Catalyst 6500/6000 QoS FAQ

Document ID: 64026

Contents

Introduction

This document addresses frequently asked questions (FAQs) about the Quality of Service (QoS) feature of the Catalyst 6500/6000 with Supervisor 1 (Sup1), Supervisor 1A (Sup1A), Supervisor 2 (Sup2), and Supervisor 720 (Sup720) that run Catalyst OS (CatOS). In this document, these switches are referred to as Catalyst 6500 (Cat6K) Switches that run CatOS. Refer to Configuring PFC QoS for QoS features on Catalyst 6500/6000 Switches that run Cisco IOS® software.

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Q. Is QoS enabled by default on Catalyst 6500 Switches?

A. By default, QoS is not enabled. Issue the **set qos enable** command in order to enable QoS.

Q. What is the default differentiated services code point (DSCP) value that is assigned to packets?

A. All traffic that enters an untrusted port is marked with a DSCP of 0. Specifically, DSCP is re−marked to 0 by the egress port.

Q. Can I set up VLAN−based QoS on a 6500?

A. The default setting is port−based. You can change that if you issue the **set port qos**

mod/*port* **vlan−based** command.

Q. What are the port capabilities for each line card and how can I interpret the queue capabilities?

A. Refer to the port capabilities table in the Understanding the Queueing Capability of a Port section of QoS Output Scheduling on Catalyst 6500/6000 Series Switches Running CatOS System Software.

Q. What are the default QoS configurations on a 6500 when QoS is initially enabled?

A. Refer to the Default Configuration for QoS on the Catalyst 6000 section of QoS Output Scheduling on Catalyst 6500/6000 Series Switches Running CatOS System Software.

Q. Where are each of the QoS processes performed in the Catalyst 6000?

A. Input Scheduling Done by PINNACLE/COIL port application−specific integrated circuits (ASICs). Layer 2 only, with or without a Policy Feature Card (PFC).

Classification Done by Supervisor or by PFC via the access control list (ACL) engine. Layer 2 only, without a PFC; Layer 2 or Layer 3 with a PFC.

Policing Done by PFC via the Layer 3 forwarding engine. Layer 2 or Layer 3 with a PFC (required).

Packet Re−write Done by PINNACLE/COIL port ASICs. Layer 2 or Layer 3 based on classification done previously.

Output Scheduling Done by PINNACLE/COIL port ASICs. Layer 2 or Layer 3 based on classification done previously.

Q. Can I implement QoS features without a Policy Feature Card (PFC)?

A. In Catalyst 6000 Family Switches, the heart of QoS functionality resides on the PFC and is a requirement for Layer 3 or Layer 4 QoS processing. However, a supervisor without a PFC can be used for Layer 2 QoS classification and marking.

Q. What is the difference in QoS functionality between the Policy Feature Card 1 (PFC1) and PFC2?

A. PFC2 lets you push down the QoS policy to a Distributed Forwarding Card (DFC). PFC2 also adds support for an excess rate, which indicates a second policing level at which policy actions can be taken. Refer to the Hardware Support for QoS in the Catalyst 6000 Family section of Understanding Quality of Service on Catalyst 6000 Family Switches for more information.

Q. What are the default class of service (CoS) to transmit queue mapping configurations when auto−qos is enabled?

A. set qos map 2q2t tx queue 2 2 cos 5,6,7

set qos map 2q2t tx queue 2 1 cos 1,2,3,4

set qos map 2q2t tx queue 1 1 cos 0

Q. What is the default differentiated services code point (DSCP) to class of service (CoS) mapping?

A. 8 to 1 (divide DSCP by 8 to get CoS).

Q. On egress queuing, if the strict priority queue is saturated, is traffic eventually served in the weighted round−robin (WRR) queues?

A. No, the WRR queues are not served until the priority queue is completely empty.

Q. Does weighted round−robin (WRR) determine bandwidth allocation based on number of packets or on a certain number of bytes?

A. Based on a certain number of bytes, which can represent more than one packet. The final packet that exceeds the bytes allocated is not sent. With an extreme weight configuration, such as 1% for queue 1 and 99% for queue 2, the exact configured weight might not be reached. The switch uses a WRR algorithm to transmit frames from one queue at a time. WRR uses a weight value to decide how much to transmit from one queue before it switches to the other queue. The higher the weight assigned to a queue, the more transmit bandwidth is allocated to it.

