Quality of Service Configuration, Cisco Catalyst PON Series Switches

First Published: 2020-11-09

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

CHAPTER 3

CHAPTER 1

Configuring Quality of Service and ACL

Overview of Quality of Service and ACL

Typically, networks operate on a best-effort delivery basis. By enabling the Quality of Service feature, you can provide preferential treatment to certain types of traffic using the congestion-management and congestion-avoidance techniques. Quality of Service (QoS) allows you to classify your network traffic, police and prioritize traffic flow, and provide congestion avoidance. You can configure QoS on physical ports and on switch virtual interfaces (SVIs).

To implement QoS, the device must perform the following tasks:

- Classify the traffic: Distinguish packets or flows from one another.
- Assign a label: Indicate the given QoS as the packets move through the device.
- Police and mark the traffic: Make the packets comply with the configured resource usage limits.
- Queue and schedule traffic: Provide a different treatment in all those situations where resource contentions exist.
- Shape traffic: Ensure that traffic sent from the device meets a specific traffic profile.

With QoS enabled, an Ethernet switching device uses Ethernet QoS technology to provide different levels of QoS guarantees to support traffic flows that have higher delay and jitter requirements.

Access control list (ACL) contains an ordered list of access control entries (ACEs). Each ACE specifies *permit* or *deny* and a set of conditions that a packet must meet in order to match the ACEs. When an interface receives a packet, the device tests the packet against the conditions in the ACL. The first match decides whether the device accepts or rejects the packet. The device stops testing after the first match.

Combining QoS and ACL associates traffic rules with traffic operations that use ACL. You can perform QoS functions, such as, packet filtering, commit access rate, traffic mirroring, traffic redirection, and so on, by referencing an ACL.

Traffic Classification Based on QoS and ACL

Classification is the process of distinguishing one type of traffic from another by examining the fields in a packet.

You can use Standard, Extended, or Layer 2 ACL to define a group of packets with the same characteristics (class). After a traffic class is defined with an ACL, you can attach a policy to it. A policy contains multiple classes with actions that are specified for each one of them. A policy can also include commands to classify the class as a particular aggregate (for example, assign a DSCP) or rate-limit the class. This policy is then attached to the port on which it becomes effective.

Prioritization in Layer 2 Frames

Each host that supports IEEE 802.1Q protocol adds a 4-byte 802.1Q tag header to the source address when sending packets. A 3-bit priority field is a part of this 4-byte header. These three bits indicate the priority of the frame; this determines which packet is sent first when the device is blocked. There are eight priorities that range from 0 to 7.

Table 1: IEEE 802.1Q PRI Field Values

Class of Service (Decimal)	Class of Service (Binary)	Meaning
0	000	Spare
1	001	Background
2	010	Best effort
3	011	Excellent effort
4	100	Controlled load
5	101	Video
6	110	Voice
7	111	Network management

Prioritization in Layer 3 Packets

Layer 3 IP packets carry the classification information in the type of service (ToS) field that has eight bits. The ToS field carries either an IP precedence value or a Differentiated Services Code Point (DSCP) value. IP precedence values range from 0 to 7. DSCP values range from 0 to 63. Based on DSCP or IP precedence, traffic is put into particular service class. Packets within a service class are treated the same way.

If an IP precedence value is used, a 1-byte ToS field consists of three bits of IP precedence and four bits of ToS, and one unused bit. Four bits of ToS field represent minimum latency, maximum throughput, maximum reliability, and, minimal cost. If all the four bits are zero, the service is a general service.

Table 2: IP Precedence Values

IP Precedence（Decimal）	IP Precedence（Binary）	Meaning
0	000	Routine
1	001	Priority
2	010	Immediate
3	011	Flash
4	100	Flash override
5	101	Critical
6	110	Internet
7	111	Network

Differentiated Services, which is defined in RFC 2474, increases the number of definable priority levels. The Differenciated Services field in a packet makes per-hop behavior decisions about packet classification and traffic conditioning functions, such as metering, marking, shaping, and policing.

In a Differenciated Services field, the first six bits (0 to 5) of a ToS field represent DSCP. The Differentiated Services network defines the following four types of traffic:

- Expedited Forwarding (EF) class, which is applicable to low-delay, low-loss, low-jitter, and bandwidth-priority services (such as virtual leased lines), regardless of whether other traffic share its link.
- Assured Forwarding (AF) class, which is divided into four subcategories (AF1, AF2, AF3, AF4). Each AF class is divided into three drop precedence, which is used to classify the AF business. An AF class has a lower QoS level than an EF class.
- Class Selector (CS) evolves from the IP ToS field, which has a total of eight categories.
- Best Effort (BE) is a special category of CS, and there is no guarantee. An AF class is downgraded to BE class after overrun. The existing IP network traffic is also defaulted to this category.

