Catalyst 6500 Switches QoS Troubleshooting

Document ID: 71600

Contents

Introduction

This document contains the basic troubleshooting steps, the quality of service (QoS) limitations, and provides information to troubleshoot common QoS issues on the Catalyst 6500 Switches. This document also discusses QoS issues that occur at classification, and marking and policing.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Catalyst 6500 Series Switches.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Background Information

QoS is a network feature to classify the traffic and to provide deterministic delivery services. These items explain the various steps in the QoS process:

- **Input Scheduling** It is handled by hardware port ASICs and it is a Layer 2 QoS operation. It does not require a Policy Feature Card (PFC).
- **Classification** It is handled by the supervisor and/or PFC via the Access Control List (ACL) engine. The supervisor handles the Layer 2 QoS operation. PFC handles the Layer 2 and Layer 3 QoS operation.
- **Policing** It is handled by PFC via the Layer 3 forwarding engine. PFC is required and it handles the Layer 2 and Layer 3 QoS operation.
- **Packet Re−write** It is handled by hardware port ASICs. It is a Layer 2 and Layer 3 QoS operation based on the classification done previously.
- **Output Scheduling** It is handled by hardware port ASICs. It is a Layer 2 and Layer 3 QoS operation based on the classification done previously.

Troubleshoot QoS

QoS works differently in Catalyst 6500 Switches than in the routers. The QoS architecture is quite complex in Catalyst 6500 Switches. It is recommended that you understand Multilayer Switch Feature Card (MSFC), PFC, and Supervisor Engine architecture in the Catalyst 6500. Configuration of QoS in Hybrid OS needs more understanding of the Layer 2 CatOS functionality and the Layer 3 MSFC with Cisco IOS® functionality. It is recommended to read these documents in depth before you configure QoS:

- Configuring PFC QoS − Native IOS
- Configuring QoS − CatOS

Step−by−Step Troubleshooting Procedure

This section contains the basic step−by−step troubleshooting procedure for QoS in order to isolate the issue for further troubleshooting.

1. **Enable QoS** The **show mls qos command** shows the policing statistics and the status of QoS, whether enabled or disabled.

```
Switch#show mls qos
  QoS is enabled globally
  QoS ip packet dscp rewrite enabled globally
  Input mode for GRE Tunnel is Pipe mode
  Input mode for MPLS is Pipe mode
  Vlan or Portchannel(Multi−Earl)policies supported: Yes
  Egress policies supported: Yes


 ----- Module [5] -----
  QoS global counters:
    Total packets: 244
    IP shortcut packets: 0
    Packets dropped by policing: 0
    IP packets with TOS changed by policing: 5
    IP packets with COS changed by policing: 4
    Non−IP packets with COS changed by policing: 0
    MPLS packets with EXP changed by policing: 0
```

2. **Classification of inbound traffic using trust port** This classification categorizes the inbound traffic into one of the seven class of service (CoS) values. The inbound traffic can have the CoS value

already assigned by the source. In this case, you need to configure the port to trust the CoS value of the inbound traffic. Trust enables the switch to maintain the CoS or type of service (ToS) values of the received frame. This command shows how to verify the port trust state:

```
Switch#show queueing int fa 3/40
  Port QoS is enabled
Trust state: trust CoS
  Extend trust state: not trusted [CoS = 0]
  Default CoS is 0


!--- Output suppressed.
```

The CoS value is carried only by Inter−Switch Link (ISL) and dot1q frames. Untagged frames do not carry CoS values. Untagged frames do carry ToS values which are derived from IP precedence or differentiated services code point (DSCP) from the IP packet header. In order to trust the ToS value, you need to configure the port to trust IP precedence or DSCP. DSCP is backward compatible to IP precedence. For example, if you have configured a switch port as Layer 3 port, it does not carry dot1q or ISL frames. In this case, you need to configure this port to trust DSCP or IP precedence.

```
Switch#show queueing interface gigabitEthernet 1/1
Interface GigabitEthernet1/1 queueing strategy:  Weighted Round−Robin
  Port QoS is enabled
  Trust state: trust DSCP
  Extend trust state: not trusted [COS = 0]
  Default CoS is 0


!--- Output suppressed.
```

