Restrictions for PFC QoS

Note
- For complete syntax and usage information for the commands used in this chapter, see these publications:

  http://www.cisco.com/en/US/products/ps11845/prod_command_reference_list.html

- Cisco IOS Release 15.0SY supports only Ethernet interfaces. Cisco IOS Release 15.0SY does not support any WAN features or commands.

Tip For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum

General Guidelines

- With Release 15.0(1)SY1 and later releases, you can increase the supported number of QoS TCAM entries:

	TCAM Banks	QoS TCAM Entries	
		PFC4 Mode	PFC4XL Mode
Release 15.0(1)SY • Not configurable in Release 15.0(1)SY. • Default for 15.0(1)SY1 and later releases. • Command in Release 15.0(1)SY1 and later releases: `platform hardware acl reserve qos-banks 1`	1	16K	64K
Release 15.0(1)SY1 and later releases. Command: `platform hardware acl reserve qos-banks 2`	2	32K	128K

Changes to the supported number of QoS TCAM entries take effect after a reload. Enter the **show platform hardware acl global-config** command to display the QoS TCAM entry configuration:

```
Router# show platform hardware acl global-config | include [Bb]anks
Reserved QoS Banks:
 Current 1 banks
 Latest set 1 banks
 After next reload 1 banks
Router#
```

Enter the **show platform hardware pfc mode** command to display the PFC mode.

- PFC QoS supports IGMP, MLD, and PIM traffic.

- The **match ip precedence** and **match ip dscp** commands filter only IPv4 traffic.

- The **match precedence** and **match dscp** commands filter IPv4 and IPv6 traffic.

- The **set ip dscp** and **set ip precedence** commands are saved in the configuration file as **set dscp** and **set precedence** commands.

- PFC QoS supports the **set dscp** and **set precedence** policy map class commands for IPv4 and IPv6 traffic.

- The flowmask requirements of QoS, NetFlow, and NetFlow data export (NDE) might conflict, especially if you configure microflow policing.

- With egress ACL support for remarked DSCP and VACL capture both configured on an interface, VACL capture might capture two copies of each packet, and the second copy might be corrupt.

- You cannot configure egress ACL support for remarked DSCP on tunnel interfaces.

- Egress ACL support for remarked DSCP supports IP unicast traffic.

- Egress ACL support for remarked DSCP is not relevant to multicast traffic. PFC QoS applies ingress QoS changes to multicast traffic before applying egress QoS.

- NetFlow and NetFlow data export (NDE) do not support interfaces where egress ACL support for remarked DSCP is configured.

- When egress ACL support for remarked DSCP is configured on any interface, you must configure an interface-specific flowmask to enable NetFlow and NDE support on interfaces where egress ACL support for remarked DSCP is not configured. Enter either the **platform flow ip interface-destination-source** or the **platform flow ip interface-full** global configuration mode command.

- Interface counters are not accurate on interfaces where egress ACL support for remarked DSCP is configured.

- You cannot apply microflow policing to traffic that has been permitted by egress ACL support for remarked DSCP.

- Traffic that has been permitted by egress ACL support for remarked DSCP cannot be tagged as MPLS traffic. (The traffic can be tagged as MPLS traffic on another network device.)

- When you apply both ingress policing and egress policing to the same traffic, both the input policy and the output policy must either mark down traffic or drop traffic. PFC QoS does not support ingress markdown with egress drop or ingress drop with egress markdown. (CSCea23571)

- If traffic is both aggregate and microflow policed, then the aggregate and microflow policers must both be in the same policy-map class and each must use the same **conform-action** and **exceed-action** keyword option: **drop**, **set-dscp-transmit**, **set-prec-transmit**, or **transmit**.

- You cannot configure PFC QoS features on tunnel interfaces.

- PFC QoS does not rewrite the payload ToS byte in tunnel traffic.

- PFC QoS filters only by ACLs, dscp values, or IP precedence values.

