ERICSSON

Configuring Rate-Limiting and Class-Limiting

SYSTEM ADMINISTRATOR GUIDE

55/1543-CRA 119 1170/1-V1 Uen H

Contents

1 Overview

This document provides an overview of the SmartEdge router rate- and class-limiting quality-of-service (QoS) features (metering and policing policies) and describes the tasks used to configure, monitor, and administer these features. This document also provides examples of rate- and class-limiting configurations.

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.

For information about other QoS configuration tasks and commands, see the following documents:

- *Configuring Queuing and Scheduling*—Scheduling features (scheduling policies)
- *Configuring Circuits for QoS*—Port, channel, and circuit configuration for all QoS policies and features
- *Configuring IP Multicast*—Configuring IGMP service profiles for QoS rate adjustment on multicast traffic.

The Internet provides only best-effort service, offering no guarantees on when or whether a packet is delivered to the receiver. However, the SmartEdge router differentiates traffic based on the subscriber record, the traffic type, and the application. QoS policies create and enforce quality of service levels, bandwidth rates, and prioritize how incoming and outgoing packets are scheduled. The SmartEdge router classifies, marks, and rate-limits incoming packets as described in the following sections.

1.1 PD QoS Priority Groups

Incoming packets can be classified by assignment to a packet descriptor (PD) QoS priority group. A priority group is an internal value used by the SmartEdge router to determine into which egress queue the inbound packet should be placed. The actual queue number depends upon the queue map used and the number of queues configured on the circuit. The type of service (ToS) value

and the IP Differentiated Services Code Point (DSCP) bits are not changed when assigned to a PD QoS priority group.

1.2 QoS Policing and Metering

A QoS policing policy can classify, mark, rate-limit, or perform all actions on incoming packets; a QoS metering policy performs the same operations for outgoing packets. You can apply both types of policies at one of two levels or at both levels, simultaneously. Either type of policy can apply to all packets on a particular circuit; this application is referred to as a circuit-based action. In addition or instead, you can define sections of a policy to apply to only a particular class of packets traveling across the circuit. The corresponding marking and rate-limiting actions defined in the policy are referred to as a class-based action. The criteria for assigning packets to classes are established by configuring a policy ACL or class-definition and referencing it in the policy.

1.2.1 Circuit-Based QoS Policing and Metering

The following sections describe circuit-based marking and rate-limiting.

1.2.2 Circuit-Based Marking

When a QoS policy is applied to a circuit without a policy ACL or class definition, all packets traveling over the circuit are affected by the QoS policy.

The value of packets traveling over the circuit can be modified by the SmartEdge router and sent out with the new value through either the **`mark dscp`** or **`mark precedence`** command in policing policy configuration mode (for incoming packets) or in metering policy configuration mode (for outgoing packets).

Or, packets can be prioritized by the SmartEdge router for internal flow of traffic through the device using only the **`mark priority`** command in policing policy configuration mode (for incoming packets) or in metering policy configuration mode (for outgoing packets). In this case, when packets are sent out from the router, they retain their original value.

1.2.3 Circuit-Based Rate-Limiting

When a QoS policy is applied to a circuit without a policy ACL or class definition, all packets traveling over the circuit are affected by the QoS policy.

By default, inbound packets that conform to the policing or metering rate are admitted with no additional action taken, while packets that exceed the rate are dropped. To modify the action taken by the SmartEdge router, use the **`conform`** and **`exceed`** commands in policy rate configuration mode; see Figure 1.

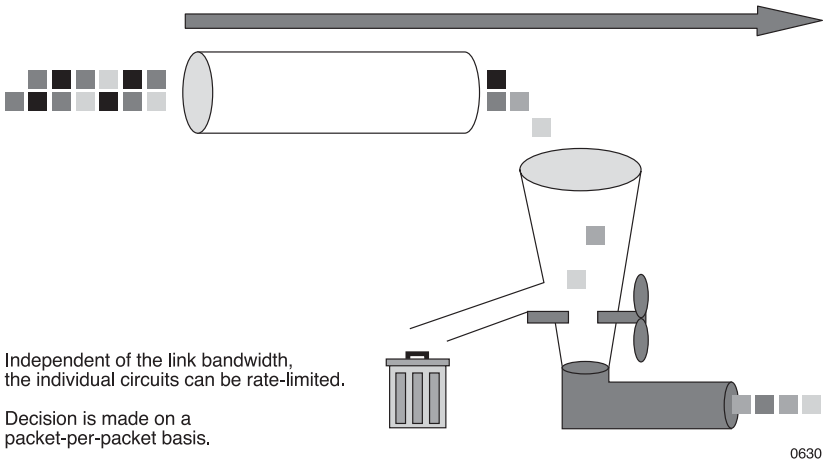


Figure 1 Circuit-Based Rate-Limiting (630)