Table 3: DSCP Values

DSCP（Decimal）	DSCP（Decimal）	Meaning
0	000000	BE
46	101110	EF
10	001010	AF1
18	010010	AF2
26	011010	AF3
34	100010	AF4

DSCP（Decimal）	DSCP（Decimal）	Meaning
8	001000	CS1
16	010000	CS2
24	011000	CS3
32	100000	CS4
40	101000	CS5
48	110000	CS6
56	111000	CS7

Configure Quality of Service and ACL

The following sections provide information about the various tasks involved in configuring QoS and ACL.

Configure Traffic Speed Limit

You can monitor the rate of traffic that enters a switch. If the traffic rate exceeds a configured threshold, you can define policies to take suitable measures.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**rate-limit input** {［**ip-group** { *num* | *name* } ［**subitem** *subitem*］ ］［ **link-group** { *num* | *name* } **[subitem** *subitem* ］ ］} *target-rate* **Example:** `Device(config)# rate-limit input ip-group 4 100`	(Optional) Sets the traffic rate limit. Some devices support traffic only in the inbound direction. Some other devices support both inbound and outbound traffic.

Configure Message Redirection

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters the global configuration mode.

	Command or Action	Purpose
	`Device#` **`configure terminal`**	

Step 2	**traffic-redirect** { [**ip-group {** *num* | *name* } [**subitem** *subitem*]] [**link-group**{ *num* | *name* } [**subitem** *subitem*]] } { [**interface** *interface-num* | **cpu**] }
	Example:
	`Device(config)#` **`traffic-redirect link-group link1 interface ethenet0/1`**
		(Optional) Sets an instruction to forward the messages to an egress port.

Copy Messages to a CPU

You can copy specific messages that are defined by the ACL rule to a CPU.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#` **`configure terminal`**	Enters global configuration mode.

Step 2	**traffic-copy-to-cpu** { [**ip-group** { *num* | *name*} [**subitem** *subitem*]] [**link-group** { *num*| *name* } [**subitem** *subitem*]] }
	Example:
	`Device(config)#` **`traffic-copy-to-cpu ip-group 3`**
		Copies the packets that match an ACL rule to a CPU.

Configure Traffic Statistics

You can get the statistics of the packets that match an ACL rule on the specified ports, in terms of packet numbers and bytes.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#` **`configure terminal`**	Enters global configuration mode.
Step 2	**traffic-statistic** { [**ip-group** { *num* | *name* } [**subitem** *subitem*]] [**link-group** { *num*| *name* } [**subitem** *subitem*]] } **Example:**	(Optional) Configures the device to collect traffic statistics. This command displays a cumulative value of the count of the number of packets that match the ACL rule.

	Command or Action	Purpose
	`Device# traffic-statistic ip-group 4`	If you reconfigure traffic statistics, the packet count information is lost.

Step 3	**clear traffic-statistic** { [**all** | [**ip-group** { *num* | *name* }[**subitem** *subitem*]][**link-group** { *num*| *name* } [**subitem** *subitem*]]] }
	Example:
	`Device# clear traffic-statistic all`
		(Optional) Clears the traffic statistics information.

Display Quality of Service and ACL Configurations

Use the following **show** commands to view the QoS and ACL configurations and perform maintenance operations.

Table 4: QoS and ACL show Commands

Command	Operation
show qos-info all	Displays all parameters of QoS that are set for a device.
show qos-info statistic	Displays the total number of rules that are configured for each QoS parameter.
show qos-info traffic-copy-to-cpu	Displays the parameter settings for copying the messages to a CPU.
show qos-info mirrored-to	Displays the ports to which the messages are copied.
show qos-info traffic-priority	Displays the parameters that are configured for priority marking of the packets that match an ACL rule.
show qos-info traffic-redirect	Displays the parameters that are configured for redirecting the packets that match an ACL rule.
show qos-info traffic-statistic	Displays the statistics for the QoS traffic.
show qos-interface all	Displays the configurations of rate limit on a port.
show qos-interface rate-limit	Displays the rate-limit configuration information of all ports.
show qos-interface statistic	Displays all the rules for rate limit that are set on a device.