Note: The actual number of bytes transmitted does not match the calculation because whole frames are transmitted before it switches to the other queue.

Q. My new 65xx line card documentation says it supports deficit weighted round−robin (DWRR). What is DWRR and what does it mean?

A. DWRR transmits from the queues without starving the low−priority queue, because it keeps track of low−priority queue under−transmission and compensates for it in the next round. If a queue is not able to send a packet because its packet size is larger than the available bytes, then the unused bytes are credited to the next round.

Q. What are the default weights on a 2q2t port, and how do I modify them?

A. Issue the **set qos wrr 2q2t** *q1_weight q2_weight* command in order to modify the default weights for Queue 1 (the low priority queue served 5/260th of time) and Queue 2 (the high priority queue served 255/260th of time).

Q. I would like to use Simple Network Management Protocol (SNMP) to gather the number of dropped packets by individual policer. Is this possible? If so, what MIB is used?

A. Yes, SNMP supports the CISCO−QOS−PIB−MIB and CISCO−CAR−MIB.

Q. Is there a show command which displays the number of dropped packets by policer?

A. The **show qos statistics aggregate−policer** and **show qos statistics l3stats** commands display the number of dropped packets by policer.

Q. I would like to use Simple Network Management Protocol (SNMP) to modify a policer so that the rate and burst parameters can be changed dynamically. For example, by time of day. Is this possible? If so, what MIB is used?

A. Yes, SNMP supports the CISCO−QOS−PIB−MIB and CISCO−CAR−MIB.

Q. Is it possible to implement time−of−day−based QoS specifically, to modify the maximum and burst rates through Cisco IOS software on the Multilayer Switch Feature Card (MSFC) in hybrid mode? If possible, is this QoS done in hardware and not by the MSFC processor?

A. No, this cannot be done. In hybrid mode (CatOS), all QoS policing is done by the supervisor.

Q. I did not see a description of how the policer rate and policer burst values are implemented. I would like to complete technical documentation on these, so that I can understand the impact that they have on my network.

A. The policer rate and policer burst values are implemented in this manner:

```
burst = sustained rate bps × 0.00025 (the leaky bucket rate) + MTU kbps
```

For example, if you want a 20 Mbps policer and a maximum transmission unit (MTU) (on Ethernet) of 1500 bytes, then this is how the burst is calculated:

```
burst = (20,000,000 bps × 0.00025) + (1500 × 0.008 kbps)
      = 5000 bps + 12 kbps
      = 17 kbps
```

However, due to granularity of policer hardware with Sup1 and Sup2, you need to round this to 32 kbps, which is the minimum.

Refer to these documents for more information about the policer rate and burst values implementation:

- QoS Output Scheduling on Catalyst 6500/6000 Series Switches Running CatOS System Software
- Configuring QoS

Q. I plan on replacing my Sup1A Supervisors with Sup2s. Do the mechanics of QoS, such as the burst rate, change between Sup1A and Sup2?

A. Yes, there is difference between two supervisors when a Catalyst 6500 Switch has SUP2/PFC2. If it runs Cisco Express Forwarding (CEF), then the behavior is slightly different when you configure the netflow in SUP2.

Q. What are some commands that I can use to monitor my QoS settings?

A. Refer to the Monitoring and Verifying a Configuration section of QoS Classification and Marking on Catalyst 6500/6000 Series Switches Running CatOS Software.

Q. When I run Catalyst operating system (CatOS) code on a 6500 and Cisco IOS software in the Multilayer Switch Feature Card (MSFC), do I issue the QoS commands on the MSFC or on the supervisor?

A. When you run hybrid code (CatOS), you issue the QoS commands on the supervisor/Policy Feature Card (PFC). The 6500 performs QoS in three places:

- Software−based in the MSFC
- Hardware−based (multi−layer switching−based) in the PFC
- Software−based on some line cards

This issue occurs when you work with hybrid IOS (CatOS + IOS for MSFC). The CatOS and IOS have two sets of configuration commands. However, when you configure QoS under native IOS, for example with the newer Sup32 or Sup720 engines, you are further from the hardware, and the line card part is invisible to the user. This is important because most of the traffic is multi−layer switched (hardware switched). Therefore, it is handled by the PFC logic. The MSFC never sees that traffic. If you are not setting up PFC−based QoS, most of the traffic is lost.

