
pppoe	PPP over Ethernet (PPPoE) process
qos	quality of service (QoS) process
rcm	Router Configuration Manager (RCM) process
rib	Routing Information Base (RIB) process
rip	Routing Information Protocol (RIP) process
rpm	Routing Policy Manager (RPM) process
rsvp	Resource Reservation Protocol Traffic Engineering (RSVP-TE) process
sctp	Stream Control Transmission Protocol (SCTP) process
shm_ribd	Shared Memory RIB process
snmp	Simple Network Management Protocol (SNMP) process
static	static routing process
stats	statistics process
sysmon	system monitor process
tunnel	tunnel management process
vrrp	Virtual Router Redundancy Protocol (VRRP) process
xcd	cross-connect process daemon

(1) The SmartEdge 100 router does not support 802.1Q.
(2) Not all controller cards support flow.
(3) The SmartEdge 100 router does not support Frame Relay.

Caution!

Risk of system crash. If more than one process has been stopped, you must restart each process individually, monitoring the SmartEdge router and waiting for it to stabilize before trying to restart the stopped process. Contact technical support before stopping and restarting multiple processes.

Caution!

Risk of data loss. The **process stop** command causes the specified process to terminate and the services provided by the process to become unavailable until the process is restarted using the **process start** command. To reduce the risk, do not stop a process unless you intend to restart the process immediately.

1.47.6 Examples

The following example stops the BGP process:

```
[local]Redback#process stop bgp
```

1.48 profile

profile *prof-name*

no profile

1.48.1 Purpose

Assigns an existing named profile to the subscriber.

1.48.2 Command Mode

subscriber configuration

1.48.3 Syntax Description

prof-name	Existing profile.

1.48.4 Default

The default profile is assigned to the subscriber.

1.48.5 Usage Guidelines

Use the **profile** command to assign an existing named profile to the subscriber.

If this subscriber will be a user of clientless IP service selection (CLIPS), adhere to the following guidelines:

- For static CLIPS circuits, the profile that you assign must have one and only one IP address; to assign an IP address to a subscriber profile, use the **ip address** command (in subscriber configuration mode).
- For dynamic CLIPS circuits, the profile that you assign must not include an IP address; instead, set the maximum number of IP addresses to **1**, using the **dhcp max-addrs** command (in subscriber configuration mode). For more information about the **dhcp max-addr** command, see the *Command List*.

Use the **no** form of this command to assign the default profile to the subscriber.

1.48.6 Examples

The following example assigns the existing profile, **hi-perf**, to subscriber **joe** in the **isp1** context:

```
[local]Redback(config)#context ips1
[isp1]Redback(config-ctx)#subscriber name joe
[isp1]Redback(config-sub)#profile hi-perf
```

1.49 profile (VPLS)

profile ***prof-name*** [**pw-id** ***pw-num***]

no profile ***prof-name***

1.49.1 Purpose

In VPLS configuration mode, applies an existing Virtual Private LAN Services (VPLS) profile to a VPLS instance.

1.49.2 Command Mode

VPLS configuration

1.49.3 Syntax Description

prof-name	Name of the VPLS profile that contains the neighbor attributes for establishing the pseudowires (maximum 40 characters).
pw-id ***pw-num***	Optional. Pseudowire number. The value of the ***pw-num*** argument is a 4-byte number. The remote provider edge (PE) device uses the pseudowire number and the local IP address to identify the pseudowire and the associated VPLS instance.

1.49.4 Default

None

1.49.5 Usage Guidelines

Use the **profile** command to apply an existing VPLS profile to a VPLS instance. When a VPLS profile is applied, a VPLS peer instance is created for each neighbor defined in the profile, and a pseudowire connection is established using the attributes defined for the neighbor.

A VPLS profile must be configured using the **vpls profile** command (in global configuration mode) before it can be applied.

Use the **pw-id** ***pw-num*** construct to optionally specify a pseudowire ID (number or name) to signal the ID for pseudowires to the neighbor defined in the profile. If a pseudowire ID is not configured for a VPLS profile, then the VPLS instance-level default pseudowire ID is used.

Multiple VPLS profiles can be applied to the same VPLS instance. If two or more profiles reference the same PE (same IP address), then the neighbor from the first profile is used. The same profile cannot be applied multiple times, even if the pseudowire IDs are different.

Use the **no** form of this command to delete a VPLS profile.

1.49.6 Examples

The following example applies the **foo** VPLS profile to the VPLS instance on the **to-pe4** bridge:

```
[local]Redback#config
[local]Redback(config)#context local
[local]Redback(config-ctx)#bridge to-pe4
[local]Redback(config-bridge)#vpls
[local]Redback(config-vpls)#profile foo pw-id 20
[local]Redback(config-vpls)#
```

1.50 propagate qos from ethernet

propagate qos from ethernet [**class-map** ***map-name***]

no propagate qos from ethernet

1.50.1 Purpose

For incoming packets, translates Ethernet 802.1p user priority marking to internal packet descriptor (PD) quality of service (QoS) priority marking.

1.50.2 Command Mode

dot1q profile configuration

1.50.3 Syntax Description

class-map ***map-name***	Optional. Name of an ingress Ethernet classification map for mapping Ethernet 802.1p user priority bits to PD QoS priority.

1.50.4 Default

Ethernet 802.1p user priority bits are not propagated to DSCP bits.

1.50.5 Usage Guidelines

Use the **propagate qos from ethernet** command to translate Ethernet 802.1p user priority bits to PD QoS priority bits.

Note: This command applies to incoming packets transmitted over 802.1Q permanent virtual circuits (PVCs) that reference the dot1q profile.

You can use the **qos class-map** command to define an optional mapping schema. If you specify the **class-map** ***map-name*** construct for the **propagate qos from ethernet** command, only the PD QoS values are affected. If you do not specify the **class-map** ***map-name*** construct, the Ethernet 802.1p bits are also copied to the priority bits of the DSCP field in the IP header.

PD QoS bits applied to packets carried by a VLAN are also inherited and applied to children (PPPoE and CLIPS subscriber sessions) of the VLAN.

If they are applied to an outer VLAN, by default they are inherited by an inner (q-in-q) VLAN unless it has its own specific PD QoS priority settings. The inner VLAN's priority setting, direct or inherited, is in turn inherited by its children (PPPoE and CLIPs subscriber sessions).

The 802.1p field to be referenced or modified in each case is determined by where the dot1q profile with the relevant **propagate qos to ethernet** or **propagate qos from ethernet** command was applied or configured, as follows:

- If it was configured on an outer VLAN, the 802.1p value from the outer 802.1q header is used when setting the PD QoS priority bits for the VLAN and the children and grand-children that inherit the settings.
- If it was configured on an inner VLAN, the 802.1p value from the inner 802.1q header is used when setting the PD QoS priority value for the inner VLAN and it's children.

Use the **no** form of this command to disable the propagation of Ethernet 802.1p bits to PD QoS bits.

1.50.6 Examples

The following example propagates Ethernet 802.1p user priority bits to DSCP bits for incoming packets for all 802.1Q PVCs that reference the 802.1Q profile, **8021p-on**:

```
[local]Redback(config)#dot1q profile 8021p-on
[local]Redback(config-dot1q-profile)#propagate qos from ethernet
```

1.51 propagate qos from ip

propagate qos from ip class-map ***map-name***

{**no** | **default**} **propagate qos from ip**

1.51.1 Purpose

For incoming packets, enables the propagation of Differentiated Services Code Point (DSCP) marking in the IP packet header to internal packet descriptor (PD) quality of service (QoS) marking in the packet that transits the system.

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

1.51.2 Command Mode

- subscriber configuration
- interface configuration

1.51.3 Syntax Description

class-map ***map-name***	Name of the schema for mapping DSCP bits to PD priority bits.

1.51.4 Default

DSCP values are copied to the PD QoS priority values using a default mapping.

1.51.5 Usage Guidelines

Use the **propagate qos from ip** command to enable the translation of the DSCP bits in the IP packet header to the PD QoS priority bits for incoming IP packets. The DSCP bits are translated from the received IP packet according to the specified classification map. In subscriber configuration mode, this command allows you to customize the mapping for traffic received on a specific subscriber session. In interface configuration mode, this command allows you to customize the mapping for all IP traffic received through the interface. The SmartEdge router propagates classification values and marks packets before it applies any metering policy.

Note: This command enables translating the IPv4 ToS field or the IPv6 Traffic Class field, depending on the IP version.

Custom classification mappings configured for either a subscriber or an interface affect Layer 3 (IP-routed) circuits only.

Use the **qos class-map** command with the **ip in** keywords (in global configuration mode) to define a mapping schema to be referenced by the **propagate qos from ip** command.

You can use the **propagate qos from subscriber** command (in L2TP peer configuration mode) to copy DSCP bits to PD QoS values for Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) sessions, and then use the **propagate qos from ip** command to specify a custom value mapping.

Use the **no** or **default** form of this command to remove a customized DSCP-to-PD QoS priority mapping.

1.51.6 Examples

The following example customizes the propagation of IP header DSCP values to PD QoS priority values for incoming packets of all subscriber sessions in the local context:

```
[local]Redback(config-sub)#qos class-map ip-to-pd ip in
[local]Redback(config-class-map)#ip df to qos af43
[local]Redback(config-class-map)#exit
[local]Redback(config)#context local
[local]Redback(config-ctx)#subscriber default
[local]Redback(config-sub)#propagate qos from ip class-map ip-to-pd
```

1.52 propagate qos from l2tp

propagate qos from l2tp [**class-map** *map-name*]

{**no** | **default**} **propagate qos from l2tp**

1.52.1 Purpose

When the SmartEdge router is configured as an LNS, for incoming packets, enables the translation of Differentiated Services Code Point (DSCP) bits to the internal PD QoS priority bits or to the DSCP bits of the inner (subscriber) IP header.

1.52.2 Command Mode

L2TP peer configuration (default peer only)

1.52.3 Syntax Description

class-map *map-name*	Optional. Name of an ingress IP classification map for mapping DSCP values in the IP packet header to PD QoS priority values.

1.52.4 Default

The DSCP bits in the incoming L2TP IP packet headers are not propagated to the DSCP bits in subscriber IP packet headers.

1.52.5 Usage Guidelines

Use the **propagate qos from l2tp** command to propagate the PD QoS priority bits to the DSCP bits of the inner (subscriber) IP header if no classification map is specified for incoming L2TP packets. Propagation occurs after the outer IP DSCP bits have been propagated to the PD QoS priority bits as part of IP forwarding. If you specify a classification map, this command customizes the default mapping from the outer IP header DSCP value to the PD QoS value and leaves the inner IP header DSCP value unmodified.

Note: This propagation occurs only in the upstream direction; this command applies only to a SmartEdge router that is configured as an LNS to receive packets from an L2TP access concentrator (LAC).

You can use the **qos class-map** command to define an optional mapping schema. If you do not specify the **class-map** *map-name* construct with the **propagate qos from l2tp** command, the SmartEdge router overwrites the value in the inner IP header with the DSCP value from the received outer IP header. If you specify the **class-map** *map-name* construct, the SmartEdge

router customizes the default mapping from the outer IP header DSCP value to the PD QoS value and leaves the inner IP header DSCP value unmodified.

L2TP tunnels are User Datagram Protocol (UDP)/IP-encapsulated circuits that carry subscriber-based IP traffic encapsulated in Point-to-Point (PPP) sessions between routers. The LNS is the IP termination point for subscriber traffic. DSCP bits from the L2TP IP packet header can be propagated into subscriber traffic.

Use the **no** or **default** form of this command to disable the propagation of DSCP bits to the inner (subscriber) IP header or to remove the customized propagation to the QoS PD value.

1.52.6 Examples

The following example propagates DSCP bits from outer L2TP IP packet headers to DSCP bits in inner IP packet headers:

```
[local]Redback(config-ctx)#l2tp-peer default
[local]Redback(config-l2tp)#propagate qos from l2tp
```

1.53 propagate qos from mpls

propagate qos from mpls [**class-map** *map-name*] [**l2vpn class-map** *map-name*]

no propagate qos from mpls

1.53.1 Purpose

When the SmartEdge router is configured as a MPLS egress router, for incoming packets, this enables translating Multiprotocol Label Switching (MPLS) experimental (EXP) bits to Differentiated Services Code Point (DSCP) bits in the IP header or enables customized mapping of EXP to packet descriptor (PD) quality of service (QoS) values for incoming packets.

1.53.2 Command Mode

- MPLS router configuration
- L2VPN peer profile configuration

1.53.3 Syntax Description

class-map *map-name*	Optional. Name of the ingress MPLS classification map for mapping MPLS EXP values to PD QoS priority values.
l2vpn class-map *map-name*	Optional. Name of the ingress MPLS classification map for mapping packets received from Layer 2 MPLS VPNs. This argument is valid only in the MPLS router configuration mode.

1.53.4 Default

MPLS EXP bits are mapped to PD QoS priority bits.

1.53.5 Usage Guidelines

Use the **propagate qos from mpls** command to enable mapping MPLS EXP bits to DSCP bits in the IP header or enable customized mapping of EXP to PD QoS priority values for incoming packets when the SmartEdge router is configured as a MPLS egress router.

Incoming MPLS packets EXP values are propagated by default to PD QoS priority values, unless you configure this command or one of the following is true:

- There are no EXP bits in the MPLS packet header, because they were removed by PHP action before arrival. In this case, the IP header DSCP value is mapped to the PD QoS priority.

- The **egress prefer-dscp-qos** command is configured; in this case, the IP header DSCP value is also used.

To map the EXP bits to PD QoS priority bits and the upper three bits of the DSCP field in the IP header (and clear the lower three bits of the DSCP field), configure this command but do not include the optional **class-map** ***map-name*** construct

To map the EXP bits to PD QoS priority bits and not affect the DSCP bits, configure this command with the optional **class-map** ***map-name*** construct.

In this case, use the **qos class-map** command to define a mapping schema, then reference the schema using the **class-map** ***map-name*** construct.

For Layer 2 virtual private network (L2VPN) traffic, if you do not specify a classification map, the standard classification map applies to both Layer 2 and Layer 3 traffic. If you specify the optional **l2vpn class-map** ***map-name*** construct without the **class-map** ***map-name*** construct, the L2VPN classification map applies to Layer 2 traffic and Layer 3 traffic uses the default 8P0D mapping schema; for more information, see the **mapping schema** command description. If you specify both the **l2vpn class-map** ***map-name*** construct and the **class-map** ***map-name*** construct, Layer 2 traffic uses the L2VPN classification map and Layer 3 traffic uses the standard classification map.

If you use the **mpls use-ethernet** command to perform a secondary lookup and the encapsulated packet contains no virtual LAN (VLAN) header, the PD QoS priority value is determined by mapping the MPLS EXP value using the default 8P0D schema.

When issued from L2VPN peer profile configuration mode, a per-pseudowire (PW) class map is associated with a port PW using the L2VPN profile. All PWs that use the same L2VPN profile are associated with the same class map grid. The global L2VPN and per-PW class maps can coexist on the same system. When both are present, the per-PW class map takes precedence over the global class map in both the inbound and outbound directions.

Use the **no** form of this command to disable the mapping of PD QoS priority values from MPLS EXP bits.

Use **propagate qos from mpls** without any optional constructs to disable this command and return to the default settings where MPLS EXP bits are not mapped to DSCP bits.

1.53.6 Examples

The following example enables the mapping of MPLS EXP bits to DSCP bits for outgoing packets:

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

The following example specifies a customized mapping of MPLS EXP bits to PD QoS priority values by referencing the existing MPLS ingress classification map **exp-to-pd:**

```
[local]Redback(config-ctx)#router mpls
[local]Redback(config-mpls)#propagate qos from mpls class-map exp-to-pd
```

1.54 propagate qos from subscriber

propagate qos from subscriber [**upstream** | **downstream** | **both**]

{**no** | **default**} **propagate qos from subscriber**

1.54.1 Purpose

For incoming packets when the SmartEdge router is configured as a Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC), propagates the Differentiated Services Code Point (DSCP) bits in the subscriber's IP packet header to the packet descriptor (PD) QoS priority bits.

1.54.2 Command Mode

L2TP peer configuration (default peer only)

1.54.3 Syntax Description

upstream	Optional. Performs the propagation on inbound packets from the subscriber.
downstream	Optional. Performs the propagation on inbound packets from the L2TP network server (LNS).
both	Optional. Performs the propagation on inbound packets from the subscriber and inbound packets from the LNS.

1.54.4 Default

DSCP bits are not propagated from the incoming subscriber IP packet header to the PD QoS priority bits on the subscriber IP packet.

1.54.5 Usage Guidelines

For incoming packets when the SmartEdge router is configured as a LAC, use the **propagate qos from subscriber** command to propagate the DSCP bits in the subscriber's IP packet header to the PD QoS priority bits.

Use the **upstream** keyword to propagate from inbound packets from the subscriber. Use the **downstream** keyword to propagate from inbound packets from the network. Use the **both** keyword to propagate in both directions.

The SmartEdge router copies the DSCP bits in the IP header. L2TP tunnels are User Datagram Protocol (UDP)/IP-encapsulated circuits that carry subscriber-based Point-to-Point Protocol (PPP) sessions between routers. On L2TP tunnels, subscriber IP packets are encapsulated in PPP packets, which themselves are encapsulated in L2TP packets. DSCP bits can be propagated from inner IP packet headers to outer L2TP IP packet headers, and vice versa.

DSCP bits are propagated between layers of encapsulated packets so that any Layer 3 device located between an LNS and a LAC can recognize and apply DSCP priority settings.

Use the **no** or **default** form of this command to disable the propagation of DSCP bits in the specified direction or, if neither keyword is specified, in both directions.

1.54.6 Examples

The following example propagates the DSCP bits in a subscriber IP packet header to the PD QoS priority bit in the subscriber IP packet header in the upstream direction only:

```
[local]Redback(config-ctx)#l2tp-peer default
[local]Redback(config-l2tp)#propagate qos from subscriber upstream
```

The following example propagates the DSCP bits from subscriber IP packet headers to DSCP bits in L2TP IP packet headers in both directions:

```
[local]Redback(config-ctx)#l2tp-peer default
[local]Redback(config-l2tp)#propagate qos from subscriber
```

1.55 propagate qos to ethernet

propagate qos to ethernet [**class-map** *map-name*]

no propagate qos to ethernet

1.55.1 Purpose

Translates Differentiated Services Code Point (DSCP) priority values to Ethernet 802.1p user priority bits in outgoing packets.

1.55.2 Command Mode

dot1q profile configuration

1.55.3 Syntax Description

class-map *map-name*	Optional. Name of the egress Ethernet classification map for mapping quality of service (QoS) PD values to Ethernet 802.1p user priority bits.

1.55.4 Default

DSCP bits are not translated to Ethernet 802.1p user priority bits in outgoing packets.

1.55.5 Usage Guidelines

Use the **propagate qos to ethernet** command to propagate DSCP values on internal packets to Ethernet 802.1p user priority bits for outgoing packets.

Note: This command applies to outgoing packets transmitted over 802.1Q permanent virtual circuits (PVCs) that reference the dot1q profile.

You can use the **qos class-map** command to define an optional mapping schema. If you do not specify the **class-map** *map-name* construct for the **propagate qos to ethernet** command, the default 8P0D mapping is used. For more information about 8P0D mapping, see the **mapping schema** command usage guidelines.

By default, when the SmartEdge OS functions as an L2VPN egress provider edge (PE) node, 802.1p user priority bits on the outgoing 802.1q access circuit will remain as they were set in the VLAN tags that were received from the pseudowire (PW). If no 802.1q tags are present in the frames received on the PW, the outgoing 802.1p bits on the access circuit are set to zero. If the **propagate qos from ethernet** command is configured, the 802.1p user priority bits on the outgoing access circuit may be modified based on the

packet's PD QoS priority value and any classification map associated with the **propagate** command. The applicable 802.1q tag to be modified (inner or outer) is determined by the standard rules and behavior associated with the **propagate qos from ethernet** command.

Use the **no** form of this command to disable the propagation of DSCP bits.

1.55.6 Examples

The following example copies DSCP bits from IP packets to Ethernet 802.1p user priority bits for 802.1Q PVCs that reference the 802.1Q profile, **8021p-on**:

```
[local]Redback(config)#dot1q profile 8021p-on
[local]Redback(config-dot1q-profile)#propagate qos to ethernet
```

1.56 propagate qos to ip

propagate qos to ip [**class-map** *map-name*]

{**no** | **default**} **propagate qos to ip**

1.56.1 Purpose

For outgoing packets, enables the propagation of internal packet descriptor (PD) QoS priority values in subscriber IP packets to Differentiated Services Code Point (DSCP) bits in the IP packet header. For IPv4 packets, the DSCP marking is the upper six bits of the IPv4 header Type of Service (ToS) field. For IPv6 packets, the DSCP marking is the upper six bits of the IPv6 header Traffic Class field.

1.56.2 Command Mode

- interface configuration
- subscriber configuration

1.56.3 Syntax Description

class-map *map-name*	Optional. Name of the schema for mapping PD QoS priority bits to DSCP bits in the IP packet header.

1.56.4 Default

PD QoS values are not propagated to the DSCP bits in the IP packet header.

1.56.5 Usage Guidelines

Use the **propagate qos to ip** command to propagate PD QoS priority values in the subscriber IP packet to DSCP bits in the IP packet header for outgoing IP packets. In subscriber configuration mode, this command allows you to enable propagation or customize mapping for traffic sent on a specific subscriber session. In interface configuration mode, this command affects all IP traffic transmitted through the interface. The SmartEdge router propagates classification values and marks packets before it applies any metering policy.