3. **Classification of inbound traffic using ACL and ACEs** You can also configure the switch to classify and mark the traffic. The steps included to configure classification and marking are: create access−lists, class−map, and policy−map, and issue the **service−policy input** command in order to apply the policy−map into the interface. You can verify the policy−map statistics as shown here:

```
Switch#show policy−map interface fa 3/13
 FastEthernet3/13

  Service−policy input: pqos2

    class−map: qos1 (match−all)
      Match: access−group 101
      set precedence 5:
      Earl in slot 5 :
        590 bytes
       5 minute offered rate 32 bps
        aggregate−forwarded 590 bytes

    Class−map: class−default (match−any)
      36 packets, 2394 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any

Switch#show mls qos ip ingress
 QoS Summary [IPv4]:      (* − shared aggregates, Mod − switch module)

      Int Mod Dir  Class−map DSCP  Agg  Trust Fl   AgForward−By   AgPoliced−By
                                    Id         Id
−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−
    Fa3/13  5  In       qos1   40    1     No  10           590              0

       All  5   −    Default    0    0*    No  0          365487             0
```

Notice that the counters **AgForward−By** that corresponds to the class−map qos1 increases. If you do not see the statistics for the corresponding class−map, verify the access−list attached to the class−map.

4. **Input Scheduling** PFC is not required to configure input scheduling. You cannot configure the **rcv−queue threshold** or **set qos drop−threshold** commands on a single 10/100 port. This is because input scheduling is handled by Coil ASIC ports which contain twelve 10/100 ports. Therefore, you have to configure the input scheduling in sets of 12 ports, such as 1−12, 13−24, 25−36, 37−48.

   The queueing architecture is built into the ASIC and cannot be reconfigured. Issue the **show queueing interface fastethernet slot/port | include type** command to see the queue structure of a LAN port.

```
Switch#show queueing interface fastEthernet 3/40
Queueing Mode In Rx direction: mode-cos
    Receive queues [type = 1q4t]:         <--------- 1 Queue 4 Threshold
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       1         Standard            4


    queue tail-drop-thresholds
    --------------------------
    1     50[1] 60[2] 80[3] 100[4]  <------ Threshold levels 50%, 60%, 80% and 100%


  Packets dropped on Receive:
    BPDU packets:  0

    queue thresh    dropped  [cos-map]
    ---------------------------------------------------
    1     1               0  [0 1 ]
    1     2               0  [2 3 ]
    1     3               0  [4 5 ]
    1     4               0  [6 7 ]


!--- Output suppressed.
```

   By default, all of the 4 thresholds are 100%. You can issue the **rcv−queue threshold** *<Queue Id> <Threshold 1> <Threshold 2> <Threshold 3> <Threshold 14>* command in order to configure the threshold levels. In this way, the higher CoS values data are not dropped before lower CoS value data during congestion.

```
Switch(config)#interface range fa 3/37 - 48
Switch(config-if-range)#rcv-queue threshold 1 50 60 80 100
```

5. **Mapping** If the port is configured to trust the CoS, then use the CoS−DSCP map table in order to map the received CoS value into an internal DSCP value.

```
Switch#show mls qos maps cos-dscp
   Cos-dscp map:
        cos:   0  1  2  3  4  5  6  7
      ----------------------------------
         dscp:   0  8 16 24 32 40 48 56
```

   If the port is configured to trust the trust IP precedence, then use the ip−prec−dscp map table in order to map the received IP precedence value into an internal DSCP value.

```
Switch#show mls qos maps ip-prec-dscp
   IpPrecedence-dscp map:
      ipprec:   0  1  2  3  4  5  6  7
      ----------------------------------
```

```
dscp:   0  8 16 24 32 40 48 56
```

If the port is configured to trust the DSCP, then the received DSCP value is used as the internal DSCP value.

These tables should be same on all the switches in your network. If any one of the switches has a table with different mappings, you do not receive the desired result. You can change these table values as shown here:

```
Switch(config)#mls qos map cos-dscp 0 8 16 24 40 48 48 56
Switch(config)#mls qos map ip-prec-dscp 0 8 16 24 40 48 48 56
```

6. **Policing** There are two types of policing available in Catalyst 6500 Switches:

   - **Aggregate policing** Aggregate policing controls the bandwidth of a flow in the switch. The **show mls qos aggregate-policer** command shows all the configured aggregate policer configured on the switch. These are the policing statistics:

```
Switch#show mls qos ip fastEthernet 3/13
   [In] Policy map is pqos2   [Out] Default.
 QoS Summary [IPv4]:      (* - shared aggregates, Mod - switch module)

      Int Mod Dir  Class-map DSCP  Agg  Trust Fl   AgForward-By   AgPoliced-B
                                   Id         Id
-------------------------------------------------------------------------------
    Fa3/13  5  In       qos1    0    1*  dscp  0          10626         11886
    Fa3/13  5  In class-defa   40    2     No  0           3338

Switch#show mls qos
  QoS is enabled globally
  QoS ip packet dscp rewrite enabled globally
  Input mode for GRE Tunnel is Pipe mode
  Input mode for MPLS is Pipe mode
  Vlan or Portchannel(Multi-Earl) policies supported: Yes
  Egress policies supported: Yes


 ----- Module [5] -----
  QoS global counters:
    Total packets: 163
    IP shortcut packets: 0
    Packets dropped by policing: 120
    IP packets with TOS changed by policing: 24
    IP packets with COS changed by policing: 20
    Non-IP packets with COS changed by policing: 3
    MPLS packets with EXP changed by policing: 0
```

   - **Microflow policing** Microflow policing controls bandwidth of a flow per interface in the switch. By default, microflow policers affect only routed traffic. Issue the **mls qos bridged** command in the VLAN interface in order to enable microflow policing for bridged traffic. This is the verification of the microflow policing statistics:

```
Switch#show mls ip detail
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f         :AdjPtr
-------------------------------------------------------------------------------
Pkts         Bytes         Age   LastSeen  Attributes
-----------------------------------------------

Mask Pi R CR Xt Prio Dsc IP_EN OP_EN Pattern Rpf FIN_RDT FIN/RST
----+--+-+--+--+----+---+-----+-----+-------+---+-------+-------
Ig/acli Ig/aclo Ig/qosi Ig/qoso Fpkt Gemini MC-hit Dirty Diags
-------+-------+-------+-------+----+------+------+-----+------
```

```
    QoS     Police Count Threshold    Leak     Drop Bucket  Use-Tbl Use-Enabl
-----------+------------+---------+-----------+----+-------+-------+---------
10.175.50.2     10.175.51.2     icmp:8      :0        --               :0x0
43           64500          84    21:37:16   L3 - Dynamic
1    1  0  0  1  0    0    1     1     0       0     0      0
0           0       0       0      0    0       0     0     0
  0x0           0               0        0       NO   1518       NO       NO
10.175.50.2     10.175.51.2     icmp:0      :0        --               :0x0
43           64500          84    21:37:16   L3 - Dynamic
1    1  0  0  1  0    0    1     1     0       0     0      0
0           0       0       0      0    0       0     0     0
  0x0          664832          0        0       NO   1491       NO       NO
0.0.0.0         0.0.0.0         0   :0      :0        --               :0x0
1980         155689         1092  21:37:16   L3 - Dynamic
0    1  0  0  1  0    0    1     1     0       0     0      0
0           0       0       0      0    0       0     0     0
  0x0           0               0        0       NO   0          NO       NO

Switch#show mls qos
  QoS is enabled globally
  QoS ip packet dscp rewrite enabled globally
  Input mode for GRE Tunnel is Pipe mode
  Input mode for MPLS is Pipe mode
  Vlan or Portchannel(Multi-Earl) policies supported: Yes
  Egress policies supported: Yes


 ----- Module [5] -----
  QoS global counters:
    Total packets: 551
    IP shortcut packets: 0
    Packets dropped by policing: 473
    IP packets with TOS changed by policing: 70
    IP packets with COS changed by policing: 44
    Non-IP packets with COS changed by policing: 11
    MPLS packets with EXP changed by policing: 0
```

Note: The **show mls qos ip** *type mod/number* command does not show the microflow policing statistics. It only shows the aggregate policing statistics.

If you do not see the desired policing statistics, verify the policing configuration. Refer to QoS Policing on Catalyst 6500/6000 Series Switches to see the configuration example. Also, see the QoS Guidelines and Limitations on Catalyst 6500 Switches section of this document.

7. Check the release notes of your OS version and make sure there are no bugs related to your QoS configuration.
8. Note your switch supervisor model, PFC model, MSFC model and Cisco IOS/CatOS version. See the QoS Guidelines and Limitations on Catalyst 6500 Switches with reference to your specifications. Make sure your configuration is applicable.

QoS Guidelines and Limitations on Catalyst 6500 Switches

There are QoS limitations that you need to be aware of before you configure QoS on Catalyst 6500 Switches:

- General Guidelines
- PFC3 Guidelines
- PFC2 Guidelines
- Class Map Command Restrictions
- Policy Map Command Restrictions
- Policy Map Class Command Restrictions
- Queue and Drop Threshold Mapping Guidelines and Restrictions

- trust−cos in ACL Entry Limitations
- Limitations of the WS−X6248−xx, WS−X6224−xx, and WS−X6348−xx Line Cards
- PFC or PFC2 do not provide QoS for the WAN traffic. With PFC or PFC2, PFC QoS does not change the ToS byte in the WAN traffic.
- Ingress LAN traffic that is Layer 3 switched does not go through the MSFC or MSFC2 and retains the CoS value that is assigned by the Layer 3 switching engine.
- QoS does not implement ingress port congestion avoidance on the ports that are configured with the **untrusted**, **trust−ipprec**, or **trust−dscp** keywords. The traffic goes directly to the switching engine.
- The switch uses the tail−drop threshold for the traffic that carries the CoS values that are mapped only to the queue. The switch uses the WRED−drop thresholds for the traffic that carries the CoS values that are mapped to the queue and a threshold.
- Classification with a Layer 3 switching engine uses the Layer 2, 3, and 4 values. Marking with a Layer 3 switching engine uses the Layer 2 CoS values and the Layer 3 IP precedence or DSCP values.
- A trust−cos ACL cannot restore the received CoS in the traffic from the untrusted ports. The traffic from the untrusted ports always has the port CoS value.

Note: PFC QoS does not detect the use of unsupported commands until you attach a policy map to an interface.

QoS_TCAM Limitation

The Ternary CAM (TCAM) is a specialized piece of memory designed for rapid table lookups, based on packets passing through the switch, performed by the ACL engine on PFC, PFC2, and PFC3. ACLs are processed in hardware in Cisco Catalyst 6500 Series Switches that are called TCAM. When you configure ACL, map the ACL to the QoS and when you apply the QoS policy on the interface, the switch programs the TCAM. If you have already utilized all of the avilable TCAM space on the switch for the QoS, you encounter this error message:

```
Switch(config)#interface vlan 52
Switch(config−if)#service−policy input test
Switch(config−if)#
3w0d: %QM−4−TCAM_ENTRY: Hardware TCAM entry capacity exceeded
```

This **show tcam count** command ouput shows that the TCAM entry Masks are 95% used. Because of this, when you apply the QoS policy on the interface you encounter the %QM−4−TCAM_ENTRY: error message.

```
Switch#show tcam count
           Used        Free        Percent Used       Reserved
           ----        ----        ------------       --------
 Labels:(in) 43        4053            1
 Labels:(eg)  2        4094            0

ACL_TCAM
--------
  Masks:     19        4077            0                  72
Entries:     95       32673            0                 576

QOS_TCAM
--------
  Masks:   3902         194           95                  18
Entries:  23101        9667           70                 144

    LOU:      0         128            0
  ANDOR:      0          16            0
  ORAND:      0          16            0
    ADJ:      3        2045            0
```

TCAM entries and ACL labels are limited resources. Therefore, depending on your ACL configuration, you might need to be careful not to exhaust the available resources. In addition, with large QoS ACL and VLAN Access Control List (VACL) configurations, you also might need to consider Non−Volatile Random Access Memory (NVRAM) space. The available hardware resources differ on Supervisor 1a with PFC, Supervisor 2 with PFC2, and Supervisor 720 with PFC3.

Supervisor Module	QoS TCAM	ACL Labels
Supervisor 1a and PFC	2K masks and 16K patterns shared between Router Access Control Lists (RACLs), VACLs and QoS ACLs	512 ACL labels shared between RACLs, VACLs, and QoS ACLs
Supervisor 2 and PFC2	4K masks and 32K patterns for QoS ACLs	512 ACL labels shared between RACLs, VACLs, and QoS ACLs
Supervisor 720 and PFC3	4K masks and 32K patterns for QoS ACLs	512 ACL labels shared between RACLs, VACLs, and QoS ACLs

Note: Independent of the 512 ACL label limit, there is an additional software limit in Cisco CatOS of 250 QoS ACLs system−wide when you use the default (binary) configuration mode. This restriction is removed in text configuration mode. Issue the **set config mode text** command in order to change the configuration mode to text mode. Text mode typically uses less NVRAM or Flash memory space than what the binary configuration mode uses. You must issue the **write memory** command while you operate in text mode in order to save the configuration in NVRAM. Issue the **set config mode text auto−save** command in order to save the text configuration in NVRAM automatically.