Consider the following rules when configuring rate limiting for circuits:

- When a dynamic circuit does not share its handle with a static circuit:
  - The dynamic binding is rate limited by the Dynamic QoS Parameter (DQP).
  - The static binding is rate limited as configured by the *rate circuit out* command.
- When a dynamic and static circuit share the same handle and the binding is attached to the dynamic (or subscriber) circuit, rate limiting configuration that is done on the static circuit (using the **`rate circuit out`** command) is not applied to the dynamic circuit binding.

1.2.4 Class-Based Policing and Metering

The following sections describe class-based policing and metering.

1.2.5 Policy Access Control Lists

A classification filter is configured by a policy ACL or class definition. Each policy ACL supports up to eight unique classes. Packets can be classified according to IP precedence value, protocol number, IP source and destination address, Internet Control Message Protocol (ICMP) attributes, Internet Group Management Protocol (IGMP) attributes, Transmission Control Protocol (TCP) attributes, and User Datagram Protocol (UDP) attributes.

A policy ACL or class definition can be applied to incoming or outgoing packets on a port, or circuit, or for a subscriber record. A policy ACL or class definition is applied to incoming packets through a QoS policing policy and to outgoing packets through a QoS metering policy. For details about policy ACLs, see *Configuring ACLs*.

1.2.6 Class Definitions

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 packet descriptor (PD) classification values.

Class-definition policing or metering is an alternative to ACL policing or metering. For each metering or policing policy, you can specify either an ACL group or a class group, but not both. Unlike ACL metering and policing policies, which require access to the packet's IP header, you can apply class-definition metering and policing policies to Layer 2 circuits, such as Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) sessions, Layer 2 Virtual Private Networks (VPNs) and cross-connections, and bridged circuits. When you apply policing and metering policies to Layer 2 circuits, you cannot use the **`mark dscp`** and **`mark precedence`** commands to mark packets and assign priority because these commands also require access to the packet's IP header. When a packet arrives, the router applies any ingress classification propagation and mapping to determine a packet's initial packet descriptor (PD) value. If you use a class definition to apply a policing policy, the resulting PD value for the packet determines its class. Layer 3 can be accessed with the use-ip option for Layer 2 circuits.

1.2.7 Class-Based Marking

When a QoS policy is applied to a circuit in conjunction with a policy ACL, only particular classes of packets traveling over the circuit are affected by the QoS policy. To configure up to eight classes to prioritize packets differently, use the **`class`** command (in policy group configuration mode). For details about policy ACLs, see *Configuring ACLs*.

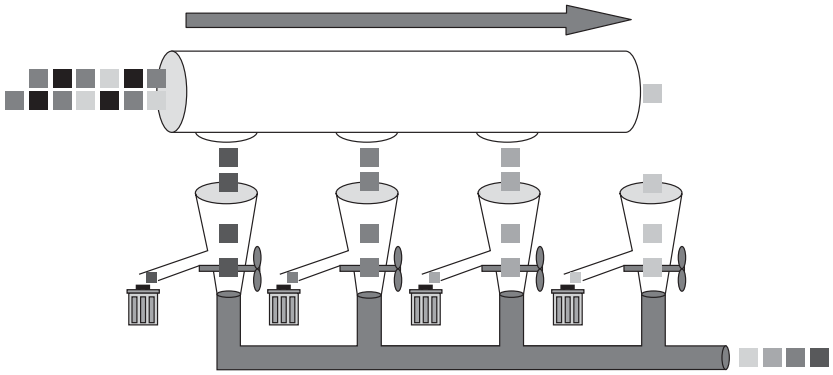
The prioritization for particular classes of packets can be modified and sent out the router with the new value using the **`mark dscp`** or **`mark precedence`** command (in policy ACL class configuration mode).

Classes of packets can be also be prioritized for only internal flow of traffic through the router using the **`mark priority`** command (in policy group class configuration mode), so that when packets are sent out from the router, they retain their original value.

1.2.8 Class-Based Rate-Limiting

When a QoS policy is applied to a circuit in conjunction with a policy ACL or class-definition, only particular classes of packets traveling over the circuit are affected by the QoS policy.

By default, inbound packets that conform to the QoS policy rate are admitted with no additional action taken, while packets that exceed the rate are dropped. You can modify the default behavior for classes of packets using the **`conform`** and **`exceed`** commands in policy class rate configuration mode; see Figure 2.



Independent of the link bandwidth, the traffic can be rate-limited on a traffic class basis.

Decision is made on a packet-per-packet basis within each traffic class.

0631

Figure 2 Class-Based Rate-Limiting (631)

1.2.9 Circuit-Based and Class-Based Rate-Limiting

A circuit can be rate-limited for an overall bandwidth, while each traffic class on the circuit is assigned a specific rate. Class-based rate limiting is applied to the packets first; see Figure 3. Then the circuit rate limit is applied to all packets, regardless of class and including packets that do not belong to any class.

If the total of the class-based rates is less than or equal to the circuit rate, traffic that matches one of these classes and conforms to its rate is not dropped by circuit-level rate enforcement. Any remaining bandwidth is available for traffic that does not match any class or that matches a class without any rate configured. If the total of the class-based rates is close to or equal to the circuit rate, class-based traffic can severely limit other traffic to the point where no other traffic can be forwarded.

If the total of class-based rates exceeds the circuit rate, the traffic of any class is subject to circuit-level rate enforcement and may be dropped.

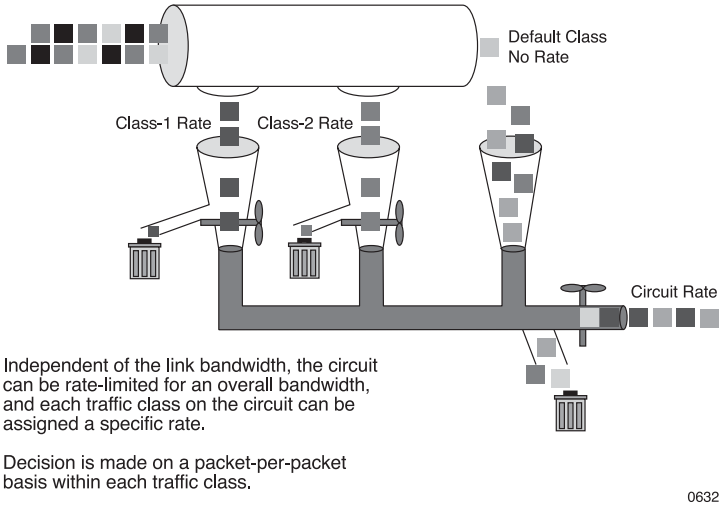


Figure 3 Circuit-Based and Class-Based Rate-Limiting (632)

1.2.10 Single Rate Three-Color Markers

The single rate three-color marker implementation meters traffic and assigns a color to packets for rate limiting purposes according to the following three configurable traffic thresholds:

- The traffic rate
- The burst tolerance
- The excess burst tolerance

The traffic rate, burst tolerance, and excess burst tolerance are configurable thresholds that you can use to specify how packets are dropped or marked. Depending on which thresholds are exceeded, packets are classified, using one of the following colors:

- Green—Packets that do not exceed the traffic rate or the burst tolerance. To configure the rate limiting action taken for these packets, use one of the **`conform`** commands in policy class rate configuration or policy rate configuration mode.
- Yellow—Packets that exceed the burst tolerance, but do not exceed the excess burst tolerance. To configure the rate limiting action taken for these packets, use one of the **`exceed`** commands in policy class rate configuration or policy rate configuration mode.
- Red—Packets that exceed the excess burst tolerance. To configure the rate limiting action taken for these packets, use one of the **`violate`** commands in policy class rate configuration or policy rate configuration mode.

The SmartEdge router implementation of a single rate three-color marker conforms to RFC 2697, *A Single Rate Three Color Marker*.

1.2.11 Policy Inheritance

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 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.

The following types of inheritance are supported:

- 802.1Q permanent virtual circuit (PVC) or tunnel from a parent Ethernet port
- 802.1Q PVC from a parent 802.1Q tunnel
- Point-to-Point Protocol over Ethernet (PPPoE) or CLIPS sessions from a parent Ethernet port or 802.1Q PVC

- PPP and PPPoE sessions from a parent ATM PVC

1.2.12 Mapping a Child Policy Class to a Parent Class

Traffic subject to both an individual metering or policing policy and a hierarchical metering or policing policy configured on the parent circuit cannot be classified twice. However, the mapping of a metering or policing policy class to a parent policy class is supported when applying the hierarchical metering or policing policy to traffic on a child circuit that has its own metering and policing policy.

You can configure the **`parent-class`** keyword within the class-level configuration mode within the child metering or policing policy. The **`parent-class`** keyword allows you to map a child class, which is determined during policy ACL or class-definition map classification, to a parent class. This mapping allows the class determination at the child level to also determine the class assignment at the parent level. This mapping occurs during the second phase of rate limiting that is applied to the child circuit traffic (when enforcing the parent metering or policing policy). The **`parent-class`** keyword configured in the child policy class specifies the parent class this packet is assigned to.

Here is a summary of the steps that take place when a hierarchical metering or policing policy is configured along with an ACL class or a class-definition map:

- The metering or policing actions specified for the child class (determined during policy ACL or class-definition map classification) are applied to the packets destined for the child circuit. The child metering or policing policy is enforced during this step of the rate-limiting process.

- The metering or policing actions specified for the parent class to which the child class is mapped are applied to the packets destined for the child circuit. The parent hierarchical metering or policing policy is applied during this step of the rate-limiting process.

- The metering or policing actions specified for the parent class (determined during policy ACL or class-definition map classification) are applied to the packets destined for the parent circuit. The parent metering or policing policy is enforced during this step of the rate-limiting process.

Note that the metering or policing enforcement phase for child circuit traffic and the single metering or policing enforcement phase for the parent circuit traffic transpires concurrently. The traffic of all the child circuits subject to the parent policy, and the parent circuit traffic itself, are treated in aggregate for enforcing any rate limits specified in the policy of the parent circuit.

Note: The policy ACL map classification for a given child class is only performed once when hierarchical metering or policing is enabled. This class is then mapped to a different class—a parent class. The policy ACL map classification itself is not performed again when hierarchical metering or policing is enabled.

If the **parent-class** keyword is specified for a child class, and the specified parent class name does not exist in the parent hierarchical metering or policing policy, then traffic for the child class is not mapped to any parent class and is subject only to the metering or policing parameters specified for the parent policy level rate (if specified) during the second rate-limiting phase to be applied to this traffic.

If the **parent-class** keyword is not specified for a child class, then traffic for the given child class is not mapped to any parent class and is only subject to the metering or policing parameters specified for the parent's policy level rate (if specified) during the second rate-limiting phase applied to this traffic.

If the child circuit does not have its own metering or policing policy, then the policy ACL (or class-definition map) configured on the parent whose hierarchical metering or policing policy is to be applied is used to classify traffic on the child circuit.

During periods of traffic congestion at the parent circuit level, the rate limiting at the parent circuit level is processed on a "first come, first serve" basis. This means any packet destined for either the child circuit or the parent circuit can be dropped if the SmartEdge router determines that the traffic exceeds the rate limit threshold specified in the parent hierarchical metering or policing policy.

1.3 Summary

The following provides a high-level view of QoS traffic through the SmartEdge router:

1. (Prioritization) The packet is assigned an internal priority level and an internal drop precedence. Priority and precedence is determined by a default mapping from a priority specified in the packet's protocol headers, or it can be customized with a class map.

2. (Policing) As the packet enters the SmartEdge router, the packet may be subject to a policing policy configured on the incoming port, or circuit, or subscriber record:

    a As the packet enters the SmartEdge router, the packet may be subject to a classification filter configured by a policy ACL or class-definition, identifying the packet as belonging to one of up to eight defined classes.

    b Packets belonging to each class can be rate-limited, marked or dropped. The per-class traffic can be treated as follows:

        a Per-class rate limits may be set, and different marking or dropping actions can be defined for the traffic, depending on whether it conforms to or exceeds the target rate and burst allowance.

        b If it is not dropped due to rate-limiting, the packet can have its internal priority or drop-precedence values modified, or it can be marked by changing its external IP precedence (DSCP) value.

3. At this point, the SmartEdge router transports the packet to the appropriate outbound traffic card.

4. (Metering) Before the packet is queued for transmission, the packet may be subject to a metering policy configured on the outgoing port, or circuit, or subscriber record:

    a Before the packet exits the SmartEdge router, the packet may be subject to a classification filter configured by a policy ACL or class-definition, identifying the packet as belonging to one of up to eight defined classes.

    b Packets belonging to each class can be rate limited, marked or dropped. The per-class traffic can be treated as follows:

        a Per-class rate limits may be set, and different marking or dropping actions can be defined for the traffic depending on whether it conforms to or exceeds the target rate and burst allowance.

        b If it is not dropped due to rate-limiting, the packet can have its internal priority and/or drop-precedence values modified and/or it can be marked by changing its external IP precedence (DSCP) value.

5. Optionally, the packet's internal priority and drop-precedence value assigned by the SmartEdge router can be used as the basis to modify the packet's external priority markings in its protocol headers. This assignment can use a default mapping or be customized using a class-map.

