

Understanding JUNOS CoS Components for EX-series Switches

This topic describes the JUNOS CoS components for EX-series switches:

- Code-Point Aliases on page 1
- Policers on page 1
- Classifiers on page 1
- Forwarding Classes on page 2
- Tail Drop Profiles on page 2
- Schedulers on page 2
- Rewrite Rules on page 2

Code-Point Aliases

A code-point alias assigns a name to a pattern of code-point bits. You can use this name instead of the bit pattern when you configure other CoS components such as classifiers, drop-profile maps, and rewrite rules.

Policers

Policers limit traffic of a certain class to a specified bandwidth and *burst size*. Packets exceeding the policer limits can be discarded. You define policers with filters that can be associated with input interfaces.

For more information about policers, see Understanding the Use of Policers in Firewall Filters.



NOTE: You can configure policers to discard packets that exceed the rate limits. If you want to configure CoS parameters such as **loss-priority** and **forwarding-class**, you must use firewall filters.

Classifiers

Packet classification associates incoming packets with a particular CoS servicing level. In JUNOS software, *classifiers* associate packets with a forwarding class and loss priority and assign packets to output queues based on the associated forwarding class. JUNOS software supports two general types of classifiers:

- Behavior aggregate or CoS value traffic classifiers—Examines the CoS value in the packet header. The value in this single field determines the CoS settings applied to the packet. BA classifiers allow you to set the forwarding class and loss priority of a packet based on the Differentiated Services code point (DSCP) value, IP precedence value, and IEEE 802.1p value.
- Multifield traffic classifiers—Examines multiple fields in the packet such as source and destination addresses and source and destination port numbers of the packet.

With multifield classifiers, you set the forwarding class and loss priority of a packet based on firewall filter rules.

Forwarding Classes

Forwarding classes group the packets for transmission. Based on forwarding classes, you assign packets to output queues. Forwarding classes affect the forwarding, scheduling, and marking policies applied to packets as they transit a switch. By default, four categories of forwarding classes are defined: best effort, assured forwarding, expedited forwarding, and network control. For EX-series switches, 16 forwarding classes are supported, providing granular classification capability.

Tail Drop Profiles

Drop profile is a mechanism that defines parameters that allow packets to be dropped from the network. Drop profiles define the meanings of the loss priorities. When you configure drop profiles you are essentially setting the value for queue fullness. The queue fullness represents a percentage of the queue used to store packets in relation to the total amount that has been allocated for that specific queue.

Loss priorities set the priority of dropping a packet. Loss priority affects the scheduling of a packet without affecting the packet's relative ordering. You can use the loss priority setting to identify packets that have experienced congestion. Typically you mark packets exceeding some service level with a high loss priority.

Schedulers

Each switch interface has multiple queues assigned to store packets. The switch determines which queue to service based on a particular method of scheduling. This process often involves determining which type of packet should be transmitted before another. You can define the priority, bandwidth, delay buffer size, and tail drop profiles to be applied to a particular queue for packet transmission.

A scheduler map associates a specified forwarding class with a scheduler configuration. You can associate up to four user-defined scheduler maps with the interfaces.

Rewrite Rules

A *rewrite rule* sets the appropriate CoS bits in the outgoing packet, thus allowing the next downstream device to classify the packet into the appropriate service group. Rewriting, or marking, outbound packets is useful when the switch is at the border of a network and must alter the CoS values to meet the policies of the targeted peer.



NOTE: Rewrite rules are applied when the packets are routed. Rewrite rules are not applied when the packets are forwarded.

Egress firewall filters can also assign forwarding class and loss priority so that the packets are rewritten based on forwarding class and loss priority.

- Related Topics**
- Understanding CoS Code-Point Aliases
 - Understanding CoS Classifiers
 - Understanding CoS Forwarding Classes
 - Understanding CoS Tail Drop Profiles
 - Understanding CoS Schedulers
 - Understanding CoS Two-Color Marking
 - Understanding CoS Rewrite Rules
 - Example: Configuring CoS on EX-series Switches

