Configuring Ingress Policing

This chapter contains the following sections:

Information About Ingress Policing

Policing allows you to monitor the data rates for a particular class of traffic. When the data rate exceeds user-configured values, the switch drops packets immediately. Because policing does not buffer the traffic; transmission delays are not affected. When traffic exceeds the data rate on a specific class, the switch drops the packets.

You can define single-rate and two-color Ingress Policing.

Single-rate Ingress Policing monitors the committed information rate (CIR) of traffic.

Note The committed information rate (CIR) is a value specified as a bit rate from 1 to 80000000000 or a percentage of the link rate.

In addition, Ingress Policing can monitor associated burst sizes of the packets. Two colors, or conditions, are determined by Ingress Policing for each packet depending on the data rate parameters that you supply.

You can configure only one action for each condition. For example, you might police for traffic in a class to conform to the data rate of 256000 bits per second with up to 200 millisecond bursts.

Color-aware Ingress Policing assumes that traffic has been previously marked with a color.

Table 1: Maximum Supported Hardware Configuration for Policers

	Nexus 5500 Series	Nexus 2232	Nexus 2248TP-E	Nexus 6000 Series
Burst Size	64 MB	32 MB	32 MB	64 MB

	Nexus 5500 Series	Nexus 2232	Nexus 2248TP-E	Nexus 6000 Series
Max Rate	96 Gbps	12 Gbps	8 Gbps	8 Gbps
Granularity	732 kbps	732 kbps	488 kbps	122 kbps

Guidelines and Limitations for Ingress Policing

- The configuration for Ingress Policing is a part of the Quality of Service (QoS) policy configuration. You can configure QoS policies with Ingress Policing on the following :
  - Layer 2 switch ports
  - Host interface (HIF) ports
  - Port channels with switch ports
  - Port channels with HIF ports
  - Layer 3 interfaces (but not sub-interfaces or Switched Virtual Interfaces (SVIs))
  - Virtual Port Channel (vPC)
- Statistics are provided with Ingress Policing. Statistics include the drop count and allowed count. You can display the statistics by entering the **show policy-map interface ethernet** command.
- QoS policies that you configure on the attachments are installed in the QoS region of the Ternary Content Addressable Memory (TCAM) and causes the switch to apply Ingress Policing.
- If you configure a QoS policy with Ingress Policing on a HIF port or HIF port channel, Ingress Policing is offloaded to the Fabric Extender (FEX). Policy rewrites occur only in the switch. So QOS policy offload to FEX is required if there is any QOS policy rewrites which affects policer.
- All the match/set criteria that are supported in a QoS policy are supported even with Ingress Policing present in the policy. A Fabric Extender (FEX) supports Layer 3 operations (fragments) and Layer 4 operations (source and destination port ranges) but not the Transmission Control Protocol (TCP) flags and Layer 2 operations.
- You can define match criteria for a QoS policy so that it matches the control protocol traffic. If the type of policy is configured with Ingress Policing on an HIF port, the control traffic also gets policed. Therefore, the match criteria must be specific to the required flow of traffic.
- The **police** command is not supported on the Cisco Nexus device ASICs.
- The switch cannot apply a QoS policy with Ingress Policing to an HIF port that has virtual Ethernet interfaces attached.
- If the switch applies Ingress Policing on the HIF port, the policer is applied to traffic with no Virtual Network Tag (VNTAG).
- A policy with Ingress Policing is allowed only on switch ports, HIF ports, and port channels with switch/HIF ports.
- Ingress Policing with Layer 2 operations and TCP flags in the match criteria is not allowed on FEX interfaces.

- Ingress Policing is not supported on Enhanced VPC (2LayerVPC) ports.
- It is recommended that you apply identical Ingress Policing on Dual-homed (AA) HIF interfaces.
- The **police** command is not supported on system QoS policies.
- The **show policy-map interface** command is recommended to check that the ingress rate limiter is conformed and to display violated statistics. The CLI displays conformed/violated packets and packet per second statistics on HIF interfaces (regular as well as port-channel), whereas on the switchport (regular as well as port-channel) the command displays conformed/violated bytes and bits per second (bps).

Creating a Policy Map Using a Committed Information Rate

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map** [**type qos**] [*qos-policy-map-name*]	Creates a named object that represents a set of policies that are applied to a set of traffic classes. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	switch(config-pmap-qos)# **class** [**type qos**] {*class-map-name* | **class-default**}	Associates a class map with the policy map and enters configuration mode for the specified system class. Use the **class-default** keyword to select all traffic that is currently not matched by classes in the policy map. The *class-map-name* argument can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.
Step 4	switch(config-pmap-c-qos)# **police** [**cir**] {*committed-rate* [*data-rate*] | **percent** *cir-link-percent*} [[**bc**] {*committed-burst-rate*}][**conform**{**transmit**} [**violate** {**drop**}]]]	Polices **cir** in bits, kbps, mbps, or gbps. The **conform** action is applied if the data rate is less than or equal to **cir**, otherwise, the **violate** action is applied. The **cir** keyword specifies to use the committed information rate, or desired bandwidth, as a bit rate or a percentage of the link rate. The *committed-rate* value can range from 1 to 80 Gbps. The *data-rate* value can be one of the following: • bps—bits per second • kbps—1000 bits per second

	Command or Action	Purpose
		• mbps—1,000,000 bits per second • Gbps—1,000,000,000 bits per second Values for *committed-burst-rate* are the following: • bytes—bytes • kbytes—1000 bytes • mbytes—1,000,000 bytes • ms—milliseconds • us—microseconds The following are the Ingress Policing actions: • **conform**—The action to take if the traffic data rate is within bounds. The default action is **transmit.** • **transmit**—Transmits the packet. This is available only when the packet conforms to the parameters. • **violate**—The action to take if the traffic data rate violates the configured rate values. The basic and default action is **drop.** • **drop**—Drops the packet. This action is available only when the packet exceeds or violates the parameters.

Step 5	(Optional) switch(config-pmap-c-qos)# **set** {{**dscp** {*dscp-val* | *dscp-enum*}} | {**precedence** {*prec-val* | *prec-enum*}} |{ **qos-group** *qos-grp-val*}}	Sets the **dscp**, **precedence**, or **qos-group** actions.
		
		The arguments are as follows:
		• *dscp-val*—DSCP value or parameter to assign for this class of traffic. Valid values are from 0 to 63.
		• *dscp-enum*—Valid values are from 0 to 63.
		
		`af11 AF11 dscp (001010)`
		`af12 AF12 dscp (001100)`
		`af13 AF13 dscp (001110)`
		`af21 AF21 dscp (010010)`
		`af22 AF22 dscp (010100)`
		`af23 AF23 dscp (010110)`
		`af31 AF31 dscp (011010)`
		`af32 AF32 dscp (011100)`
		`af33 AF33 dscp (011110)`

	Command or Action	Purpose
		af41 AF41 dscp (100010) af42 AF42 dscp (100100) af43 AF43 dscp (100110) cs1 CS1(precedence 1) dscp (001000) cs2 CS2(precedence 2) dscp (010000) cs3 CS3(precedence 3) dscp (011000) cs4 CS4(precedence 4) dscp (100000) cs5 CS5(precedence 5) dscp (101000) cs6 CS6(precedence 6) dscp (110000) cs7 CS7(precedence 7) dscp (111000) default Default dscp (000000) ef EF dscp (101110) • *prec-val*—IP precedence value to assign for this class of traffic. Valid values are from 0 to 7. • 0—routine • 1—priority • 2—immediate • 3—flash • 4—flash-override • 5—critical • 6—internet • 7—network **Note** You enter only the numeric value. *prec-enum*—Valid values are as follows: • routine • priority • immediate • flash • flash-override • critical • internet • network *qos-grp-val*—QoS group value to assign for this class of traffic, which is other than 0.
Step 6	switch(config-pmap-c-qos)# **exit**	Exits policy-map class configuration mode and enters policy-map mode.

	Command or Action	Purpose
Step 7	switch(config-pmap-qos)# **exit**	Exits policy-map mode and enters configuration mode.
Step 8	(Optional) switch(config)# **show policy-map** [**type qos**] [*policy-map-name*]	Displays information about all configured policy maps or a selected policy map of **type qos**.

Example

This example shows how to create a policy map with Ingress Policing using the committed information rate:

```
switch# configure terminal
switch(config)# policy-map type qos pm1
switch(config-pmap-qos)# class type qos cm1
switch(config-pmap-c-qos)# police cir 10 mbps bc 20 kbytes
switch(config-pmap-c-qos)# set qos-group 4
switch(config-pmap-c-qos)# end
switch# show policy-map type qos pm1

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

  policy-map type qos pm1
  class type qos cm1
  set qos-group 4
  police cir 20 mbytes conform transmit violate drop
  set qos-group 4
  class type qos class-default
  set qos-group 1
  switch#
```

Creating a Policy Map Using a Percentage of the Interface Rate

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map** [**type qos**] [*qos-policy-map-name*]	Creates a named object that represents a set of policies that are applied to a set of traffic classes. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	switch(config-pmap-qos)# **class** [**type qos**] {*class-map-name* | **class-default**}	Associates a class map with the policy map and enters configuration mode for the specified system class. Use the **class-default** keyword to

