运行 CatOS 软件的 Catalyst 6500/6000 系列交换机上的 QoS 分类和标记

目录

简介

本文调查发生何事在其在Catalyst 6000机箱内的旅途期间关于数据包的标记和分类在不同的地方。它提及特殊情况，限制，并且提供短缺案例研究。

本文没有打算是所有Catalyst OS (CatOS)命令详尽列表关于服务质量(QoS)或标记的。关于CatOS命令行界面(CLI)的更多信息，参考以下文档：

- 配置 QoS

注意： 本文只考虑IP数据流。

开始使用前

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

先决条件

本文档没有任何特定的前提条件。

使用的组件

本文为运行CatOS软件和使用以下Supervisor引擎之一的Catalyst 6000系列交换机是有效：

- SUP1A + PFC
- SUP1A + PFC + MSFC
- SUP1A + PFC + MSFC2
- SUP2+ PFC2
- SUP2+ PFC2 + MSFC2

所有示例命令，然而，在有运行软件版本6.3的SUP1A/PFC的一台Catalyst 6506尝试。

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

术语

下列是用于本文的术语列表：

- 差分服务代码点：服务类型(ToS)字节的前六个位在IP报头的。DSCP 只存在于 IP 数据包中。**注意：** 您也分配内部DSCP到每数据包(IP或非IP)，此内部DSCP分配将是被选派的以后在本文。
- IP优先级：Tos字节的前三个位在IP报头的。
- 业务类别(CoS) ：能使用标记数据包在Layer2的唯一的字段(L2)。它包括以下三个位中的任一个：dot1q的三个dot1p位为IEEE dot1q数据包标记。三个位呼叫“用户字段” ISL封装数据包的交换机间链路(ISL)报头的。没有Cos提交在non-dot1q或ISL数据包里面。
- 分类：用于的进程选择将被标记的流量。
- 标记：设置在数据包的一个第3层(L3) DSCP值进程。在本文中，标记的定义被扩展包括设置L2 Cos值。

Catalyst 6000系列交换机能做根据以下三个参数的分类：

- DSCP
- IP 优先级
- Cos

Catalyst 6000系列交换机是进行的分类和标记在不同的地方。下列是查看在什么在这些不同的地方发生：

- 输入端口(入口Application-specific integrated circuit (ASIC))
- 交换引擎(策略特性卡(PFC))
- 输出端口（出口 ASIC）