Note: This command refers to the IPv4 Type of Service (TOS) field or the IPv6 Traffic Class field, depending on the IP version.

If you specify the optional **class-map** *map-name* construct, the **propagate qos to ip** command maps PD QoS priority values to DSCP bits in the IP packet header. In this case, use the **qos class-map** command (in global

configuration mode) to define a mapping schema, then reference the schema using the optional **class-map** ***map-name*** construct.

If you do not specify the **class-map** ***map-name*** construct, PD QoS values are copied directly to DSCP values.

Use the **no** or **default** form of this command to disable the propagation of PD QoS priority values to DSCP bits.

Custom classification mappings configured for either a subscriber or an interface affect Layer 3 (IP-routed) circuits only.

1.56.6 Examples

The following example enables propagation of PD QoS priority values in the subscriber IP packet to DSCP bits in the IP packet header for outgoing IP packets:

```
[local]Redback(config-ctx)#interface SJ_red
[local]Redback(config-if)#propagate qos to ip
```

1.57 propagate qos to l2tp

propagate qos to l2tp [**class-map** *map-name*]

{**no** | **default**} **propagate qos to l2tp**

1.57.1 Purpose

When the SmartEdge router functions as a Layer 2 Tunneling Protocol (L2TP) network server (LNS) or an L2TP access concentrator (LAC), for outgoing packets, translates the internal packet descriptor (PD) QoS priority bits to the Differentiated Services Code Point (DSCP) bits in the IP packet header.

1.57.2 Command Mode

L2TP peer configuration (default peer only)

1.57.3 Syntax Description

class-map *map-name*	Optional. Name of the egress IP classification map for mapping PD QoS priority values to DSCP values in the IP packet header.

1.57.4 Default

DSCP bits are not propagated from the PD QoS priority bits to the L2TP IP packet header.

1.57.5 Usage Guidelines

For a SmartEdge router configured as an L2TP LNS or an LAC, for outgoing packets, use the **propagate qos to l2tp** command to propagate the internal PD QoS priority bits to the DSCP bits. For the LNS configuration, the DSCP bits are propagated from the incoming network packet headers, and for the LAC configuration, the DSCP bits are propagated from the incoming subscriber packet headers.

As an LNS, the PD QoS priority value is derived from the subscriber's inner DSCP value as part of IP forwarding. As a LAC, the PD QoS priority defaults to a low priority. If you configure the **propagate qos from subscriber** command (in L2TP peer configuration mode) with the **upstream** keyword, the PD QoS priority is derived from subscriber's inner DSCP value.

L2TP tunnels are User Datagram Protocol (UDP)/IP-encapsulated circuits that carry subscriber-based Point-to-Point (PPP) sessions between routers. On L2TP tunnels, subscriber IP packets are encapsulated in PPP packets, which themselves are encapsulated in L2TP packets. DSCP bits are propagated

between layers of encapsulated packets so that any Layer 3 device located between an LNS and a LAC can recognize and apply DSCP settings.

You can use the **qos class-map** command (in global configuration mode) to define an optional mapping schema. If you do not specify the **class-map** ***map-name*** construct for the **propagate qos to l2tp** command, the unmodified PD QoS value is copied to the outer DSCP field in the IP header.

Use the **no** or **default** form of this command to disable the propagation of DSCP bits.

1.57.6 Examples

The following example propagates DSCP bits from incoming network or subscriber IP packet headers to L2TP IP packet headers:

```
[local]Redback(config-ctx)#l2tp-peer default
[local]Redback(config-l2tp)#propagate qos to l2tp
```

1.58 propagate qos to mpls

propagate qos to mpls [**class-map** *map-name*] [**l2vpn class-map** *map-name*]

no propagate qos to mpls

1.58.1 Purpose

When the SmartEdge router is configured as a Multiprotocol Label Switching (MPLS) ingress router, for outgoing packets, enables the mapping of packet descriptor (PD) quality of service (QoS) priority values to the MPLS experimental (MPLS EXP) bits.

1.58.2 Command Mode

- MPLS router configuration
- L2VPN peer profile configuration

1.58.3 Syntax Description

class-map *map-name*	Optional. Name of the egress MPLS classification map for mapping QoS PD QoS priority values to MPLS EXP bits.
l2vpn class-map *map-name*	Optional. Name of the egress MPLS classification map for mapping packets received from Layer 2 Virtual Private Networks (L2VPNs). This argument is valid only in the MPLS router configuration mode.

1.58.4 Default

PD QoS priority values are mapped to the MPLS EXP bits.

1.58.5 Usage Guidelines

When the SmartEdge router is configured as an MPLS ingress router, use the **propagate qos to mpls** command to enable the mapping of PD QoS priority values to the MPLS EXP bits for outgoing packets. If you do not specify the optional **class-map** *map-name* construct, the default mapping is used.

If you specify the optional **class-map** *map-name* construct, the **propagate qos to mpls** command specifies a custom value mapping for PD QoS values to MPLS EXP bits. The Differentiated Services Code Point (DSCP) values are unaffected. In this case, use the **qos class-map** command to define a mapping schema, then reference the schema using the **class-map** *map-name* construct. If you do not specify an L2VPN classification map, the standard classification map applies to both Layer 2 and Layer 3 traffic.

If you specify the optional **l2vpn class-map** ***map-name*** construct without the **class-map** ***map-name*** construct, the L2VPN classification map applies to Layer 2 traffic. Layer 3 traffic uses the default 8P0D mapping schema. If you specify both the **l2vpn class-map** ***map-name*** construct and the **class-map** ***map-name*** construct, Layer 2 traffic uses the L2VPN classification map and Layer 3 traffic uses the standard classification map.

When issued from L2VPN peer profile configuration mode, a per-PW class map is associated with a port PW using the L2VPN profile. All PWs that use the same L2VPN profile are associated with the same class map grid. The global L2VPN and per-PW class maps can coexist on the same system. When both are present, the per-PW class map takes precedence over the global class map in both the inbound and outbound directions.

Use the **no** form of this command to disable the mapping of PD QoS priority values to MPLS EXP bits. Use **propagate qos to mpls** without any optional constructs to disable this command and return to the default settings.

1.58.6 Examples

The following example enables the mapping of the PD values to the MPLS EXP bits at the ingress router:

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

1.59 propagate qos transport use-vlan-header

propagate qos transport {**in** | **out** | **both**} **use-vlan-header** {**inner** | **outer** | **both**}

no propagate qos transport

1.59.1 Purpose

Specifies whether propagation between packet descriptor (PD) QoS priority values and Ethernet uses the 802.1p value from the outer permanent virtual circuit (PVC) header or the inner PVC header, when both are present.

1.59.2 Command Mode

dot1q profile configuration

1.59.3 Syntax Description

in	Uses the specified VLAN header 802.1p value when propagating 802.1p to PD QoS priority for incoming packets.
out	Uses the specified VLAN header 802.1p value when propagating PD QoS priority to 802.1p to outgoing packets.
both	Uses the specified VLAN header 802.1p value for both incoming and outgoing packets.
inner	Uses the 802.1p value from the inner PVC header. This is the default value.
outer	Uses the 802.1p value from the outer PVC header.
both	Modifies both the inner PVC 802.1p field and the outer PVC 802.1p field with the same value, if both fields are present. Valid only when the **out** keyword is specified (egress propagation only).

1.59.4 Default

The 802.1p value from the inner PVC header is used.

1.59.5 Usage Guidelines

Use the **propagate qos transport use-vlan-header** command to specify whether propagation between PD QoS priority values and Ethernet uses the 802.1p value from the outer PVC header or the inner PVC header, when both are present. This command applies only to transport ranges defined for 802.1Q PVCs.

Use the **no** form of this command to revert values.

1.59.6 Examples

The following example shows how to configure the `propagate qos transport use-vlan-header` option in a dot1q profile. In this example, circuits that have the `vlan_in_1` profile attached use the 802.1p value from the inner PVC header when propagating between PD QoS priority values and Ethernet for incoming packets:

```
[local]Redback(config)#dot1q profile vlan_in_1
[local]Redback(config-dot1q-profile)#propagate qos transport in use-v
```

1.60 propagate qos use-vlan-ethertype

propagate qos use-vlan-ethertype ***tunl-type***

no propagate qos use-vlan-ethertype

1.60.1 Purpose

Specifies the virtual LAN (VLAN) Ethernet type field that determines whether the packet is examined for an enclosed IP header and Differentiated Services Code Point (DSCP) value or for an inner VLAN header and 802.1p value for incoming Multiprotocol Label Switching (MPLS) packets that encapsulate 802.1q Ethernet frames.

1.60.2 Command Mode

MPLS router configuration

1.60.3 Syntax Description

tunl-type	Type of incoming 802.1Q traffic according to one of the following argument or keywords (in hexadecimal format): • ***user***—Custom traffic type; the range of values is 0x0 to 0xffff. • **8100**—Specifies the 8100 packet type; this is the default packet type. • **88a8**—Specifies the 88a8 packet type. • **9100**—Specifies the 9100 packet type. • **9200**—Specifies the 9200 packet type.

1.60.4 Default

The 8100 packet type is used.

1.60.5 Usage Guidelines

Use the **propagate qos use-vlan-ethertype** command to specify the VLAN Ethernet type field that determines whether the packet is examined for an enclosed IP header and DSCP value or for an inner VLAN header and 802.1p value for incoming MPLS packets that encapsulate 802.1q Ethernet frames. In addition to packets with the specified VLAN Ethernet type field, packets with Ethernet type of 0x8100 are also examined for enclosed header values. The SmartEdge router either maps packets with other outer PVC Ethernet types based on the outer PVC 802.1p value (for the **mpls use-ethernet** command in class map configuration mode) or uses the default 8P0D mapping based on the MPLS EXP value (for the **mpls use-ip** command in class map configuration mode).

Use the **mpls use-ethernet** or **mpls use-ip** command to enable propagation.

Use the **no** form of this command to disable the use of VLAN header values to identify incoming packets for propagation.

1.60.6 Examples

The following example shows how to specify incoming 88a8 traffic for the VLAN Ethernet type field:

```
[local]Redback(config-ctx)#router mpls 234
[local]Redback(config-mpls)#propagate qos use-vlan-ethertype 88a8
```

1.61 propagate qos use-vlan-header

propagate qos use-vlan-header {**inner** | **outer**}

no propagate qos use-vlan-header

1.61.1 Purpose

Specifies whether 802.1p-to-packet descriptor (PD) propagation uses the 802.1p value from the outer permanent virtual circuit (PVC) header or the inner PVC header, when both values are present, for incoming Multiprotocol Label Switching (MPLS) packets that encapsulate 802.1q Ethernet frames.

1.61.2 Command Mode

MPLS router configuration

1.61.3 Syntax Description

inner	Uses the 802.1p value from the inner PVC header.
outer	Uses the 802.1p value from the outer PVC header.

1.61.4 Default

The 802.1p value from the inner PVC header is used.

1.61.5 Usage Guidelines

Use the **propagate qos use-vlan-header** command to specify whether 802.1p-to-PD propagation uses the 802.1p value from the outer PVC header or the inner PVC header, when both values are present, for incoming MPLS packets that encapsulate 802.1q Ethernet frames.

Use the **mpls use-ethernet** command (in class map configuration mode) to enable propagation.

Use the **no** form of this command to revert to the default setting, which uses the inner PVC 802.1p value.

1.61.6 Examples

The following example shows how to specify whether 802.1p-to-PD propagation uses the 802.1p value from the inner PVC header for incoming MPLS packets that encapsulate 802.1q Ethernet frames:

```
[local]Redback(config-ctx)#router mpls 234
[local]Redback(config-mpls)#propagate qos use-vlan-header inner
```

1.62 propagate ttl ip-to-mpls

propagate ttl ip-to-mpls

no propagate ttl ip-to-mpls

1.62.1 Purpose

Enables the propagation of the IP time-to-live (TTL) to the Multiprotocol Label Switching (MPLS) tunnel label TTL at the ingress router.

1.62.2 Command Mode

MPLS router configuration

1.62.3 Syntax Description

This command has no keywords or arguments.

1.62.4 Default

The IP TTL is propagated to the MPLS tunnel label TTL at the ingress router.

1.62.5 Usage Guidelines

Use the **propagate ttl ip-to-mpls** command to enable the propagation of the IP TTL to the MPLS tunnel label TTL at the ingress router.

Use the **no** form of this command to disable the propagation of the IP TTL to the MPLS tunnel label TTL at the ingress router.

Note: The default behavior of the SmartEdge router is to propagate the IP TTL to the MPLS tunnel label TTL at the ingress router; therefore, the **propagate ttl ip-to-mpls** command is only used to return the router to its default behavior after it has been changed using the **no** form of this command.

1.62.6 Examples

The following example enables the propagation of the IP TTL to the MPLS tunnel label TTL:

```
[local]Redback(config-ctx)#router mpls 234
[local]Redback(config-mpls)#propagate ttl ip-to-mpls
[local]Redback(config-mpls)#
```

1.63 propagate ttl mpls-to-ip

propagate ttl mpls-to-ip

no propagate ttl mpls-to-ip

1.63.1 Purpose

Enables the propagation of the Multiprotocol Label Switching (MPLS) tunnel label time-to-live (TTL) to the IP TTL at the egress router.

1.63.2 Command Mode

MPLS router configuration

1.63.3 Syntax Description

This command has no keywords or arguments.

1.63.4 Default

The MPLS TTL tunnel label is propagated to the IP TTL at the egress router.

1.63.5 Usage Guidelines

Use the **propagate ttl mpls-to-ip** command to enable the propagation of the MPLS tunnel label TTL to the IP TTL at the egress router.

Use the **no** form of this command to disable the propagation of the MPLS tunnel label TTL to the IP TTL at the egress router.

Note: The default behavior of the SmartEdge router is to propagate of the MPLS tunnel label TTL to the IP TTL at the egress router, so the **propagate ttl mpls-to-ip** command is only used to return the router to its default behavior after it has been changed using the **no** form of this command.

1.63.6 Examples

The following example enables the propagation of the MPLS tunnel label TTL to the IP TTL at the egress router:

```
[local]Redback(config-ctx)#router mpls 234
[local]Redback(config-mpls)#propagate ttl mpls-to-ip
[local]Redback(config-mpls)#
```

1.64 protect-group

protect-group {round-robin | incoming-port}

{no | default} protect-group

1.64.1 Purpose

Specifies the selection algorithm by which a port in the access link group is chosen for outgoing subscriber traffic.

1.64.2 Command Mode

link group configuration

1.64.3 Syntax Description

round-robin	Uses the ports in the link group in round-robin order; this is the default.
incoming-port	Uses the first port on which the control protocol packets were received.

1.64.4 Default

The round-robin algorithm is used to select the port for outgoing subscriber traffic.

1.64.5 Usage Guidelines

Use the **protect-group** command to specify the selection algorithm by which a port in the access link group is chosen for outgoing subscriber traffic. The selection algorithm determines how the SmartEdge OS load balances outgoing traffic.

Note: This command is available for access link groups only.

1.64.6 Examples

The following example shows how to specify the incoming port as the selection algorithm for the link group **foo**:

```
[local]Redback(config)#link-group foo access
[local]Redback(config-link-group)#protect-group incoming-port
```

1.65 protocol

protocol {*protocol-name* | *protocol-number*} **port** *start-port-number* [*end-port-number*]]

no protocol {*protocol-name* | *protocol-number*}

1.65.1 Purpose

Specifies the protocol and, optionally, port numbers for the application under which this command is entered.

1.65.2 Command Mode

flow IP application configuration

1.65.3 Syntax Description

protocol-name	Identifies a protocol. Use one of the following keywords to specify the desired protocol: • **ahp**—Specifies the Authentication Header Protocol (AHP). • **esp**—Specifies Encapsulation Security Payload (ESP). • **gre**—Specifies Generic Routing Encapsulation (GRE). • **icmp**—Specifies the Internet Control Message Protocol (ICMP) • **igmp**—Specifies the Internet Group Management Protocol (IGMP). • **ipinip**—Specifies the IP in IP tunneling. • **ospf**—Specifies Open Shortest Path First (OSPF). • **pcp**— Specifies the Payload Compression Protocol (PCP). • **pim**— Specifies Protocol Independent Multicast (PIM). • **tcp**—Specifies the Transmission Control Protocol (TCP). • **udp**—Specifies the User Datagram Protocol (UDP).
protocol-number	Number that identifies a particular protocol.
port *start-port-number*	(Optional) Individual port or the starting port in a range of ports within the specified IP protocol. If you specify ports, protocol statistics are collected for the specified ports only. Range is 1 through 65535.
end-port-number	(Optional) Ending port in a range of ports. Range is 1 through 65535.

1.65.4 Default

Statistics are collected for all ports that support the specified protocol.

1.65.5 Usage Guidelines

Use the **protocol** command to specify the protocol and, optionally, port numbers for the application under which this command is entered.

Note: You cannot configure the same protocol and port number within two separate applications. Such conflicting configurations fail. For example, if protocol 6 is configured under an application called **app-tcp**, you cannot add protocol 6 to the application called **app-udp**, as shown in the following example configuration:

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

[local]Redback(config-flow-ip-app)#protocol 6 port
5200 5400

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

[local]Redback(config-flow-ip-app)#protocol 6 port
5225
```

1.65.6 Examples

The following example shows how to use the **protocol** command to add port number **25** in the **tcp** protocol:

```
[local]Redback# configure
[local]Redback(config)# flow ip application-list app-list1
[local]Redback(config-flow-ip-app-list)# application app1
[local]Redback(config-flow-ip-app)# protocol tcp port 25
```

1.66 protocol maintenance isis

protocol maintenance isis [***downtime***]

1.66.1 Purpose

Stops the Intermediate System-to-Intermediate System (IS-IS) process for a brief period without affecting IP forwarding in the network, enabling the system to prepare information about IS-IS operations up to that point.

1.66.2 Command Mode

exec (10)

1.66.3 Syntax Description

downtime	Optional. Number of seconds of down time. The range of values is 30 to 900 seconds; the default value is 600.

1.66.4 Default

The command is disabled.

1.66.5 Usage Guidelines

Use the **protocol maintenance isis** command to stop the IS-IS process for a brief period without affecting IP forwarding in the network, enabling the system to prepare information about IS-IS operations up to that point.

1.66.6 Examples

The following examples stops the IS-IS process for a period of two minutes (or **120** seconds):

```
[local]Redback#protocol maintenance isis 120
```

1.67 protocol trigger isis csnp

protocol trigger isis [*instance-name*] **csnp** [**level-1** | **level-2**] [**interface** *if-name*] [**re-start**]

1.67.1 Purpose

Forces Intermediate System-to-Intermediate System (IS-IS) complete sequence number protocol data units (CSNPs) to be sent out through all interfaces or through a particular interface.

1.67.2 Command Mode

exec (10)

1.67.3 Syntax Description

instance-name	Optional. IS-IS instance name. Forces CSNPs to be sent for only the specified instance.
level-1	Optional. Forces CSNPs to be sent for IS-IS level 1 only.
level-2	Optional. Forces CSNPs to be sent for IS-IS level 2 only.
interface *if-name*	Optional. Interface name. Forces CSNPs to be sent for only the specified interface.
re-start	Optional. Forces the triggered Hello packets to be sent out with Restart Request bit set inside the restart type-length-value (TLV).

1.67.4 Default

None

1.67.5 Usage Guidelines

Use the **protocol trigger isis csnp** command to force CSNPs to be sent out through all interfaces or through a particular interface. This command is useful for lab testing, network troubleshooting, or to manually synchronize the IS-IS database across point-to-point links.

Use the **re-start** keyword to trigger the neighbors to consider this router as restarted. It may receive the CSNPs and link-state protocol data units (LSPs) from the neighbors.

1.67.6 Examples

The following example triggers an IS-IS **level-2** CSNP packet to be sent out through all interfaces:

```
[local]Redback#protocol trigger isis csnp level-2
```

1.68 protocol trigger isis hello

protocol trigger isis [*instance-name*] **hello** [**level-1** | **level-2**] [**interface** *if-name*] [**padding**] [**re-start**]

1.68.1 Purpose

Forces an Intermediate System-to-Intermediate System (IS-IS) Hello packet to be sent out through a particular interface or out through all interfaces.

1.68.2 Command Mode

exec (10)

1.68.3 Syntax Description

instance-name	Optional. IS-IS instance name. Forces a Hello packet to sent for only the specified instance.
level-1	Optional. Forces a Hello packet to be sent for IS-IS level 1 only.
level-2	Optional. Forces a Hello packet to be sent for IS-IS level 2 only.
interface *if-name*	Optional. Interface name. Forces a Hello packet to be sent for only the specified interface.
padding	Optional. Enables Hello packet padding. Forced Hello packets are padded to the maximum transmission unit (MTU) of the interface over which the packets are sent. By default, triggered Hello packets are not padded.
re-start	Optional. Forces the triggered Hello packets to be sent out with Restart Request bit set inside the restart type-length-value (TLV).

1.68.4 Default

Forced Hello packets are not padded.

1.68.5 Usage Guidelines

Use the **protocol trigger isis hello** command to force an IS-IS Hello packet to be sent out through a particular interface or out through all interfaces. This command is useful for lab testing, network troubleshooting, or to manually synchronize the IS-IS database across point-to-point links.

Use the **re-start** keyword to trigger the neighbors to consider this router is restarted. It may receive the complete sequence number protocol data unit (CSNP) and link-state protocol data units (LSPs) from the neighbors.

1.68.6 Examples

The following example forces an IS-IS **level-2** Hello packet to be sent out the **pos 3/2** interface:

```
[local]Redback#protocol isis hello level-2 interface pos 3/2
```

1.69 protocol trigger isis lsp

protocol trigger isis [*instance-name*] **lsp** [**level-1** | **level-2**] [**interface** *if-name*] [**all** | **local** | **lsp-id** *lsp-id*] [**update**] [**re-start**]

1.69.1 Purpose

Forces an Intermediate System-to-Intermediate System (IS-IS) link-state protocol data unit (LSP) to be sent out a particular interface or out all interfaces.

1.69.2 Command Mode

exec (10)

1.69.3 Syntax Description

instance-name	Optional. IS-IS instance name. Triggers an event for only the specified instance.
level-1	Optional. Triggers an LSP event for IS-IS level 1 only.
level-2	Optional. Triggers an LSP event for IS-IS level 2 only.
interface *if-name*	Optional. Interface name. Triggers an event for only the specified interface.
all	Optional. Sends all LSPs in the database.
local	Optional. Sends only locally generated LSPs. This is the default setting.
lsp-id *lsp-id*	Optional. LSP ID. Sends only the specified LSP. The ID is in ***xxxx.xxxx.xxxx*** format or it can be the hostname.
update	Optional. Updates all local LSPs and sends them out.
re-start	Optional. Forces the triggered Hello packets to be sent out with Restart Request bit set inside the restart type-length-value (TLV).

1.69.4 Default

If this command is enabled without using any options, only locally generated LSPs are sent out.

1.69.5 Usage Guidelines

Use the **protocol trigger isis lsp** command to force an IS-IS LSP to be sent out a particular interface or out all interfaces. This command is useful for lab testing, network troubleshooting, or to manually synchronize the IS-IS database across point-to-point links.

Use the **re-start** keyword to trigger the neighbors to consider this router is restarted. It may receive the complete sequence number protocol data unit (CSNP) and LSPs from the neighbors.

1.69.6 Examples

The following example triggers an IS-IS **level-1** LSP to be refreshed and sent out on all interfaces:

```
[local]Redback#protocol trigger isis lsp level-1 update lsp-id core3.00-01
```

1.70 protocol trigger isis psnp

protocol trigger isis [*instance-name*] **psnp** [**level-1** | **level-2**] [**interface** *if-name*]

no protocol trigger isis [*instance-name*] **psnp** [**level-1** | **level-2**] [**interface** *if-name*]

1.70.1 Purpose

Forces Intermediate System-to-Intermediate System (IS-IS) partial sequence number protocol data units (PSNPs) to be sent out through all interfaces or through a particular interface.

1.70.2 Command Mode

exec (10)

1.70.3 Syntax Description

instance-name	Optional. IS-IS instance name. Forces PSNPs to be sent for only the specified instance.
level-1	Optional. Forces PSNPs to be sent for IS-IS level 1 only.
level-2	Optional. Forces PSNPs to be sent for IS-IS level 2 only.
interface ***if-name***	Optional. Interface name. Forces PSNPs to be sent for only the specified interface.

1.70.4 Default

None

1.70.5 Usage Guidelines

Use the **protocol trigger isis csnp** command to force PSNPs to be sent out through all interfaces or through a particular interface. The content of the PSNP packets should include all the current version of the link state database. This can be useful during lab testing or network troubleshooting.

1.70.6 Examples

The following example triggers an IS-IS **level-1** PSNP packet to be sent out over all the interfaces:

```
[local]Redback#trigger isis psnp level-1
```

1.71 protocol trigger isis spf

protocol trigger isis [*instance-name*] **spf** [**level-1** | **level-2**] [**re-start**]

1.71.1 Purpose

Forces an Intermediate System-to-Intermediate System (IS-IS) Shortest Path First (SPF) calculation to run immediately instead of waiting for the next interval.

1.71.2 Command Mode

exec (10)

1.71.3 Syntax Description

instance-name	Optional. IS-IS instance name. Triggers an SPF calculation for only the specified instance.
level-1	Optional. Triggers an SPF calculation for IS-IS level 1 only.
level-2	Optional. Triggers an SPF calculation for IS-IS level 2 only.
re-start	Optional. Forces the triggered Hello packets to be sent out with Restart Request bit set inside the restart type-length-value (TLV).

1.71.4 Default

None

1.71.5 Usage Guidelines

Use the **protocol trigger isis spf** command to force an IS-IS SPF calculation to run immediately instead of waiting for the next interval.

Use the **re-start** keyword to trigger the neighbors to consider this router is restarted. It may receive the complete sequence number protocol data unit (CSNP) and link-state protocol data units (LSPs) from the neighbors.

1.71.6 Examples

The following example triggers an IS-IS **level-2** SPF calculation to run immediately:

```
[local]Redback#protocol trigger isis spf level-2
```

1.72 proto-down-on-dad

proto-down-on-dad

{**no** | **default**} **proto-down-on-dad**

1.72.1 Purpose

Enable the SmartEdge router to send a request to bring down the IPv6 stack of the subscriber circuit in which a duplicate address detection (DAD) failure is detected.

1.72.2 Command Mode

ND profile configuration

1.72.3 Syntax Description

This command has no keywords or arguments.

1.72.4 Default

By default, this ND profile parameter is disabled.

1.72.5 Usage Guidelines

Use the **proto-down-on-dad** command to enable the SmartEdge router to send a request to bring down the IPv6 stack of the subscriber circuit in which a DAD failure is detected. If the subscriber circuit consists of only an IPv6 stack (without an IPV4 stack), then the entire subscriber circuit is brought down. For more information about DAD, see *Configuring ND*.

1.72.6 Examples

The following example enables the parameter in the ND profile **ndprofile7** to allow the SmartEdge router to send a request to bring down the IPv6 subscriber circuit on which a DAD failure is detected:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#nd profile ndprofile7
[local]Redback(config-nd-profile)#proto-down-on-dad
```

1.73 proxy-reporting

proxy-reporting

no proxy-reporting

1.73.1 Purpose

Enables proxy reporting on a bridge.

1.73.2 Command Mode

- IGMP snooping bridge configuration

1.73.3 Syntax Description

This command has no keywords or arguments.

1.73.4 Default

Proxy reporting is disabled by default.

1.73.5 Usage Guidelines

Use the **proxy-reporting** command to enable proxy reporting on a bridge. The IGMP proxy manages IGMP host tracking, messages, and queries. By default, the IGMP proxy is disabled, and the router is passive and does not suppress IGMP messages. When the IGMP proxy is disabled, the router queries only IGMP messages.

Use the **no** form of this command to return the bridge to the default setting in which proxy reporting is disabled.

1.73.6 Examples

The following example shows how to enable proxy reporting on a bridge called `sj1`:

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#bridge sj1
[local]Redback(config-bridge)#igmp snooping
[local]Redback(config-igmp-snooping)#proxy-reporting
```

1.74 pseudowire ignore-mtu

pseudowire ignore-mtu

no pseudowire ignore-mtu

1.74.1 Purpose

The **pseudowire ignore-mtu** command overrides RFC 4447 compliance with regard to MTU matching.

1.74.2 Command Mode

global configuration

1.74.3 Syntax Description

This command has no keywords or arguments.

1.74.4 Default

RFC 4447 compliance with regard to MTU matching is the default system behavior.

1.74.5 Usage Guidelines

Use the **pseudowire ignore-mtu** command to override RFC 4447 compliance with regard to MTU matching.

By default, LDP-based L2VPN pseudowires (except ATM AAL2 pseudowires) comply with MTU matching described in RFC 4447. The MTUs across the endpoints are compared and must be same for the pseudowire to be operational. The **pseudowire ignore-mtu** command is provided to override this default behavior. When the **pseudowire ignore-mtu** command is enabled, the SmartEdge system falls into non-RFC 4447 compliance mode with regard to MTU matching; and when disabled, adheres to RFC 4447 compliance with regard to MTU matching.

RFC 4447 compliance with regard to MTU matching.is the default system behavior.

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

1.74.6 Examples

```
[local]Redback(config)#pseudowire ignore-mtu
```

1.75 pseudowire multi-path

pseudowire multi-path

no pseudowire multi-path

1.75.1 Purpose

Load balances pseudowire (PW) traffic among the links in a link-group.

1.75.2 Command Mode

global configuration

1.75.3 Syntax Description

This command has no keywords or arguments.

1.75.4 Default

PW load balancing is disabled. Each PW travels is encapsulated in only one member link in a LAG bundle so that PW traffic is sent based on the inner virtual circuit label (pseudowire label) as a single link in the link-group.

1.75.5 Usage Guidelines

Use the **pseudowire multi-path** command to distribute PW traffic among the links in a link-group, spanning over different member links, taking multiple paths based on hashing the IP source and destination address.

See the *Load Balancing* document for context where this command is used.

Use the **no** form of this command to disable PW load balancing.

1.75.6 Examples

```
[local]Redback#configure
[local]Redback(config)#pseudowire multi-path
```

1.76 pseudowire router-id

pseudowire router-id ipaddress *ip-address* context *context-id*

1.76.1 Purpose

Configures the global pseudowire settings for CESoPSN snd SAToP connections.

1.76.2 Command Mode

Global Config Mode.

1.76.3 Syntax Description

ip-address	Loopback source IP address or router ID for a UDP pseudowire.
context-id	Cotext ID where the loopback IP address is configured. Default is local.

1.76.4 Default

No pseudowire is defined..

1.76.5 Usage Guidelines

None..

1.76.6 Examples

The following example shows how to configure the global settings for a CESoPSN pseudowire:

```
[local]Redback(config)#pseudowire router-id ipaddress
xxx.xxx.xxx.xxx context local
```

1.77 pseudowire threshold drop

pseudowire threshold drop {cell-concatenation *cell-concaten ation-value* | out-of-sequence *out-of-sequence-value*}

{no | default} pseudowire threshold drop {cell-concatenation | out-of-sequence}

1.77.1 Purpose

To enable statistics collection for the number of cells the system receives

1.77.2 Command Mode

stats collection mode

1.77.3 Syntax Description

cell-concatenation *cell-concatenation-value*	Identifies the maximum number of concatenated cells allowed in received pseudowire packets. After that limit, the system will drop all packets.
out-of-sequence *out-of-sequence-value*	Identifies the maximum number of out of sequence cells allowed in received pseudowire packets. After that limit, the system will drop all packets.

1.77.4 Default

The system does not save counters for the number of cells received.

1.77.5 Usage Guidelines

Use the **pseudowire threshold drop** command to configure the maximum number of concatenated cells and out of sequence cells allowed in received pseudowire packets. After that limit, the system will drop all packets. The packet count is measured by the number of cells and the byte count by the number of cells multiplied by the size of the cell.

You can display the information in this counter by using the **show circuit counters** command. This counter also records the number of frames that were out of order that the system received and discarded.

Use the **no** and **default** forms of this command stop saving the count of the number of cells received for concatenated cells and out of sequence drops.

1.77.6 Examples

The following example shows how to configure the system to concatenate a maximum of 100 packets for the pseudowire threshold. After that limit is met, all remaining packets will be dropped.

```
[local]Redback(config-stats-collect)#pseudowire threshold drop cell-concatenation 100
```

The following example shows how to configure the maximum number of out of sequence cells allowed in received pseudowire packets as 1000 packets/byte.

```
[local]Redback(config-stats-collect)#pseudowire threshold drop out-of-sequence 1000
```

1.78 public-key

public-key {**DSA** | **RSA**} [{**after-key** ***existing-key***} | {**position** ***key-position***}] {***new-key*** | **ftp** ***url***}

no public-key {**DSA** |**RSA**} {**all** | **position** ***key-position***}

1.78.1 Purpose

Specifies public key authentication for any administrator accessing the SmartEdge command-line interface (CLI) through Secure Shell (SSH).

1.78.2 Command Mode

administrator configuration

1.78.3 Syntax Description

DSA	Identifies the Digital Signature Algorithm (DSA).
RSA	Identifies the Rivest-Shamir-Adelman (RSA) algorithm.
after-key ***existing-key***	Optional. Existing key string after which the new key string should follow.
position ***key-position***	Optional. Position in which the new key is to be placed within a string of keys. When used with the **no** form of this command, it is not optional, and it deletes the key in the specified position. The range of values is 1 to 100,000.
new-key	New DSA or RSA key string.
ftp ***url***	URL for the file that contains DSA or RSA keys. The file resides on an File Transfer Protocol (FTP) server. The ***url*** of the file argument is ***//admin-name***[**:***passwd***]**@***ip-addr*[***//directory***]**/***filename.ext***.
all	Deletes all DSA or RSA keys. Used only with the **no** form of this command.

1.78.4 Default

None

1.78.5 Usage Guidelines

Use the **public-key** command to specify public key authentication for administrators accessing the SmartEdge router CLI through SSH.

Use the **//** if the pathname to the directory on the remote server is an absolute pathname; use a single **/** if it is a relative pathname (under the hierarchy of ***username*** account home directory).

SSH uses cryptographic keys instead of relying on a password scheme. A key is a digital identity based on a unique string of binary data. By using keys, the

SSH client can prove to the SSH server on the SmartEdge router that the client is genuine and can prove its identity.

SSH uses a pair of keys—a public key and a private key. The private key, known only to the SSH client, is used to prove the client's identity. The public key is known by all parties. The public key can be stored on the SmartEdge router if the administrator has an account on the router.

When an administrator logs on to the CLI, the SSH client and the SSH server on the SmartEdge router both compare the private key of the client with the public key on the SmartEdge router. If the keys match, the administrator is authenticated by the SmartEdge router.

An administrator can have multiple RSA and DSA keys. The SmartEdge router maintains the list of keys in the preferred order of the administrator. This is also the order in which the keys are searched when each administrator attempts to log on to the SmartEdge router.

SSH-1 uses the RSA cryptographic algorithm. SSH-2 uses the DSA. For more information, see the Internet Draft, ***Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRL Profile***, draft-ietf-pkix-ipki-pkalgs-05.txt.

Use the **no** form of this command to disable public key authentication.

1.78.6 Examples

The following example configures a public RSA key for the administrator **jewel**:

```
[local]Redback(config-administrator)#public-key RSA

Enter public key for the user

$05313627638219386996124676l admin@local

% adding public key 1024 35 13877892548755011249626406025749447395347780214577723471190493135601780425356384229093001105445048536324328024640019971773131984441883108926459349685280917083378983989152738587950064526673253249893854977936260102627149373407590302521645739523172785841447489051486168865249795082968405313627638219386996124676l to user jewel
```

For the following example, the administrator **jenny** configures a public RSA key from the file, **nextkey.pub**, located on an FTP server at IP address, **155.53.36.231:**

```
[local]Redback(config-administrator)#public-key RSA
ftp//jenny@155.53.36.231/.ssh/nextkey.pub

Connected to 155.53.36.231.

220-

220 pepper.redback.com FTP server (NetBSD-ftpd 20000723) ready.

Remote system type is UNIX.

Using binary mode to transfer files.

331 Password required for jenny.

Password:

230-

NetBSD 1.5.1_ALPHA (NETZUUL) #34: Mon Jan 27 19:22:08 PST 2003

Welcome to NetBSD!

230 User jenny logged in.

200 Type set to I.

250 CWD command successful.

local: /tmp/tmp_public_key remote: nextkey.pub

227 Entering Passive Mode (155,53,36,231,219,44)

150 Opening BINARY mode data connection for 'nextkey.pub' (326 bytes).

100% |************************************|   326     780.29 KB/s
00:00 ETA

226 Transfer complete.

326 bytes received in 00:00 (1.67 KB/s)

221-

Data traffic for this session was 326 bytes in 1 file.

Total traffic for this session was 1030 bytes in 1 transfer.

221 Thank you for using the FTP service on pepper.corpA.com.

key added 1024 41 10655058848965185319838794285855513719015022151067720
19169405797369479122367748656007049848153282885605837885928788721880508 7
46785971425628850076859766411974048627245637829747980541102632417616482 1
84609568692439737685795227832130912128498712411351623849997825790586906 9
62354902145486419150014255658614488939 91
```

1.79 pwd

pwd

1.79.1 Purpose

Displays the current working directory.

1.79.2 Command Mode

exec (10)

1.79.3 Syntax Description

This command has no keywords or arguments.

1.79.4 Default

None

1.79.5 Usage Guidelines

Use the **pwd** command to display the current working directory.

1.79.6 Examples

The following example displays the current working directory:

```
[local]Redback#pwd

/flash/config
```

1.80 pw-encap

pw-encap {**ether** | **vlan**}

{**no** | **default**} **pw-encap**

1.80.1 Purpose

Specifies the pseudowire encapsulation type.

1.80.2 Command Mode

VPLS profile neighbor configuration

1.80.3 Syntax Description

ether	Specifies the encapsulation type as Ethernet encapsulation.
vlan	Specifies the encapsulation type as Ethernet virtual LAN (VLAN) encapsulation.

1.80.4 Default

The default pseudowire encapsulation type is Ethernet encapsulation.

1.80.5 Usage Guidelines

Use the **pw-encap** command to specify the pseudowire encapsulation type.

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

1.80.6 Examples

The following example specifies the pseudowire encapsulation type as Ethernet VLAN encapsulation:

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

1.81 pw-id

pw-id *pw-num*

no pw-id *pw-num*

1.81.1 Purpose

Configures a default pseudowire number for use with all the pseudowires signaled by the Virtual Private LAN Services (VPLS) instance.

1.81.2 Command Mode

VPLS configuration

1.81.3 Syntax Description

pw-num	Default pseudowire number, used to identify the pseudowire endpoints when signaling using Label Distribution Protocol (LDP). Valid values are 1 to 4,294,967,295.

1.81.4 Default

None

1.81.5 Usage Guidelines

Use the **pw-id** command to configure a default pseudowire number for use with all the pseudowires signaled by the VPLS instance. The default pseudowire number is used for VPLS profiles that do not have a pseudowire ID (number or name) specified.

Remote provider edge (PE) devices use the pseudowire ID and the local IP address to identify the pseudowire and the associated VPLS instance.

A VPLS instance can have only one default pseudowire ID number. If a default pseudowire ID numberexists for a VPLS instance and a new pseudowire ID number is configured, the new pseudowire ID replaces the previous pseudowire ID.

Use the **no** form of this command to remove the default pseudowire number.

1.81.6 Examples

The following example configures the default pseudowire number, **1234**, for use with all the pseudowires signaled by the VPLS instance:

```
[local]Redback#config
[local]Redback(config)#context local
[local]Redback(config-ctx)#bridge to-pe4
[local]Redback(config-bridge)#vpls
[local]Redback(config-vpls)#pw-id 1234
[local]Redback(config-vpls)#
```

1.82 pw-label

pw-label in ***in-label-num*** **out** ***out-label-num***

no pw-label

1.82.1 Purpose

Configures pseudowire labels for a static pseudowire.

1.82.2 Command Mode

- VPLS profile neighbor configuration

1.82.3 Syntax Description

in ***in-label-num***	Number of the incoming (ingress) pseudowire label. The range of values is 4,096 to 65,535.
out ***out-label-num***	Number of the outgoing (egress) pseudowire label. The range of values is 4,096 to 65,535.

1.82.4 Default

No pseudowire labels are configured.

1.82.5 Usage Guidelines

Use the **pw-label** command to configure pseudowire labels for a static pseudowire. When the pseudowire labels are configured, the pseudowire is not signaled using a targeted LDP session to the neighbor. Instead, a static mapping for the pseudowire is created using the specified pseudowire labels. A pseudowire label can be used only once. Trying to configure a pseudowire label that is already in use causes the **pw-label** command to be rejected. Pseudowire labels must be configured on both ends of the VPLS peering session for the static pseudowire to operate properly.

Note: Static pseudowires (inner tunnels) can be configured in either static or signalled outer tunnels, including static, LDP and RSVP LSPs, and GRE tunnels.

When the outer tunnel is broken or no next hop to the peer exists, the static pseudowire is marked down, and a standby pseudowire is used if it has been configured.

Note: MAC flush TLVs sent using the clear vpls mac-flush command (in exec mode) can be sent over both signaled and static pseudowires.

Use the **no** form of this command to delete the pseudowire labels.

1.82.6 Examples

The following example creates ingress and egress pseudowire labels, with the values **5000** and **15000**, respectively, for a static pseudowire to the VPLS profile neighbor, **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)#pw-label in 5000 out 15000
[local]Redback(config-vpls-profile-neighbor)#
```

1.83 pw-mtu

pw-mtu ***bytes***

{no | **default} pw-mtu**

1.83.1 Purpose

Configures the maximum transmission unit (MTU) for a static pseudowire.

1.83.2 Command Mode

- VPLS profile neighbor configuration

1.83.3 Syntax Description

bytes	MTU size in bytes. Enter a value from 1200 to 9198.

1.83.4 Default

MTU default is 1500.

1.83.5 Usage Guidelines

Use the **pw-mtu** command to configure the MTU for a static pseudowire.

Use the **no** or **default** form of this command to set the pseudowire MTU to its default value.

1.83.6 Examples

The following example shows how to set the pseudowire MTU to **9198** bytes:

```
[local]Redback(config)#vpls profile hub
[local]Redback(config-vpls-profile)#neighbor 4.4.4.4
[local]Redback(config-vpls-profile-neighbor)#pw-mtu 9198
```

1.84 qos class

qos {*pd-value* | **all**} **class** *class-name*

{**no** | **default**} **qos** {*pd-value* | **all**} [**class** *class-name*]

1.84.1 Purpose

Assigns an internal packet descriptor (PD) classification value to a class name.