Q. What happens if the set port qos trust command is not supported by my line card?

A. You can create a QoS access control list (ACL) to trust the differentiated services code point (DSCP) value of the incoming packet. For example, issue the **set qos acl ip test trust−dscp any** command.

Q. What is the difference between aggregate and microflow policers?

A. Refer to the Classification and Policing with the PFC section of Understanding Quality of Service on Catalyst 6000 Family Switches.

Q. What commands allow me to view statistics for aggregate or microflow policers?

A. With Supervisor Engine 1 and 1A, it is not possible to have policing statistics for individual aggregate policers. Issue the **show qos statistics l3stats** command in order to view the per−system policing statistics.

With the Supervisor Engine 2, you can view aggregate policing statistics on a per−policer basis with the **show qos statistics aggregate−policer** command. Issue the **show mls entry qos short** command in order to check microflow policing statistics.

Q. Is traffic shaping supported on the Catalyst 6500 (Cat6K) Switch?

A. Traffic shaping is only supported on certain WAN modules for the Catalyst 6500/7600 Series, such as the Optical Services Modules (OSMs) and FlexWAN modules. Refer to Configuring Class−Based Traffic Shaping and Traffic Shaping for more information.

Q. How many aggregate or microflow policers are supported on the Catalyst 6500 (Cat6K) Switch?

A. The Catalyst 6500/6000 supports up to 63 microflow policers and up to 1023 aggregate policers.

Q. What Catalyst operating system (CatOS) or Multilayer Switch Feature Card (MSFC) Cisco IOS image is required to support policing?

A. The Supervisor Engine 1A supports ingress policing in CatOS version 5.3(1) and later, and Cisco IOS Software Release 12.0(7)XE and later.

The Supervisor Engine 2 supports ingress policing in CatOS version 6.1(1) and later, and Cisco IOS Software Release 12.1(5c)EX and later. However, microflow policing is supported only in Cisco IOS software.

Q. I upgraded from a Sup2 to a Sup720 and my policed traffic rate statistics show differently with the same traffic. Why?

A. An important change in policing on the Supervisor Engine 720 is that it can count traffic by the Layer 2 length of the frame. This differs from the Supervisor Engine 1 and Supervisor Engine 2, which count IP and IPX frames by their Layer 3 length. With some applications, Layer 2 and Layer 3 length might not be consistent. One example is a small Layer 3 packet inside a large Layer 2 frame. In this case, the Supervisor Engine 720 might display a slightly different policed traffic rate as compared to the Supervisor Engine 1 and Supervisor Engine 2.

Q. How do I know what values to use for rate and burst when I configure a policer?

A. These parameters control the operation of the token bucket:

- **Rate** Defines how many tokens are removed at each interval. This effectively sets the policing rate. All traffic below the rate is considered in−profile.
- **Interval** Defines how often tokens are removed from the bucket. The interval is fixed at 0.00025 seconds, so tokens are removed from the bucket 4,000 times per second. The interval cannot be changed.
- **Burst** Defines the maximum number of tokens that the bucket can hold at any one time. Burst should be no less than the rate times the interval in order to sustain the specified traffic rate. Another consideration is that the maximum−size packet must fit into the bucket.

Use this equation in order to determine the burst parameter:

```
Burst = (rate bps * 0.00025 sec/interval) or (maximum packet size bits)
[whichever is greater]
```

For example, if you want to calculate the minimum burst value needed to sustain a rate of 1 Mbps on an Ethernet network, the rate is defined as 1 Mbps and the maximum Ethernet packet size is 1518 bytes. This is the equation:

```
Burst = (1,000,000 bps * 0.00025) or (1518 bytes * 8 bits/byte) = 250 or 12144
```

The larger result is 12144, which you round to 13 kbps.

Note: In Cisco IOS software, the policing rate is defined in bits per second (bps). In Catalyst operating system (CatOS), it is defined in kbps. Also, in Cisco IOS software, the burst rate is defined in bytes, but in CatOS, it is defined in kilobits.

Note: Due to hardware policing granularity, the exact rate and burst is rounded to the nearest supported value. Be sure that the burst value is not less than the maximum−size packet. Otherwise, all packets larger than the burst size are dropped.