This is the workaround for the TCAM issue:

- If you have implemented the **service−policy** command on many Layer 2 interfaces which belong to one VLAN, you can implement VLAN based policing instead of switch port based. This is an example:

```
Switch(config)#interface range fastethernet x/y – Z
Switch(config−if)#mls qos vlan−based
Switch(config−if)#exit
Switch(config)#interface vlan 100
Switch(config−if)#service−policy input Test_Policy
```

- Disable QoS marking statistics. The **no mls qos marking statistics** command does not allow the max of 1020 AgIDs to be implemented. This is because it allocates the default policer for set dscp policers. The downside of this is there are no statistics for the specific policer because they all share the default policer.

```
Switch(config)#no mls qos marking statistics
```

- If possible, use the same ACLs across multiple interfaces in order to reduce TCAM resource contention.

NBAR Limitation

Network−Based Application Recognition (NBAR) is a classification engine that recognizes a wide variety of applications, which includes web−based and other difficult−to−classify protocols that utilize dynamic TCP/UDP port assignments. When an application is recognized and classified by NBAR, a network can invoke services for that specific application. NBAR classifies packets and then applies QoS to the classified traffic in order to ensure that network bandwidth is used efficiently. There are some restrictions in how to implement QoS when you use NBAR:

- PFC3 does not support NBAR.
- With a Supervisor Engine 2, PFC2, and MSFC2:
    - You can configure NBAR on Layer 3 interfaces instead of PFC QoS.
    - PFC2 provides hardware support for input ACLs on ports where you configure NBAR.
    - When PFC QoS is enabled, the traffic through ports where you configure NBAR passes through the ingress and egress queues and drop thresholds.
    - When PFC QoS is enabled, the MSFC2 sets egress CoS equal to egress IP precedence in NBAR traffic.
    - After all traffic passes through an ingress queue, it is processed in software on the MSFC2 on interfaces where you configure NBAR.

The cos−map commands Missing in Supervisor 2

Under Native IOS Software Releases 12.1(8a)EX−12.1(8b)EX5 and 12.1(11b)E and later, the default QoS CoS−mappings for the Gigabit uplinks located on the Supervisor2 have changed. All CoS values have been assigned to queue 1 and threshold 1, and cannot be changed.

These commands cannot be configured on a Sup2 Gigabit Uplink Port on these releases:

```
rcv−queue cos−map
priority−queue
wrr−queue cos−map
```

QoS configurations are limited, and the strict priority queue cannot be utilized. This affects only the Gigabit ports physically located on the Supervisor 2 Engine. Gigabit ports on other line card modules are not affected.

There is a firmware upgrade that resolves this issue. This upgrade can be done via software. Contact Technical Support if a firmware upgrade is required. Note that a firmware upgrade is needed only if the HW version of the Supervisor2 is less than 4.0. If the HW version of the Supervisor2 is 4.0 or later, QoS should be allowable on the Gigabit uplink ports without the firmware upgrade. You can issue the **show module** command in order to find the firmware level. This issue is identified in Cisco bug ID CSCdw89764 (registered customers only) .

Service−Policy Limitations

In order to apply policy−map to the interface, issue the **service−policy** command. If you have an unsupported command in policy−map, after you apply it with the **service−policy** command, the switch prompts the error messages on the console. These points need to be considered while you troubleshoot **service−policy** related issues.

- Do not attach a service policy to a port that is a member of an EtherChannel.
- With Distributed Forwarding Cards (DFCs) installed, PFC2 does not support VLAN−based QoS. You cannot issue the **mls qos vlan−based** command or attach service policies to VLAN interfaces.

- PFC QoS supports the output keyword only with PFC3 and only on Layer 3 interfaces (either LAN ports configured as Layer 3 interfaces or VLAN interfaces). With PFC3, you can attach both an input and an output policy map to a Layer 3 interface.
- VLAN−based or port−based PFC QoS on Layer 2 ports are not relevant to policies attached to Layer 3 interfaces with the output keyword.
- Policies attached with the output keyword do not support microflow policing.
- You cannot attach a policy map that configures a trust state with the **service−policy** command output.
- PFC QoS does not support ingress markdown with egress drop or ingress drop with egress markdown.

Service−Policy Output Statements Do Not Show Up in the running−config Command Output

When you configure QoS on the multilink on the FlexWan Module, you cannot see the **service−policy** command output in the **show running−config** command output. This occurs when the switch runs Cisco IOS versions earlier than 12.2SX. The FlexWAN for the Cisco 7600 Series supports dLLQ on non−bundle interfaces. It does not support dLLQ on MLPPP bundle interfaces. Such support is available with Cisco IOS Software Release 12.2S.