启用 QoS

默认情况下， QoS在Catalyst 6000交换机禁用。QoS可以通过发出catos命令**set qos enable**启用。

当QoS禁用时没有分类或交换机完成的标记，以及同样，每数据包留下有，当输入交换机时有DSCP/IP优先的交换机。

输入端口处理

入站端口的主要配置参数，关于分类，是端口的信任状态。系统的每个端口能有以下信任状态之一：

- trust-ip-precedence
- trust-dscp
- trust-cos
- 不信任

此部分剩余描述端口信任状态如何影响数据包的最终分类。使用以下catos命令，端口信任状态可以设置或更改：

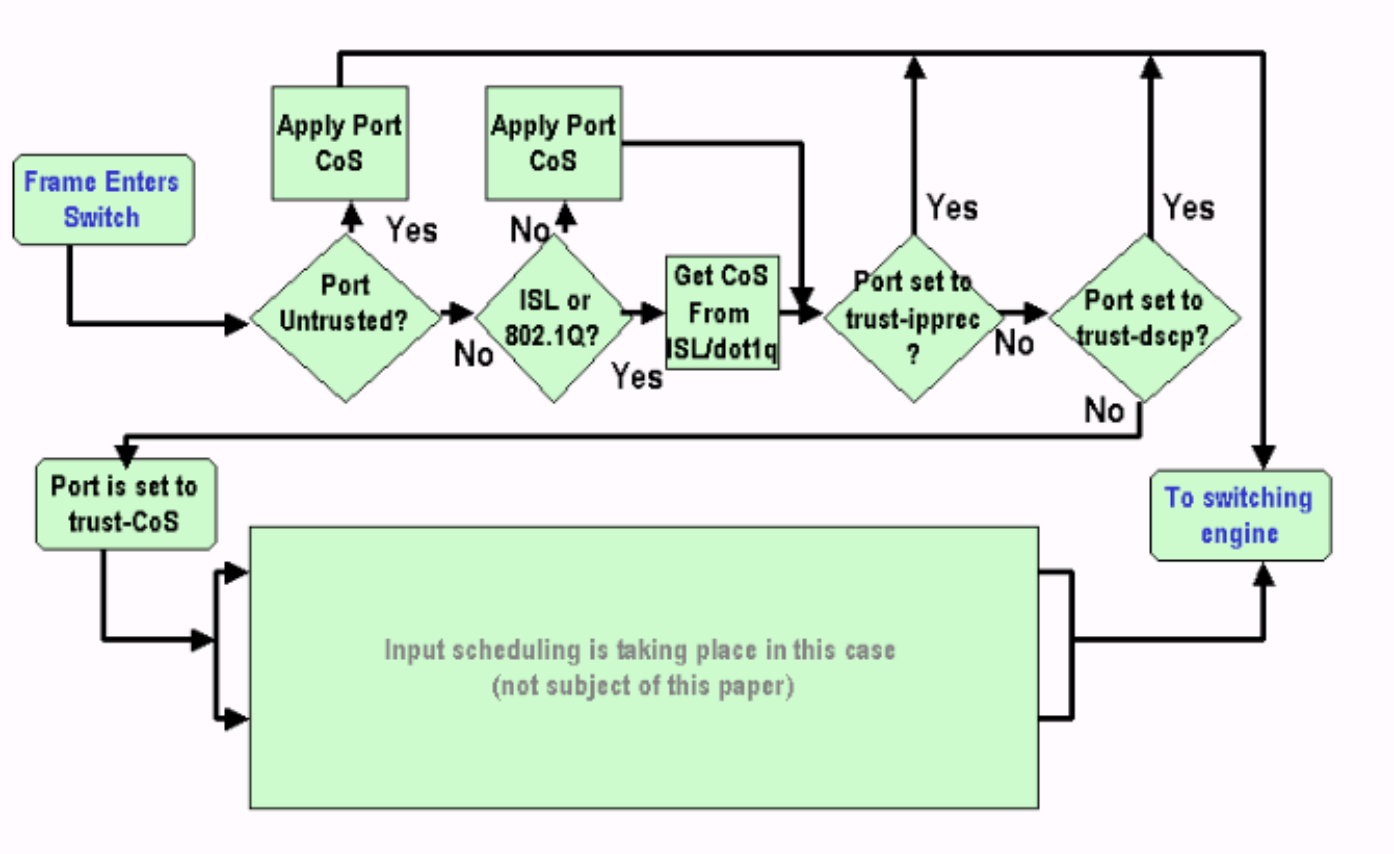
set port qos mod/port trust {不信任|trust-cos|trust-ipprec|trust-dscp}

注意： 默认情况下所有端口在不信任的状态，当QoS启用时。

在输入端口级别您能也应用默认Cos每个端口，正如在以下示例：

set port qos mod/port cos cos-value

如果端口设置为不信任的状态，用端口默认Cos请标记帧并且传递报头到交换引擎(PFC)。如果端口设置到其中一信任状态，请应用默认端口CoS (如果帧没有已接收Cos (dot1q或ISL))或者请保持Cos，它(dot1q和ISL帧)并且通过帧到交换引擎。输入分类在以下流程图说明：



注意： 如上述流程图所显示，每帧将有内部Cos分配(已接收Cos或者默认端口CoS)，包括不运载任何实时Cos的无标记帧。此内部Cos和已接收DSCP在特殊信息包包头写入(呼叫数据总线头)并且在数据总线发送到交换引擎。这发生在进入线路卡，并且这时不知道此内部Cos是否在流出的帧将运载对egresss ASIC并且插入。此所有依靠什么PFC在下一部分执行和进一步描述。

交换引擎 (PFC)

一旦报头到达了交换引擎，交换引擎编码地址识别逻辑(EARL)将分配每成帧内部DSCP。此内部DSCP是内部优先级分配到帧由PFC作为它传输交换机。这不是 IPv4 报头中的 DSCP。当帧退出交换机，它从派生现有设置的Cos或的Tos和用于重置Cos或Tos。此内部 DSCP 由 PFC 分配给所有交换（或路由）的帧，甚至非 IP 帧。