6. Each outgoing packet is assigned to an egress queue based on the destination circuit and its internal priority setting. Egress queues on outbound traffic cards have associated scheduling parameters such as rates, depths, and relative weights. The traffic card’s scheduler draws packets from the queues based on weight, rate, or strict priority:

    a A packet can be dropped when queues back up over a configured discard threshold or because of a random early detection (RED) parameter setting.

    b If a packet is not dropped, it is scheduled for transmission based on its PD QoS priority group and its scheduling policy.

2 Configuration and Operations Tasks

To configure a metering or policing policy, perform the tasks described in the following sections.

Note: In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see *Command List*.

2.1 Policy Configuration Guidelines

The following guidelines apply to the configuration of QoS metering and policing policies:

- You can either mark or establish a rate for packets on a single circuit, or port, or subscriber record; these conditions are mutually exclusive.
- Only one marking instruction can be in effect at a time. Any succeeding command supersedes the previous instruction.

2.2 Configure a Metering Policy

To configure a metering policy, perform the tasks described in Table 1; enter all commands in metering policy configuration mode, unless otherwise noted.

Table 1 Configure a Metering Policy

Step	Task	Root Command	Notes
1.	Create or select a metering policy and access metering policy configuration mode.	*qos policy metering (global)*	Enter this command in global configuration mode.
2.	Optional. Mark outgoing packets associated with the policy with one of the following tasks:		
	Assign a DSCP priority.	*mark dscp*	Only one marking instruction can be in effect at any time.
	Assign a drop precedence value.	*mark precedence*	
	Assign with a PD QoS priority number, a drop-precedence value, or both.	*mark priority*	

Table 1 Configure a Metering Policy

Step	Task	Root Command	Notes
3.	Set the policy rate for outgoing packets and access policy rate configuration mode.	*rate*	
4.	Optional. Specify the treatment of outgoing packets that conform to a set rate with one of the following tasks:		Enter these commands in policy rate configuration mode.
	Specify that no action is taken on packets.	*conform no-action*	
	Mark packets with a DSCP class.	*conform mark dscp*	Only one marking instruction can be in effect at any time.
	Mark packets with a drop precedence value.	*conform mark precedence*	
	Mark packets with a PD QoS priority number, a drop-precedence value, or both.	*mark priority*	
5.	Optional. Specify the treatment of outgoing packets that exceed a set rate with one of the following tasks:		Enter these commands in policy rate configuration mode.
	Drop outgoing packets.	*exceed drop*	
	Specify that no action is taken on packets.	*exceed no-action*	
	Mark packets with a DSCP class.	*exceed mark dscp*	Only one marking instruction can be in effect at any time.
	Mark packets with a drop precedence value.	*exceed mark precedence*	
	Mark packets with a PD QoS priority number, a drop-precedence value, or both.	*exceed mark priority*	

Table 1 Configure a Metering Policy

Step	Task	Root Command	Notes
6.	Optional. Specify the treatment of outgoing packets that violate a set rate with one of the following tasks:		Enter these commands in policy rate configuration mode.
	Drop outgoing packets.	*violate drop*	
	Specify that no action is taken on packets.	*violate no-action*	
	Mark packets with a DSCP class.	*violate mark dscp*	Only one marking instruction can be in effect at any time.
	Mark packets with a drop precedence value.	*violate mark precedence*	
	Mark packets with a PD QoS priority number, a drop-precedence value, or both.	*violate mark priority*	
7.	Optional. Apply a policy ACL to this policy.		See Section 2.4 on page 15.

2.3 Configure a Policing Policy

To configure a policing policy, perform the tasks described in Table 2; enter all commands in policing policy configuration mode, unless otherwise noted.

Table 2 Configure a Policing Policy

Step	Task	Root Command	Notes
1.	Create or select a policing policy and access policing policy configuration mode.	*qos policy policing (global)*	Enter this command in global configuration mode.
2.	Optional. Mark incoming packets associated with the policy with one of the following tasks:		
	Assign a DSCP priority.	*mark dscp*	Only one marking instruction can be in effect at any time.
	Assign a drop precedence value.	*mark precedence*	