Example: Configuring Quality of Service and ACL

Consider a network topology where device A and device B are connected by an Ethernet switch, which is in turn connected to the internet. A and B do not belong to the same network segment. A connects to the switch through its Ethernet port e1/1, and B connects to the switch through its Ethernet port e1/2.

The following example shows how you can redirect traffic through port e1/1 using HTTP to access internet through e1/2:

```
Device# configure terminal
Device(config)# time-range a
Device(config-timerange-a)# periodic weekdays daily 08:30:00 to 18:00:00
Device(config-timerange-a)# exit

Device(config)# time-range b
Device(config-timerange-b)# periodic weekdays 00:00:00 to 08:30:00
Device(config-timerange-b)# periodic weekend 00:00:00 to 23:59:00
Device(config-timerange-b)# exit
```

The following example shows to configure an ACL to access the internet using HTTP message classification at different time periods:

```
Device(config)# access-list 100 permit tcp any 192.168.0.1 0 80 time-range a
Device(config)# access-list 100 permit tcp any 192.168.0.1 0 80 time-range b
```

CHAPTER 2

Configuring Class of Service Control

Overview of Class of Service Control

Class of Service (CoS) helps resolve the problem of network congestion by giving certain types of traffic priority over others. Network congestion occurs when multiple messages are competing for network resources at the same time.

Common queue scheduling algorithms such as First Come First Serve (FCFS), Strict-Priority Queue scheduling, Weighted Round Robin (WRR) scheduling, and Strict-Priority Queue + WRR scheduling help decongest a network.

First Come First Serve

The FCFS algorithm does not classify a message. It simply follows a first-in-first-out method. When a message arrives at an interface faster that the interface can send it, the FCFS algorithm forwards the message to the queue in the order of receiving the message. It sends out messages in the same order as receiving them.

Strict-Priority Queuing

Strict-Priority Queuing is designed for critical business applications, wherein services are prioritized in order to reduce the latency of response when a congestion occurs. A priority queue classifies all messages into eight classes—7, 6, 5, 4, 3, 2, 1, and 0, in the order of priority. The group of critical services is put into the higher-priority queue, and noncritical business group is put into the lower-priority queue. The higher-priority queue is emptied before the messages in the lower-priority queue are sent. Messages in the group of noncritical business are transmitted in the idle gap of handling critical business data.

The disadvantage of Strict-Priority Queuing is that the messages in the lower-priority group are not sent if the higher-priority queue is not emptied.

Weighted Round Robin Scheduling

Weighted Round Robin (WRR) queue scheduling divides each port into eight output queues—7, 6, 5, 4, 3, 2, 1, and 0, in that order of priority, with 7 being the highest priority. All the queues are scheduled by turns and each queue gets a certain service time. Each queue of WRR can be configured with weighted values of w7, w6, w5, w4, w3, w2, w1, or w0. The weighted value represents the weight of the resource. For example, on a 100 Mb port, if you configure the WRR for 80, 70, 60, 50, 50, 40, 30, and 20, in that order of priority, the WRR of 20 is assured of at least 5 Mbps bandwidth.

An advantage of WRR queuing is that although multiple queues are scheduled by polling, each queue is not assigned a fixed time slot. If a queue is empty, it immediately switches to the next queue schedule so that the bandwidth and resources of that queue can be fully utilized.

Strict-Priority Queuing and Weighted Round Robin Scheduling

Strict-Priority queuing and WRR scheduling combine their algorithms. If the weight of a queue is set to 0, the queue follows the Strict-Priority queuing algorithm to send messages. A non-0 value of the weight switches the queue to the WRR scheduling mechanism.

Weighted Fair Queuing

Weighted Fair Queuing (WFQ) is flow-based queuing that schedules interactive traffic to the front of the queue to reduce response time. WFQ shares the remaining bandwidth between high-bandwidth flows.

Configure Class of Service Control

The following sections provide information about configuring class of service control.

Configure Class of Service

Note By default, Strict-Priority Queuing is configured.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**queue-scheduler strict-priority** **Example:** `Device(config)# queue-scheduler strict-priority`	(Optional) Configures Strict-Priority Queuing mode.

	Command or Action	Purpose
Step 3	**queue-scheduler wrr** *w1 w2 w3 w4 w5 w6 w7 w8* **Example:** `Device(config)# queue-scheduler wrr 1 2 3 4 5 6 7 8`	(Optional) Configures WRR scheduling mode.
Step 4	**queue-scheduler sp-wrr** *w1 w2 w3 w4 w5 w6 w7 w8* **Example:** `Device(config)# queue-scheduler sp-wrr 1 2 3 4 5 6 7 8`	(Optional) Configures Strict-Priority and WRR scheduling mode.
Step 5	**no queue-scheduler** **Example:** `Device(config)# no queue-scheduler`	(Optional) Restores the default scheduler, which is Strict-Priority Queuing.
Step 6	**show queue-scheduler** **Example:** `Device(config)# show queue-scheduler`	(Optional) Displays information about the queue scheduler.