For example, if you try to set the burst to 1518 in Cisco IOS software, it is rounded to 1000. This causes all frames larger than 1000 bytes to be dropped. The solution is to configure the burst to 2000.

When you configure the burst rate, take into account that some protocols, such as TCP, implement a flow−control mechanism that reacts to packet loss. For example, TCP reduces windowing by half for each lost packet. Consequently, when policed to a certain rate, the effective link utilization is lower than the configured rate. You can increase the burst to achieve better utilization. A good start for such traffic is to double the burst size. In this example, the burst size is increased from 13 kbps to 26 kbps. Then, monitor performance and make further adjustments if needed.

For the same reason, it is not recommended that you benchmark the policer operation with connection−oriented traffic. This generally shows lower performance than the policer permits.

Q. I am configuring QoS over a port channel. Are there any restrictions that I need to know?

A. When you configure QoS on ports which are part of a port channel on Catalyst operating system (CatOS), you must apply the same configuration to all physical ports in the port channel. These parameters must agree for all ports in the port channel:

- Port trust type
- Receive port type (2q2t or 1p2q2t)
- Transmit port type (1q4t or 1p1q4t)
- Default port class of service (CoS)
- Port−based QoS or VLAN−based QoS
- Access control list (ACL) or protocol pair that the port carries

Q. Why am I unable to adjust the min−threshold value?

A. With Catalyst operating system (CatOS) versions earlier than 6.2, the weighted random early detection (WRED) threshold command only sets the max−threshold, while the min−threshold is hard coded to 0%. This is corrected in CatOS 6.2 and later, which allow the configuration of the min−threshold value.The default min−threshold depends on the precedence. The min−threshold for IP precedence 0 corresponds to one half of the max−threshold. The values for the precedences that remain fall between one half the

max−threshold, and the max−threshold at evenly spaced intervals.

Q. I am having difficulty adjusting the transmit queue buffers. Are there any restrictions?

A. If you have three queues (1p2q2t), the high priority weighted round−robin (WRR) queue and the strict priority queue must be set at the same level.

Q. I have a 62xx/63xx line card. I cannot apply the set command that trusts differentiated services code point (DSCP) on a port. Is there a limitation on this line card for QoS features?

A. Yes, because you cannot issue the **trust−dscp**, **trust−ipprec**, or **trust−cos** commands on the WS−X6248−xx, WS−X6224−xx, and WS−X6348−xx line cards. The easiest method in this situation is to leave all of the ports as untrusted and change the default access control list (ACL) to the **trust−dscp** command:

```
set qos enable

set port qos 2/1−16 trust untrusted

set qos acl default−action ip trust−dscp
```

Refer to the Limitations of the WS−X6248−xx, WS−X6224−xx, and WS−X6348−xx Line Cards section of QoS Classification and Marking on Catalyst 6500/6000 Series Switches Running CatOS Software for addition line card−specific limitations.

Q. What Catalyst operating system (CatOS) versions and supervisors are required to support policing?

A. The Supervisor Engine 1A supports ingress policing in CatOS version 5.3(1) and later, and in Cisco IOS Software Release 12.0(7)XE and later.

Note: A Policy Feature Card (PFC) daughter card is required for policing with the Supervisor Engine 1A.

The Supervisor Engine 2 supports ingress policing in CatOS version 6.1(1) and later, and in Cisco IOS Software Release 12.1(5c)EX and later. The Supervisor Engine 2 supports the excess rate policing parameter.

The Supervisor 720 supports ingress policing at the port and VLAN interface level. Refer to the Policing Features Update for Supervisor Engine 720 section of QoS Policing on Catalyst 6500/6000 Series Switches for more information about the Sup720 policing features.

Q. What do I need to know about the configuration of QoS over EtherChannel?

A. When you configure QoS on a port that is part of an EtherChannel on CatOS, you must always configure it on a per−port basis. Also, you must ensure that you apply the same QoS configuration to all ports, because the EtherChannel can only bundle ports with the same QoS configurations. This means that you need to configure these parameters the same:

- Port trust type
- Receive port type (2q2t or 1p2q2t)
- Transmit port type (1q4t or 1p1q4t)
- Default port class of service (CoS)
- Port−based QoS or VLAN−based QoS
- Access control list (ACL) or protocol pair that the port carries

Q. Where can I find examples of the use of QoS access control lists (ACLs) to mark or police traffic?

A. Refer to the Case 1: Marking at the Edge section of QoS Classification and Marking on Catalyst 6500/6000 Series Switches Running CatOS Software for an example of marking traffic.

