



CHAPTER 4

Configuring QoS Policing

This chapter describes how to configure policing of traffic classes for Cisco Nexus 1000V.

Information About Policing

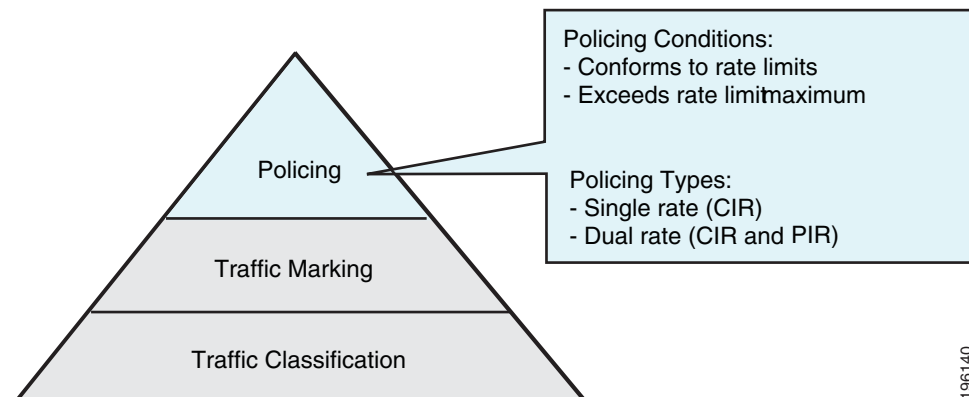
Policing is the monitoring of data rates for a particular class of traffic. The Cisco Nexus 1000V can also monitor associated burst sizes.

Three conditions are determined by the policer depending on the data rate parameters supplied: conform (green), exceed (yellow), or violate (red). You can configure only one action for each condition. When the data rate exceeds the user-supplied values, packets are either marked down or dropped.

You can define single-rate or dual-rate policers. Single-rate policers monitor the specified committed information rate (CIR) of traffic. Dual-rate policers monitor both CIR and peak information rate (PIR) of traffic. [Figure 4-1](#) shows policing conditions and types.

For more information about policies, see [RFC 2697](#), [RFC 2698](#), and [RFC 4115](#).

Figure 4-1 Policing Conditions and Types



The following conditions trigger actions by the policer depending on the defined data rate:

Condition	Color	Description	Policer Action (only one allowed per condition)
Conform	Green	The packet traffic data rate is within the defined boundaries.	The policer either transmits these packets as is, or changes the value in the header (DSCP, precedence, or CoS), and then transmits these packets.
Exceed	Yellow	The packet traffic data rate exceeds the defined boundary.	The policer can drop or mark down these packets.
Violate	Red	The packet traffic data rate violates the defined boundaries.	The policer can drop or mark down these packets.

Prerequisites for Policing

Policing has the following prerequisites:

- You must be familiar with [RFC 2698](#).
- You are logged on to the CLI in EXEC mode.

Guidelines and Limitations

Use the following guideline to configure policing:

- Each module polices independently, which might affect a policer that is applied to traffic distributed across more than one module, such as in the case of a port channel interface.

Configuring Policing

You can configure a single- or dual-rate policer in the Cisco Nexus 1000V.

Configuring 1-Rate and 2-Rate, 2-Color and 3-Color Policing

The type of policer that is created by the Cisco Nexus 1000V is based on a combination of the **police** command arguments described in [Table 4-1](#).



Note

Specify the identical value for **pir** and **cir** to configure 1-rate 3-color policing.

Table 4-1 Arguments to the Police Command

Argument	Description
cir	Committed information rate, or desired bandwidth, specified as a bit rate or a percentage of the link rate. Although a value for cir is required, the argument itself is optional. The range of values is from 1 to 80000000000; the range of policing values that are mathematically significant is 8000 to 80 Gbps.
percent	Specifies the rate as a percentage of the interface rate. The range of values is from 1 to 100%.
bc	Indication of how much the cir can be exceeded, either as a bit rate or an amount of time at cir . The default is 200 milliseconds of traffic at the configured rate. The default data rate units are bytes, and the Gigabit per second (gbps) rate is not supported for this parameter.
pir	Peak information rate, which is specified as a PIR bit rate or a percentage of the link rate. There is no default. The range of values is from 1 to 80000000000; the range of policing values that are mathematically significant is from 8000 to 80 Gbps. The range of percentage values is from 1 to 100%.
be	Indication of how much the pir can be exceeded, either as a bit rate or an amount of time at pir . When the bc value is not specified, the default is 200 milliseconds of traffic at the configured rate. The default data rate units are bytes, and the Gigabit per second (gbps) rate is not supported for this parameter. Note You must specify a value for pir before the device displays this argument.
conform	Single action to take if the traffic data rate is within bounds. The basic actions are transmit or one of the set commands listed in Table 4-4. The default is transmit.
exceed	Single action to take if the traffic data rate exceeds the specified boundaries. The basic actions are drop or markdown. The default is drop.
violate	Single action to take if the traffic data rate violates the configured rate values. The basic actions are drop or markdown. The default is drop.