1.84.2 Command Mode

- class definition configuration

1.84.3 Syntax Description

pd-value	An integer from 0 to 63 (six bits), with the packet priority encoded in three higher-order bits and the packet drop precedence in the three lower-order bits. You can enter the value in decimal or hexadecimal format, for example **16** or **0x10**. You can also enter a standard Differentiated Services Code Point (DSCP) marking label as defined in *DSCP Class Keywords* in the **mark dscp** command. 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.
all	Assigns all valid PD values for the source value to the specified class. Any existing configuration for the class definition is overridden.
class-name	An alphanumeric string of up to 39 characters that specifies the class name. Optional only for the **no** form of this command.

1.84.4 Default

The PD value is not assigned to any class.

1.84.5 Usage Guidelines

Use the **qos class** command to assign an internal PD QoS classification value to a class name. The PD QoS value can be referenced in policing or metering policies. The SmartEdge router creates the class when you assign the first PD QoS value in the class definition to the class. Subsequent PD QoS values assigned to this class join the existing class. Removing or modifying the last class-definition entry that references a class deletes the class. Remove all metering and policing policy references to the class definition before you delete a class.

Each class definition can define up to eight metering or policing classes based on PD QoS classification values. Multiple class-definition entries can reference the same class.

The SmartEdge router processes class definitions and assigns packet classes before it applies any metering or policing policy that references the class definition. Use the **qos class-definition** command (in global configuration mode) to create the class definition.

Use the **no** or **default** form of this command to return the PD QoS value to the default state.

1.85 qos class-definition

qos class-definition *class-definition-name*

no qos class-definition *class-definition-name*

1.85.1 Purpose

Specifies or creates a class definition and enters class definition configuration mode.

1.85.2 Command Mode

global configuration

1.85.3 Syntax Description

class-definition-name	An alphanumeric string of up to 39 characters that specifies the class-definition name. If a class definition with the specified name does not exist, it is created.

1.85.4 Default

No class definition is defined.

1.85.5 Usage Guidelines

Use the **qos class-definition** command to specify or create a class definition and enter class definition configuration mode. Class definitions define metering and policing classes using internal packet priority and drop precedence values. You can create up to 15 class definitions; each class definition can define up to eight metering or policing classes based on PD QoS classification values.

Use the **qos class** command (in class definition configuration mode) to edit the contents of a class definition.

Note: You can use class definitions without configuring classification maps to propagate the QoS settings.

Use the **no** form of this command to delete a class definition. Remove all metering and policing policy references to the class definition before you delete it.

1.86 qos class-map

qos class-map *map-name marking-type* {**in** | **out**}

no qos class-map *map-name marking-type* {**in** | **out**}

1.86.1 Purpose

Defines a configurable schema for customized packet mappings to and from the SmartEdge router internal packet descriptor (PD) QoS markings, and accesses class map configuration mode.

1.86.2 Command Mode

- global configuration

1.86.3 Syntax Description

map-name	Name of the classification map, an alphanumeric string of up to 39 characters. The name must be unique. You can configure up to 128 classification maps for all marking types and directions. If the classification map does not exist, the SmartEdge router creates it.
marking-type	Marking type for this classification map, according to one of the following keywords: • **ethernet**—802.1p marking • **mpls**—EXP marking • **ip**—Differentiated Services Code Point (DSCP) marking • **atm**—Cell loss priority (CLP) marking
in	Maps incoming packets as they are received. This type of classification map can be applied to **propagate qos from** commands.
out	Maps outgoing packets as they are prepared for transmission. This type of classification map can be applied to **propagate qos to** commands.

1.86.4 Default

None

1.86.5 Usage Guidelines

Use the **qos class-map** command to create and configure customized mappings between internal and external packet priority and drop precedence values.

You can use the **mapping-schema** command to define a set of default values for all mapping entries, then override that value for a subset of entries by entering subsequent mapping commands. The mapping commands that are available depend on the direction and *marking-type* values specified by this

command. For example, if you enter the **qos class-map** command with the **my_class_map ethernet out** keywords, only the **mapping-schema**, **qos to ethernet**, and **qos use-ip** commands are available. The classification map can then be applied using the **propagate qos to ethernet** command with the **class-map my_class_map** keywords.

A classification map can function either as a primary or secondary classification map, or both. For ingress mappings, a secondary classification map must have a value of ip for the ***marking-type*** argument, and a value of in specified for the mapping direction. For egress mappings, a secondary classification map must have the same values for the ***marking-type*** argument and mapping direction as the primary classification map.

The SmartEdge router uses primary classification maps during the initial packet inspection. If a secondary classification map is configured, the SmartEdge router performs a second mapping for packets containing the specified primary value. When configured for the **ethernet use-ip** or **mpls use-ip** commands, secondary classification maps translate Differentiated Services Code Point (DSCP) values to PD QoS priority values. When configured for the **qos use-ip** commands, secondary classification maps translate DSCP values to external Multiprotocol Label Switching (MPLS) experimental (EXP) values or 802.1p priority values.

Use the **no** form of this command to remove the classification map. Remove all dependent configuration entries, such as propagation commands and other classification maps, before you remove the classification map.

Note: QoS configuration does not prevent you from removing class maps referenced by active subscribers. If you do so, the subscriber session receives an incorrect mapping (either the default mapping or a new mapping configured later). To prevent problems, do not remove a class map that is referenced by active subscriber sessions.

1.86.6 Examples

The following example creates a classification map **exp-to-pd** that maps MPLS EXP values to PD QoS values on ingress:

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

1.87 qos congestion-avoidance-map

qos congestion-avoidance-map *map-name pol-type*

no qos congestion-avoidance-map *map-name pol-type*

1.87.1 Purpose

Creates a quality of service (QoS) congestion avoidance map and accesses congestion map configuration mode.

1.87.2 Command Mode

- global configuration

1.87.3 Syntax Description

map-name	Name of the congestion avoidance map.
pol-type	Policy type to which this congestion avoidance map will be assigned, according to one of the following keywords: • **atmwfq**—Asynchronous Transfer Mode weighted fair queuing (ATMWFQ) policy. • **mdrr**—Modified deficit round-robin (MDRR) policy. • **pwfq**—Priority weighted fair queuing (PWFQ) policy.

1.87.4 Default

None

1.87.5 Usage Guidelines

Use the **qos congestion-avoidance-map** command to create a QoS congestion avoidance map and access congestion map configuration mode.

You can create up to 256 congestion avoidance maps.

Use the **queue red** command (in congestion map configuration mode) to configure the map.

To assign a map to a policy, use the **congestion-map** command (in ATMWFQ, MDRR, or PWFQ policy configuration mode).

Use the **no** form of this command to delete the specified map from the configuration.

Note: If you delete a congestion avoidance map that is assigned to an MDRR or PWFQ policy, the queue depth reverts to the default; for ATMWFQ policies, queue depth remains as specified by the ATM profile assigned to the ATM permanent virtual circuit (PVC).

1.87.6 Examples

The following example creates a congestion avoidance map, **map-red4a**:

```
[local]Redback(config)#qos congestion-avoidance-map map-red4a
[local]Redback(config-congestion-map)#
```

1.88 qos hierarchical mode strict

qos hierarchical mode strict

{**no** | **default**} **qos hierarchical mode**

1.88.1 Purpose

Specifies the strict priority quality of service (QoS) scheduling algorithm for the traffic-managed port, 802.1Q tunnel, 802.1Q permanent virtual circuit (PVC), hierarchical node group, or hierarchical node on a traffic-managed port.

1.88.2 Command Mode

- dot1q PVC configuration
- hierarchical node configuration
- hierarchical node group configuration

1.88.3 Syntax Description

This command has no keywords or arguments.

1.88.4 Default

Gigabit Ethernet ports on traffic-managed cards are the top level in the traffic management hierarchy.

1.88.5 Usage Guidelines

Use the **qos hierarchical mode strict** command to specify the strict priority QoS scheduling algorithm for the traffic-managed port, 802.1Q tunnel, 802.1Q PVC, hierarchical node group, or hierarchical node on a traffic-managed port. You can also use the **qos rate** or **qos weight** commands (in port or dot1q PVC configuration mode) to create a node in the QoS hierarchy with the default strict priority mode.

A QoS traffic-managed port is always a node at the top of the hierarchy. The scheduling algorithms service the QoS queues defined by the priority weighted fair queuing (PWFQ) policy attached to the port, 802.1Q tunnel, or 802.1Q PVC according to the priority assigned to each queue with the **queue priority** command (in PWFQ policy configuration mode). The priority determines the servicing order, and the relative maximum rate or weight determines the amount of traffic that is transmitted.

For 802.1Q PVCs, you can use this command to configure both static and on-demand PVCs. If you do not enter this command for an 802.1Q tunnel or PVC, the tunnel or PVC is not part of the QoS traffic management hierarchy. In this case, a tunnel inherits only the PWFQ policy attached to its port and a PVC inherits the policy attached to its tunnel, unless you apply a more specific PWFQ policy to the tunnel or PVC.

Use the **no** or **default** form of this command to remove the tunnel or PVC from the hierarchy.

Note: When you first configure the **qos hierarchical mode strict**, **qos rate**, or **qos weight** command for a dot1q PVC, the SmartEdge router removes previously configured QoS policy queuing commands on the circuit or any of its children. Configuring one of these commands on a circuit group for the first time deletes any QoS policy queuing commands on its existing members, and adding a member to a circuit group that has a configured L3 command removes all QoS policy queuing commands configured on the member circuit. To address this issue, reconfigure these QoS policy queuing commands.

1.88.6 Examples

The following example enables an 802.1Q PVC tunnel as a traffic-managed hierarchical node, with strict scheduling algorithm:

```
[local]Redback(config)#port ethernet 9/1
[local]Redback(config-port)#dot1q pvc 10 encapsulation 1qtunnel
[local]Redback(config-dot1q-pvc)#qos hierarchical mode strict
```

1.89 qos mode

qos mode {**alternate** | **normal** | **strict**}

{**no** | **default**} **qos mode**

1.89.1 Purpose

The **qos mode** command is no longer supported in ATM OC, link group, and port configuration modes.

1.89.2 Command Mode

- ATM OC configuration
- link group configuration
- port configuration

1.90 qos mode (MDRR)

qos mode {**priority** | **strict** | **wrr**}

no qos mode{**priority** | **strict** | **wrr**}

1.90.1 Purpose

Specifies the scheduling algorithm for this modified deficit round-robin (MDRR) policy.

1.90.2 Command Mode

- MDRR policy configuration

1.90.3 Syntax Description

priority	Specifies the priority queuing (PQ) strict priority mode. In PQ mode, the output queues on a circuit are serviced in strict priority order; that is, packets waiting in the highest-priority queue (queue 0) are serviced until that queue is empty, then packets waiting in the second-highest priority queue are serviced (queue 1), and so on. Under congestion, PQ allows the highest priority traffic to get through, at the expense of lower-priority traffic. **Note:** To use the PQ strict priority mode (using the priority keyword), you must first remove all weight configurations for the policy.
strict	Specifies the MDRR strict mode. In strict mode, queue 0 always has priority over all other queues configured on a circuit. **Note:** To use the MDRR strict mode (using the strict keyword), you must first remove the queue weight configuration on queue 0 for the policy.
wrr	Specifies the MDRR weighted round-robin (WRR) mode. In WRR mode, queue 0 is treated like all other queues on a circuit. Each queue receives its share of the circuit's bandwidth according to the weight assigned to the queue.

1.90.4 Default

MDRR policies use the WRR mode scheduling algorithm.

1.90.5 Usage Guidelines

Use the **qos mode** command to specify the scheduling algorithm for this MDRR policy.

Use the **default queue weight** command (in MDRR policy configuration mode) to remove the weight configurations.

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

1.90.6 Examples

The following example specifies the MDRR strict mode as the scheduling algorithm:

```
[local]Redback(config)#qos policy example2 mdrr
[local]Redback(config-policy-mdrr)#qos mode strict
```

1.91 qos node

qos node *node-name idx-start* [**through** *idx-end*]

no qos node *node-name*

1.91.1 Purpose

Creates one or more quality of service (QoS) hierarchical nodes as aggregation points for applying traffic shaping and accesses hierarchical node configuration mode.

1.91.2 Command Mode

- hierarchical node group configuration

1.91.3 Syntax Description

node-name	Name of the node.
idx-start	Initial index number.
through *idx-end*	Optional. Final index number.

1.91.4 Default

No nodes are created.

1.91.5 Usage Guidelines

Use the **qos node** command to create one or more QoS hierarchical nodes as aggregation points for applying traffic shaping and access hierarchical node configuration mode.

Note: This command is available only for traffic-managed ports.

Note: The command prompt for the hierarchical node configuration mode is identical to the prompt for the hierarchical node group configuration mode; see the example in the Examples section.

Each node is uniquely referenced by its name, its node index, its node group, and the index for the node group.

Use the **no** form of this command to delete one or more nodes from the configuration.

1.91.6 Examples

The following example creates **10** hierarchical node groups and 50 hierarchical nodes, with **5** nodes in each node group; the name of each node group is **home** and the name of each node is **dslam**:

```
[local]Redback(config)#port ethernet 5/1
[local]Redback(config-port)#qos node-group home 1 through 10
[local]Redback(config-h-node)#qos node dslam 1 through 5
[local]Redback(config-h-node)#
```

1.92 qos node-group

qos node-group *group-name idx-start* [**through** *idx-end*]

no qos node-group *group-name*

1.92.1 Purpose

Creates one or more quality of service (QoS) hierarchical node groups as aggregation points for applying traffic shaping and accesses hierarchical node group configuration mode.

1.92.2 Command Mode

- port configuration

1.92.3 Syntax Description

group-name	Name of the node groups.
idx-start	Initial index number.
through *idx-end*	Optional. Final index number.

1.92.4 Default

No node groups are created.

1.92.5 Usage Guidelines

Use the **qos node-group** command to create one or more QoS hierarchical node groups as aggregation points for applying traffic shaping and accesses hierarchical node group configuration mode. This command is available only for traffic-managed ports.

Each node group is uniquely referenced by its name and its index.

Use the **no** form of this command to delete the node group from the configuration.

1.92.6 Examples

The following example creates **10** hierarchical node groups; the name of each group is **home**:

```
[local]Redback(config)#port ethernet 5/1
[local]Redback(config-port)#qos node-group home 1 through 10
[local]Redback(config-h-node)#
```

1.93 qos node-reference

qos node-reference *node-name node-idx group-name group-idx*

no qos node-reference *node-name*

1.93.1 Purpose

Creates a reference to a quality of service (QoS) hierarchical node in the subscriber record, named subscriber profile, or default subscriber profile.

1.93.2 Command Mode

- subscriber configuration

1.93.3 Syntax Description

node-name	Name of the node.
node-idx	Node index number.
group-name	Name of the node group.
group-idx	Node group index number.

1.93.4 Default

No node references are created in any subscriber record, named subscriber profile, or default subscriber profile.

1.93.5 Usage Guidelines

Use the **qos node-reference** command to create a reference to a QoS hierarchical node in the subscriber record, named subscriber profile, or default subscriber profile.

Use the **no** form of this command to delete the reference from the subscriber record, named subscriber profile, or default subscriber profile.

1.93.6 Examples

The following example creates a reference to the hierarchical node group, **home**, with index **1**, in which was created the node, **dslam**, with index **5**, in the subscriber record, **joe**:

```
[local]Redback(config)#context subs
[local]Redback(config-ctx)#subscriber joe
[local]Redback(config-sub)#qos node-reference home 1 dslam 5
```

1.94 qos policy atmwfq

qos policy *pol-name* **atmwfq**

no qos policy *pol-name* **atmwfq**

1.94.1 Purpose

Creates or selects a quality of service (QoS) Asynchronous Transfer Mode weighted fair queuing (ATMWFQ) policy and enters ATMWFQ policy configuration mode.

1.94.2 Command Mode

global configuration

1.94.3 Syntax Description

pol-name	Name of the ATMWFQ policy to be created or selected.

1.94.4 Default

No ATMWFQ policy is created.

1.94.5 Usage Guidelines

Use the **qos policy atmwfq** command to create or select a QoS ATMWFQ policy and enter ATMWFQ policy configuration mode. An ATMWFQ policy defines QoS for outbound packets on the circuit to which the policy is attached. Up to eight queues per circuit can be serviced.

To attach an ATMWFQ policy to the circuit, use the **qos policy queuing** command (in ATM PVC configuration mode).

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

Note: An ATMWFQ policy is applicable only to ATM permanent virtual circuits (PVCs)—not ports—on second-generation ATM OC traffic cards. An ATMWFQ policy cannot be attached to a PVC that is shaped as unspecified bit rate, enhanced (UBRe).

Caution!

Risk of traffic loss. Modifying the parameters of an ATMWFQ policy momentarily interrupts the traffic on all ATM PVCs using the policy. To reduce the risk, use caution when modifying ATMWFQ policy parameters.

Use the **no** form of this command to delete an ATMWFQ policy from the configuration.

1.94.6 Examples

The following example creates the ATMWFQ policy, **example1**, configures **4** queues, and assigns a congestion map:

```
[local]Redback(config)#qos policy example1 atmwfq
[local]Redback(config-policy-atmwfq)#num-queues 4
[local]Redback(config-policy-atmwfq)#congestion-map red4
```

1.95 qos policy edrr

qos policy ***pol-name*** **edrr**

no qos policy ***pol-name*** **edrr**

1.95.1 Purpose

This command is no longer supported.

1.96 qos policy mdrr

qos policy ***pol-name*** **mdrr**

no qos policy ***pol-name*** **mdrr**

1.96.1 Purpose

Creates or selects a quality of service (QoS) modified deficit round-robin (MDRR) policy and enters MDRR policy configuration mode.

1.96.2 Command Mode

global configuration

link group

1.96.3 Syntax Description

pol-name	Name of the MDRR policy to be created or selected.

1.96.4 Default

No MDRR policy is configured.

1.96.5 Usage Guidelines

Use the **qos policy mdrr** command to create a QoS MDRR policy and enter MDRR policy configuration mode. An MDRR policy defines QoS for outgoing packets on the port or circuit to which the policy is attached. Up to eight queues per circuit can be serviced.

MDRR policies can be applied to Ethernet ports and the 802.1Q tunnels and 802.1Q PVCs that are configured on them. In addition, they can be applied

to Ethernet ports that are members of a link group and to hitless access link groups. Be aware that MDRR policies are not supported on economical link aggregation groups (LAGs).

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

To attach an MDRR policy to a port or circuit, enter the **qos policy queuing** command (in the appropriate port or circuit configuration mode).

Note: The maximum number of unique MDRR rates that can be applied to circuits on a single slot by configuration in the MDRR policy using the **rate** command and per-circuit customization through the **rate circuit** *out* command is 200.

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

1.96.6 Examples

The following example configures the MDRR policy, **example1**, and attaches the policy to a 10 Gigabit Ethernet (10GE) port:

```
[local]Redback(config)#qos policy example1 mdrr
[local]Redback(config-policy-mdrr)#exit
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#qos policy queuing example1
```

1.97 qos policy metering

qos policy metering *pol-name* [**inherit** | **hierarchical**] [**[ip] [ipv6] acl-counters**]

no qos policy metering *pol-name*

1.97.1 Purpose

Attaches a metering policy to the specified circuit, port, or subscriber record to be enforced on outbound packets.

1.97.2 Command Mode

- ATM PVC configuration
- dot1q PVC configuration
- Frame Relay PVC configuration
- link group configuration
- port configuration
- subscriber configuration

1.97.3 Syntax Description

pol-name	Name of the metering policy to be attached.
inherit	Optional. Inherits policy to children. Attaches the specified policy as follows: • In port configuration mode—Use this policy for any circuit (802.1Q tunnel, 802.1Q permanent virtual circuit (PVC), and any child circuit configured on an 802.1Q PVC) that is configured on this Ethernet port, unless overridden by a quality of service (QoS) metering policy attached to that circuit. • In dot1Q PVC configuration mode—Use this policy for any circuit configured on this 802.1Q tunnel or PVC (including child circuits), unless overridden by a QoS metering policy attached to that 802.1Q PVC or child circuit. • In ATM PVC configuration mode—Use this policy for any child circuit configured on this Asynchronous Transfer Mode (ATM) PVC, unless overridden by a QoS metering policy attached to that child circuit. This keyword is available only for Ethernet ports, 802.1Q tunnels, and 802.1Q PVCs, and ATM PVCs. Inheritable QoS attributes applied to constituent ports of a link group are inherited by and applied to the aggregate PVCs defined under the link group.
hierarchical	Optional. Enables aggregate rate-limiting on the children. Attaches the specified policy as follows: • In port configuration mode—Use this policy for any circuit (802.1Q tunnel, 802.1Q permanent virtual circuit (PVC), and any child circuit configured on an 802.1Q PVC) that is configured on this Ethernet port. • In dot1Q PVC configuration mode—Use this policy for any circuit configured on this 802.1Q tunnel or PVC (including child circuits). • In ATM PVC configuration mode—Use this policy for any child circuit configured on this Asynchronous Transfer Mode (ATM) PVC. This keyword is available only for Ethernet ports, 802.1Q tunnels and PVCs, and ATM PVCs.
ip acl-counters **ipv6 acl-counters**	Optional. Enables per-rule access control list (ACL) counters for a policy access-group associated with the policy. Specify the **ip acl-counters** to enable counters for an IPv4 ACL, **ipv6 acl-counters** to enable counters for an IPv6 ACL, or **ip ipv6 acl-counters** to enable counters for both IPv4 and IPv6, if applicable.