	Command or Action	Purpose
		select all traffic that is currently not matched by classes in the policy map. The *class-map-name* argument can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.
Step 4	switch(config-pmap-c-qos)# **police** [**cir**] {*committed-rate* [*data-rate*] | **percent** *cir-link-percent*} [[**bc**] {*committed-burst-rate*}][**conform**{**transmit**} [**violate** {**drop**}]]]	Polices **cir** in bits, kbps, mbps, or gbps. The **conform** action is applied if the data rate is less than or equal to **cir**, otherwise, the **violate** action is applied. The **cir** keyword specifies to use the committed information rate, or desired bandwidth, as a bit rate or a percentage of the link rate. The *cir-link-percent* value can range from 1 to 100 percent. Values for *committed-burst-rate* are the following: • bytes—bytes • kbytes—1000 bytes • mbytes—1,000,000 bytes **Note** The maximum supported policer rate is 8 Gbps. If you configure more than 20 percent on a 40 Gbps interfaces or more than 80 percent on a 10 Gbps interfaces, the maximum policer rate of 8 Gbps is used. The following are the Ingress Policing actions: • **conform**—The action to take if the traffic data rate is within bounds. The default action is **transmit.** • **transmit**—Transmits the packet. This is available only when the packet conforms to the parameters. • **violate**—The action to take if the traffic data rate violates the configured rate values. The basic and default action is **drop.** • **drop**—Drops the packet. This is available only when the packet exceeds or violates the parameters.

	Command or Action	Purpose
Step 5	(Optional) switch(config-pmap-c-qos)# **set** {{**dscp** {*dscp-val* | *dscp-enum*}} | {**precedence** {*prec-val* | *prec-enum*}} | {**qos-group** *qos-grp-val*}}	Sets the **dscp**, **precedence**, or **qos-group** actions. *dscp-val*—DSCP value or parameter to assign for this class of traffic. Valid values are from 0 to 63. *prec-val*—IP precendence value to assign for this class of traffic. Valid values from 0 to 7. *qos-grp-val*—QoS group value to assign for this class of traffic. The range is from 1 to 5.
Step 6	switch(config-pmap-c-qos)# **exit**	Exits policy-map class configuration mode and enters policy-map mode.
Step 7	switch(config-pmap-qos)# **exit**	Exits policy-map mode and enters configuration mode.
Step 8	(Optional) switch(config)# **show policy-map** [**type qos**] [*policy-map-name* | **qos-dynamic**]	Displays information about all configured policy maps or a selected policy map of **type qos**.

Example

This example shows how to create a policy map with Ingress Policing using the percentage of the interface rate:

```
switch# configure terminal
switch(config)# policy-map type qos pm-test1
switch(config-pmap-qos)# class type qos cm-cos4
switch(config-pmap-c-qos)# police cir percent 10 bc 40 kbytes conform transmit violate drop
switch(config-pmap-c-qos)# end
switch# show policy-map type qos pm-test1

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

policy-map type qos pm-test1
class type qos cm-cos4
set qos-group 4
police cir percent 10 bc 40 kbytes conform transmit violate drop
class type qos class-default
set qos-group 1
switch#
```

Verifying Ingress Policing Configuration

To verify Ingress Policing configuration information, perform one of the following tasks:

Command	Purpose
switch# **show policy-map interface** [*interface number*]	Displays the policy map settings for an interface or all interfaces.
switch# **show policy-map** [**type qos**] [*policy-map-name*]	Displays information about all configured policy maps or a selected policy map of **type qos**.

Configuration Examples for Ingress Policing

The following example shows the Committed Information Rate (CIR) being specified as a percentage where the Ingress Policing rate is calculated based on the port/port-channel speed:

```
switch(config)# policy-map type qos pm-cos
switch(config-pmap-qos)# class cm-cos
switch(config-pmap-c-qos)# police cir percent 10 bc 20 mbytes conform transmit violate drop

switch(config-pmap-c-qos)#
```

The following example shows the output of the **show policy-map** command with Ingress Policing configured:

```
switch(config-pmap-c-qos)# show policy-map pm-cos


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

  policy-map type qos pm-cos
    class type qos cm-cos
      set qos-group 4
      police cir percent 10 bc 20 mbytes conform transmit violate drop
    class type qos class-default
      set qos-group 1
switch(config-pmap-c-qos)#
```

The following example shows a policy being applied to an interface with the **service-policy** command:

```
switch(config)# interface ethernet 1/1
switch(config-if)# service-policy type qos input pm-cos
```

The following example shows policy statistics being displayed by using the **show policy-map** command:

```
switch(config-if)# show policy-map interface ethernet 1/1
Global statistics status :   disabled

Ethernet1/1

  Service-policy (qos) input:   qos-police
    policy statistics status:   disabled

    Class-map (qos):   qos-police (match-all)
      0 packets
      Match: dscp 10
```

```
police cir percent 100 bc 200 ms
  conformed 0 bytes, 0 bps action: transmit
  violated 0 bytes, 0 bps action: drop
```