Table 2 Configure a Policing Policy

Step	Task	Root Command	Notes
	Assign a PD QoS priority number, a drop-precedence value, or both.	*mark priority*	
3.	Set the policy rate for incoming packets and access policy rate configuration mode.	*rate*	
4.	Optional. Specify the treatment of incoming packets that conform to a set rate with one of the following tasks:		Enter these commands in policy rate configuration mode.
	Specify that no action is taken on packets.	*conform no-action*	
	Mark packets with a DSCP class.	*conform mark dscp*	Only one marking instruction can be in effect at any time.
	Mark packets with a drop precedence value.	*conform mark precedence*	
	Mark packets with a PD QoS priority number, a drop-precedence value, or both.	*conform mark priority*	
5.	Optional. Specify the treatment of incoming packets that exceed a set rate with one of the following tasks:		Enter these commands in policy rate configuration mode.
	Drop inbound packets.	*exceed drop*	
	Specify that no action is taken on packets.	*exceed no-action*	
	Mark packets with a DSCP class.	*exceed mark dscp*	Only one marking instruction can be in effect at any time.
	Mark packets with a drop precedence value.	*exceed mark precedence*	
	Mark packets with a PD QoS priority number, a drop-precedence value, or both.	*exceed mark priority*	

Table 2 Configure a Policing Policy

Step	Task	Root Command	Notes
6.	Optional. Specify the treatment of incoming packets that violate a set rate with one of the following tasks:		Enter these commands in policy rate configuration mode.
	Drop inbound packets.	*violate drop*	
	Specify that no action is taken on packets.	*violate no-action*	
	Mark packets with a DSCP class.	*violate mark dscp*	Only one marking instruction can be in effect at any time.
	Mark packets with a drop precedence value.	*violate mark precedence*	
	Mark packets with a PD QoS priority number, a drop-precedence value, or both.	*violate mark priority*	
7.	Optional. Apply a policy ACL to this policy.	See Section 2.4 on page 15.	

2.4 Configure Classes

To define classes associated with a QoS metering or policing policy and complete the configuration of the policy, perform the tasks described in Table 3.

Table 3 Apply a Policy ACL

Step	Task	Root Command	Notes
1.	Define class-matching criteria for a QoS metering or policing policy by applying a policy ACL or ACLs or a class- definition, and access policy group configuration mode.	*ip access-group (circuits)* *ip access-group (interfaces and subs)* *ipv6 access-group (interface)* *ip access-group (policy)* *ipv6 access-group (policy)*	Enter these commands in policing policy or metering policy configuration mode. Each policing and metering policy can reference an IPv4 policy ACL, an IPv6 policy ACL, both an IPv4 ACL and an IPv6 ACL, or a class-definition. Note that a single QoS policy cannot reference both an ACL and a class-definition.
	Apply a class-definition.	*class-group*	
2.	Specify a class and access policy group class configuration mode.	*class*	Enter this command in policy group configuration mode. The class name must match the name of a class specified in a **`permit`** command in the policy ACL.
3.	Optional. Specify a mapping of a child class to a parent class.	*parent-class*	This configuration is only applicable when the policy is applied to a circuit that is also subject to a metering policy applied hierarchically to a parent of the circuit. Enter this command in the policy group class configuration mode.
4.	Optional. Specify the rate for this class, using one of the following tasks:		Enter these commands in policy group class configuration mode.
	Set the rate and burst tolerance and access policy class rate configuration mode.	*rate*	

Table 3 Apply a Policy ACL

Step	Task	Root Command	Notes
	Assign a percentage of the overall policy rate to this class of traffic and access policy class rate configuration mode.	*rate percentage*	
5.	Optional. Specify the treatment of packets that conform to the rate, using one of the following tasks:		Enter these commands in policy class rate configuration mode.
	Specify that no action is taken on packets.	*conform no-action*	
	Mark packets with a DSCP class.	*conform mark dscp*	Only one marking instruction can be in effect at any time.
	Mark packets with a drop precedence value.	*conform mark precedence*	
	Mark packets with a PD QoS priority number, a drop-precedence value, or both.	*conform mark priority*	
6.	Optional. Specify the treatment of packets that exceed a set rate, using one of the following tasks:		Enter these commands in policy class rate configuration mode.
	Drop inbound packets.	*exceed drop*	
	Specify that no action is taken on packets.	*exceed no-action*	
	Mark packets with a DSCP class.	*exceed mark dscp*	
	Assign a drop precedence value to packets.	*exceed mark precedence*	
	Assign a PD QoS priority number to packets.	*exceed mark priority*	
7.	Optional. Specify the treatment of packets that violate a set rate, using one of the following tasks:		Enter these commands in policy class rate configuration mode.
	Drop inbound packets.	*violate drop*	
	Specify that no action is taken on packets.	*violate no-action*	

Table 3 Apply a Policy ACL

Step	Task	Root Command	Notes
	Mark packets with a DSCP class.	*violate mark dscp*	
	Mark packets with a drop precedence value.	*violate mark precedence*	
	Mark packets with a PD QoS priority number, a drop-precedence value, or both.	*violate mark priority*	

2.5 Customize Classification Mappings

To customize classification mappings for QoS bits, perform the tasks described in Table 4.