Refer to the Configure and Monitor Policing in CatOS Software section of QoS Policing on Catalyst 6500/6000 Series Switches for an example of policing traffic.

Q. What is the difference between port−based and VLAN−based QoS access control lists (ACLs)?

A. Each QoS ACL can be applied either to a port or to a VLAN, but there is an additional configuration parameter to take into account: the ACL port type. A port can be configured to be VLAN−based or port−based. These are the two types of configurations:

1. If a VLAN−based port with an applied ACL is assigned to a VLAN that also has an applied ACL, then the VLAN−based ACL takes priority over the port−based ACL.
2. If a port−based port with an applied ACL is assigned to a VLAN that also has an applied ACL, then the port−based ACL takes priority over the VLAN−based ACL.

Refer to the Which of the Four Possible Sources for Internal DSCP will be Used? section of QoS Classification and Marking on Catalyst 6500/6000 Series Switches Running CatOS Software for more information.

Q. What is the typical value of burst size to be used for rate−limiting on Layer 3 switches?

A. Layer 3 switches implement an approximation of the single token bucket algorithm in firmware. A reasonable burst size for the range of traffic rates is about 64000 bytes. The burst size should be chosen to include at least one maximum−size packet. With each arriving packet, the policing algorithm determines the time between this packet and the last packet, and calculates the number of tokens generated during the elapsed time. Then, it adds this number of tokens to the bucket and determines whether the arriving packet conforms to, or exceeds the specified parameters.

Q. Why is it that I receive a lower performance for TCP traffic with rate−limiting?

A. TCP applications behave poorly when packets are dropped as a result of rate−limiting. This is due to the inherent windowing scheme used in flow control. You can adjust the burst size parameter or rate parameter to obtain the required throughput.

Q. What is the advantage of weighted random early detection (WRED), and how do I know if my line card can support WRED?

A. For congestion avoidance on output scheduling, the Catalyst 6500 (Cat6K) Switch supports WRED on some egress queues. Each queue has a configurable size and threshold. Some have WRED. WRED is a congestion−avoidance mechanism which randomly drops packets with a certain IP precedence when the buffers reach a defined threshold filling. WRED is a combination of two features: tail drop and random early detection (RED). The early Catalyst operating system (CatOS) implementation of WRED only set the max−threshold, while the min−threshold was hard−coded to 0%. Note that the drop probability for a packet is always non−null, as they always are above the min−threshold. This behavior is corrected in CatOS 6.2 and later. WRED is a very useful congestion−avoidance mechanism for when the traffic type is TCP−based. For other types of traffic, RED is not very efficient because RED takes advantage of the windowing mechanism that is used by TCP to manage congestion.

Refer to the Understanding the Queueing Capability of a Port section of QoS Output Scheduling on Catalyst 6500/6000 Series Switches Running CatOS System Software in order to determine whether a line card or queue structure can support WRED. You can also issue the **show port capabilities** command in order to see the queue structure of your line card.

Q. What is the internal differentiated services code point (DSCP)?

A. Each frame has an internal class of service (CoS) assigned, either the received CoS or the default port CoS. This includes untagged frames that do not carry any real CoS. This internal CoS and the received DSCP are written in a special packet header (called a Data Bus header) and are sent over the Data Bus to the switching engine. This happens at the ingress line card. At this point, it is not known yet whether this internal CoS is carried to the egress application−specific integrated circuit (ASIC) and inserted in the outgoing frame. Once the header reaches the switching engine, the switching engine Encoded Address Recognition Logic (EARL) assigns each frame an internal DSCP. This internal DSCP is an internal priority assigned to the frame by the Policy Feature Card (PFC) as it transits the switch. This is not the DSCP in the IPv4 header. It is derived from an existing CoS or type of service (ToS) setting, and is used to reset the CoS or ToS as the frame exits the switch. This internal DSCP is assigned to all frames switched (or routed) by the PFC, even non−IP frames.