The workaround to bypass this limitation is to attach the service−policy to unbundled interfaces or upgrade the Cisco IOS version to 12.2SX or later, where the feature is supported.

Policing Limitation

Policing is performed in hardware on PFC without the impact of switch performance. Policing cannot occur on the 6500 platform without PFC. In Hybrid OS, policing must be configured on the CatOS. These points needs to be considered while you troubleshoot policing issues:

- 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.
- When you create a policer that does not use the pir keyword and the maximum_burst_bytes parameter is equal to the normal_burst_bytes parameter (which is the case if you do not enter the maximum_burst_bytes parameter), the exceed−action policed−dscp−transmit keywords cause PFC QoS to mark traffic down as defined by the policed−dscp max−burst markdown map.
- When the exceed action is drop, PFC QoS ignores any configured violate action.
- When you configure drop as the conform action, PFC QoS configures drop as the exceed action and the violate action.
- The flowmask requirements of microflow policing, NetFlow, and NetFlow Data Export (NDE) might conflict.

Rate−Limit or Policing Issues with MSFC in Hybrid OS

On Catalyst 6500 Switches that run Hybrid OS, the configuration of rate−limit does not give the desired output. For example, if you configure the **rate−limit** command under the **interface vlan** command on the MSFC, it does not actually rate−limit the traffic.

```
interface Vlan10
 rate−limit input 256000 2000 2000 conform−action transmit exceed−action drop
 rate−limit output 256000 2000 2000 conform−action transmit exceed−action drop
```

Or:

```
interface Vlan10
service−policy input Test_Policy
```

The reason behind this is that the MSFC takes care of only control functions, but actual traffic forwarding occurs on PFC ASICs on the supervisor. The MSFC compiles the FIB and adjacency tables, as well as other control information, and downloads it to PFC to implement in hardware. With the configuration you have created, you rate−limit only the software switched traffic, which should be minimal (or none).

The workaround is to use the CatOS command−line interface (CLI) in order to configure the rate−limit on the supervisor. Refer to CatOS QoS for the detailed explanation of how to configure the QoS policing in CatOS. You can also refer to QoS Policing on Catalyst 6500/6000 Series Switches to see the configuration example.

Command Shape Average not Supported in VLAN Interfaces of Cisco 7600

When you apply a service policy input to an interface on Cisco 7600, this error message appears:

```
7600_1(config)#int Gi 1/40
7600_1(config−if)#service−policy input POLICY_1
shape average command is not supported for this interface
```

The **shape average** command is not supported for the VLAN interfaces in Cisco 7600. Instead you need to use policing.

```
7600_1(config)#policy−map POLICY_1
7600_1(config−pmap)#class TRAFFIC_1
7600_1(config−pmap−c)#police <x> <y> conform−action transmit exceed−action drop
```

Refer to Configuring Policy Map Class Policing for more information on how to implement policing to rate−limit traffic.

As you attach this service−policy to a VLAN interface (SVI), you need to enable VLAN−based QoS on all those Layer 2 ports that belong to this VLAN in which you want this policy−map to be applied.

```
7600_1(config)#interface Gi 1/40
7600_1(config−if)#mls qos vlan−based
```

Refer to Enabling VLAN−Based PFC QoS on Layer 2 LAN Ports for more information..

QoS−ERROR: Addition/Modification made to policymap [chars] and class [chars] is not valid, command is rejected

```
QoS−ERROR: Addition/Modification made to policymap vtc−map and class voice−video is
not valid, command is rejected
```

This error message indicates that the actions defined in the mentioned class is not allowed in Cisco Catalyst 6500 series switches. There are some restrictions during the configuration of policy map class actions.

- You cannot do all three of these in a policy map class:
    - ♦ Mark traffic with the **set** commands
    - ♦ Configure the trust state
    - ♦ Configure policing

  You can only either mark traffic with the **set** commands.

  OR

  Configure the trust state and/or configure policing.

- For hardware−switched traffic, PFC QoS does not support the **bandwidth**, **priority**, **queue−limit**, or **random−detect** policy map class commands. You can configure these commands because they can be used for software−switched traffic.
- PFC QoS does not support the **set qos−group** policy map class commands.

Refer to Configuring Policy Map Class Actions for more information on such restrictions.

Related Information

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

Contacts & Feedback | Help | Site Map
© 2013 − 2014 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: Oct 03, 2006 Document ID: 71600