Table 4 Customize Classification Mappings

Step	Task	Root Command	Notes
1.	Create a classification map and access class map configuration mode.	*qos class-map*	Enter this command in global configuration mode.
2.	Optional. Define the default QoS translation schema to use with a classification map.	*mapping-schema*	Enter this command in class map configuration mode.
3.	Optional. Define class definitions to group packets:		
	Specify a class definition and access policy group configuration mode.	*class-group*	Enter this command in metering and policing policy configuration modes. You can reference class names in this class definition, and assign actions to perform on packets assigned to the specified class.

Table 4 Customize Classification Mappings

Step	Task	Root Command	Notes
	Create or specify a class definition, and access class definition configuration mode.	*qos class-definition*	Enter this command in global configuration mode.
	Edit the contents of the specified class definition.	*qos class*	Enter this command in class definition configuration mode. Packets with the specified internal packet descriptor classification value are assigned to a class name that you can reference in policing or metering policies.

2.6 Operations Tasks

To monitor and administer QoS rate- and class-limiting features, perform the appropriate tasks described in Table 5. Enter the **`debug`** command in exec mode; enter the **`show`** commands in any mode.

Table 5 Monitor and Administer QoS Features

Task	Command
Display the contents of QoS class definitions.	*show qos class-definition*
Display QoS classification mappings.	*show qos class-map*
Display information for all QoS policies.	*show qos policy*
Display information about one or more QoS metering policies.	*show qos policy metering*
Display information about one or more QoS policing policies.	*show qos policy policing*

3 Configuration Examples

This section provides examples of rate limiting and class-based marking, using policing policy configurations in the following sections.

3.1 Circuit-Based Marking

The following example simply marks all packets on the circuit to which the policy, **circuit**, is applied with a DSCP value of **ef**, which indicates a high priority through expedited forwarding. Packets are not required to conform to a specific traffic rate:

```
[local]Redback(config)#qos policy circuit policing
[local]Redback(config-policy-policing)#mark dscp ef
```

3.2 Circuit-Based Rate-Limiting

The following example configures the QoS policy, **circuit**. Packets conforming to **10000** kbps are marked with a DSCP value of **ef**, which indicates a high priority through expedited forwarding. Packets that exceed the rate are dropped by default. The **counters** keyword in the **rate** command records the number of packets conforming to the rate limit and the number of packets exceeding the rate limit:

```
[local]Redback(config)#qos policy circuit policing
[local]Redback(config-policy-policing)#rate 10000 burst 1000 counters
[local]Redback(config-policy-rate)#conform mark dscp ef
```

3.3 Class-Based and Circuit-Based Rate Limiting

The following example creates a policy ACL, **qosmet**, in the **local** context and attaches it to the QoS metering policy, **meter**. The ACL classifies packets into three classes: **priority**, **immediate**, **flash**, and a default class, **default**. The QoS policy assigns a different rate to the **priority**, **immediate**, and **flash** classes; packets classified as default are marked with priority 7:

```
[local]Redback(config-ctx)#policy access-list qosmet
[local]Redback(config-access-list)#seq 10 permit ip any precedence priority
 class class-1
[local]Redback(config-access-list)#seq 20 permit ip any precedence immediate
class class-2
[local]Redback(config-access-list)#seq 30 permit ip any precedence flash
class class-3
[local]Redback(config-access-list)#seq 40 permit ip any any class default
[local]Redback(config-access-list)#exit
[local]Redback(config-ctx)#exit
!
!
[local]Redback(config)#qos policy meter metering
[local]Redback(config-policy-metering)#rate 1000 burst 50000 excess-burst 200000
counters
[local]Redback(config-policy-metering)#ip access-group qosmet local
[local]Redback(config-policy-group)#class class-1
[local]Redback(config-policy-group-class)#rate 1000 burst 50000 excess-burst 200000
counters
[local]Redback(config-policy-class-rate)#exit
[local]Redback(config-policy-group-class)#exit
!
!
[local]Redback(config-policy-group)#class class-2
[local]Redback(config-policy-group-class)#rate 2000 burst 50000 excess-burst 200000
counters
[local]Redback(config-policy-class-rate)#exit
[local]Redback(config-policy-group-class)#exit
!
!
[local]Redback(config-policy-group)#class class-3
[local]Redback(config-policy-group-class)#rate 3000 burst 50000 excess-burst 200000
counters
[local]Redback(config-policy-class-rate)#exit
[local]Redback(config-policy-group-class)#exit
!
!
[local]Redback(config-policy-group)#class default
[local]Redback(config-policy-group-class)#mark priority 7
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#exit
[local]Redback(config-policy-policing)#exit
```