Configure DSCP to 802.1p Mapping

Differentiated Services Code Point (DSCP) marking operates in Layer 3 and determines traffic classification for network data. 802.1p marking is a Layer 2 Class of Service. You can define what level of service you want to allocate to specific markings. DSCP allows 64 priority values, whereas 802.1p (hardware queue) allows only eight priority values. By default, the following is the mapping between DSCP and 802.1p:

Table 5: DSCP-802.1p (Hardware Priority Queue) Mapping

DSCP	802.1p
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

Note

- DSCP mapping is disabled by default. Enable DSCP mapping before you perform related configurations.
- You can change the mapping relation between DSCP precedence and output queues by changing the mapping between DSCP priorities and 802.1p priorities according to the actual network requirements.

To configure DSCP to 802.1p mapping, perform the following procedure:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	[**no**] **queue-scheduler dscp-map** **Example:** `Device(config)# queue-scheduler dscp-map`	(Optional) Enables DSCP mapping function. Use the **no** form of the command to disable DSCP mapping.
Step 3	**queue-scheduler dscp-map** *dscp-v priority-v* **Example:** `Device(config)# queue-scheduler dscp-map 1 4`	(Optional) Maps DSCP values to 802.1p values (hardware priority queue).
Step 4	**show queue-scheduler dscp-map** **Example:** `Device(config)# show queue-scheduler dscp-map`	(Optional) Displays the mapping between DSCP and 802.1p values.

Configure 802.1p and Hardware Queue Mapping

802.1p is used to classify the outgoing traffic at the egress port based on the 802.1p priority. For each message that enters the switch, the system maps the specific hardware queue priority according to the 802.1p priority of the message.

The default mapping relation between 802.1p and hardware priority is shown in the following table:

Table 6: 802.1p and Hardware Queue Mapping

802.1p	Hardware Priority Queue
0	0
1	1
2	2

802.1p	Hardware Priority Queue
3	3
4	4
5	5
6	6
7	7

Note

- Changing the mapping relation between 802.1p priority and hardware queues changes the mapping relation between 802.1p priorities and output queues.
- If two 802.1p priorities are mapped to the same hardware priority queue, messages of the two 802.1p priorities cannot be forwarded with 1:1 forwarding.

To configure 802.1p to hardware queue mapping, perform the following procedure:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**queue-scheduler cos-map** *queue-v priority-v* **Example:** `Device(config)# queue-scheduler cos-map 1 10`	(Optional) Configures 802.1p and the hardware queue map.
Step 3	**show queue-scheduler cos-map** **Example:** `Device(config)# show queue-scheduler cos-map`	(Optional) Displays 802.1p and the hardware queue mapping information.

Examples: Configuring Class of Service Control

The following example shows how to view the default queue scheduling mode:

```
Device(config)# show queue-scheduler

Queue scheduler status : enable
Queue scheduler mode   : SP (Strict Priority)
```

The following example displays the priority-mapping relationship between 802.1p and hardware queues.

```
Device(config)# show queue-scheduler cos-map

Information about map of cos:
802.1P Priority  Queue of class
-------------------------------
0                0
1                1
2                2
3                3
4                4
5                5
6                6
7                7
```

The following example shows how to modify the priority-mapping relationship between 802.1p and hardware queue by mapping the packets with priority 0 to queue 1:

```
Device(config)# queue-scheduler cos-map 1 10
Configured successfully.

Device(config)# show queue-scheduler cos-map

Information about map of cos:
802.1P Priority  Queue of class
-------------------------------
0                1
1                1
2                2
3                3
4                4
5                5
6                6
7                7
```

The following example shows how to configure WRR queue scheduling:

```
Device(config)# queue-scheduler wrr 1 2 3 4 5 6 7 8
Configured queue scheduler successfully

Device(config)# show queue-scheduler

Queue scheduler status : enable
Queue scheduler mode   : WRR (Weighted Round Robin)
Queue0 weight is 1
Queue1 weight is 2
Queue2 weight is 3
Queue3 weight is 4
Queue4 weight is 5
Queue5 weight is 6
Queue6 weight is 7
Queue7 weight is 8
```