- For these commands, PFC QoS applies identical configuration to all LAN ports controlled by the same application-specific integrated circuit (ASIC):

    – **rcv-queue cos-map**

    – **wrr-queue cos-map**

- Except for WS-X6904-40G-2T, WS-X6908-10GE, WS-X6816-10T-2T, WS-X6716-10T, WS-X6816-10G-2T, WS-X6716-10GE, WS-X6704-10GE, WS-X6848-SFP-2T, WS-X6748-SFP, WS-X6824-SFP-2T, WS-X6724-SFP, WS-X6848-TX-2T, WS-X6748-GE-TX modules, PFC QoS applies identical configuration to all LAN ports controlled by the same application-specific integrated circuit (ASIC) for these commands:

    – **rcv-queue random-detect**

    – **rcv-queue queue-limit**

    – **wrr-queue queue-limit**

    – **wrr-queue bandwidth**

    – **priority-queue cos-map**

    – **wrr-queue threshold**

    – **rcv-queue threshold**

    – **wrr-queue random-detect**

    – **wrr-queue random-detect min-threshold**

    – **wrr-queue random-detect max-threshold**

- Configure these commands only on physical ports. Do not configure these commands on logical interfaces:

    – **priority-queue cos-map**

    – **wrr-queue cos-map**

- **wrr-queue random-detect**

- **wrr-queue random-detect max-threshold**

- **wrr-queue random-detect min-threshold**

- **wrr-queue threshold**

- **wrr-queue queue-limit**

- **wrr-queue bandwidth**

- **rcv-queue cos-map**

- **rcv-queue bandwidth**

- **rcv-queue random-detect**

- **rcv-queue random-detect max-threshold**

- **rcv-queue random-detect min-threshold**

- **rcv-queue queue-limit**

- **rcv-queue cos-map**

- **rcv-queue threshold**

Note   IP multicast switching using egress packet replication is not compatible with QoS. In some cases, egress replication can result in the incorrect COS or DSCP marking of packets. If you are using QoS and your switching modules are capable of egress replication, enter the **platform ip multicast replication-mode ingress** command to force ingress replication.

PFC and DFC Guidelines

- The PFC and DFCs support QoS for IPv6 unicast and multicast traffic.

- To display information about IPv6 PFC QoS, enter the **show platform qos ipv6** command.

- The QoS features implemented in the port ASICs (queue architecture and dequeuing algorithms) support IPv4 and IPv6 traffic.

- The PFC and DFCs support IPv6 named extended ACLs and named standard ACLs.

- The PFC and DFCs support the **match protocol ipv6** command.

- With egress ACL support for remarked DSCP configured, the PFC and DFCs do not provide hardware-assistance for these features:

  - Cisco IOS reflexive ACLs

  - Network Address Translation (NAT)

- You cannot apply microflow policing to ARP traffic.

- The PFC and DFCs do not apply egress policing to traffic that is being bridged to the RP.

- The PFC and DFCs do not apply egress policing or egress DSCP mutation to multicast traffic from the RP.

- PFC QoS does not rewrite the ToS byte in bridged multicast traffic.

- The PFC and DFCs support up to 1022 aggregate policers, but some PFC QoS commands other than the **police** command will be included in this count. By default, any policy using a **set** or **trust** command will be included in the aggregate policer count. You can disable the addition of the **set** or

trust commands to the aggregate policer count by entering the **no platform qos marking statistics** command, but you will then be unable to collect statistics for the classmaps associated with these commands. You can view the aggregate policer count in the QoS Policer Resources section of the output of the **show platform hardware capacity qos** command.

Class Map Command Restrictions

- PFC QoS supports a single **match** command in **class-map match-all** class maps, except that the **match protocol** command can be configured in a class map with the **match dscp** or **match precedence** command.

- PFC QoS supports multiple **match** commands in **class-map match-any** class maps.

> **Note**   PFC QoS supports a maximum of 9 commands that match DSCP or IP precedence values in class maps and ACLs.

- PFC QoS does not support these class map commands:
  - **match classmap**
  - **match destination-address**
  - **match input-interface**
  - **match source-address**

Policy Map Class Command Restrictions

PFC QoS does not support these policy map class commands:

- **set qos-group**
- **service-policy**

Supported Granularity for CIR and PIR Rate Values

CIR and PIR Rate Value Range	Granularity
32768 to 2097152 (2 Mbs)	32768 (32 Kb)
2097153 to 4194304 (4 Mbs)	65536 (64 Kb)
4194305 to 8388608 (8 Mbs)	131072 (128 Kb)
8388609 to 16777216 (16 Mbs)	262144 (256 Kb)
16777217 to 33554432 (32 Mbs)	524288 (512 Kb)
33554433 to 67108864 (64 Mbs)	1048576 (1 Mb)
67108865 to 134217728 (128 Mbs)	2097152 (2 Mb)
134217729 to 268435456 (256 Mbs)	4194304 (4 Mb)
268435457 to 536870912 (512 Mbs)	8388608 (8 Mb)