The following example creates a policy ACL, **qos-class**, in the **local** context and attaches it to the QoS metering policy, **sub-rate**. The ACL defines three classes: **tcp**, **voip**, and **default:**

```
[local]Redback(config-ctx)#policy access-list qos-class
[local]Redback(config-access-list)#sequence 10 permit ip precedence tcp any any
class tcp
[local]Redback(config-access-list)#sequence 20 permit ip precedence ip any any dscp
equ cs6 class voip
[local]Redback(config-access-list)#sequence 30 permit ip any any class default
[local]Redback(config-access-list)#exit
[local]Redback(config-ctx)#exit
!
!
[local]Redback(config)#qos policy sub-rate metering
[local]Redback(config-policy-metering)#rate 2000 burst 100000 excess-burst 200000
counters
[local]Redback(config-policy-metering)#ip access-group qos-class local
[local]Redback(config-policy-group)#class tcp
[local]Redback(config-policy-group-class)#rate 1000 burst 50000 excess-burst 100000
conform mark priority 3
[local]Redback(config-policy-group)#class voip
[local]Redback(config-policy-group-class)#rate 200 burst 20000 excess-burst 40000
conform mark priority 0
[local]Redback(config-policy-class-rate)#exit
[local]Redback(config-policy-group-class)#exit
!
[local]Redback(config-policy-group)#class default
[local]Redback(config-policy-group-class)#mark priority 7
```

The following example configures the QoS policing policy, **combined**, which combines circuit-based rate-limiting and class-based rate-limiting and marking:

```
[local]Redback(config)#qos policy combined policing
[local]Redback(config-policy-policing)#rate 10000 burst 5000
[local]Redback(config-policy-rate)#conform mark precedence 2
[local]Redback(config-policy-rate)#exit
[local]Redback(config-policy-policing)#ip access-group qos local
[local]Redback(config-policy-group)#class web
[local]Redback(config-policy-group-class)#rate 5000 burst 1000
[local]Redback(config-policy-class-rate)#conform mark dscp AF11
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#class voip
[local]Redback(config-policy-group-class)#mark dscp ef
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#class default
[local]Redback(config-policy-group-class)#mark dscp df
```

3.4 QoS Policies

The following example creates an IPv4 policy ACL, `class_ipv4`, and an IPv6 policy ACL, `class_ipv6`, in the local context and attaches them to the QoS policing policy, `POL1`. Each ACL defines two classes: `B` and `C`, that are referenced by `POL1`:

```
[local]Redback#config
Enter configuration commands, one per line, 'end' to exit
[local]Redback#context local
[local]Redback(config-ctx)#policy access-list class-ipv4
!
!
[local]Redback(config-access-list)#seq 10 permit ip any 15.1.0.0 0.0.255.255 class B
[local]Redback(config-access-list)#seq 20 permit ip any 15.2.0.0 0.0.255.255 class C
[local]Redback(config-access-list)#exit
[local]Redback(config-ctx)#ipv6 policy access-list class_ipv6
[local]Redback(config-ipv6-access-list)#seq 10 permit ipv6 any 2000:1:2:3::/64 class B
[local]Redback(config-ipv6-access-list)#seq 20 permit ipv6 any 2000:1:2:3::/64 class C
[local]Redback(config-ipv6-access-list)#exit
[local]Redback(config-ctx)#exit
[local]Redback(config)#qos policy POL1 policing
[local]Redback(config-policy-policing)#ip access-group class_ipv4 local
[local]Redback(config-policy-group)#exit
[local]Redback(config-policy-policing)#ipv6 access-group class_ipv6 local
[local]Redback(config-policy-group)#class B
[local]Redback(config-policy-group-class)#rate 50 burst 20000 counters
[local]Redback(config-policy-class-rate)#conform mark dscp af11
[local]Redback(config-policy-class-rate)#exit
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#class C
[local]Redback(config-policy-group-class)#rate 200 burst 90000 counters
[local]Redback(config-policy-class-rate)#conform mark dscp ef
[local]Redback(config-policy-class-rate)#exit
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#exit
[local]Redback(config-policy-policing)#exit
[local]Redback(config)#
```