1.97.4 Default

No metering policy is attached to outbound packets on the specified circuit, or subscriber record.

1.97.5 Usage Guidelines

Use the **qos policy metering** command to attach a metering policy to a specified circuit, or port, or subscriber record to be enforced on outbound packets in any of the listed configuration modes, except link group configuration mode.

Note: Configuring the **qos policy metering** command on an ATM port is not supported. In order to limit ATM traffic, configure this command on ATM PVCs.

Use the **qos policy metering** command in port configuration mode to attach the policy to an Ethernet or 802.1Q link group. When you attach the policy to any type of link group, you effectively attach it to all ports or circuits in the link group.

For 802.1Q PVCs, this command can be used to configure both static and on-demand PVCs.

Child circuits can inherit the QoS metering and policing policies attached to the parent circuit on which the child circuits are configured if the keyword **inherit** or **hierarchical** is specified on the parent binding. If you attach a different metering or policing policy to a child circuit, those policies override the metering or policing policy attached to the parent circuit unless the parent policy applied is configured with the keyword **hierarchical**.

By default, using the optional keyword **inherit** when configuring a metering or policing policy for a parent circuit results in all of the children of the parent circuit inheriting the parent circuit policy, unless the children have a more specific policy configured. In this case, rate limiting is applied collectively to the child circuit and the parent circuit, which means all circuits to which the parent policy is to be applied are collectively subject to the rate limitations specified in the parent circuit's metering or policing policy.

Using the optional keyword **hierarchical** when configuring a metering or policing policy for a parent circuit results in applying both the child circuit policy and the parent circuit policy to the traffic on the child circuit. With hierarchical metering or policing policy, rate limiting is applied on the packets destined for the child circuit first using the child policy. If the child metering or policing policy includes a drop policy, then the SmartEdge router drops the appropriate packets if the traffic rate exceeds the rate limit. Those packets that were not dropped are processed and rate-limited once again, along with all the other packets destined for the parent circuit, using the parent policy.

Essentially, the child circuit traffic is processed and rate-limited twice and the parent circuit's native traffic is processed and rate-limited once. With hierarchical metering or policing policy enabled, a child is subject to its own specified rate limitations and then is collectively subject to the rate limitations specified in the parent circuit metering or policing policy, along with its parent and peers.

Note: Only one level of hierarchical metering or policing can be applied to a circuit. A circuit can have a maximum of two policing or metering policies applied: one individual or inherited through the **inherit** keyword, and one inherited through the **hierarchical** keyword. If a circuit is subject to two "hierarchical" parents (for example, a PPPoX session with a hierarchical metering binding on its 802.1q PVC parent and a hierarchical metering binding on its Ethernet port grandparent), only the binding on its closest relative (the PVC in this example) applies.

Use the **no** form of this command to remove a metering policy from outbound packets on a circuit, port, subscriber record, or link group (of any type).

1.97.6 Examples

The following example creates the metering policy, **example2**, and attaches it to an Ethernet port:

```
[local]Redback(config)#qos policy example2 metering
[local]Redback(config-policy-metering)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#exceed drop
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-metering)#exit
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#qos policy metering example2
```

The following example configures an outbound rate limit for all traffic on a particular port and an individual rate-limit for each 802.1Q VLAN configured under the port:

```
[local]Redback(config)#qos policy port-hierarchical-policy metering
[local]Redback(config-policy-metering)#rate 500 burst 50000
[local]Redback(config-policy-rate)#exceed mark priority 6
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-metering)#exit
[local]Redback(config)#qos policy vlan-individual-policy metering
[local]Redback(config-policy-metering)#rate 100 burst 10000
[local]Redback(config-policy-rate)#conform mark priority 0
[local]Redback(config-policy-rate)#exceed mark priority 5
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-metering)#exit
.
.
[local]Redback(config)#port ethernet 12/2
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#qos policy metering port-hierarchical-policy hierarchical
[local]Redback(config-port)#dot1q pvc 30 thr 40 encapsulation
[local]Redback(config-port)#qos policy metering vlan-individual-policy
```

1.98 qos policy metering (global)

qos policy *pol-name* **metering** [**radius-guided**]

no qos policy *pol-name* **metering**

1.98.1 Purpose

Creates or selects a quality of service (QoS) metering policy and enters metering policy configuration mode.

1.98.2 Command Mode

- global configuration

1.98.3 Syntax Description

pol-name	Name of the metering policy.
radius-guided	Optional. Allows this policy to be modified by dynamic access control lists (ACLs).

1.98.4 Default

No metering policy is created.

1.98.5 Usage Guidelines

Use the **qos policy metering** command to create or select a metering policy and enter metering policy configuration mode.

Use the **radius-guided** keyword to allow a dynamic policy ACL to modify this policy. You cannot remove a dynamic policy ACL from the policy after you have configured it, nor can you change the type of the policy from static to RADIUS-guided. To remove the dynamic policy ACL or to change the type of the policy, delete the policy and then re-create it as a static policy.

Note: Link group support for QoS metering policies is limited to Multilink Point-to-Point Protocol (MLPPP) bundles.

Note: Virtual LAN (VLAN) bridge circuits and Layer 2 Tunneling Protocol (L2TP) Virtual Private Network (VPN) circuits do not support policy access control lists (ACLs), classes, and actions within classes. Rate limiting is supported; however, the **conform dscp**, **mark dscp**, **exceed dscp**, and **mark precedence** commands (in metering policy configuration mode) are not allowed.

Use the **no** form of this command in global configuration mode to delete a metering policy.

1.98.6 Examples

The following example creates the metering policy, **example2**, and attaches it to an Ethernet port:

```
[local]Redback(config)#qos policy example2 metering
[local]Redback(config-policy-metering)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#exceed drop
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-metering)#exit
```

1.99 qos policy policing

qos policy policing *pol-name* [**inherit** | **hierarchical**] [**[ip] [ipv6] acl-counters**]

no qos policy policing *pol-name*

1.99.1 Purpose

Attaches a policing policy to the specified circuit, port, or subscriber record to be enforced on inbound packets.

1.99.2 Command Mode

- ATM PVC configuration
- dot1q PVC configuration
- Frame Relay PVC configuration
- link group configuration
- port configuration
- subscriber configuration

1.99.3 Syntax Description

pol-name	Name of the policing policy to be attached.
inherit	Optional. Inherits policy to children. Attaches the specified policy as follows: • In port configuration mode—Use this policy for any circuit (802.1Q tunnel, 802.1Q permanent virtual circuit (PVC), and any child circuit configured on an 802.1Q PVC) that is configured on this Ethernet port, unless overridden by a quality of service (QoS) metering policy attached to that circuit. • In dot1Q PVC configuration mode—Use this policy for any circuit configured on this 802.1Q tunnel or PVC (including child circuits), unless overridden by a QoS metering policy attached to that 802.1Q PVC or child circuit. • In ATM PVC configuration mode—Use this policy for any child circuit configured on this Asynchronous Transfer Mode (ATM) PVC, unless overridden by a QoS policing policy attached to the child circuit. This keyword is available only for Ethernet ports, 802.1Q tunnels, and 802.1Q PVCs, and ATM PVCs. Inheritable QoS attributes applied to constituent ports of a link group are inherited by and applied to the aggregate PVCs defined under the link group.
hierarchical	Optional. Enables aggregate rate-limiting on the children. Attaches the specified policy as follows: • In port configuration mode—Use this policy for any circuit (802.1Q tunnel, 802.1Q permanent virtual circuit (PVC), and any child circuit configured on an 802.1Q PVC) that is configured on this Ethernet port. • In dot1Q PVC configuration mode—Use this policy for any circuit configured on this 802.1Q tunnel or PVC (including child circuits). • In ATM PVC configuration mode—Use this policy for any child circuit configured on this Asynchronous Transfer Mode (ATM) PVC. This keyword is available only for Ethernet ports, 802.1Q tunnels and PVCs, and ATM PVCs.
ip acl-counters **ipv6 acl-counters**	Optional. Enables per-rule access control list (ACL) counters for a policy access-group associated with the policy. Specify the **ip acl-counters** to enable counters for an IPv4 ACL, **ipv6 acl-counters** to enable counters for an IPv6 ACL, or **ip ipv6 acl-counters** to enable counters for both IPv4 and IPv6, if applicable.

1.99.4 Default

No policing policy is attached to inbound packets on the port, or circuit, or subscriber record.

1.99.5 Usage Guidelines

Use the **qos policy policing** command to attach a policing policy to inbound packets on a specific port, or circuit, or subscriber record in any of the listed configuration modes, except link group configuration mode.

Note: Configuring the **qos policy policing** command on an ATM port is not supported. To limit ATM traffic, configure this command on ATM PVCs.

Use the **qos policy policing command** in port configuration mode to attach the policy to an Ethernet or 802.1Q link group. When you attach the policy to any type of link group, you effectively attach it to all ports or circuits in the link group.

For 802.1Q PVCs, you can use this command to configure both static and on-demand PVCs.

Use the **no** form of this command to remove a policing policy from inbound packets on a port, circuit, subscriber record, or link group (of any type).

1.99.6 Examples

The following example creates the **example2** policing policy and attaches it to an Ethernet port:

```
[local]Redback(config)#qos policy example2 policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#exceed drop
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-policing)#exit
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#qos policy policing example2
```

The following example attaches the **WholePort** policing policy to a Gigabit Ethernet port, and then attaches the **OneVC** policing policy to one of the 802.1Q PVCs. The policy attached to the PVC supersedes the policy attached to the port. For all the other PVCs on the port, the policy attached to the port takes effect:

```
[local]Redback(config)#qos policy OneVC policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#conform mark dscp ef
[local]Redback(config-policy-rate)#exceed mark dscp df
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-policing)#exit
[local]Redback(config)#qos policy WholePort policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#exceed drop
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-policing)#exit
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#qos policy policing WholePort
[local]Redback(config-port)#dot1q pvc 100
[local]Redback(config-dot1q-pvc)#bind interface if_100 local
[local]Redback(config-dot1q-pvc)#qos policy policing OneVC
```

The following example configures an inbound rate limit to be enforced on all traffic on a particular 802.1Q tunnel SVLAN and an individual rate limit for each CVLAN configured under SVLAN:

```
[local]Redback(config)#qos policy svlan-hierarchical-policy policing
[local]Redback(config-policy-policing)#rate 1000 burst 50000
[local]Redback(config-policy-rate)#exceed mark priority 6
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-policing)#exit
[local]Redback(config)#qos policy cvlan-individual-policy policing
[local]Redback(config-policy-policing)#rate 100 burst 10000
[local]Redback(config-policy-rate)#conform mark priority 0
[local]Redback(config-policy-rate)#exceed mark priority 5
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-policing)#exit

[local]Redback(config)#port ethernet 12/2
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 30 encapsulation 1qtunnel
[local]Redback(config-dot1q-pvc)#$svlan-hierarchical-policy hierarchical
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 30:1 through 100
[local]Redback(config-dot1q-pvc)#qos policy policing cvlan-individual-policy
```

1.100 qos policy policing (global)

qos policy *pol-name* **policing** [**radius-guided**]

no qos policy *pol-name* **policing**

1.100.1 Purpose

Creates or selects a quality of service (QoS) policing policy and enters policing policy configuration mode.

1.100.2 Command Mode

- global configuration

1.100.3 Syntax Description

pol-name	Name of the policing policy to be attached.
radius-guided	Optional. Allow this policy to be modified by dynamic access control lists (ACLs).

1.100.4 Default

No policing policy is created.

1.100.5 Examples

The following example creates the **example2** policing policy:

```
[local]Redback(config)#qos policy example2 policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#exceed drop
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-policing)#exit
```

The following example creates the **WholePort** policing policy for an Ethernet port and the **OneVC** policing policy for an 802.1Q PVC on that port. When the **OneVC** policy is attached to the PVC, it supersedes the **WholePort** policy attached to the port for that PVC; for all the other PVCs on the port, the policy attached to the port takes effect:

```
[local]Redback(config)#qos policy OneVC policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#conform mark dscp ef
[local]Redback(config-policy-rate)#exceed mark dscp df
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-policing)#exit
[local]Redback(config)#qos policy WholePort policing
[local]Redback(config-policy-policing)#rate 10000 burst 100000
[local]Redback(config-policy-rate)#exceed drop
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-policing)#exit
```

1.101 qos policy protocol-rate-limit

qos policy protocol-rate-limit *pol-name*

no qos policy protocol-rate-limit *pol-name*

1.101.1 Purpose

Attaches a protocol-specific rate-limiting policy to a port, subscriber record, link group, or PVC.

1.101.2 Command Mode

- ATM PVC configuration
- dot1q PVC configuration
- link-group configuration
- port configuration
- subscriber configuration

1.101.3 Syntax Description

pol-name	Name of the protocol-specific rate-limiting policy.

1.101.4 Default

No protocol-specific rate-limiting policies are attached to entities.

1.101.5 Usage Guidelines

Use the **qos policy protocol-rate-limit** command to apply an existing protocol-specific rate-limiting policy to a port, subscriber record, link group, or PVC. To create the policy, use the **qos policy protocol-rate-limit** command in global configuration mode.

For information on how to configure the policy to rate-limit incoming ARP packets, see *Configuring ARP*.

Use the **no** version of this command to remove a protocol-specific rate-limiting policy from an entity.

1.101.6 Examples

The following example creates and configures the **ARPDOS** policy and applies it to Ethernet port `5/1`:

```
[local]Redback(config)#qos policy ARPDOS protocol-rate-limit
[local]Redback(config-policy-protocol)#arp rate 5000 burst 100000
[local]Redback(config-policy-protocol)#exit
[local]Redback(config)#port ethernet 5/1
[local]Redback(config-port)#qos policy protocol-rate-limit ARPDOS
```

The following example creates and configures the **ARPDOS** policy and applies it to subscriber circuits where the default subscriber profile is applied:

```
[local]Redback(config)#qos policy ARPDOS protocol-rate-limit
[local]Redback(config-policy-protocol)#arp rate 5000 burst 100000
[local]Redback(config-policy-protocol)#exit
[local]Redback(config)#subscriber default
[local]Redback(config-sub)#qos policy protocol-rate-limit ARPDOS
```

1.102 qos policy protocol-rate-limit (global)

qos policy *pol-name* **protocol-rate-limit**

no qos policy *pol-name* **protocol-rate-limit**

1.102.1 Purpose

Creates or selects a protocol-specific rate-limiting policy with the specified name and enters protocol-rate-limit policy configuration mode.

1.102.2 Command Mode

- global configuration

1.102.3 Syntax Description

pol-name	Specifies the policy name. An alphanumeric string of up to 39 characters.

1.102.4 Default

No protocol-specific rate-limiting policies exist.

1.102.5 Usage Guidelines

Use the **qos policy protocol-rate-limit** command, in global configuration mode, to create a named rate-limiting policy that can be applied to protocol-specific packets. After you have created and configured the policy, apply it to an entity using the **qos policy protocol-rate-limit** command in subscriber, ATM PVC, dot1q PVC, port, or link-group configuration mode.

For information on how to configure the policy to rate-limit incoming ARP packets, see *Configuring ARP*.

Use the **no** form of this command to delete the named policy from the configuration.

1.102.6 Examples

The following example creates and configures the **ARPDOS** policy and applies it to Ethernet port `5/1`:

```
[local]Redback(config)#qos policy ARPDOS protocol-rate-limit
[local]Redback(config-policy-protocol)#arp rate 5000 burst 100000
[local]Redback(config-policy-protocol)#exit
[local]Redback(config)#port ether 5/1
[local]Redback(config-port)#qos policy protocol-rate-limit ARPDOS
```

The following example creates and configures the **ARPDOS** policy and applies it to subscriber circuits where the default subscriber profile is applied:

```
[local]Redback(config)#qos policy ARPDOS protocol-rate-limit
[local]Redback(config-policy-protocol)#arp rate 5000 burst 100000
[local]Redback(config-policy-protocol)#exit
[local]Redback(config)#subscriber default
[local]Redback(config-sub)#qos policy protocol-rate-limit ARPDOS
```

1.103 qos policy pq

qos policy ***pol-name*** **pq**

no qos policy ***pol-name*** **pq**

1.103.1 Purpose

This command is no longer supported.

1.104 qos policy pwfq

qos policy ***pol-name*** **pwfq**

no qos policy ***pol-name*** **pwfq**

1.104.1 Purpose

Creates or selects quality of service (QoS) priority weighted fair queuing (PWFQ) policy and enters PWFQ policy configuration mode.

1.104.2 Command Mode

- global configuration

1.104.3 Syntax Description

pol-name	Name of the policy to be created.

1.104.4 Default

No PWFQ policy is created.

1.104.5 Usage Guidelines

Use the **qos policy pwfq** command to create a QoS PWFQ policy and enter PWFQ policy configuration mode.

Note: PWFQ policies are supported on traffic-managed circuits only.

Use the **no** form of this command to delete the named QoS PWFQ policy.

1.104.6 Examples

The following example creates a QoS PWFQ policy, **ge3**, with two queues and attaches the policy to a Gigabit Ethernet 3 (GE3) port:

```
[local]Redback(config)#qos policy ge3 pwfq
[local]Redback(config-policy-pwfq)#num-queues 2
[local]Redback(config-policy-pwfq)#exit
[local]Redback(config)#port ethernet 5/1
[local]Redback(config-port)#qos policy queuing ge3
```

1.105 qos policy queuing

qos policy queuing ***pol-name***

no qos policy queuing ***pol-name***

1.105.1 Purpose

Attaches a quality of service (QoS) scheduling policy to the port, circuit, link group, or hierarchical node, or subscriber record.

1.105.2 Command Mode

- ATM OC configuration
- ATM PVC configuration
- dot1q PVC configuration
- Frame Relay PVC configuration
- hierarchical node configuration
- link group configuration
- port configuration
- subscriber configuration

1.105.3 Syntax Description

pol-name	Name of the scheduling policy to be attached.

1.105.4 Default

No queuing policy is not attached to the circuit or port.

1.105.5 Usage Guidelines

Use the **qos policy queuing** command to attach a QoS scheduling policy to the port, circuit, link group, or hierarchical node, or subscriber record.

Note: Configuring the **qos policy queuing** command on an ATM port is not supported. To limit ATM traffic, configure this command on ATM PVCs.

Use this command in link group configuration mode to attach the policy to a , access link aggregation group (LAG), or hitless access LAG. Use it in port configuration mode to attach the policy to an Ethernet or 802.1Q link group.

Inheritable QoS attributes applied to constituent ports of a link group are inherited by and applied to the aggregate PVCs defined under the link group.

The specified QoS scheduling policy must already exist. The types of scheduling policies are Asynchronous Transfer Mode weighted fair queuing (ATMWFQ), modified deficit round-robin (MDRR), and priority weighted fair queuing (PWFQ).

For 802.1Q permanent virtual circuits (PVCs), this command can be used to configure both static and on-demand PVCs.

Note: QoS scheduling policies are not supported on VLAN bridge circuits and Layer 2 Tunneling Protocol (L2TP) Virtual Private Network (VPN) circuits.

Note: ATMWFQ policies are applicable only to ATM PVCs—not ports—on second-generation ATM OC traffic cards. However, an ATMWFQ policy cannot be attached to a PVC that is shaped as unspecified bit rate extended (UBRe).

Caution!

Risk of data loss. Modifying the parameters of an ATMWFQ policy momentarily interrupts the traffic on all ATM PVCs using the policy. To reduce the risk, modify an ATMWFQ policy only when traffic is light.

Note: MDRR policies can be applied to Ethernet ports and the 802.1Q tunnels and 802.1Q PVCs that are configured on them. In addition, they can be applied to Ethernet ports that are members of a link group and to hitless LAGs. Be aware that MDRR policies are not supported on economical link aggregation groups (LAGs).

[.

Note: PWFQ policies are supported only on traffic-managed ports, and the 802.1Q tunnels, 802.1Q PVCs, and hierarchical nodes configured on them. You can attach the same PWFQ policy to a port, its 802.1Q tunnels, its PVCs, and its hierarchical nodes; similarly, you can attach different PWFQ policies to a port, its tunnels, PVCs and hierarchical nodes. For examples, see the Examples section.

Note: Layer 2 Tunneling Protocol (L2TP) network server (LNS) subscriber sessions support only PWFQ policies; an LNS subscriber session initiated on any type of port except a traffic-managed port will not be governed by the PWFQ policy attached to the subscriber record.

Slot redundancy is not supported; if an LNS subscriber session moves to a traffic-managed port in a different slot, it is no longer governed by the PWFQ policy attached to the LNS subscriber session. If the session moves to a different port in the same slot, the PWFQ policy resumes queuing after a temporary traffic disruption.

Note: You can attach only one type of queuing policy to ports and circuits on a single traffic card. That is, you can attach either ATMWFQ or PWFQ policies, but not both. You can, however, attach several queuing policies of the same type to ports, subscribers, and circuits on a single traffic card.

Note: ATMWFQ policies are not supported on link groups.

Use the **no** form of this command to remove a QoS scheduling policy from the port, circuit, link group, or hierarchical node, or subscriber record.