Q. What are the possible sources for the internal differentiated services code point (DSCP)?

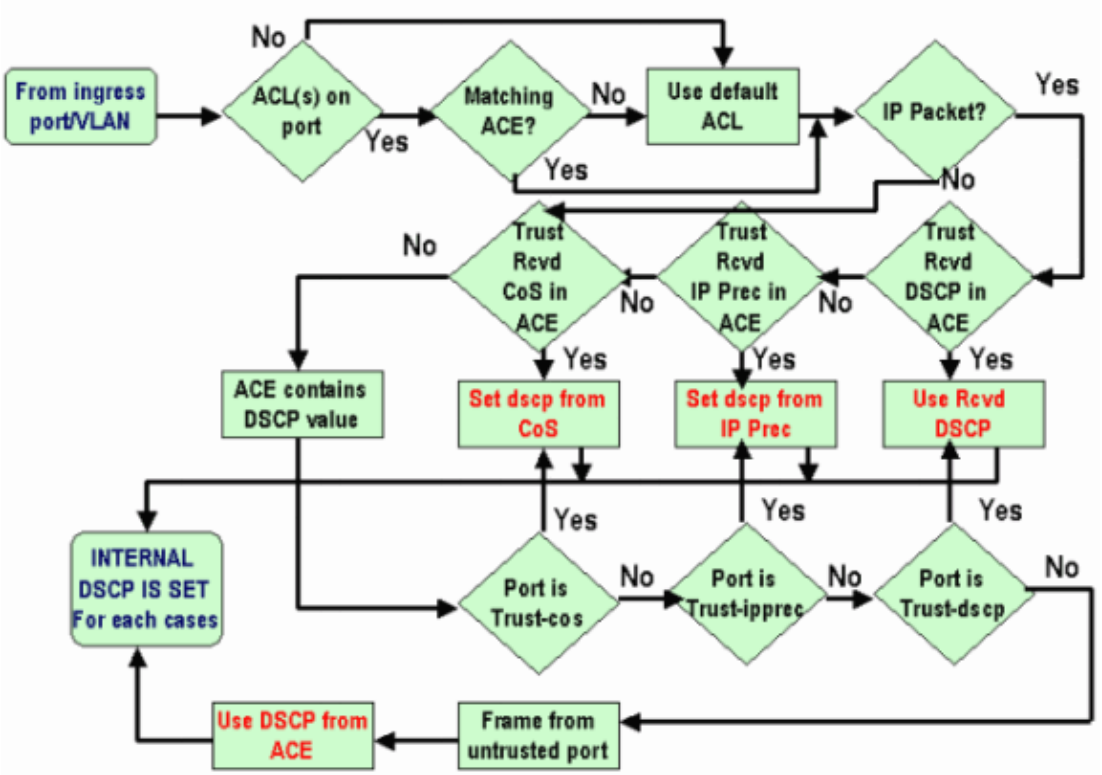
A. Refer to the Four Possible Sources for Internal DSCP section of QoS Classification and Marking on Catalyst 6500/6000 Series Switches Running CatOS Software.

Q. How is the internal differentiated services code point (DSCP) chosen?

A. The internal DSCP depends on these factors:

- Port trust state
- Access control list (ACL) attached to the port
- Default ACL
- VLAN−based or port−based, in regards to the ACL

This flow chart summarizes how the internal DSCP is chosen based on the configuration:



Q. Is class−based weighted fair queuing (CBWFQ) or low latency queuing (LLQ) supported in the Catalyst 6500 (Cat6K) Switch?

A. Yes, CBWFQ allows you to define a class of traffic and assign it a minimum bandwidth guarantee. The algorithm behind this mechanism is weighted fair queuing (WFQ), which explains the name. You define specific classes in map−class statements in order to configure CBWFQ. Then you assign a policy to each class in a policy−map. This policy−map is then attached to the inbound/outbound of an interface.

Q. Is the Layer 2 class of service (CoS) value retained for routed packets?

A. Yes, the internal differentiated services code point (DSCP) is used to reset the CoS on egress frames.

Q. Does QoS apply the identical configuration to all LAN port which are controlled by the same ASIC?

A. Yes, when these commands are configured, QoS applies identical configuration to all LAN/routed ports controlled by the same Application Specific Integrated Circuit (ASIC). QoS settings are propagated to other ports that belong to the same ASIC irrespective of whether the port is an access port, trunk port or a routed port.