Although all the arguments in Table 4-1 are optional, you must specify a value for **cir**. In this section, **cir** indicates what is its value but not necessarily the keyword itself. The combination of these arguments and the resulting policer types and actions are shown in Table 4-2.

Table 4-2 Policer Types and Actions

Police Arguments Present	Policer Type	Policer Action
cir , but not pir , be , or violate	1-rate, 2-color	≤ cir , then conform ; otherwise violate
cir and pir	1-rate, 3-color	≤ cir , then conform ; ≤ pir , then exceed ; otherwise violate Note You must specify identical values for cir and pir .
cir and pir	2-rate, 3-color	≤ cir , then conform ; ≤ pir , then exceed ; otherwise violate

The policer actions that you can specify are described in Table 4-3 and Table 4-4.

Table 4-3 *Policer Actions for Exceed or Violate*

Action	Description
drop	Drops the packet. This action is available only when the packet exceeds or violates the parameters.
set dscp dscp table { <i>cir-markdown-map</i> <i>pir-markdown-map</i> }	Sets the specified fields from a table map and transmits the packet. For more information on the system-defined, or default table maps, see Chapter 3, “Configuring QoS Marking Policies.” This is available only when the packet exceeds the parameters (use the <i>cir-markdown-map</i>) or violates the parameters (use the <i>pir-markdown-map</i>).

Table 4-4 *Policer Actions for Conform*

Action	Description
transmit	Transmits the packet. This action is available only when the packet conforms to the parameters.
set-prec-transmit	Sets the IP precedence field to a specified value and transmits the packet. This action is available only when the packet conforms to the parameters.
set-dscp-transmit	Sets the DSCP field to a specified value and transmits the packet. This action is available only when the packet conforms to the parameters.
set-cos-transmit	Sets the CoS field to a specified value and transmits the packet. This action is available only when the packet conforms to the parameters.
set-qos-transmit	Sets the QoS group internal label to specified value and transmits the packet. This action can be used only in input policies and is available only when the packet conforms to the parameters.
set-discard-class-transmit	Sets the discard-class internal label to a specified value and transmits the packet. This action can be used only in ingress policies and is available only when the packet conforms to the parameters.

**Note**

The policer can only drop or mark down packets that exceed or violate the specified parameters. See [Chapter 3, “Configuring QoS Marking Policies”](#) for information on marking down packets.

The data rates that are used in the **police** command are described in [Table 4-5](#).

Table 4-5 *Data Rates for the police Command*

Rate	Description
bps	Bits per second (default)
kbps	1,000 bits per seconds
mbps	1,000,000 bits per second
gbps	1,000,000,000 bits per second

Burst sizes that are used in the **police** command are described in [Table 4-6](#).

Table 4-6 Burst Sizes for the police Command

Speed	Description
bytes	bytes
kbytes	1,000 bytes
mbytes	1,000,000 bytes
ms	milliseconds
us	microseconds

SUMMARY STEPS**Note**

You must specify the identical value for **pir** and **cir** to configure 1-rate, 3-color policing.

1. **config t**
2. **policy-map [type qos] [match-first] policy-map-name**
3. **class [type qos] {class_map_name | class-default}**
4. **police [cir] {committed-rate [data-rate] | percent cir-link-percent} [bc committed-burst-rate [link-speed]] [pir] {peak-rate [data-rate] | percent cir-link-percent} [be peak-burst-rate [link-speed]] {conform {transmit | set-prec-transmit | set-dscp-transmit | set-cos-transmit | set-qos-transmit | set-discard-class-transmit} [exceed {drop | set dscp dscp table {cir-markdown-map}}] [violate {drop | set dscp dscp table {pir-markdown-map}}]}**
5. **show policy-map [type qos] [policy-map-name]**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into global configuration mode.
Step 2	policy-map [type qos] [match-first] policy-map-name Example: n1000v(config)# policy-map policy1 n1000v(config-pmap-qos)#	Places you into policy map QoS configuration mode and creates or accesses the specified policy map. The <i>policy_map_name</i> argument is an alphabetic string that can be up to 40 case-insensitive characters long, including hyphen (-) and underscore (_) characters.