1.105.6 Examples

The following example creates a PWFQ policy and then attaches the policy to a GE3 port:

```
[local]Redback(config)#qos policy example1 pwfq
[local]Redback(config-policy-pwfq)#exit
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#qos policy queuing example1
```

The following example attaches two PWFQ policies, **pwfq1** and **pwfq2**, to a GE3 port, an 802.1Q tunnel on that port, and an 802.1Q PVC within that tunnel:

```
[local]Redback(config)#port ethernet 5/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#qos policy queuing pwfq1
[local]Redback(config-port)#dot1q pvc 10 encapsulation 1qtunnel
[local]Redback(config-dot1q-pvc)#qos policy queuing pwfq1
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 10:20
[local]Redback(config-dot1q-pvc)#qos policy queuing pwfq2
[local]Redback(config-dot1q-pvc)#exit
```

1.106 qos port-map (card)

qos port-map ***port-group-map-name***

no qos port-map

1.106.1 Purpose

Applies a predefined or a user-defined port group map to the traffic card you are configuring.

1.106.2 Command Mode

- card configuration

1.106.3 Syntax Description

port-group-map-name	The ***port-group-map-name*** argument specifies the name of the port group map to apply to the card. You have at least 2 options, and these are the predefined and default port map names. If you configured one or more user-defined port maps, then these port maps are also valid options. A list of valid predefined and user-defined port group map names depends on card type and can be obtained by entering "?" after the **qos port-map** command.
	Name of the default port group map to which to apply to the card. The name that displays as an option varies depending on the type of traffic card you are configuring and is one of the following: • tm_fe_perf • tm_max_perf • fwd_max_perf • tm_max_perf • fwd_max_perf • tm_max_perf (1)

(1) The ge-5-port card does not have a predefined port group map.

1.106.4 Default

The default port group map is applied.

1.106.5 Usage Guidelines

Use the **qos port-map** command to apply a predefined or a user-defined port group map to the traffic card you are configuring. Type "?" after **qos port-map** command to obtain a list of applicable port group maps.

For more information about port group maps, see *Port Grouping for Traffic Scheduling* .

Note: This command is available for supported traffic cards only.

Use the **no** form of this command to remove a port group map from the card and revert to the default port-map.

1.106.6 Examples

The following example shows how to apply the predefined port group map named `fwd_max_perf` to the `ge3-4-port` card in slot 2:

```
[local]Redback(config)#card ge3-4-port 2
[local]Redback(config-card)#qos port-map fwd_max_perf
```

1.107 qos port-map (global)

qos port-map ***port-map-name*** **card-type** ***card-type-name***

no qos port-map ***port-map-name*** **card-type** ***card-type-name***

1.107.1 Purpose

Defines the name of a port group map for a specified traffic card type and enters port group map configuration mode.

1.107.2 Command Mode

- global configuration

1.107.3 Syntax Description

port-map-name	Specifies the name of the port group map, which can be up to 39 alphanumeric characters long.
card-type ***card-type-name***	Specifies the name of the card type to associate with the port group map. The following are the supported values: • carrier—Specifies the Fast Ethernet (FE) or Gigabit Ethernet (GE) media interface cards (MICs) for the SmartEdge 100 router. • fege-60-2-port—Specifies the Fast Ethernet–Gigabit Ethernet card (60-port FE, 2-port GE). • gigaether-4-port—Specifies the Advanced Gigabit Ethernet card (4-port). • ge3-4-port—Specifies the Gigabit Ethernet 3 (GE3) card (4-port). • ge-10-port—Specifies the Gigabit Ethernet 1020 (GE1020) card (10-port). • ge-20-port—Specifies the Gigabit Ethernet 1020 (GE1020) card (20-port). • ge-5-port—Specifies the Gigabit Ethernet (5-port). • ge4-20-port—Specifies the Gigabit Ethernet (20-port). • ge2-10-port—Specifies the Gigabit Ethernet DDR (10-port). • 10ge-1-port—Specifies the 10-Gigabit Ethernet card (1-port). • 10ge-4-port—Specifies the 10-Gigabit Ethernet card (4-port). • 10ge-oc192-1-port—Specifies the 10 Gigabit Ethernet/OC-192c DDR (1-port).

1.107.4 Default

None

1.107.5 Usage Guidelines

Use the **qos port-map** command to define the name of a port group map for a specified traffic card type and enter port group map configuration mode.

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

For more information about port group maps, see *Port Grouping for Traffic Scheduling*.

1.107.6 Examples

The following example shows how to define a QoS port map named `portmap7` for the `ge-10-port` card type:

```
[local]Redback(config)#qos port map portmap7 card-type ge-10-port
[local]Redback(config-port-group-map)#
```

1.108 qos priority

qos priority *group-num*

{no | default} qos priority

1.108.1 Purpose

Sets the internal Packet Descriptor (PD) Quality of Service (QoS) priority field of all packets received on the circuit to a fixed value. The PD QoS priority field determines a packet's priority on the SmartEdge router packet switching fabric and priority for purposes of class-definition-based classification.

1.108.2 Command Mode

- ATM PVC configuration
- dot1q PVC configuration
- Frame Relay PVC configuration
- link group configuration
- port configuration

1.108.3 Syntax Description

group-num	PD QoS priority number. By default, packets with a value of 0 receive the highest priority treatment and 7 receive the lowest. The range of values is 0 to 7.

1.108.4 Default

The initial PD QoS priority value of packets received on the circuit is set according to a default value as described in the Usage Guidelines section.

1.108.5 Usage Guidelines

Use the **qos priority** command to set the internal PD QoS priority field of all packets received on the circuit to a fixed value.

The PD QoS priority determines a packet's priority on the SmartEdge router packet switching fabric and priority for purposes of class-definition-based classification. The type of service (ToS) value, IP Differentiated Services Code Point (DSCP) value, and Multiprotocol Label Switching (MPLS) experimental (EXP) bits are not changed by this command. The actual queue number depends upon the queuing policy and queue-map; see the queue-map and queue-priority commands.

Note: A packet's initial PD QoS priority assignment can be subsequently modified by marking operations specified by QoS policing and metering policies (see **mark priority** and the related policing and metering commands).

Note: Configuring the **qos priority** command on an ATM port is not supported. To classify ATM traffic with a PD QoS priority number, configure the **qos priority** command on ATM PVCs.

This command is not supported for dynamic 802.1Q permanent virtual circuits (PVCs).

Use the **no** or **default** form of this command to remove any existing QoS priority configuration and to revert the circuit to assigning the default PD QoS priority value to all packets received on the circuit. The default PD QoS value depends on the circuit type:

- Layer 3 circuits (that is, circuits with a traffic binding such as to an IP interface or subscriber that results in the packets being forwarded by IP routing)— For IPv4 traffic, the initial PD QoS priority value of received packets is based on the upper three bits of the DSCP value in the Type of Service (ToS) field of the packet's IP header; see Table 8. For IPv6 traffic, the initial PD QoS priority value of received packets is based on the Traffic Class field of the packet's IP header.

- Layer 2 circuits (that is, circuits that have a non-IP-routed traffic binding such as to a bridged interface, Layer 2 cross-connect, or Layer 2 VPN)—The initial PD QoS priority value is 7, which is the lowest value.

- MPLS circuits—The initial PD QoS priority value of packets received by a SmartEdge router functioning as an MPLS transit router is determined based on the EXP field of the packet's MPLS header; see Table 9.

Table 8 Default Mapping for Layer 3 Circuits: DSCP Value to PD QoS Priority Value

DSCP Value	PD QoS Priority
CS7	0
CS6	1
CS5, EF	2
CS4, AF4*n*	3
CS3, AF3*n*	4
CS2, AF2*n*	5
CS1, AF1*n*	6
CS0, DF	7

Table 9 Default Mapping for MPLS Circuits: MPLS EXP Value to PD QoS Priority Value

MPLS EXP Value	PD QoS Priority Value
7	0
6	1
5	2
4	3
3	4
2	5
1	6
0	7

The **no** or **default** form of this command does not require you to specify the ***group-num*** argument.

1.108.6 Examples

The following example assigns a priority of **2** to packets received on port **1** on the Ethernet traffic card in slot **13:**

```
[local]Redback(config)#port ethernet 13/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface eth-pc05 local
[local]Redback(config-port)#qos priority 2
```

1.109 qos profile overhead (global)

qos profile ***profile-name*** **overhead**

no qos profile ***profile-name*** **overhead**

1.109.1 Purpose

Creates or selects a quality of service (QoS) overhead profile and enters overhead profile configuration mode.

1.109.2 Command Mode

- global configuration

1.109.3 Syntax Description

This command has no keywords or arguments.

1.109.4 Default

No overhead profile is created.

1.109.5 Usage Guidelines

Use the **qos profile overhead** command to create or select a QoS overhead profile and enter overhead profile configuration mode. For more information about overhead profiles, see *Overhead Profiles*.

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

1.109.6 Examples

The following example creates the **example1** overhead profile:

```
[local]Redback(config)#qos profile example1 overhead
```

1.110 qos profile overhead

qos profile overhead ***profile-name*** [**inherit**]

no qos profile overhead ***profile-name*** [**inherit**]

1.110.1 Purpose

Attaches an overhead profile to a port, a link group, a subscriber record, or an 802.1Q permanent virtual circuit (PVC) to configure how shaping rate calculations take into account packet headers used for encapsulation..

1.110.2 Command Mode

- port configuration
- link group configuration
- subscriber configuration
- dot1q PVC configuration

1.110.3 Syntax Description

profile-name	Name of the existing overhead profile to be attached to the port, link group, subscriber record, or 802.1Q PVC.
inherit	Optional. Applies the overhead profile to any child circuit configured on an 802.1Q PVC that is configured on this Ethernet port (unless it is overridden by a quality of service [QoS] overhead profile attached to the circuit). This keyword is available only for Ethernet ports, link groups, and 802.1Q PVCs. Inheritable QoS attributes applied to constituent ports of a link group are inherited by and applied to the aggregate PVCs defined under the link group.

1.110.4 Default

No overhead profile is attached to any entity.

1.110.5 Usage Guidelines

Use the **qos profile overhead** command to attach an overhead profile to a port, link group, subscriber record, or 802.1Q PVC. The overhead profiles command modifies how shaping rate calculations take into account packet headers used for encapsulation.

Note: You must also configure the **qos policy queuing** command for this command to take effect.

The **qos profile overhead** command also enters overhead profile configuration mode, where you can configure the following commands:

- **encaps-access-line**—Sets the encapsulation overhead on the access line
- **rate-factor**—Sets the rate factor for the overhead profile
- **reserved**—Sets the number of reserved bytes per packet
- **type**—Sets the access line type

Use the **inherit** keyword with the **qos profile overhead** command to apply the overhead profile to any configured child circuit (unless it is overridden by a QoS overhead profile attached to that circuit). If you do not specify the **inherit** keyword, the child circuits do not inherit the overhead profile of the parent.

Note: The **inherit** keyword is not available when you apply an overhead profile to a subscriber record.

Use the **no** form of this command to delete an overhead profile from an entity.

For more information about overhead profiles, see *Overhead Profiles*.

1.110.6 Examples

The following example allows the child circuits of the 802.1Q PVC to inherit the **example1** overhead profile:

```
[local]Redback(config)#port ethernet 2/1
[local]Redback(config-port)#dot1q pvc 100 encapsulation 1qtunnel
[local]Redback(config-port)#qos profile overhead example1 inherit
[local]Redback(config-port)#exit
```

1.111 qos pwfq scheduling

qos pwfq scheduling {**physical-port** | **virtual-port**}

{**no** | **default**} **qos pwfq scheduling**

1.111.1 Purpose

Enables an access link group to use priority weighted fair queuing (PWFQ) or traffic management (TM) scheduling and specifies a scheduling mode.

1.111.2 Command Mode

link group configuration

1.111.3 Syntax Description

physical-port	Use the physical-port PWFQ scheduling mode. Restricts link-group membership to cards that support PWFQ on physical ports.
virtual-port	Use the virtual-port PWFQ scheduling mode. Restricts link-group membership to cards that support PWFQ on virtual ports, such as a 10 GE 4-port card.

1.111.4 Usage Guidelines

Use the **qos pwfq scheduling** command to enable an access link group to use PWFQ (or TM) scheduling and specify the scheduling mode. If the link group consists of ports from a 10 GE 4-port card, specify virtual-port PWFQ scheduling mode using the **virtual-port** keyword. For dot1q PVCs created under a link access group (LAG) to be members of a virtual-port circuit group, the link group must have the PWFQ scheduling mode set to **virtual-port**. If the link group consists of ports from other TM-capable traffic cards, specify the physical-port mode using the **physical-port** keyword.

Note: No PWFQ- or TM-related configuration can be applied under a link group until the **qos pwfq scheduling** command has been configured for the link group.

For more information about virtual ports, see *Hierarchical Scheduling in Virtual-port TM* and *Virtual Port Circuit Groups*.

1.111.5 Examples

The following example shows how to enable the link group LG2 to use physical-port PWFQ scheduling mode:

```
[local]Redback(config)#link-group LG2 access
[local]Redback(config-link-group)#qos pwfq scheduling physical-port
```

The following example shows how to enable the link group LG4 to use virtual-port PWFQ scheduling mode:

```
[local]Redback(config)#link-group LG4 access
[local]Redback(config-link-group)#qos pwfq scheduling virtual-port
```

1.112 qos queue-map

qos queue-map ***map-name***

no qos queue-map ***map-name***

1.112.1 Purpose

Creates a quality of service (QoS) queue map and enters queue map configuration mode.

1.112.2 Command Mode

global configuration

1.112.3 Syntax Description

map-name	Queue map name.

1.112.4 Default

The SmartEdge router assigns PD QoS priority groups to queues as listed in the Usage Guidelines section.

1.112.5 Usage Guidelines

Use the **qos queue-map** command to create a QoS queue map and enter queue map configuration mode. You can create up to three customized queue maps.

By default, the SmartEdge router maps PD QoS priority groups, Differentiated Services Code Point (DSCP) classes, IP precedence values, Multiprotocol Label Switching (MPLS) experimental (EXP) bits, and Ethernet 802.1p bits to the specified number of queues as shown in Table 10.

Table 10 Default Mapping of Packets into Queues Using Priority Groups

Priority Group	DSCP Value(1)	IP Prec	MPLS EXP	802.1p	8 Queues	4 Queues	2 Queues	1 Queue
0	Network control	7	7	7	Queue 0	Queue 0	Queue 0	Queue 0
1	Reserved	6	6	6	Queue 1	Queue 1	Queue 1	Queue 0
2	Expedited Forwarding (EF)	5	5	5	Queue 2	Queue 1	Queue 1	Queue 0
3	Assured Forwarding (AF) level 4	4	4	4	Queue 3	Queue 2	Queue 1	Queue 0
4	AF level 3	3	3	3	Queue 4	Queue 2	Queue 1	Queue 0
5	AF level 2	2	2	2	Queue 5	Queue 2	Queue 1	Queue 0
6	AF level 1	1	1	1	Queue 6	Queue 2	Queue 1	Queue 0
7	Default Forwarding (DF)	0	0	0	Queue 7	Queue 3	Queue 1	Queue 0

(1) For more information about DSCP values, see RFC 2474, ***Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*** *and RFC 2475,* ***An Architecture for Differentiated Services****.*

Use the **num-queues** command (in queue map configuration mode) to specify the number of queues for the queue map, and then use the **queue priority** command (in num-queues configuration mode) to customize the mapping of one or more PD QoS priority groups to each queue. Finally, use the **queue-map** command (in ATMWFQ policy or PWFQ policy configuration mode) to assign the queue map to a scheduling policy.

Use the **no** form of this command to remove the QoS queue map from the configuration.

1.112.6 Examples

The following example configures the QoS queue map, **qmap**, and changes the default mapping of PD QoS priority groups to queues when **4** queues are configured:

```
[local]Redback(config)#qos queue-map qmap
[local]Redback(config-queue-map)#num-queues 4
[local]Redback(config-num-queues)#queue 0 priority 0 1
[local]Redback(config-num-queues)#queue 1 priority 2 3 4 5
[local]Redback(config-num-queues)#queue 2 priority 6
[local]Redback(config-num-queues)#queue 3 priority 7
```

1.113 qos rate

For traffic-managed ports, or the 802.1Q tunnels or permanent virtual circuits (PVCs) configured on them, the syntax is:

qos rate {**maximum** | **minimum**} ***kbps***

no qos rate {**maximum** | **minimum**}

For all other Gigabit Ethernet ports, the syntax is:

qos rate maximum ***mbps*** **burst** ***bytes***

no qos rate maximum

1.113.1 Purpose

Sets the rate for outgoing traffic on a Gigabit Ethernet port, or on an 802.1Q tunnel, 802.1Q PVC, or hierarchical node group or node configured on a traffic-managed port.

1.113.2 Command Mode

- dot1q PVC configuration
- hierarchical node configuration
- hierarchical node group configuration
- port configuration

1.113.3 Syntax Description

maximum	Specifies the maximum rate for the port, tunnel, PVC, or hierarchical node group, or hierarchical node.
minimum	Specifies the minimum rate for the port; available only for traffic-managed ports and the 802.1Q tunnels, PVCs, and hierarchical node groups, and hierarchical nodes configured on them.
kbps	Rate in kbps for traffic-managed ports, tunnels, PVCs, and hierarchical node groups. In hierarchical node and hierarchical node group configuration modes, the range of values is 64 to 1,000,000; in dot1q PVC and port configuration modes, the range of values is 10,000 to 1,000,000.
mbps	Rate in Mbps for all other Gigabit Ethernet ports. The range of values is 100 to 1,000; the default value is 1,000 (the full speed of the port).
burst ***bytes***	Burst tolerance in bytes. For all other Gigabit Ethernet ports except traffic-managed ports, the range of values is 1 to 4,250,000,000. This construct is not available for traffic-managed ports.

1.113.4 Default

Outgoing traffic is transmitted at the full speed of the port.

1.113.5 Usage Guidelines

Use the **qos rate** command to set the maximum rate for outgoing traffic on a Gigabit Ethernet port, or an 802.1Q tunnel, 802.1Q PVC, or hierarchical node group or node configured on a traffic-managed port. You can set the burst for any Gigabit Ethernet port, except for a traffic-managed port.

If you have not already entered the **qos hierarchical mode strict** command (in port or dot1q PVC configuration mode) for this tunnel or PVC, this command also makes the tunnel or PVC a node in the hierarchy. A Gigabit Ethernet 3 port is always a node at the top of the hierarchy.

Note: The maximum rate set by this command is the rate at which the port operates; any priority weighted fair queuing (PWFQ) queue or circuit with a PWFQ policy is limited by the rate specified by this command for the circuit. Also, the sum of all traffic on the port carried by the queues belonging to the circuits or subscribers is limited to the rate specified by this command.

Use the **no** form of this command to set the port, tunnel, or PVC to the default port rate.

Note: When you first configure the **qos hierarchical mode strict**, **qos rate**, or **qos weight** command for a dot1q PVC, the SmartEdge router removes previously configured QoS policy queuing commands on the circuit or any of its children. Configuring one of these commands on a circuit group for the first time deletes any QoS policy queuing commands on its existing members, and adding a member to a circuit group that has a configured L3 command removes all QoS policy queuing commands configured on the member circuit. To address this issue, reconfigure these QoS policy queuing commands.

1.113.6 Examples

The following example sets the maximum rate for outgoing traffic for port **1** on the Gigabit Ethernet traffic card in slot **14** to **600** Mbps with a burst size of **1,000** bytes:

```
[local]Redback(config)#port ethernet 14/1
[local]Redback(config-port)#qos rate maximum 600 burst 1000
```

1.114 qos to atm

qos {*pd-value* | **all**} **to atm** *clp-value*

{**no** | **default**} **qos** {*clp-value* | **all**}

1.114.1 Purpose

Translates packet descriptor (PD) quality of service (QoS) values to Asynchronous Transfer Mode (ATM) cell loss priority (CLP) values on egress.

1.114.2 Command Mode

class map configuration

1.114.3 Syntax Description

pd-value	An integer from 0 to 63 (six bits), with the packet priority encoded in three higher-order bits and the packet drop precedence in the three lower-order bits. You can enter the value in decimal or hexadecimal format, for example **16** or **0x10**. You can also enter a standard Differentiated Services Code Point (DSCP) marking label as defined in *DSCP Class Keywords*. The scale used by this command for packet priority, from 0 (lowest priority) to 7 (highest priority), is the relative inverse of the scale used by the **mark priority** command. For details on this command, see *Configuring Rate-Limiting and Class-Limiting*.
all	Maps all valid values for the source value to the specified target value. Any existing configuration for the classification map is overridden.
clp-value	Either 0 or 1. In case of network congestion, ATM cells marked with a value of 1 have been tagged to be dropped ahead of those with a value of 0.

1.114.4 Default

Egress ATM classification map entries use the default PD-to-CLP mapping described in Table 11.

1.114.5 Usage Guidelines

Use the **qos to atm** command to translate PD QoS values to ATM CLP values on egress.

If you specify the **all** keyword, all valid PD QoS values are mapped to the specified CLP 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 **no** or **default** form of this command to revert values for one or all map entries to their default values defined in Table 11.

Table 11 ATM CLP Bits Mapped to the PD QoS Value

ATM CLP Bit	PD Priority Value	PD Drop-Precedence Value	DSCP Label	QoS PD Value
0	1	2	AF11	10
1	0	0	DF	0

1.115 qos to ethernet

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

default qos {*pd-value* | **all**}

1.115.1 Purpose

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

1.115.2 Command Mode

class map configuration

1.115.3 Syntax Description

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

1.115.4 Default

None

1.115.5 Usage Guidelines

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

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

Use the **default** form of this command to revert one or all Ethernet 802.1p values to either the default 8P0D or mapping schema values, if a mapping schema has been specified.