The following example shows how to restore the default queue schedule:

```
Device(config)# no queue-scheduler

Recovered queue scheduler to default value(strict-priority) successfully.

Device(config)#show queue-scheduler
Queue scheduler status : enable
Queue scheduler mode   : SP (Strict Priority)
```

CHAPTER 3

Configuring Forward Control

Overview of Forward Control

This chapter describes the following aspects of forward control in a network:

- Bandwidth limit for a port: You can shape the outgoing or egress traffic transmission rate on a device by setting the bandwidth limit for its port.
- Storm control: The storm-control function prevents a traffic storm from occurring because of excessive messages in the network. The function monitors the number of messages on each port to understand the bandwidth usage, and ensures that the bandwidth is within the configured threshold. It discards all the packets that are received after the threshold is reached.

Configure Forward Control

The following sections provide information about configuring forward control.

Configure Bandwidth Limit for a Port

Bandwidth is the amount of data that can be transferred through a network path. You can set the total rate of incoming or outgoing traffic on a port.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface ethernet** *port-number* **Example:**	Enters interface configuration mode.

	Command or Action	Purpose
	`Device(config)# interface ethernet 1/1`	
Step 3	[**no**] **bandwidth egress** *rate* **Example:** `Device(config-if-ethernet-1-1)# bandwidth egress 1024`	(Optional) Sets the bandwidth limit on the outbound traffic on a port.
Step 4	**exit** **Example:** `Device(config-if-ethernet-1-1)# exit`	Exits interface configuration mode.
Step 5	**show bandwidth egress interface** [**ethernet** *port-number*] **Example:** `Device(config)# show bandwidth egress interface ethernet 1/1`	Displays the bandwidth control information of the port.

Example: Configuring Bandwidth Limit

The following example shows how to configure the bandwidth limit on port number 1, whose speed at ingress is set at 1024 kilo bytes:

```
Device# configure terminal
Device(config)# interface ethernet 1/1
Device(config-if-ethernet-1-1)# bandwidth ingress 1024
Device(config-if-ethernet-1-1)# exit

Device(config)# show bandwidth-control interface ethernet 1/1
port    Ingress bandwidth control  Egress bandwidth control
e1/1  1024 kbps                  disable

Total entries: 1.
```

Configure Storm Control

The Storm Control functionality prevents a port from being disrupted when a traffic storm occurs. Traffic storms occur when excess packets flood the LAN and degrade network performance.

The Storm Control functionality monitors the number of messages on a port. It controls the bandwidth of messages ensuring that they are within the configured threshold, and discards those packets that exceed the threshold limit.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**interface ethernet** *slot/port* **Example:** `Device(config)# interface ethernet 1/1`	Enters interface configuration mode.
Step 3	**storm-control** {**broadcast** | **multicast** | **unicast** } *target-rate* **Example:** `Device(config-if-ethernet-1/1)# storm-control multicast 256`	(Optional) Enables unicast, broadcast, or multicast traffic storm control on the interface and sets the threshold limit for the number of packets that the interface can process.
Step 4	**show storm-control interface** [**ethernet** | **gpon** *port-number*] **Example:** `Device(config)# show storm-control interface ethernet 1/1`	Displays storm control information for the specified interface.

Example: Configuring Storm Control

The following example shows how to configure storm control on port 1, and set the broadcast, multicast, and unicast storm suppression threshold values:

```
Device# configure terminal
Device(config)# interface ethernet 1/1
Device(config-if-ethernet-1/1)# storm-control broadcast 128
Device(config-if-ethernet-1/1)# storm-control multicast 256

Device(config-if-ethernet-1/1)# storm-control unicast 512
```

The following example shows how to view the port's storm control settings:

```
Device(config)# show storm-control interface ethernet 1/1
Ethernet e1/1 is enabled, port link is down
 Hardware address is 00:00:53:28:00:0a
 SetSpeed is auto, ActualSpeed is unknown, Duplex mode is unknown
 Current port type: 1000BASE-T
 Priority is 0
 Flow control is disabled
 Broadcast storm control target rate is 128Kbps
 Multicast storm control target rate is 256Kbps
 Unicast storm control target rate is 512Kbps
 PVID is 1
 Port mode: hybrid
 Untagged  VLAN ID : 1
 Input  : 0 packets, 0 bytes
         0 broadcasts, 0 multicasts, 0 unicasts
 Output : 0 packets, 0 bytes
         0 broadcasts, 0 multicasts, 0 unicasts
```