CIR and PIR Rate Value Range	Granularity
536870913 to 1073741824 (1 Gbs)	16777216 (16 Mb)
1073741825 to 2147483648 (2 Gbs)	33554432 (32 Mb)
2147483649 to 4294967296 (4 Gbs)	67108864 (64 Mb)
4294967296 to 8589934592 (8 Gbs)	134217728 (128 Mb)
8589934593 to 17179869184 (16 Gbs)	268435456 (256 Mb)
17179869185 to 34359738368 (32 Gbs)	536870912 (512 Mb)
34359738369 to 68719476736 (64 Gbs)	1073741824 (1024 Mb)

Within each range, PFC QoS programs the PFC with rate values that are multiples of the granularity values.

Supported Granularity for CIR and PIR Token Bucket Sizes

CIR and PIR Token Bucket Size Range	Granularity
1 to 32768 (32 KB)	1024 (1 KB)
32769 to 65536 (64 KB)	2048 (2 KB)
65537 to 131072 (128 KB)	4096 (4 KB)
131073 to 262144 (256 KB)	8196 (8 KB)
262145 to 524288 (512 KB)	16392 (16 KB)
524289 to 1048576 (1 MB)	32768 (32 KB)
1048577 to 2097152 (2 MB)	65536 (64 KB)
2097153 to 4194304 (4 MB)	131072 (128 KB)
4194305 to 8388608 (8 MB)	262144 (256 KB)
8388609 to 16777216 (16 MB)	524288 (512 KB)
16777217 to 33554432 (32 MB)	1048576 (1 MB)

Within each range, PFC QoS programs the PFC with token bucket sizes that are multiples of the granularity values.
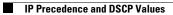
IP Precedence and DSCP Values

3-bit IP Precedence	6 most significant bits of ToS						6-bit DSCP	3-bit IP Precedence	6 most significant bits of ToS						6-bit DSCP
	8	7	6	5	4	3			8	7	6	5	4	3	
0	0	0	0	0	0	0	0	4	1	0	0	0	0	0	32
	0	0	0	0	0	1	1		1	0	0	0	0	1	33
	0	0	0	0	1	0	2		1	0	0	0	1	0	34
	0	0	0	0	1	1	3		1	0	0	0	1	1	35
	0	0	0	1	0	0	4		1	0	0	1	0	0	36
	0	0	0	1	0	1	5		1	0	0	1	0	1	37
	0	0	0	1	1	0	6		1	0	0	1	1	0	38
	0	0	0	1	1	1	7		1	0	0	1	1	1	39
1	0	0	1	0	0	0	8	5	1	0	1	0	0	0	40
	0	0	1	0	0	1	9		1	0	1	0	0	1	41
	0	0	1	0	1	0	10		1	0	1	0	1	0	42
	0	0	1	0	1	1	11		1	0	1	0	1	1	43
	0	0	1	1	0	0	12		1	0	1	1	0	0	44
	0	0	1	1	0	1	13		1	0	1	1	0	1	45
	0	0	1	1	1	0	14		1	0	1	1	1	0	46
	0	0	1	1	1	1	15		1	0	1	1	1	1	47
2	0	1	0	0	0	0	16	6	1	1	0	0	0	0	48
	0	1	0	0	0	1	17		1	1	0	0	0	1	49
	0	1	0	0	1	0	18		1	1	0	0	1	0	50
	0	1	0	0	1	1	19		1	1	0	0	1	1	51
	0	1	0	1	0	0	20		1	1	0	1	0	0	52
	0	1	0	1	0	1	21		1	1	0	1	0	1	53
	0	1	0	1	1	0	22		1	1	0	1	1	0	54
	0	1	0	1	1	1	23		1	1	0	1	1	1	55
3	0	1	1	0	0	0	24	7	1	1	1	0	0	0	56
	0	1	1	0	0	1	25		1	1	1	0	0	1	57
	0	1	1	0	1	0	26		1	1	1	0	1	0	58
	0	1	1	0	1	1	27		1	1	1	0	1	1	59
	0	1	1	1	0	0	28		1	1	1	1	0	0	60
	0	1	1	1	0	1	29		1	1	1	1	0	1	61
	0	1	1	1	1	0	30		1	1	1	1	1	0	62
	0	1	1	1	1	1	31		1	1	1	1	1	1	63

Tip   For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum