Catalyst 6500交换机QoS故障排除

目录

简介
先决条件
要求
使用的组件
规则
背景信息
排除 QoS 故障
排除故障的逐步过程
Catalyst 6500 交换机的 QoS 准则和限制
QoS_TCAM 限制
NBAR 限制
cos-map 命令在 Supervisor 2 中缺失
服务策略限制
服务策略输出语句没有出现在 running-config 命令输出中
监察限制
在混合 OS 中使用 MSFC 的速率限制或监察问题
命令形状平均在 Cisco 7600 的 VLAN 接口不受支持
QoS-ERROR:Addition/Modification made to policymap [chars] and class [chars] is not valid, command is rejected
相关信息

简介

本文档包含基本故障排除步骤、服务质量 (QoS) 限制，并提供有关排除 Catalyst 6500 交换机常见 QoS 问题故障的信息。本文档还讨论分类时发生的 QoS 问题、标记和监察。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于 Catalyst 6500 系列交换机。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

QoS 是一种对流量进行分类及提供确定性交付服务的网络功能。以下各项解释 QoS 进程中的各个步骤：

- **输入调度 - 由硬件端口 ASIC 进行处理，并且是第 2 层 QoS 操作。**不需要 Policy Feature Card (PFC)。
- **分类 - 由 Supervisor 和/或 PFC 通过访问控制表 (ACL) 引擎进行处理。**Supervisor 处理第 2 层 QoS 操作。PFC 处理第 2 层和第 3 层 QoS 操作。
- **监察- 由 PFC 通过第 3 层转发引擎进行处理。**PFC 是必需的，其处理第 2 层和第 3 层 QoS 操作。
- **数据包重写 - 由硬件端口 ASIC 进行处理。**它是基于之前完成的第 2 层和第 3 层 QoS 操作。
- **输出调度 - 由硬件端口 ASIC 进行处理。**它是基于之前完成的第 2 层和第 3 层 QoS 操作。

排除 QoS 故障

QoS 在 Catalyst 6500 交换机中的工作方式与在其他路由器中的工作方式不同。Catalyst 6500 交换机中的 QoS 体系结构非常复杂。我们建议您了解 Catalyst 6500 中的多层交换机特性卡 (MSFC)、PFC 和 Supervisor 引擎体系结构。混合 OS 中的 QoS 配置需要更多地了解第 2 层 CatOS 功能和第 3 层 MSFC Cisco IOS® 功能。建议您在配置 QoS 前，仔细阅读以下文档：

- 配置 PFC QoS - 本地 IOS
- 配置 QoS - CatOS

排除故障的逐步过程

本部分包含适用于 QoS 的故障排除基本逐步过程，可用于隔离问题，以进一步排除故障。

1. **启用 QoS - 无论启用或禁用，show mls qos 命令都会显示监察统计信息和 QoS 状态。**

```
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. **使用信任端口对入站流量进行分类 - 此分类将入站流量归为七种服务等级 (CoS) 值的其中一种**

。入站流量可以拥有源已分配的 CoS 值。这种情况下，您需要配置端口以信任入站流量的 CoS 值。信任可使交换机保持所收到帧的 CoS 或服务类型 (ToS) 值。以下命令显示如何验证端口信任状态：

```
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.
```

CoS 值仅由交换机间链路 (ISL) 和 dot1q 帧传输。无标记帧不传输 CoS 值。无标记帧可传输派生自 IP Precedence 或 IP 数据包报头差分服务代码点 (DSCP) 的 ToS 值。要信任 ToS 值，您需要将端口配置为信任 IP Precedence 或 DSCP。DSCP 向后兼容 IP Precedence。例如，如果将交换机端口作为第 3 层端口配置，则该端口不会传输 dot1q 或 ISL 帧。这种情况下，您需要将该端口配置为信任 DSCP 或 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. **使用 ACL 和 ACE 对入站流量进行分类 - 您也可以将交换机配置配分类和标记流量。**配置分类和标记包括以下步骤：创建访问列表、类映射和策略映射，以及发出 **service-policy input 命令将策略映射应用到接口。**可按如下所示验证策略映射统计信息：

```
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
```

注意，对应于类映射 qos1 的计数器 **AgForward-By 将增加。**如果您无法看到对应类映射的统计信息，则验证附加到类映射的访问列表。

4. **输入调度 - 配置输入调度时不需要 PFC。**您不能在单个 10/100 端口上配置 **rcv-queue threshold 或 set qos drop-threshold 命令。**这是因为输入调度由包含 12 个 10/100 端口的 Coil ASIC 端口进行处理。因此，您必须在包含 12 个端口的端口集（如 1-12、13-24、25-36、37-

48）中配置输入调度。队列体系结构在 ASIC 中构建，且无法重新配置。发出 **show queueing interface fastethernet slot/port | include type**命令查看LAN端口的队列结构。

```
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.
```

默认情况下，所有 4 个阈值都为 100%。可通过发出 **rcv-queue threshold***<Queue Id> <Threshold 1> <Threshold 2> <Threshold 3> <Threshold 14>* 命令配置阈值级别。这样，在较低 CoS 值数据拥塞之前，较高 CoS 值数据不会丢失。

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

5. **映射 - 如果端口配置为信任 CoS，则使用 CoS-DSCP 映射表，以便将收到的 CoS 值映射到内部 DSCP 值。**

```
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
```

如果端口配置为信任信任 IP Precedence，则使用 ip-prec-dscp 映射表，以便将收到的 IP Precedence 值映射到内部 DSCP 值。

```
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
```

如果端口配置为信任 DSCP，则将收到的 DSCP 值用作内部 DSCP 值。这些表在网路中的所有交换机上都应相同。如果其中任何一个交换机的表有不同的映射，则您不会收到预期效果。您可以按如下所示更改这些表值：

```
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. **监察 - Catalyst 6500 交换机中两种类型的可用监察：聚合监察 - 聚合监察可控制交换机中流的带宽。show mls qos aggregate-policer 命令显示交换机上配置的所有已配置聚合监察器。**以下是监察统计信息：

```
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-By
                                    Id         Id
-------------------------------------------------------------------------------
    Fa3/13  5  In       qos1    0    1*  dscp  0          10626         118860
    Fa3/13  5  In class-defa   40    2     No  0           3338              0

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
```

微流监察 - 微流监察可控制交换机中各接口的流带宽。默认情况下，微流监察器仅影响路由流量。在 VLAN 接口中发出 mls qos bridged 命令，**以便启用桥接流量的微流监察。**以下是微流监察统计信息的验证：

```
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-Enable
-----------+------------+---------+----------+----+-------+-------+----------+
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
```

注意：show mls qos ip type mod*/number命令*不显示微流策略统计信息。只显示聚合监察统计信息。如果看不到需要的监察统计信息，则验证监察配置。请参阅 Catalyst 6500/6000 系列交换机上的 QoS 监察查看配置示例。另外，请查阅本文档的 Catalyst 6500 交换机的 QoS 准则和限制部分。

7. 检查您 OS 版本的发行版本注释并确保没有与 QoS 配置相关的 bug。
8. 记下交换机 Supervisor 型号、PFC 型号、MSFC 型号以及 Cisco IOS/CatOS 版本。有关规格，请参阅 Catalyst 6500 的 QoS 准则和限制。确保您的配置适用。

Catalyst 6500 交换机的 QoS 准则和限制

在 Catalyst 6500 交换机上配置 QoS 之前，需要知道的 QoS 限制如下：

- 一般准则
- PFC3 准则
- PFC2 准则
- 类映射命令限制
- 策略映射命令限制
- 策略映射类命令限制
- 队列与丢弃阈值映射准则和限制
- ACL 条目限制中的 trust-cos
- WS-X6248-xx、WS-X6224-xx 和 WS-X6348-xx 线路卡限制
- PFC 或 PFC2 不为 WAN 流量提供 QoS。使用 PFC 或 PFC2，PFC QoS 不会更改 WAN 流量中的 Tos 字节。
- 第 3 层交换的入口 LAN 流量不会通过 MSFC 或 MSFC2，并将保留由第 3 层交换引擎分配的 CoS 值。
- QoS 不会在使用 **untrusted**、**trust-ipprec** 或 **trust-dscp 关键字配置的端口上实施入口端口拥塞避免。**流量直接流向交换引擎。
- 交换机将尾端丢弃阈值用于传输仅映射到队列的 CoS 值的流量。交换机将 WRED 丢弃阈值用于传输映射到队列和阈值的 CoS 值的流量。
- 第 3 层交换引擎分类使用第 2、3 和 4 层的值。第 3 层交换引擎标记使用第 2 层 CoS 值和第 3 层 IP Precedence 或 DSCP 值。
- trust-cos ACL 无法恢复流量中从不受信任端口收到的 CoS。来自不受信任端口的流量通常都有端口 CoS 值。

注意：在将策略映射附加到接口之前，PFC QoS不会检测不受支持的命令的使用。

QoS_TCAM 限制

三进制CAM(TCAM)是专用内存，根据通过交换机的数据包，由PFC、PFC2和PFC3上的ACL引擎

执行。ACL在Cisco Catalyst 6500系列交换机（称为TCAM）的硬件中处理。当您配置 ACL、将 ACL 映射到 QoS 时，以及当您在接口上应用 QoS 策略时，交换机会对 TCAM 进行编程。如果您已将交换机上的所有可用 TCAM 空间用于 QoS，则会遇到以下错误消息：

```
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
```

此 **show tcam count 命令输出显示 TCAM 条目掩码已使用 95%。**因此，当您在接口上应用 QoS 策略时，您会遇到 %QM-4-TCAM_ENTRY:错误消息。

```
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 条目和 ACL 标签是有限资源。所以，根据您的 ACL 配置，您也许需要注意，避免耗尽可用资源。另外，使用大型 QoS ACL 和 VLAN 访问控制列表 (VACL) 配置时，您也许还需要考虑非易失性随机访问存储器 (NVRAM) 空间。可用硬件资源在具有 PFC 的 Supervisor 1a、具有 PFC2 的 Supervisor 2 以及具有 PFC3 的 Supervisor 720 上各不相同。

Supervisor 模块	QoS TCAM	ACL 标签
Supervisor 1a 和 PFC	路由器访问控制列表 (RACL)、VACL 和 QoS ACL 之间共享的 2K 掩码和 16K 模式	RACL、VACL 和 QoS ACL 之间共享的 512 ACL 标签
Supervisor 2 和 PFC2	QoS ACL 的 4K 掩码和 32K 模式	RACL、VACL 和 QoS ACL 之间共享的 512 ACL 标签
Supervisor 720 和 PFC3	QoS ACL 的 4K 掩码和 32K 模式	RACL、VACL 和 QoS ACL 之间共享的 512 ACL 标签

注意：与512 ACL标签限制无关，在使用默认（二进制）配置模式时，Cisco CatOS系统范围内有250个QoS ACL的附加软件限制。在文本配置模式中，本限制被删除。发出 **set config mode text 命令可将配置模式更改为文本模式。**通常情况下，文本模式使用的 NVRAM 或闪存空间比二进制配置模式使用的少。当以文本模式运行时，必须发出 **write memory 命令，以便将配置保存在 NVRAM 中。**发出 **set config mode text auto-save 命令，以便自动将文本配置保存在 NVRAM 中。**

以下是 TCAM 问题的应急方案：

- 如果在属于一个 VLAN 的许多第 2 层接口上实施了 **service policy 命令，则可以实施基于 VLAN 的监察，而不是基于交换机端口的监察。**示例如下：

```
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
```

- 禁用 QoS 标记统计信息。**no mls qos marking statistics 命令不允许实施最多 1020 个 AgID。**这是因为该命令会为 set dscp 监察器分配默认的监察器。由此带来的负面影响是，由于特定监察器都共享默认的监察器，因此不会有统计信息。

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

- 如果可能，在多个接口中使用相同的 ACL，以减少 TCAM 资源争用。

NBAR 限制

基于网络的应用程序识别 (NBAR) 是可识别各种应用程序（包括使用动态 TCP/UDP 端口分配的基于 Web 的协议及其他难以分类的协议）的分类引擎。如果某个应用程序被 NBAR 识别并进行分类，则网络可以为此特定应用程序调用服务。NBAR 对数据包进行分类，然后将 QoS 应用到已分类的流量，以确保高效利用网络带宽。有关如何在使用 NBAR 时实施 QoS 的一些限制如下：

- PFC3 不支持 NBAR。
- 使用 Supervisor 引擎 2、PFC2 和 MSFC2：您可以在第 3 层接口上，而不是在 PFC QoS 上配置 NBAR。PFC2 在您配置 NBAR 的端口上为输入 ACL 提供硬件支持。启用 PFC QoS 后，通过您配置 NBAR 的端口的流量会通过入口和出口队列并丢弃阈值。启用 PFC QoS 后，MSFC2 将出口 CoS 设置为与 NBAR 流量中的出口 IP Precedence 相等。所有流量通过入口队列后，将在您配置 NBAR 的接口的 MSFC2 软件中进行处理。

cos-map 命令在 Supervisor 2 中缺失

在本机 IOS 软件版本 12.1(8a)EX-12.1(8b)EX5 和 12.1(11b)E 及以上版本下，位于 Supervisor2 上的 Gigabit 上行链路的默认 QoS CoS 映射已经更改。所有 CoS 值均已分配到队列 1 和阈值 1，且无法更改。

上述发行版本上的 Sup2 Gigabit 上行链路端口无法配置以下命令：

```
rcv-queue cos-map
priority-queue
wrr-queue cos-map
```

QoS 配置是有限的，并且无法使用严格优先级队列。这只会影响实际位于 Supervisor 2 引擎上的

Gigabit 端口。其他线路卡模块上的 Gigabit 端口不会受到影响。

存在可解决此问题的固件升级。该升级可通过软件完成。如果需要固件升级，请联系技术支持。请注意，仅当Supervisor2的硬件版本低于4.0时，才需要固件升级。如果Supervisor2的硬件版本为4.0或更高版本，则QoS应在千兆上行链路端口上允许，而无需固件升级。可发出 **show module 命令查找固件级别。**此问题已在 Cisco Bug ID CSCdw89764（仅限注册用户）中得到确定。

服务策略限制

要将策略映射应用到接口，请发出 **service-policy 命令。**如果策略映射中有不受支持的命令，则在将其与 **service-policy 命令一起应用后，交换机会在控制台上提示错误消息。**排除**服务策略相关问题故障时，需要考虑这几点。**

- 请勿将服务策略附加到属于 EtherChannel 成员的端口。
- 如果安装了分布式转发卡 (DFC)，则 PFC2 不支持基于 VLAN 的 QoS。不能发出 **mls qos vlan-based 命令将服务策略附加到 VLAN 接口。**
- PFC QoS 支持仅具有 PFC3 并且仅在第 3 层接口（作为第 3 层接口配置的 LAN 端口或 VLAN 接口）上的输出关键字。 使用 PFC3，您可以将输入和输出策略映射附加到第 3 层接口。
- 第 2 层端口上基于 VLAN 或基于端口的 PFC QoS 与附加到具有输出关键字的第 3 层接口的策略无关。
- 附加有输出关键字的策略不支持微流监察。
- 不能使用 **service-policy 命令输出附加配置信任状态的策略映射。**
- PFC QoS 不支持具有出口丢弃的入口减价或具有出口减价的入口丢弃。

服务策略输出语句没有出现在 running-config 命令输出中

当在 FlexWAN 模块的多链路上配置 QoS 时，您无法在 **show running-config 命令输出中看到 service-policy 命令输出。**当交换机运行早于 12.2SX 的 Cisco IOS 版本时，会发生这种情况。Cisco 7600 系列的 FlexWAN 支持非捆绑接口上的 dLLQ。不支持 MLPPP 捆绑接口上的 dLLQ。Cisco IOS 软件版本 12.2S 提供此类支持。

绕过此限制的应急方案是，将服务策略附加到非捆绑接口，或者将 Cisco IOS 版本升级到支持该功能的 12.2SX 或更高版本。

监察限制

监察在 PFC 的硬件中执行，不会影响交换机性能。监察不会在没有 PFC 的 6500 平台上发生。在混合 OS 中，必须在 CatOS 上配置监察。当您排除监察问题故障时，需要考虑以下几点：

- 当您将入口监察和出口监察应用到同一流量时，输入策略和输出策略必须对流量减价或丢弃流量。PFC QoS 不支持具有出口丢弃的入口减价或具有出口减价的入口丢弃。
- 当创建不使用 pir 关键字并且 maximum_burst_bytes 参数与 normal_burst_bytes 参数相等（这种情况下，您没有输入 maximum_burst_bytes 参数）的监察器时，exceed-action policed-dscp-transmit 关键字会导致 PFC QoS 按照 policed-dscp max-burst 减价映射的规定对流量减价。
- 丢弃超额操作时，PFC QoS 将忽略任何已配置违规操作。
- 将丢弃配置为确认操作时，PFC QoS 会将丢弃配置为超额操作和违规操作。
- 微流监察、NetFlow 和 NetFlow 数据输出 (NDE) 的流掩码需求可能发生冲突。

在混合 OS 中使用 MSFC 的速率限制或监察问题

在运行混合 OS 的 Catalyst 6500 交换机上，速率限制的配置不会产生想要的输出。例如，如果您在 MSFC 的 **interface vlan 命令下配置 rate-limit 命令，则实际上并不会对流量进行速率限制。**

```
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
```

或者:

```
interface Vlan10
service-policy input Test_Policy
```

背后的原因是，MSFC 只关心控制功能，但 Supervisor 的 PFC ASIC 上会发生实际流量转发。MSFC 编译 FIB、邻接表和其他控制信息，并将其下载到 PFC，以在硬件中实施。使用您已创建的配置，您只能对软件交换流量进行速率限制，这种限制程度极低（或没有限制）。

应急方案是，使用 CatOS 命令行界面 (CLI)，以便在 Supervisor 上配置速率限制。有关如何在 CatOS 中配置 QoS 监察的详细说明，请参阅 CatOS QoS。还可参阅 Catalyst 6500/6000 系列交换机上的 QoS 检查查看配置示例。

命令形状平均在 Cisco 7600 的 VLAN 接口不受支持

当您将服务策略输入应用到 Cisco 7600 的接口时，会出现以下错误消息：

```
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
```

shape average 命令在 Cisco 7600 的 VLAN 接口不受支持。相反，您需要使用监察。

```
7600_1(config)#policy-map POLICY_1
7600_1(config-pmap)#class TRAFFIC_1
7600_1(config-pmap-c)#police conform-action transmit exceed-action drop
```

有关如何实施监察以限制流量速率的详细信息，请参阅配置策略映射类监察。

当您将此服务策略附加到 VLAN 接口 (SVI) 时，您需要在所有第 2 层端口上启用基于 VLAN 的 QoS，这些第 2 层端口属于您想要对其应用此策略映射的此 VLAN。

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

有关详细信息，请参阅在第 2 层 LAN 端口上启用基于 VLAN 的 PFC QoS。

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
```

此错误消息表明所提类中定义的操作在 Cisco Catalyst 6500 系列交换机中不被允许。配置策略映射类操作期间，存在以下一些限制。

- 不能在一个策略映射类中执行以下所有三个操作：使用 **set 命令标记流量**配置信任状态配置监察只能使用 **set 命令标记流量。**或者配置信任状态和/或配置监察。
- 对于硬件交换流量，PFC QoS 不支持 **bandwidth、priority、queue-limit** 或 **random-detect 策略映射类命令。**因为这些命令可用于软件交换流量，所以可以配置这些命令。
- PFC QoS 不支持 **set qos-group 策略映射类命令。**

有关此类限制的详细信息，请参阅配置策略映射类操作。

相关信息

- 运行 Cisco IOS 软件的 Catalyst 6500/6000 系列交换机的 QoS 分类和标记
- 运行 Cisco IOS 系统软件的 Catalyst 6500/6000 系列交换机上的 QoS 输出调度
- Catalyst 6500/6000 系列交换机上的 QoS 策略
- 运行 CatOS 软件的 Catalyst 6500/6000 系列交换机上的 QoS 分类和标记
- 运行 CatOS 系统软件的 Catalyst 6500/6000 系列交换机上的 QoS 输出调度
- LAN 产品支持页
- LAN 交换技术支持页
- 技术支持和文档 - Cisco Systems