- **rcv−queue random−detect**
- **rcv−queue queue−limit**
- **wrr−queue queue−limit**
- **wrr−queue bandwidth** (except Gigabit Ethernet LAN ports)
- **priority−queue cos−map**
- **rcv−queue cos−map**

- **wrr−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**

When the **default** *interface* command is executed on any of the ports, then the ASIC that controls the particular port resets the QoS configuration for all the ports controlled by it.

Q. Why does the show traffic−shape statistics command not show positive result even when the traffic shapping in is configured?

```
Router#show traffic−shape statistics
          Access Queue     Packets   Bytes     Packets   Bytes     Shaping
I/F       List   Depth                        Delayed   Delayed   Active
Et0       101    0         2         180       0         0         no
Et1              0         0         0         0         0         no
```

A. The Shaping Active attribute has **yes** when timers indicate that traffic shaping occurs and **no** if traffic shaping does not occur.

You can use the **show policy−map** command in order to verify if the configured traffic works.

```
Router#show policy−map
  Policy Map VSD1
    Class VOICE1
      Strict Priority
      Bandwidth 10 (kbps) Burst 250 (Bytes)
    Class SIGNALS1
      Bandwidth 8 (kbps) Max Threshold 64 (packets)
    Class DATA1
      Bandwidth 15 (kbps) Max Threshold 64 (packets)
  Policy Map MQC−SHAPE−LLQ1
    Class class−default
      Traffic Shaping
         Average Rate Traffic Shaping
                 CIR 63000 (bps) Max. Buffers Limit 1000 (Packets)
                 Adapt to 8000 (bps)
                 Voice Adapt Deactivation Timer 30 Sec
      service−policy VSD1
```

Q. Does Catalyst 6500 PFC support all the standard QoS commands?

A. Cisco Catalyst 6500 PFC QoS has some restrictions and does not support some QoS−related commands. Refer to this documents for the complete list of commands not supported.

- Class Map Command Restrictions
- Policy Map Command Restrictions
- Policy Map Class Command Restrictions

Q. Why are the Software CoPP counters greater than Hardware CoPP counters?

A. Software Control Plane Policing (CoPP) counters are the sum of packets traversing hardware CoPP and hardware rate limiting. Packets are first handled by hardware rate

limiters, and if they do not match, then hardware CoPP comes to picture. If the hardware rate limiter allows the packets, this packet goes to software where it is processed by software CoPP. Due to this software, CoPP can be greater than hardware CoPP counters.

Also there are some restrictions where CoPP is not supported in hardware. Some of them are:

- CoPP is not supported in hardware for multicast packets. The combination of ACLs, multicast CPU rate limiters, and CoPP software protection provides protection against multicast DoS attacks.
- CoPP is not supported in hardware for broadcast packets. The combination of ACLs, traffic storm control, and CoPP software protection provides protection against broadcast DoS attacks.
- Classes that match multicast are not applied in hardware but are applied in software.
- CoPP is not enabled in hardware unless MMLS QoS is enabled globally with the **mls qos** command. If the **mls qos** command is not entered, CoPP only works in software and does not provide any benefit to the hardware.

Refer to Configuring Control Plane Policing (CoPP) for more information.

Q. Does the default (interface) command QoS configuration work on other interfaces / ports?

A. When the **default** *interface* command is issued, the non−default configuration is gathered, which is similar to what is displayed in **show running−config interface** *x/y* , and each of those are set to their default values. This can be a simple negation of a command too.

If there are any QoS or other features that are configured on that interface, and those commands get negated, they can propagate to other interfaces of the linecard.

It is recommended to check the output of **show interface** *x/y* **capabilities** command, before you proceed with defaulting an interface. Refer to Does QoS apply the identical configuration to all LAN port which are controlled by the same ASIC? for more information.

The output of the **default** *interface* command also displays (if any) other interfaces that get affected for QoS and other features implemented in that port ASIC.

Q. Can I configure QoS in an interface that has a secondary IP?

A. Yes. You can configure QoS on a secondary IP.

Related Information

- **QoS Output Scheduling on Catalyst 6500/6000 Series Switches Running CatOS System Software**
- **QoS Classification and Marking on Catalyst 6500/6000 Series Switches Running CatOS Software**
- **QoS Policing on Catalyst 6500/6000 Series Switches**
- **LAN Product Support**
- **LAN Switching Technology Support**
- **Technical Support & Documentation − Cisco Systems**

Updated: Jul 28, 2006 Document ID: 64026