	Command	Purpose
Step 3	<pre>class [type qos] {class-map-name class-default} Example: n1000v(config-pmap-qos)# class class-default n1000v(config-pmap-c-qos)#</pre>	<p>Creates a reference to <i>class-map-name</i> and enters policy-map class QoS configuration mode for the specified class map. By default, the class is added to the end of the policy map. Changes are saved in the running configuration.</p> <p>Use the class-default keyword to select all traffic that is not currently matched by classes in the policy map.</p>
Step 4	<pre>police [cir] {committed-rate [data-rate] percent cir-link-percent} [bc committed-burst-rate [link-speed]] [pir] {peak-rate [data-rate] percent cir-link-percent} [be peak-burst-rate [link-speed]] [conform {transmit set-prec-transmit set-dscp-transmit set-cos-transmit set-qos-transmit set-discard-class-transmit} [exceed {drop set dscp dscp table {cir-markdown-map}}] [violate {drop set dscp dscp table {pir-markdown-map}}]]} Example: n1000v(config-pmap-c-qos)# police cir 256000 conform transmit violate set dscp dscp table pir-markdown-map n1000v(config-pmap-c-qos)#</pre>	<p>Polices cir in bits or as a percentage of the link rate. The conform action is taken if the data rate is \leq cir. If be and pir are not specified, all other traffic takes the violate action. If be or violate are specified, then the exceed action is taken if the data rate \leq pir; otherwise the violate action is taken. The actions are described in Table 4-3 and Table 4-4. The data rates and link speeds are described in Table 4-5 and Table 4-6.</p> <p>Note You must specify identical values for cir and pir.</p>
Step 5	<pre>show policy-map [type qos] [policy-map-name] Example: n1000v(config-pmap-c-qos)# show policy-map</pre>	<p>(Optional) Displays information about all configured policy maps or a selected policy map of type QoS.</p>
Step 6	<pre>copy running-config startup-config Example: n1000v(config-pmap-c-qos)# copy running-config startup-config</pre>	<p>(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.</p>

EXAMPLES

This example shows how to configure a 1-rate, 2-color policer that transmits if the data rate is within 200 milliseconds of traffic at 256000 bps and marks IP precedence to 6 if the datarate is exceeded.

```
n1000v# config t
n1000v(config)# policy-map policy1
n1000v(config-pmap-qos)# class class-default
n1000v(config-pmap-c-qos)# police cir 256000 conform transmit violate set dscp dscp table
pir-markdown-map
n1000v(config-pmap-c-qos)# show policy-map
```

```
Type qos policy-maps
=====
```

```
policy-map type qos policy1
  class class1
    set dscp af31
```

```

class class2
  set dscp af13
class class-default
  set dscp af22
  police cir 256000 bps bc 200 ms conform transmit violate set dscp dscp tab
le pir-markdown-map
n1000v(config-pmap-c-qos)# copy running-config startup-config

```

This example shows how to configure a 1-rate, 3-color policer that transmits if the data rate is within 200 milliseconds of traffic at 256000 bps, and marks DSCP to 6 if the data rate is within 300 milliseconds of traffic at 256000 bps, and drops packets otherwise.

```

n1000v# config t
n1000v(config)# policy-map policy1
n1000v(config-pmap-qos)# class class-default
n1000v(config-pmap-c-qos)# police cir 256000 pir 256000 conform transmit exceed set dscp
dscp table cir-markdown-map violate drop
n1000v(config-pmap-c-qos)# show policy-map

```

```

Type qos policy-maps
=====

```

```

policy-map type qos policy1
  class class1
    set dscp af31
  class class2
    set dscp af13
  class class-default
    set dscp af22
    police cir 256000 bps bc 200 ms pir 256000 bps be 200 ms conform transmit
exceed set dscp dscp table cir-markdown-map violate drop
n1000v(config-pmap-c-qos)# copy running-config startup-config

```

Configuring Ingress and Egress Policing

You can apply the policing instructions in a QoS policy map to ingress or egress packets by attaching that QoS policy map to an interface or port profile. To select ingress or egress, you specify either the **input** or **output** keyword in the **service-policy** command. For an example of how to use the **service-policy** command, see the [“Creating Ingress and Egress Policies” procedure on page 3-11](#).

Configuring Markdown Policing

Markdown policing is the setting of a QoS field in a packet when traffic exceeds or violates the policed data rates. You can configure markdown policing by using the **set** commands for that are described in [Table 4-3](#) and [Table 4-4](#).