1.115.6 Examples

The following example defines the classification map **pd-to-8021p** for Ethernet 802.1p values on egress, then maps the **af33** and **af21** PD QoS values to Ethernet 802.1p values **1** and **7**, respectively:

```
[local]Redback(config)#qos class-map pd-to-8021p ethernet out
[local]Redback(config-class-map)#qos af33 to ethernet 1
[local]Redback(config-class-map)#qos af21 to ethernet 7
```

1.116 qos to ip

qos {*pd-value* | **all**} **to ip** *dscp-value*

default qos {*dscp-value* | **all**}

1.116.1 Purpose

Translates packet descriptor (PD) quality of service (QoS) values to Differentiated Services Code Point (DSCP) values in the IP header on egress.

1.116.2 Command Mode

class map configuration

1.116.3 Syntax Description

pd-value	An integer from 0 to 63 (six bits), with the packet priority encoded in three higher-order bits and the packet drop precedence in the three lower-order bits. You can enter the value in decimal or hexadecimal format, for example **16** or **0x10**. You can also enter a standard DSCP marking label as defined in *DSCP Class Keywords*. The scale used by this command for packet priority, from 0 (lowest priority) to 7 (highest priority), is the relative inverse of the scale used by the **mark priority** command. For details on this command, see *Configuring Rate-Limiting and Class-Limiting*.
all	Maps all valid values for the source value to the specified target value. Any existing configuration for the classification map is overridden.
dscp-value	An integer from 0 to 63 representing the contents of the most significant six bits of the Type of Service (ToS) field in the IP header. You can enter the value in decimal or hexadecimal format, for example **16** or **0x10**. You can also enter a standard DSCP marking label as defined in *DSCP Class Keywords*.

1.116.4 Default

None

1.116.5 Usage Guidelines

Use the **qos to ip** command to translate PD QoS values to DSCP values in the IP header on egress.

If you specify the **all** keyword, all valid PD QoS values are mapped to the specified IP header values. 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 values for one or all map entries to their default values, where each PD QoS value is mapped to the equivalent DSCP value.

1.116.6 Examples

The following example defines the classification map **pd-to-dscp** for IP values on egress, then maps the **af13** PD QoS value to all DSCP values. It then overrides this mapping for PD QoS values **25** and **df**, which are mapped to DSCP values **af21** and **1**, respectively:

```
[local]Redback(config)#qos class-map pd-to-dscp ip out
[local]Redback(config-class-map)#qos all to ip af13
[local]Redback(config-class-map)#qos 25 to ip af21
[local]Redback(config-class-map)#qos df to ip 1
```

1.117 qos to mpls

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

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

1.117.1 Purpose

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

1.117.2 Command Mode

class map configuration

1.117.3 Syntax Description

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

1.117.4 Default

None

1.117.5 Usage Guidelines

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

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

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

1.117.6 Examples

The following example defines the classification map **pd-to-exp** for MPLS values on egress, then maps the **ef** and **df** DSCP bits to MPLS EXP bits **7** and **1**, respectively:

```
[local]Redback(config)#qos class-map pd-to-exp mpls out
[local]Redback(config-class-map)#qos ef to mpls 7
[local]Redback(config-class-map)#qos df to mpls 1
```

1.118 qos use-ip

qos {***pd-value*** | **all**} **use-ip** [***class-map-name***]

default qos {***pd-value*** | **all**}

1.118.1 Purpose

For outgoing IP packets, determines the 802.1p or Multiprotocol Label Switching (MPLS) experimental (EXP) values by mapping Differentiated Services Code Point (DSCP) values, based on the specified PD QoS value.

1.118.2 Command Mode

class map configuration

1.118.3 Syntax Description

pd-value	An integer from 0 to 63 (six bits), with the packet priority encoded in three higher-order bits and the packet drop precedence in the three lower-order bits. You can enter the value in decimal or hexadecimal format, for example **16** or **0x10**. You can also enter a standard DSCP marking label as defined in *DSCP Class Keywords*. The scale used by this command for packet priority, from 0 (lowest priority) to 7 (highest priority), is the relative inverse of the scale used by the **mark priority** command. For details on this command, see *Configuring Rate-Limiting and Class-Limiting*.
all	Maps all valid values for the source value to the specified target value. Any existing configuration for the classification map is overridden.
use-ip	Enables a secondary mapping lookup using the packet's DSCP bits as input. If no classification map is specified for the secondary lookup, the default DSCP-to-target mapping is used. When configuring a classification map for use as a secondary classification map on egress, omit the **use-ip** keyword.
class-map-name	Optional. Name of the classification map.

1.118.4 Default

None

1.118.5 Usage Guidelines

For outgoing packets, use the **qos use-ip** command to determine the final 802.1p or Multiprotocol Label Switching (MPLS) experimental (EXP) value based on the DSCP value in the IP header with the specified PD QoS value. Each packet is scheduled according to the PD QoS value, but the MPLS or Ethernet header is marked with the egress packet's DSCP values rather than the PD QoS values.

If you specify the **all** keyword, all PD QoS value entries use DSCP-based mappings. 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 DSCP values are mapped to 802.1p values according to the specified secondary classification map. The SmartEdge router interprets QoS-to-Ethernet or Qos-to-MPLS entries as if the QoS value actually specified a DSCP value. For example, the entry **qos 1 to ethernet 2** actually maps DSCP value **1** to 802.1p value **2**.

The secondary classification map must have the same values for the ***marking-type*** argument and mapping direction as the primary classification map and cannot include any **use-ip** classification map entries. If you do not specify a secondary classification map, the default DSCP-to-target mapping is used.

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

1.118.6 Examples

The following example defines the classification map **pd-to-exp** for MPLS values on egress and specifies **6P2D** as the default mapping schema. Then, it specifies to map PD values to DSCP values rather than QoS values, using the secondary classification map **dscp-to-exp** for translation. Finally, it maps PD bit **af33** to MPLS bit **4**, and QoS bit to the corresponding DSCP value:

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

1.119 qos weight

qos weight *weight*

no qos weight *weight*

1.119.1 Purpose

Assigns to this circuit a relative weight that is used to calculate a traffic ratio for all circuits configured on a traffic-managed port.

1.119.2 Command Mode

- dot1q PVC configuration
- hierarchical node configuration
- hierarchical node group configuration

1.119.3 Syntax Description

weight	Relative weight that is assigned to this circuit. The range of values is 1 to 4096.

1.119.4 Default

All circuits configured on this port have the same weight.

1.119.5 Usage Guidelines

Use the **qos weight** command to assign to this circuit a relative weight that is used to calculate a traffic ratio for all circuits configured on a traffic-managed port.

You can assign a relative weight, or you can set a minimum absolute rate, for the circuit, using the **qos rate** command (in dot1q PVC, hierarchical node, or hierarchical node group configuration mode), but you cannot do both; the relative weight and minimum absolute rate are mutually exclusive.

You can assign a relative weight (using this command) and set a maximum absolute rate for the circuit, using the **qos rate** command (in dot1q PVC, hierarchical node, or hierarchical node group configuration mode).

For 802.1Q permanent virtual circuits (PVCs), this command can be used to configure both static and on-demand PVCs.

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

Note: When you first configure the **qos hierarchical mode strict**, **qos rate**, or **qos weight** command for a dot1q PVC, the SmartEdge router removes previously configured QoS policy queuing commands on the circuit or any of its children. Configuring one of these commands on a circuit group for the first time deletes any QoS policy queuing commands on its existing members, and adding a member to a circuit group that has a configured L3 command removes all QoS policy queuing commands configured on the member circuit. To address this issue, reconfigure these QoS policy queuing commands.

1.119.6 Examples

The following example specifies a weight of **3** for the hierarchical nodes **dslam 1** through **dslam 5**:

```
[local]Redback(config)#port ethernet 5/2
[local]Redback(config-port)#qos rate maximum 100000000
[local]Redback(config-port)#qos node-group home 1
[local]Redback(config-h-node)#qos hierarchical mode strict
[local]Redback(config-h-node)#qos node dslam 1 through 5
[local]Redback(config-h-node)#qos weight 3
```

1.120 query-interval

query-interval ***interval***

1.120.1 Purpose

Configures the interval at which IGMP group-specific host query messages are sent on a specified bridge.

1.120.2 Command Mode

IGMP snooping bridge configuration

1.120.3 Syntax Description

interval	Interval at which IGMP group-specific host query messages are sent. The interval ranges from 1 through 65535 seconds. The default interval is 125 seconds.

1.120.4 Default

The default interval is 125 seconds.

1.120.5 Usage Guidelines

Use the **query-interval** command to configure the interval at which IGMP group-specific host query messages are sent on a specified bridge. Range is from 1 through 65535 seconds.

1.120.6 Examples

The following example shows how to configure a bridge called `sj1` to send IGMP group-specific host query messages every 185 seconds:

```
[local]Redback(config-ctx)#bridge sj1
[local]Redback(config-bridge)#igmp snooping
[local]Redback(config-igmp-snooping)#query-interval 185
```

1.121 query-max-response-time

query-max-response-time ***interval***

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

1.121.1 Purpose

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

1.121.2 Command Mode

IGMP snooping configuration

1.121.3 Syntax Description

interval	Interval, in seconds, specified in IGMP queries.

1.121.4 Default

The default IGMP maximum response time is 10 seconds.

1.121.5 Usage Guidelines

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

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

1.121.6 Examples

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

```
[local]Redback(config)#context blue
[local]Redback(config-ctx)#bridge metro
[local]Redback(config-bridge)#igmp snooping
[local]Redback(config-igmp-snooping)#query-max-response-time 20
```

1.122 query-solicitation

query-solicitation

no query-solicitation

1.122.1 Purpose

Enables and disables the generation of IGMP query solicitation messages by a bridge.

1.122.2 Command Mode

- IGMP snooping configuration

1.122.3 Syntax Description

This command has no keywords or arguments.

1.122.4 Default

The generation of IGMP query solicitation messages by a bridge is enabled.

1.122.5 Usage Guidelines

Use the **query-solicitation** command to enable the generation of IGMP query solicitation messages by a bridge. Note that the generation of IGMP query solicitation messages by a bridge is enabled on all bridges by default; use the **query-solicitation** command only if IGMP query solicitation was disabled on the bridge with the **no query-solicitation** command.

Bridges that have IGMP snooping enabled forward query solicitation messages to all IGMP routers in a system. If the interface over which an IGMP query solicitation message is received has IGMP query solicitation enabled, the router responds to IGMP query messages with an IGMP general query message.

Note: For IGMP query solicitation to work, IGMP query solicitation must also be enabled on the interface over which IGMP query messages and general response messages are exchanged. Use the **igmp query solicitation** command in interface configuration mode to enable the generation of IGMP query solicitation messages by an interface.

Use the **no** form of this command to disable the generation of IGMP query solicitation messages by a bridge.

1.122.6 Examples

The following example shows how to enable the generation of IGMP query solicitation messages by a bridge (`br-sj-1`) on which the generation of IGMP query solicitation messages was disabled:

```
[local]Redback(config)#context blue
[local]Redback(config-ctx)#bridge metro
[local]Redback(config-bridge)#igmp snooping
[local]Redback(config-igmp-snooping)#query-solicitation
```

1.123 queue 0 mode

queue 0 mode {**alternate** | **strict**}

default queue 0 mode

1.123.1 Purpose

Defines the mode of the Asynchronous Transfer Mode weighted fair queuing (ATMWFQ) algorithm for queue 0.

1.123.2 Command Mode

ATMWFQ policy configuration

1.123.3 Syntax Description

alternate	Services queue 0 and the other queues configured on the circuit in alternating fashion.
strict	Indicates that queue 0 always has priority over all other queues configured on the circuit.

1.123.4 Default

The default mode is alternate.

1.123.5 Usage Guidelines

Use the **queue 0 mode** command to define the mode of the ATMWFQ policy algorithm for queue 0.

In alternate mode, the servicing of queues alternates between queue 0 and the remaining queues. Queue 0 is served, then the next queue is served. Queue 0 is served again, and the next queue in turn is served, and so on. For example, if there are 4 queues configured, the order of servicing will be q0, q1, q0, q2, q0, q3, q0, q1, and so on.

In strict mode, high-priority queue 0 is serviced immediately and other queues are serviced in a round-robin fashion; in other words, queue 0 always has priority over all other queues configured on the circuit.

Use the **default** form of this command to return the ATMWFQ algorithm to alternate mode.

1.123.6 Examples

The following example configures the ATMWFQ policy to use **strict** mode:

```
[local]Redback(config)#qos policy atm-wfq-1 atmwfq
[local]Redback(config-policy-atmwfq)#queue 0 mode strict
```

1.124 queue congestion epd

queue *queue-num* **congestion epd threshold** *max*

{**no** | **default**} **queue** *queue-num* **congestion epd**

1.124.1 Purpose

Configure early packet discard (EPD) parameters for this quality of service (QoS) Asynchronous Transfer Mode weighted fair queuing (ATMWFQ) policy.

1.124.2 Command Mode

- ATMWFQ policy configuration

1.124.3 Syntax Description

queue-num	Queue number. The range of values is 0 to 7.
threshold *max*	EPD threshold value. The number of packets (equivalent to six ATM cells) that can be in the queue before new incoming packets begin to be discarded. The range of values is 2 to 10,000; the default value is 26.

1.124.4 Default

Random early discard (RED) is enabled for Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs) (on second-generation ATM OC traffic cards only) that reference the ATMWFQ policy.

1.124.5 Usage Guidelines

Use the **queue congestion epd** command to configure EPD parameters for the specified ATMWFQ policy.

With EPD, a threshold is set for the number of packets (equivalent to 6 ATM cells) that can be in the queue before any new incoming packets begin to be discarded. Incoming packets are broken into cells as they are being placed in the queue. If there is enough space in the queue to accept the first cell of a packet, the remaining cells in the packet are admitted. If not, the entire packet is dropped. When an entire packet is dropped, the queue is placed into EPD mode until enough packets have been sent out such that the number of packets in the queue is below the **threshold** *max* value.

Use the **no** or **default** form of this command to use the default EPD value.

Caution!

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

1.124.6 Examples

The following example specifies the EPD threshold for the **atmwfq-1** policy for queue 4:

```
[local]Redback(config)#qos policy atmwfq-1 atmwfq
[local]Redback(config-policy-atmwfg)#queue 4 congestion epd threshold 5200
```

1.125 queue congestion

queue ***queue-num*** **congestion** {**epd threshold** ***max*** | **red max-threshold** ***max*** **min-threshold** ***min*** **probability** ***prob*** **weight** ***weight-exp***}

queue ***queue-num*** **congestion** {**epd** | **red**}

1.125.1 Purpose

Configure early packet discard (EPD) parameters or modify the weighted random early detection (RED) for this quality of service (QoS) Asynchronous Transfer Mode (ATM) weighted-fair queueing (WFQ) policy.

1.125.2 Command Mode

- ATMWFQ policy configuration

1.125.3 Syntax Description

queue-num	Queue number. The range of values is 0 to 7.
epd threshold ***max***	EPD threshold value. The number of packets (equivalent to six ATM cells) that can be in the queue before new incoming packets begin to be discarded. Incoming packets are broken into cells as they are being placed in the queue. If there is enough space in the queue to accept the first cell of a packet, the remaining cells in the packet are admitted. If not, the entire packet is dropped. When an entire packet is dropped, the queue is placed into EPD mode until enough packets have been sent out such that the number of packets in the queue is below the **threshold** ***max*** value.
red	Specifies that RED parameters are to be modified.
min-threshold ***min***	Average queue occupancy in packets below which no packets are dropped. The range of values is 1 to 9,999; the default value is eight packets.
max-threshold ***max***	Average queue occupancy in packets above which all packets are dropped. As the average occupancy approaches the maximum threshold value, packets are dropped with increasing probability, as a function of the value of the **probability** ***prob*** value. The range of values is 2 to 10,000; the default value is 26 packets.
probability ***prob***	Inverse of the probability of dropping a packet as the average queue occupancy approaches the maximum threshold. The higher the value of the ***prob*** argument, the lower the probability of a packet being dropped. The resulting probability (1/***prob***) is the fraction of packets dropped when the average queue depth is at the maximum threshold. The range of values is 8 to 32,768; the default value is 16.
weight ***weight-exp***	Exponent representing the inverse of the exponentially weighted moving average of traffic. The average queue occupancy is computed as a moving average of the instantaneous queue occupancy. Traffic weight is expressed as a unit of average packet size. The average packet size is equivalent to 6 ATM cells. The larger the value of the ***weight-exp*** argument, the longer term the average. The range of values is 7 to 10; the default value is 9.

1.125.4 Default

RED is enabled for ATM PVCs (second-generation ATM OC cards only) that reference the ATM WFQ policy.

1.125.5 Usage Guidelines

Use the **queue congestion** command to configure EPD parameters or to modify RED parameters for the specified ATM WFQ policy.

With EPD, a threshold is set for the number of packets (equivalent to 6 ATM cells) that can be in the queue before any new incoming packets begin to be discarded. Incoming packets are broken into cells as they are being placed in the queue. If there is enough space in the queue to accept the first cell of a packet, the remaining cells in the packet are admitted. If not, the entire packet is dropped. When an entire packet is dropped, the queue is placed into EPD mode until it enough packets have been sent out such that the number of packets in the queue is below the threshold.

RED signals to sources of traffic that the network is on the verge of entering a congested state. This signaling is accomplished by dropping packets with a probability that varies as a function of how many packets are waiting in a queue at any particular time, and of the values of the **threshold** ***max***, **threshold** ***min***, **probability** ***prob***, and **weight** ***weight-exp*** values.

Use the **default** or **no** form of this command to use the default EPD or RED value.

Caution!

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

1.125.6 Examples

The following example specifies the RED parameters for an existing profile, `atm-pro:`

```
[local]Redback(config)#qos policy atmwfq-1 atmwfq
[local]Redback(config-policy-atmwfg)#queue congestion red min-thresh 1 max-thresh 255 probab 15 weight 10
```

1.126 queue depth

queue ***queue-num*** **depth** ***count***

{no | default} queue ***queue-num*** **depth**

1.126.1 Purpose

Specifies the depth for the specified queue.

1.126.2 Command Mode

- MDRR congestion map configuration
- PWFQ congestion map configuration

1.126.3 Syntax Description

queue-num	Queue number. The range of values is 0 to 7.
count	Depth of the queue, expressed as the number of packets. The range of values is 1 to 64,000. The default value is 4,000.
packets ***count***	**Note:** The **packets** ***count*** keyword-variable syntax is no longer supported.

1.126.4 Default

4,000 packets for all queues, 0 through 7

Caution!

Each traffic card has a finite number of memory data units (MDUs) available that determine the total number of packets that can be concurrently queued for transmitting. If all MDUs are in use on an egress card, the card cannot queue additional packets for transmission, which can severely degrade throughput and egress scheduling. When a large number of queuing policy bindings are configured on a card (each representing a unique set of queues), MDUs can be exhausted. To help prevent this issue, configure a queue depth value that is smaller than the default when a large number of queuing bindings are to be used on a traffic card. Calculate the queue depth based on the number of MDUs available per card type and the worst-case MDU usage based on queuing policy configuration and expected packet size. See the Hardware Guide for the memory size for PPA2 and PPA3 cards. Guidance on this calculation is beyond the scope of this document.

1.126.5 Usage Guidelines

Use the **queue depth** command to specify the depth for the specified queue.

Do!

To avoid loss of system processes, use the following values for the depth (***count***) of the congestion map queues that are applied to MLPPP bundles:

- 33***n*** (for DS0 circuits, where **n** = the number of DS0 circuits in the MLPPP bundle.)
- 66***n*** (for DS1 circuits, where **n** = the number of circuits in the MLPPP bundle.)
- 66***n*** (for E1 circuits, where **n** = the number of circuits in the MLPPP bundle.)
- 448***n*** (for DS3 circuits, where **n** = the number of circuits in the MLPPP bundle.)

Use the following values for the depth (***count***) of the congestion map queues that are applied to individual POS channels:

- 33 (for individual DS0 POS circuits)
- 66 (for individual DS1 POS circuits)
- 66 (for individual E1 POS circuits)
- 448 (for individual DS3 POS circuits)

Note: Queue depth for ATM PVCs that are subject to ATMWFQ queuing policies or congestion maps is set by the **congestion** command in ATM profile configuration mode. This command does not apply to configuring an **atmwfq** congestion avoidance map.

Use the **no** or **default** form of this command to set the queue depth to the default value for the entity.

1.126.6 Examples

The following example sets the depth for queue **5**. The depth is rounded to the nearest increment of 32:

```
[local]Redback(config-congestion-map)#queue 5 depth 550
```

1.127 queue exponential-weight

queue ***queue-num*** **exponential-weight** ***weight-exp***

no queue ***queue-num*** **exponential-weight**

1.127.1 Purpose

Specifies a weight for the specified queue.

1.127.2 Command Mode

- congestion map configuration

1.127.3 Syntax Description

queue-num	Queue number. The range of values is 0 to 7.
weight-exp	Exponent representing the inverse of the exponentially weighted moving average. The range of values depends on the type of congestion avoidance map: • Priority weighted fair queuing (PWFQ) policy—The range of values is 1 to 15; the default value is 9. • Asynchronous Transfer Mode weighted fair queuing (ATMWFQ) policy—The range of values is 2 to 10 the default value is 9.

1.127.4 Default

The exponential weight is assigned the default value, depending on the type of congestion map.