内部 DSCP 的四个可能的来源

内部DSCP从下列之一将派生：

1. 一个现有DSCP值，在输入交换机的帧之前的集。
2. 在IPv4报头已经设置的已接收IP优先级位。因为只有64 DSCP值和八个IP优先级值，管理员将配置由交换机使用派生DSCP的映射。如果管理员不配置地图，默认映射到位。
3. 如果没有在流入的帧的Cos已接收Cos位已经设置在输入交换机的帧之前，或者从传入端口的默认Cos。对于 IP 优先级，最多有 8 个 CoS 值，每个值都必须映射到 64 个 DSCP 值中的一个。此地图可以配置，或者交换机能已经到位使用默认映射。
4. DSCP可以为帧设置使用虽则典型地分配的DSCP默认值访问控制表(ACL)条目。

默认情况下对于在上述列表的没有2和3，使用的静态映射是，如下：

- DSCP派生了等于八次Cos， Cos的对DSCP映射。
- DSCP派生了等于八次IP优先级， IP优先级的对DSCP映射。

此静态映射可以由用户改写通过发出以下命令：

设置qos ipprec-dscp-map <dscp1> <dscp2>...<dscp8>

设置qos cos-dscp-map <dscp1> <dscp2>...<dscp8>

DSCP的第一个值与映射相应的Cos (或IP优先级的)是"0"，第二Cos的(或IP优先级)是"1"和继续在该模式。

内部 DSCP 的四个可能的来源中哪个将被使用？

此部分描述确定的规则哪些四可能的来源描述以上将使用每数据包。那取决于以下参数：

1. 什么QoS ACL将应用到数据包？以下规则取决于这：**注意：** 每数据包通过ACL条目。如果没有ACL附加对传入端口或VLAN，请应用默认ACL。如果有ACL附加对传入端口或VLAN，并且，如果流量匹配其中一个在ACL的条目，请使用此条目。如果有ACL附加对传入端口或VLAN，并且，如果流量不匹配其中一个在ACL的条目，请使用默认ACL。
2. 每个条目包含分类关键字。下列是可能的关键字和他们的说明列表：trust-ipprec ：内部DSCP从已接收IP优先级将派生根据静态映射不管什么端口信任状态可能是。trust-dscp ：内部DSCP从已接收DSCP将派生不管什么端口信任状态可能是。trust-cos ：内部DSCP从已接收Cos将派生根据静态映射，如果端口信任状态是委托(trust-cos， trust-dscp， trust-ipprec)。如果端口信任状态是trust-xx， DSCP从默认端口CoS将派生根据同一个静态映射。dscp *xx*:内部DSCP将取决于以下传入端口信任状态：如果端口不信任，内部DSCP将设置到*xx*。如果端口是trust-dscp，内部DSCP将是在流入数据包接收的DSCP。如果端口是trust-cos，内部DSCP从收到的信息包的Cos将派生。如果端口是trust-ipprec，内部DSCP从收到的信息包的IP优先级将派生。
3. 每个QoS ACL可以应用到端口或到VLAN，但是有考虑到的更多的配置参数;ACL 端口类型。可以将端口配置为基于 VLAN 或基于端口的端口。下列是配置的两种类型的说明：配置的端口基于vlan的只将查找对ACL应用对端口属于的VLAN。如果有ACL附加对端口， ACL为进来在该端口的数据包将忽略。如果属于VLAN的端口配置如基于端口的，即使有ACL附加对该VLAN，不会为进来自该端口的流量被考虑到。

下列是创建QoS ACL的语法标记IP数据流：

set qos acl ip acl_name [dscp xx|trust-cos|trust-dscp|] trust-ipprec *ACL条目规则*

以下ACL，将指示处理的所有IP数据流主机与DSCP的1.1.1.1 "40"和为其他IP数据流trust-dscp ：

set qos acl TEST_ACL dscp 40 ip any host 1.1.1.1

set qos acl TEST_ACL trust-dscp ip any any

一旦ACL创建您需要映射它到端口或VLAN，这可以由发出以下命令完成：

set qos acl map acl_name [模块/端口|VLAN]

默认情况下，每个端口为ACL是基于端口的，因此，如果要附加ACL到VLAN，您需要配置此VLAN端口如基于vlan的。这可以由发出以下命令完成：

set port qos module/port vlan-based

它可能也被恢复回到基于端口的模式通过发出以下命令：

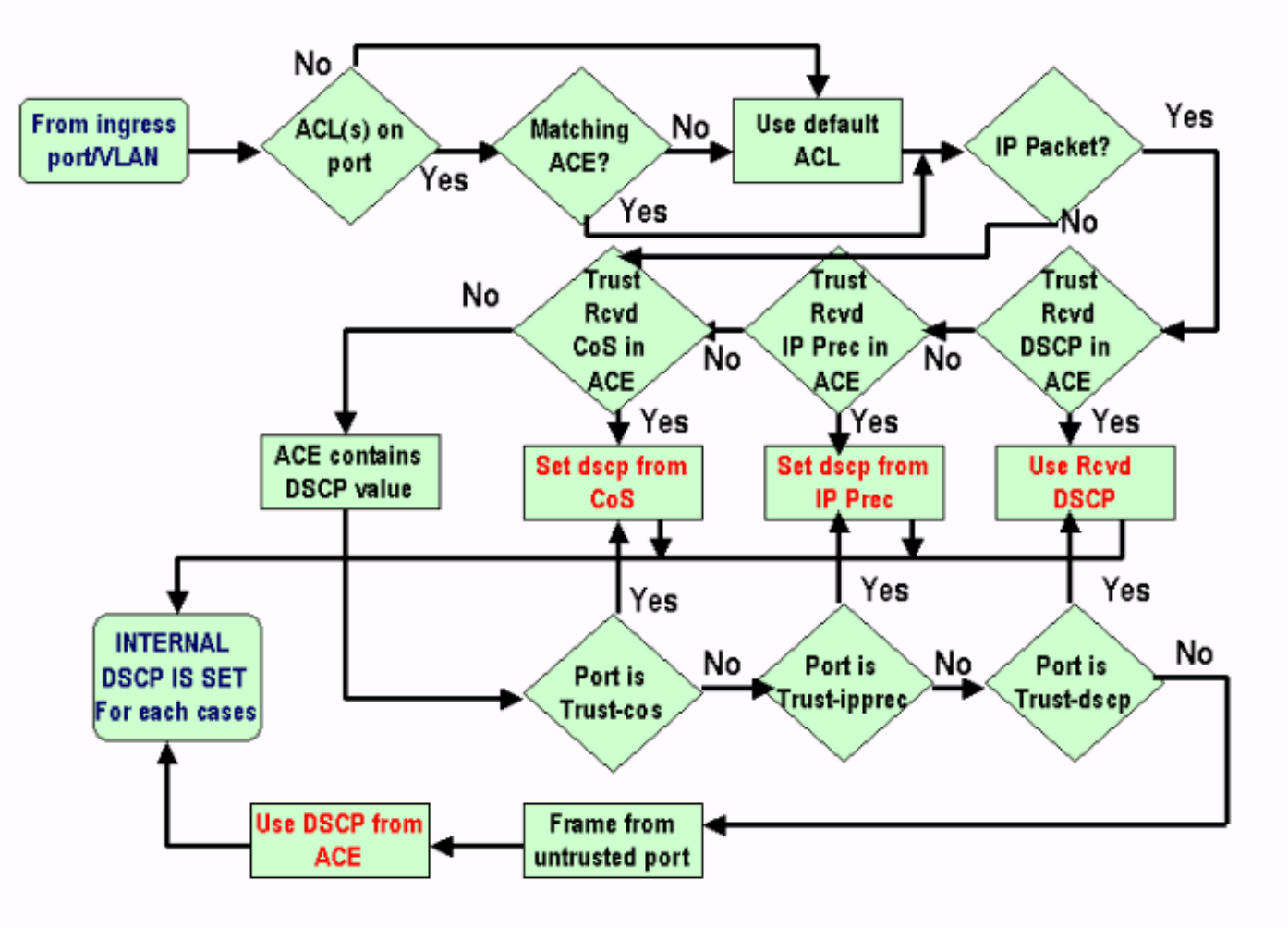
set port qos module/port port-based

摘要：内部 DSCP 如何被选择？

内部DSCP取决于以下要素：

- 端口信任状态
- ACL附加对端口
- 默认ACL
- 基于vlan的或基于端口的关于ACL

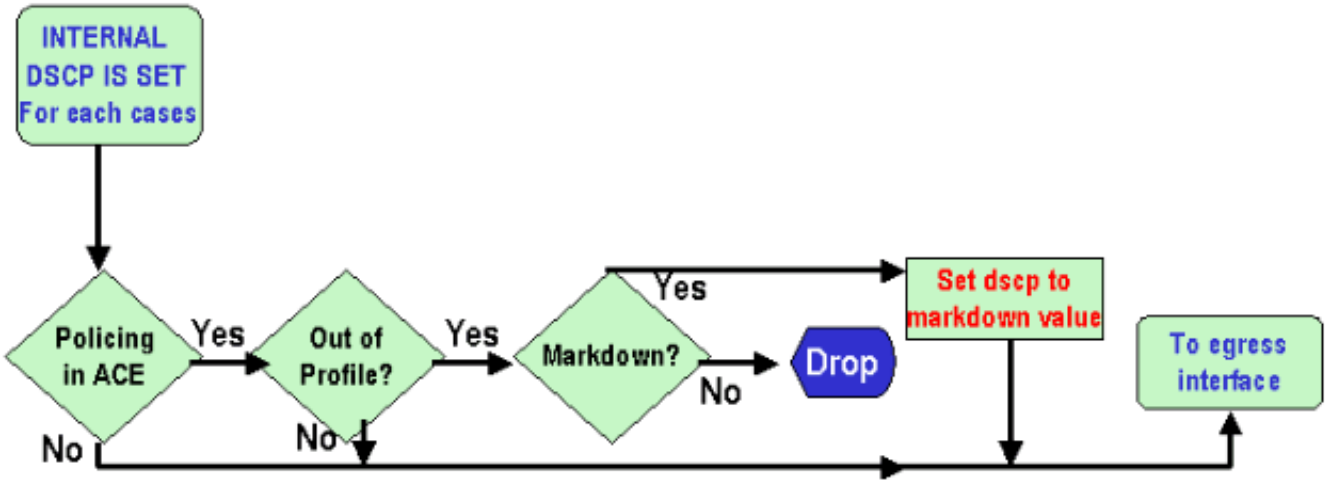
以下流程图汇总内部DSCP如何根据配置选择：



PFC 也能够制定策略。这也许最终导致内部DSCP的减价。欲了解更详细的信息在管制，参考以下文档：

- Catalyst 6000 上的 QoS 策略

以下流程图显示策略器如何应用：



输出端口处理

可以在级的输出端口完成更改分类的没什么，但是在此部分您将标记达成协议以下规则的数据包：

- 如果数据包是IPv4数据包，请复制交换引擎分配的内部DSCP到IPv4报头的Tos字节。
- 如果输出端口为ISL或dot1q封装配置，请使用从内部DSCP派生的Cos，并且复制它在ISL或dot1q帧。

注意： Cos从内部DSCP派生根据用户配置的静态发出以下命令：

注意： **设置qos dscp-cos-map** *dscp_list ：cos_value*

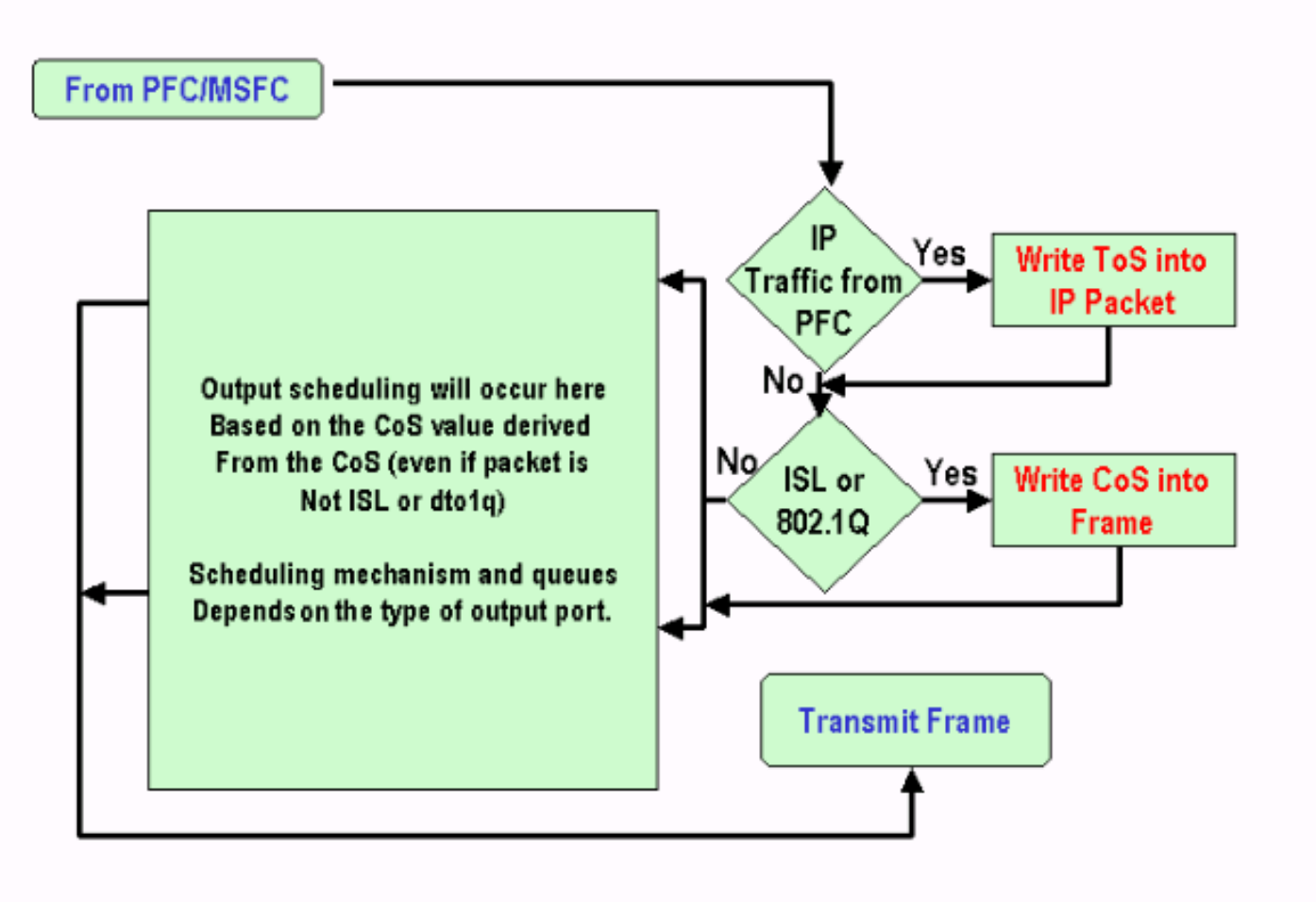
注意： 下列是默认配置。默认情况下Cos将是八除的DSCP的整数部分：

```
set qos dscp-cos-map 0-7:0
set qos dscp-cos-map 8-15:1
set qos dscp-cos-map 16-23:2
set qos dscp-cos-map 24-31:3
set qos dscp-cos-map 32-39:4
set qos dscp-cos-map 40-47:5
set qos dscp-cos-map 48-55:6
set qos dscp-cos-map 56-63:7
```

一旦DSCP写入到IP报头，并且Cos从DSCP派生，数据包将发送到其中一个根据其Cos的输出调度的输出队列(即使数据包不是dot1q或ISL)。关于输出队列日程安排的更多信息，参考以下文档：

- 在Catalyst 6000系列交换机的QoS ：在Catalyst 6000的输出调度有PFC的或PFC 2使用CatOS软件

以下流程图在输出端口汇总处理关于标记的数据包：



附注和限制

默认 ACL

默认情况下，默认ACL使用“dscp 0"作为分类关键字。那意味着输入交换机的所有流量通过不可信端口用DSCP "0"将标记，如果QoS启用。您能通过发出以下命令验证IP的默认ACL ：

```
Boris-1> (enable) show qos acl info default-action ip set qos acl default-action ----------
---------- ip dscp 0
```

默认ACL可能通过发出以下命令也更改：

set qos acl default-action ip [dscp xx|trust-cos|trust-dscp|trust-ipprec]

ACL 条目限制中的 trust-cos

有出现的一个另外的限制，当您使用在条目内的信任-COS关键字。如果接收信任状态不不信任，Cos在条目可能只委托。尝试配置与trust-cos的一个条目将显示以下警告：

```
Telix  (enable) set qos acl ip test_2 trust-CoS ip any any Warning: ACL trust-CoS should only be
used with ports that are also configured with port trust=trust-CoS test_2 editbuffer modified.
Use 'commit' command to apply changes.
```

此限制是什么的结果在Input Port Handling部分被看到了前。如在该部分中看到流程图，如果端口不信任，帧立即分配默认端口CoS。所以，流入Cos没有保留和没有发送到交换引擎，造成无法委托Cos与特定ACL。

WS-X6248-xx、WS-X6224-xx 和 WS-X6348-xx 线路卡限制

此部分只关系到以下线卡：

- WS-X6224-100FX-MT：CATALYST 6000 24多模波尔特100的FX
- WS-X6248-RJ-45：CATALYST 6000 48 端口 10/100 RJ-45 模块
- WS-X6248-TEL：CATALYST 6000 48 端口 10/100 TELCO 模块
- WS-X6248A-RJ-45：CATALYST 6000 48 端口 10/100，增强 QOS
- WS-X6248A-TEL：CATALYST 6000 48 端口 10/100，增强 QOS
- WS-X6324-100FX-MM：CATALYST 6000 24-PORT 100FX， ENH QOS， MT
- WS-X6324-100FX-SM：CATALYST 6000 24-PORT 100FX， ENH QOS， MT
- WS-X6348-RJ-45：CATALYST 6000 48-PORT 10/100，增强版QO
- WS-X6348-RJ21V：CATALYST 6000 48 端口 10/100，内联电源
- WS-X6348-RJ45V：CATALYST 6000 48-PORT 10/100， ENH QOS， INLI NE POWER

这些线卡，然而，有一些另外的限制：

- 在端口级别，您请勿能trust-dscp或trust-ipprec。
- 在端口级别，如果端口信任状态是trust-cos，以下语句应用：输入调度的接收阈值启用。另外，在接收数据包的Cos用于优先安排数据包访问总线。除非也配置该流量的ACL对trust-cos，Cos不会委托和不使用派生内部DSCP。另外，它不是足够为线卡对trust-cos在端口，您也需要有与trust-cos的ACL该流量的。
- 如果端口信任状态不信任，正常标记将发生(如同标准的案件)。这依靠ACL应用对流量。

所有尝试配置这些端口之一的信任状态将显示以下警告消息之一：

```
telix (enable) set port qos 3/24 trust trust-ipprec
Trust type trust-ipprec not supported on this port.

telix (enable) set port qos 8/4 trust trust-dscp
Trust type trust-dscp not supported on this port.

telix (enable) set port qos 3/24 trust trust-cos
Trust type trust-cos not supported on this port.
Receive thresholds are enabled on port 3/24.
Port  3/24 qos set to untrusted.
```

分类汇总

下表显示以下分类的发生的DSCP ：

- 传入端口信任状态。
- 在已应用ACL内的分类关键字。

所有端口的通用的表汇总除去WS-X62xx和WS-X63xx

ACL关键字 端口信任状态	dscp xx	trust-dscp	trust-ipprec	trust-cos
不信任	xx (1)	Rx dscp	从Rx ipprec派生	0
trust-dscp	rx-dscp	Rx dscp	从Rx ipprec派生	从Rx Cos或端口Cos派生

trust-ipprec	从Rx ipprec派生	Rx dscp	从Rx ipprec派生	从Rx Cos或端口Cos派生
trust-cos	从Rx cos或端口Cos派生	Rx dscp	从Rx ipprec派生	从Rx Cos或端口Cos派生

(1)这是做一个新的标记的唯一方法帧。

WS-X62*xx*或WS-X63*xx*的表汇总

ACL关键字 **端口信任状态**	**dscp *xx***	**trust-dscp**	**trust-ipprec**	**trust-cos**
不信任	xx	Rx dscp	从Rx ipprec派生	0
trust-dscp	不支持	不支持	不支持	不支持
trust-ipprec	不支持	不支持	不支持	不支持
trust-cos	xx	Rx dscp	从Rx ipprec派生	从Rx Cos或端口Cos派生(2)

(2)这是保留流入Cos的唯一方法为来自一62*xx*或63*xx*线卡的流量。

监视和确认配置

检查端口配置

端口设置和配置能已验证通过发出以下命令：

show port qos*模块/端口*

通过发出此命令，您能验证，在其他参数中，以下分类参数：

- 基于端口的或基于vlan的
- 信任端口类型
- ACL附加对端口

下列是此命令输出示例与重要字段的关于突出显示的分类：

```
tamer (enable) show port qos 1/1
QoS is enabled for the switch.
QoS policy source for the switch set to local.


Port  Interface Type Interface Type Policy Source Policy Source
      config         runtime        config        runtime
----- -------------- -------------- ------------- -------------
 1/1    port-based     port-based COPS local Port TxPort Type RxPort Type Trust Type Trust Type
```

```
Def CoS Def CoS config runtime config runtime ----- ------------ ------------ ------------ -----
-------- ------- ------- 1/1 1p2q2t 1p1q4t untrusted untrusted 0 0 (*)Runtime trust type set to
untrusted. Config: Port ACL name Type ----- ------------------------------ ---- 1/1 test_2 IP
Runtime: Port ACL name Type ----- ------------------------------ ---- 1/1 test_2 IP
```

注意： 对于每个字段，有配置的参数和运行时参数。将应用到数据包的那个是运行时参数。

检查 ACL

您能检查在上一个命令应用和看到的ACL通过发出以下命令：

show qos ACL信息运行时间*acl_name*

```
tamer (enable) show qos acl info run test_2
set qos acl IP test_2
---------------------------------------------
1. dscp 32 ip any host 1.1.1.1 2. trust-dscp any
```

案例分析示例

以下示例是在网络可能出现普通的案件的配置示例。

第 1 种情况：在边缘标记

假设您配置作为接入交换机使用的Catalyst 6000与许多用户连接对slot 2，是WS-X6348线卡(10/100M)。用户能发送以下：

- 正常数据流：这总是在VLAN 100，并且需要获得DSCP "0."
- 从IP电话的语音流量：这总是在语音辅助VLAN 101，并且需要获得DSCP "40."
- 任务鉴定的应用流量：这也进来VLAN 100和处理到服务器10.10.10.20。此流量需要获得DSCP "32."

此流量都没有由应用程序标记，因此您将离开端口作为不信任，并且请配置特定ACL分类流量。一个ACL将应用到VLAN 100，并且一个ACL将应用到VLAN 101。您还需要将所有端口配置为基于VLAN。下列是导致的配置的示例：

```
set qos enable
set port qos 2/1-48 vlan-based
!--- Not needed, as it is the default. set port qos 2/1-48 trust untrusted set qos acl ip
Data_vlan dscp 32 ip any host 10.10.10.20 !--- Not needed, because if it is not present you
would !--- use the default ACL which has the same effect. Set qos acl ip Data_vlan dscp 0 ip any
any set qos acl ip Voice_vlan dscp 40 ip any any commit qos acl all set qos acl map Data_vlan
100 set qos acl map Voice_vlan 101
```

第 2 种情况：委托在与仅千兆接口的核心

假设您配置有仅一千兆接口的核心Catalyst 6000在slot 1和slot 2 (在机箱的没有62xx或63xx线卡)。流量由接入交换机以前正确地标记了，因此您不需要做其中任一重新标明，但是您需要保证您委托流入DSCP。这是最容易的案件，因为所有端口将被标记作为trust-dscp，并且那应该是满足的：

```
set qos enable
set port qos 1/1-2 trust trust-dscp
set port qos 2/1-16 trust trust-dscp
...
```

实例3：其它WRR加权修改委托在与62xx或63xx机箱的波尔特的核心

假设您配置一个核心/分布设备有一千兆链路的在WS-X6416-GBIC线卡(在slot 2)和一条10/100链路在WS-X6348线卡(在slot 3)。因为被标记了前在接入交换机级别，您也需要信任所有流入的数据流。由于您在6348线卡不能trust-dscp，最容易的方法在这种情况下将离开所有端口一样不信任和更改默认ACL对trust-dscp，正如在以下示例：

```
set qos enable
set port qos 2/1-16 trust untrusted
set port qos 3/1-48 trust untrusted
set qos acl default-action ip trust-dscp
```

相关信息

- LAN 产品支持
- LAN 交换技术支持
- 技术支持 - Cisco Systems