SUMMARY STEPS

1. **config t**
2. **policy-map** [**type qos**] [**match-first**] *policy-map-name*
3. **class** [**type qos**] {*class_map_name* | **class-default**}

4. **police** [**cir**] {*committed-rate* [*data-rate*] | **percent** *cir-link-percent*} [**bc** *committed-burst-rate* [*link-speed*]] [**pir**] {*peak-rate* [*data-rate*] | **percent** *cir-link-percent*} [**be** *peak-burst-rate* [*link-speed*]] {**conform** *action* [**exceed** {**drop** | **set dscp dscp table** *cir-markdown-map*} [**violate** {**drop** | **set dscp dscp table** *pir-markdown-map*}]}}
5. **show policy-map** [**type qos**] [*policy-map-name*]
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into global configuration mode.
Step 2	policy-map [type qos] [match-first] <i>policy-map-name</i> Example: n1000v(config)# policy-map policy1 n1000v(config-pmap-qos)#	Creates or accesses the policy-map named <i>policy-map-name</i> , and then enters policy-map mode. The policy-map name can contain alphabetic, hyphen, or underscore characters, is case-insensitive, and can be up to 40 characters.
Step 3	class [type qos] { <i>class-map-name</i> class-default } Example: n1000v(config-pmap-qos)# class class-default n1000v(config-pmap-c-qos)#	Creates a reference to <i>class-map-name</i> and enters policy-map class QoS configuration mode for the specified class map. By default, the class is added to the end of the policy map. Changes are saved in the running configuration. Use the class-default keyword to select all traffic that is not currently matched by classes in the policy map.
Step 4	police [cir] { <i>committed-rate</i> [<i>data-rate</i>] percent <i>cir-link-percent</i> } [bc <i>committed-burst-rate</i> [<i>link-speed</i>]] [pir] { <i>peak-rate</i> [<i>data-rate</i>] percent <i>cir-link-percent</i> } [be <i>peak-burst-rate</i> [<i>link-speed</i>]] { conform <i>action</i> [exceed { drop set dscp dscp table <i>cir-markdown-map</i> } [violate { drop set dscp dscp table <i>pir-markdown-map</i> }]}}	Polices cir in bits or as a percentage of the link rate. The conform action is taken if the data rate is \leq cir . If be and pir are not specified, all other traffic takes the violate action. If be or violate are specified, then the exceed action is taken if the data rate \leq pir , and the violate action is taken otherwise. The actions are described in Table 4-3 and Table 4-4. The data rates and link speeds are described in Table 4-5 and Table 4-6.
Step 5	show policy-map [type qos] <i>policy-map-name</i> Example: n1000v(config-pmap-c-qos)# show policy-map	(Optional) Displays information about the policy map configuration.
Step 6	copy running-config startup-config Example: n1000v(config-pmap-c-qos)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

EXAMPLES

This example shows a 1-rate, 3-color policer that transmits if the data rate is within 300 milliseconds of traffic at 256000 bps; marks down DSCP using the system-defined table map if the data rate is within 300 milliseconds of traffic at 256000 bps; and drops packets otherwise:

```
n1000v# config t
n1000v(config)# policy-map policy1
n1000v(config-pmap-qos)# class class-default
n1000v(config-pmap-c-qos)# police cir 256000 bps bc 300 ms pir 256000 conform transmit
exceed set dscp dscp table cir-markdown-map violate drop
n1000v(config-pmap-c-qos)# show policy-map policy1
```

```
Type qos policy-maps
```

```
=====
```

```
policy-map type qos policy1
  class class-default
    police cir 256000 bps bc 300 ms pir 256000 bps be 300 ms conform transmit
  exceed set dscp dscp table cir-markdown-map violate drop
n1000v(config-pmap-c-qos)# copy running-config startup-config
```

Verifying the Policing Configuration

To verify the policing configuration, perform the following task:

Command	Description
<code>show policy-map</code>	Displays information about policy maps and policing.

Configuration Example for QoS Policing

The following example shows how to configure a 1-rate, 2-color policer:

```
config t
  policy-map policy1
    class one_rate_2_color_policer
      police cir 256000 conform transmit violate drop
```

The following example shows how to configure a 1-rate, 2-color policer with DSCP mark down:

```
config t
  policy-map policy2
    class one_rate_2_color_policer_with_dscp_markdown
      police cir 256000 conform set-dscp-transmit af11 violate set dscp dscp table
  pir-markdown-map
```

The following example shows how to configure a 1-rate, 3-color policer:

```
config t
```

```
policy-map policy3
  class one_rate_3_color_policer
    police cir 256000 pir 256000 conform transmit exceed set dscp dscp table
  cir-markdown-map violate drop
```

Feature History for QoS Policing

This section provides the QoS policing release history.

Feature Name	Releases	Feature Information
QoS Policing	4.0	This feature was introduced.