1.127.5 Usage Guidelines

Use the **queue exponential-weight** command to specify a weight for the specified queue. The queue must be one that you have configured with random early detection (RED) parameters. The weight that you specify applies to every RED profile (**default**, **profile-1**, **profile-2**) for this queue.

The average queue occupancy is computed as a moving average of the instantaneous queue occupancy. Use the ***weight-exp*** argument to set the inverse of the exponential moving average. The larger the value of the ***weight-exp*** argument, the longer term the average.

The average queue size is based on the previous average and the current size of the queue according to the following formula:

average = (old_average * (1 - 0.5**w)) + (current_queue_size * ½**w)

where w is the value of the ***weight-exp*** argument * is the multiplication operator ** is the exponential operator

Use the **no** form of this command to specify the default exponential weight for the type of congestion map.

1.127.6 Examples

The following example specifies the weights for the **default** profile in the **map-red8** congestion avoidance map:

```
[local]Redback(config)#qos congestion-avoidance-map map-red8
[local]Redback(config-congestion-map)#queue 0 exponential-weight 1
[local]Redback(config-congestion-map)#queue 1 exponential-weight 2
[local]Redback(config-congestion-map)#queue 2 exponential-weight 1
[local]Redback(config-congestion-map)#queue 3 exponential-weight 1
[local]Redback(config-congestion-map)#queue 4 exponential-weight 10
[local]Redback(config-congestion-map)#queue 5 exponential-weight 1
[local]Redback(config-congestion-map)#queue 6 exponential-weight 1
[local]Redback(config-congestion-map)#queue 7 exponential-weight 1
```

1.128 queue-map

queue-map ***map-name***

no queue-map

1.128.1 Purpose

Assigns a queue map to the quality of service (QoS) scheduling policy.

1.128.2 Command Mode

- ATMWFQ policy configuration
- MDRR policy configuration
- PWFQ policy configuration

1.128.3 Syntax Description

map-name	Queue map name.

1.128.4 Default

No queue map is assigned to any QoS scheduling policy.

1.128.5 Usage Guidelines

Use the **queue-map** command to assign a queue map to the specified QoS scheduling policy.

To create a queue map, enter the **qos queue-map** command (in global configuration mode). To specify the number of queues for the queue map, enter the **num-queues** command (in queue map configuration mode). Use the **queue priority** command (in num-queues configuration mode) to customize the mapping of a PD QoS priority group to each queue.

Use the **no** form of this command to delete the queue map from the QoS policy. It does not need any arguments.

1.128.6 Examples

The following example assigns the queue map, **q-queue-map**, to the modified deficit round-robin (MDRR) configuration policy, **qos-mdrr-test**:

```
[local]Redback(config)#qos policy qos-mdrr-test mdrr
[local]Redback(config-policy-mdrr)#queue-map q-queue-map
```

1.129 queue priority (num-queues)

queue ***queue-num*** **priority** ***group-num*** [***group-num2***[...]]

no queue ***queue-num*** **priority**

1.129.1 Purpose

In num-queues configuration mode, customizes the mapping of packet descriptor (PD) quality of service (QoS) priority groups to the specified queue.

1.129.2 Command Mode

num-queues configuration

1.129.3 Syntax Description

queue-num	Queue number. The range of values is 0 to 7.
group-num	Priority group number. The range of values is 0 to 7.
group-num2 ***group-num3***..	Optional. Additional PD QoS priority group numbers separated by spaces. The range of values is 0 to 7.

1.129.4 Default

In num-queues configuration mode, the SmartEdge router assigns a preset mapping of PD QoS priority groups to queues; for information about the default values, see the **qos queue-map** command in the *Command List*.

1.129.5 Usage Guidelines

Use the **queue priority** command in num-queues configuration mode to customize the mapping of one or more PD QoS priority groups to the specified queue.

Note: In num-queues configuration mode, this command determines the relationship between the priority in the packet (according to the type of service [ToS] or Differentiated Service Code Point [DSCP] bits) and the queue to which the packed is assigned.

Note: Although the mapping of priority to queues is arbitrary, in general, the SmartEdge router assumes that there is a correspondence between the queue number and the scheduling priority, with queue 0 having the highest priority and queue 7 the lowest priority. You could cause performance problems if you assign a lower priority to queue 0 than the other queues. For example, internally generated control packets are assigned by default to queue 1; if you have assigned that queue a priority 7, they could be dropped due to congestion from priority 7 traffic.

For queue maps:

- To apply the customized mapping of PD QoS priority groups to queues, enter the **queue-map** command.
- In num-queues configuration mode, use the **no** form of this command to remove the customized mapping for the specified queue.

1.129.6 Examples

The following example configures the queue maps, **Custom2**, **Custom4**, **Custom8**, to customize the mapping of PD QoS priority groups to queues. The assignment of PD QoS priority group to queue number varies according to the number of queues configured. The custom mapping for **4** queues is referenced by the QoS policy, **myPolicyPQ:**

```
[local]Redback(config)#qos queue-map Custom2
[local]Redback(config-queue-map)#num-queues 2
[local]Redback(config-num-queues)#queue 0 priority 0
[local]Redback(config-num-queues)#queue 1 priority 1 2 3 4 5 6 7
[local]Redback(config-num-queues)#exit

[local]Redback(config)#qos queue-map Custom4
[local]Redback(config-queue-map)#num-queues 4
[local]Redback(config-num-queues)#queue 0 priority 0
[local]Redback(config-num-queues)#queue 1 priority 1 2
[local]Redback(config-num-queues)#queue 2 priority 3 4 5 6
[local]Redback(config-num-queues)#queue 3 priority 7
[local]Redback(config-num-queues)#exit

[local]Redback(config)#qos queue-map Custom8
[local]Redback(config-queue-map)#num-queues 8
[local]Redback(config-num-queues)#queue 0 priority 0
[local]Redback(config-num-queues)#queue 1 priority 1
[local]Redback(config-num-queues)#queue 2 priority 2
[local]Redback(config-num-queues)#queue 3 priority 3
[local]Redback(config-num-queues)#queue 4 priority 4
[local]Redback(config-num-queues)#queue 5 priority 5
[local]Redback(config-num-queues)#queue 6 priority 6
[local]Redback(config-num-queues)#queue 7 priority 7
[local]Redback(config-num-queues)#exit

[local]Redback(config)#qos policy MyPolicy pwfq
[local]Redback(config-policy-pwfq)#queue-map Custom4
[local]Redback(config-policy-pwfq)#num-queues 4

[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#bind interface BackboneOne local
[local]Redback(config-port)#qos policy queuing MyPolicy
```

1.130 queue priority (PWFQ)

In PWFQ policy configuration mode, the syntax is:

queue *queue-num* **priority** *group-num* **weight** *weight*

no queue *queue-num* **priority**

1.130.1 Purpose

In PWFQ policy configuration mode, assigns an egress queue to a particular PWFQ scheduling priority "tier" and establishes that queue's relative weight among other queues of the same priority.

1.130.2 Command Mode

PWFQ policy configuration

1.130.3 Syntax Description

queue-num	Queue number. The range of values is 0 to 7.
group-num	TM queue priority group number. The range of values is 0 to 7.
group-num2 group-num3..	Optional. Additional TM queue priority group numbers separated by spaces. The range of values is 0 to 7.
weight *weight*	Relative weight that is assigned to this queue for the specified TM queue priority group; available only for queues defined in priority weighted fair queuing (PWFQ) policies. The range of values is 5 to 100.

1.130.4 Default

In PWFQ policy configuration mode, there is no default.

1.130.5 Usage Guidelines

In PWFQ policy configuration mode, use the **queue priority** command to assign a traffic management (TM) queue priority group number and relative weight inside the assigned priority group to the specified queue.

Note: The relative weights assigned by this command in PWFQ policy configuration mode are within the specified TM queue priority group.

Note: In PWFQ policy configuration mode, this command assigns a queue to a TM priority group, which is not the same as the packet priority and which is used by the PWFQ scheduler to determine when the packets are scheduled for transmission.

Note: Although the mapping of priority to queues is arbitrary, in general, the SmartEdge router assumes that there is a correspondence between the queue number and the scheduling priority, with queue 0 having the highest priority and queue 7 the lowest priority. You could cause performance problems if you assign a lower priority to queue 0 than the other queues. For example, internally generated control packets are assigned by default to queue 1; if you have assigned that queue a priority 7, they could be dropped due to congestion from priority 7 traffic.

For PWFQ policies:

- You must enter this command for each queue you have defined for the policy with the **num-queues** command (in PWFQ policy configuration mode). The system displays an error message when you attach the policy to a port, tunnel, or permanent virtual circuit (PVC) if not all defined queues have a priority and weight assigned.
- Use the **weight** ***weight*** construct to specify the traffic share for each queue. The traffic share for each queue is calculated from the specified weight divided by the sum of the weights specified for all queues in the same TM queue priority group. For an example, see the Examples section.
- In PWFQ configuration mode, use the **no** form of this command to delete the queue.

1.130.6 Examples

The following example defines **4** queues for the PWFQ policy, **pwfq4**, and assigns them to TM priority groups **0** and **1** with relative weights **70**, **30**, **60**, **40**:

```
[local]Redback(config)#qos policy pwfq4 pwfq
[local]Redback(config-policy-pwfq)#num-queues 4
[local]Redback(config-policy-pwfq)#queue 0 priority 0 weight 70
[local]Redback(config-policy-pwfq)#queue 1 priority 0 weight 30
[local]Redback(config-policy-pwfq)#queue 2 priority 1 weight 60
[local]Redback(config-policy-pwfq)#queue 3 priority 1 weight 40
[local]Redback(config-policy-pwfq)#
```

In this example, in TM priority group `0` queue `0` receives 70% traffic share and queue `1` receives 30% traffic share; in TM priority group `1` queue `2` receives 60% traffic share and queue `3` receives 40% traffic share.

1.131 queue priority-group

queue priority-group *group-num* {**rate** *kbps* [**exceed**] | **percentage** *value* [**exceed**]}

no queue priority-group *group-num*

1.131.1 Purpose

Sets the rate for the specified traffic management (TM) priority group.

1.131.2 Command Mode

- PWFQ policy configuration

1.131.3 Syntax Description

group-num	Priority group number. The range of values is 0 to 7.
rate *kbps*	Absolute rate in kilobits per second for the specified TM queue priority group; the range of values is 64 to 1,000,000.
exceed	Optional. Allows the traffic rate to be exceeded for the specified TM queue priority group. The default condition is to not allow the traffic rate or percentage to be exceeded.
percentage *value*	Relative rate, as a percentage of the policy rate, for the specified TM queue priority group; the range of values is 1 to 100.

1.131.4 Default

None

1.131.5 Usage Guidelines

Use the **queue priority-group** command to set the rate for the specified TM queue priority group. You enter this command for each priority group created for this priority weighted fair queuing (PWFQ) policy.

A TM queue priority group is a set of queues that all have the same priority group number assigned to them with the **queue priority** command (in PWFQ policy configuration mode). You enter this command for each TM queue priority group.

Use the **rate** ***kbps*** construct to specify an absolute rate for the priority group; use the **percentage** construct to specify a relative rate. You specify the policy rate using the **rate** command (in PWFQ policy configuration mode).

Use the **no** form of this command to delete the priority group from the policy.

1.131.6 Examples

The following example sets the rate and burst tolerance for the TM queue priority groups in the PWFQ policy, **pwfq4**:

```
[local]Redback(config)#qos policy pwfq4 pwfq
[local]Redback(config-policy-pwfq)#num-queues 4
[local]Redback(config-policy-pwfq)#queue 0 priority 0 weight 70
[local]Redback(config-policy-pwfq)#queue 1 priority 0 weight 30
[local]Redback(config-policy-pwfq)#queue 2 priority 1 weight 60
[local]Redback(config-policy-pwfq)#queue 3 priority 1 weight 40
[local]Redback(config-policy-pwfq)#queue priority-group 0 rate 1800
[local]Redback(config-policy-pwfq)#queue priority-group 1 rate 1600
[local]Redback(config-policy-pwfq)#
```

The following example sets relative rates for the TM queue priority groups in the PWFQ policy, **pwfq-percent:**

```
[local]Redback(config)#qos policy pwfq2 pwfq
[local]Redback(config-policy-pwfq)#rate maximum 6000
[local]Redback(config-policy-pwfq)#num-queues 4
[local]Redback(config-policy-pwfq)#queue 0 priority 0 weight 100
[local]Redback(config-policy-pwfq)#queue 1 priority 1 weight 100
[local]Redback(config-policy-pwfq)#queue 2 priority 2 weight 60
[local]Redback(config-policy-pwfq)#queue 3 priority 2 weight 40
[local]Redback(config-policy-pwfq)#queue priority-group 0 percentage 10
[local]Redback(config-policy-pwfq)#queue priority-group 1 percentage 20
[local]Redback(config-policy-pwfq)#
```

1.132 queue rate

queue *queue-num* **rate** *kbps* **burst** *bytes*

no queue *queue-num* **rate**

1.132.1 Purpose

The **queue rate** command is no longer supported.

1.133 queue red

queue *queue-num* **red {default | {{profile-1 | profile-2} dscp** *class1* **[***class2* **[...]]} max-threshold** *max* **min-threshold** *min* **probability** *prob*

no queue *queue-num* **red** *profile*

1.133.1 Purpose

Sets the random early detection (RED) parameters for the specified RED drop profile of the specified queue for the congestion avoidance map.

1.133.2 Command Mode

congestion map configuration

1.133.3 Syntax Description

queue-num	Queue number. The range of values is 0 to 7.
default	Specifies the default RED profile in the congestion avoidance map for this queue. The default profile applies to all packets whose PD QoS value does not match one of those specified by profile-1 or profile-2, if they have been configured.
profile-1	Specifies an alternate RED profile in the congestion avoidance map for this queue. Profile 1 applies only to packets whose PD QoS value matches one of those specified for the profile using the **dcsp** *class* construct. Use this keyword with the **dscp** *class* construct.
profile-2	Specifies an alternate RED profile in the congestion avoidance map for this queue. Profile 2 applies only to packets whose PD QoS value matches one of those specified for the profile using the **dcsp** *class* construct. Use this keyword with the **dscp** *class* construct.
dscp *class1* **[***class2* **[...]]**	One or more Differentiated Services Code Point (DSCP) classes. An integer from 0 to 63 or one of the keywords listed in Table 12. Use spaces to separate multiple classes.
max-threshold *max*	Average queue occupancy, in packets, above which all packets are dropped. The range of values is 2 to 10,000
min-threshold *min*	Average queue occupancy, in packets, below which no packets are dropped. The range of values is 1 to 9,999.

probability ***prob***	Inverse of the probability of dropping a packet as the average queue occupancy approaches the maximum threshold. The range of values is 8 to 32,768.
weight ***weight-exp***	Exponent representing the inverse of the exponentially weighted moving average.

1.133.4 Default

For all QoS queuing policy types, RED is disabled by default and the egress scheduler will only tail-drop packets based their default or configured queue depth.

1.133.5 Usage Guidelines

Use the **queue red** command in congestion map configuration mode to set the RED parameters for a particular drop profile of the specified queue.

RED parameters specify how buffer utilization is to be managed under congestion by signaling to the sources of traffic that the network is on the verge of entering a congested state. This signaling is accomplished by dropping packets with a probability that varies as a function of how many packets are waiting in a queue at any particular time, and of the values of the ***max***, ***min***, and ***weight-exp*** arguments.

For circuits subject to an PWFQ, ATMWFQ, or MDRR queueing policy—Use the **queue red** command to configure a congestion avoidance map specifying at least the default RED profile for each desired queue. The queuing policy must reference the congestion avoidance map using the **congestion-map** command in the configuration mode for applicable queuing policies.

When configuring a congestion avoidance map, specify one of three RED profiles for the RED parameters for the queue. Each queue supports up to three RED profiles.

- **dscp** ***class1*** **[***class2*** [...]]**

  For any non-default RED profile, use the **dscp** ***class*** construct to specify one or more DSCP classes; seeTable 12 for the possible values of the ***class*** argument.

  DSCP class is relevant only to queues that use an alternate (non-default) RED profile in their congestion avoidance map.

  Note: DSCP class values are not determined by the DSCP value in the TOS field of a packet's IP header. Instead, the class specified here selects packets based on the internal PD QoS priority value. For more information on the PD QoS internal priority value, see *Configuring Circuits for QoS*.

- **max-threshold** ***max***

Sets the average queue occupancy in packets above which the probability of a packet being dropped is 100%. As the average occupancy approaches the maximum threshold value, packets are dropped with increasing probability, as a function of the value of the ***prob*** argument. The value of the ***max*** argument must be less than the value of the ***count*** argument in the **queue depth** command for the applicable queuing policy or congestion map.

- **min-threshold** ***min***

  Sets the average queue occupancy in packets at or below which the probability of a packet being dropped is 0%. The value of the ***min*** argument must be less than the value of the ***max*** argument in this command and less than the value of the ***count*** argument in the **queue depth** command for the applicable queuing policy or congestion-map.

- **probability** ***prob***

  Specifies the inverse of the probability of a packet being dropped when the average queue occupancy reaches the maximum threshold value; that is when the average queue depth reaches maximum threshold, the probability of a packet in the queue being dropped equals (1/*prob*).

  The average queue occupancy is computed as a moving average of the instantaneous queue occupancy. .

  The average queue size is based on the previous average and the current size of the queue according to the following formula:

  average = (old_average * (1 - 0.5**w)) + (current_queue_size * $^1/_2$**w)

  where w is the value of the ***weight-exp*** argument * is the multiplication operator ** is the exponential operator.

- **weight** ***weight-exp***

  Sets the inverse of the exponential moving average. The larger the value of the ***weight-exp*** argument, the longer term the average.

  Note: When configuring congestion maps, the exponential weight factor used for a queue's weight enforcement is configured using **queue exponential-weight** command.

Table 12 DSCP Class Keywords

DSCP Class	Keyword	DSCP Class	Keyword
Assured Forwarding (AF) Class 1/ Drop precedence 1	**af11**	Class Selector 0 (same as default forwarding)	**cs0** (same as **df**)
AF Class 1/Drop precedence 2	**af12**	Class Selector 1	**cs1**
AF Class 1/Drop precedence 3	**af13**	Class Selector 2	**cs2**
AF Class 2/Drop precedence 1	**af21**	Class Selector 3	**cs3**

Table 12 DSCP Class Keywords

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

Use the **no** form of this command to remove the RED profile from the specified queue.

1.133.6 Examples

The following example specifies the RED parameters for the **default** profile and queues **0** through **7** in the congestion avoidance map, **map-red:**

```
[local]Redback(config)#qos congestion-avoidance-map map-red8 mdrr
[local]Redback(config-congestion-map)#queue 0 red default prob 10 weight 12 min-thresh 1900 max-thresh 5200
[local]Redback(config-congestion-map)#queue 1 red default prob 9 weight 12 min-thresh 1850 max-thresh 5200
[local]Redback(config-congestion-map)#queue 2 red default prob 8 weight 12 min-thresh 1800 max-thresh 5200
[local]Redback(config-congestion-map)#queue 3 red default prob 7 weight 12 min-thresh 1750 max-thresh 5200
[local]Redback(config-congestion-map)#queue 4 red default prob 6 weight 12 min-thresh 1700 max-thresh 5200
[local]Redback(config-congestion-map)#queue 5 red default prob 5 weight 12 min-thresh 1650 max-thresh 5200
[local]Redback(config-congestion-map)#queue 6 red default prob 4 weight 12 min-thresh 1600 max-thresh 5200
[local]Redback(config-congestion-map)#queue 7 red default prob 1 weight 12 min-thresh 1550 max-thresh 5200
```

1.134 queue weight

queue ***queue-num*** **weight** ***traffic-weight***

default queue ***queue-num*** **weight**

1.134.1 Purpose

Specifies the weight of the specified Asynchronous Transfer Mode weighted fair queuing (ATMWFQ) or modified deficit round-robin (MDRR) queue.

1.134.2 Command Mode

- ATMWFQ policy configuration
- MDRR policy configuration

1.134.3 Syntax Description

queue-num	Queue number. The range of values is 0 to 7.
traffic-weight	For ATMWFQ policies, the traffic weight is expressed as a unit of average packet size. The average packet size is equivalent to 6 ATM cells. For example, a traffic weight of 2,000 is equivalent to 12,000 ATM cells. The range of values is 1 to 5,461; the default value is 2. For MDRR policies, the traffic weight is expressed as a percentage of bandwidth. The range of configurable values is 5 to 100%. The default value for MDRR is 0%.

1.134.4 Default

Default values for the ***traffic-weight*** argument are specified in the Syntax Description section.

1.134.5 Usage Guidelines

Use the **queue weight** command to specify the weight of the specified ATMWFQ, or MDRR queue.

Caution!

Risk of traffic loss. Modifying the parameters of an ATMWFQ policy momentarily interrupts the traffic on all Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs) using the policy. To reduce the risk, use caution when modifying ATMWFQ policy parameters.

Caution!

Risk of performance loss. For MDRR policies, you must assign a weight to each queue that is in use, as specified by either the default queue map or a customized queue map. To reduce the risk, ensure that you assign a weight to each queue.

Use the **default** form of this command to return the queue to its default weight.

1.134.6 Examples

The following example provides queue number **3** with **30**% of the bandwidth of the circuit to which the MDRR policy, **scheduling1**, is attached:

```
[local]Redback(config)#qos policy scheduling1 mdrr
[local]Redback(config-policy-mdrr)#queue 3 weight 30
```

Glossary

PWFQ
Priority weighted fair queuing.