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

本文档将研究在Catalyst 6000机箱内传输过程中数据包在不同位置进行标记和分类的情况。它提到特殊案例、限制，并提供简短的案例研究。

本文档不是有关服务质量(QoS)或标记的所有Catalyst OS(CatOS)命令的详尽列表。有关CatOS命令行界面(CLI)的详细信息，请参阅以下文档：

- 配置 QoS

注意：本文档仅考虑IP流量。

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

本文档对运行CatOS软件的Catalyst 6000系列交换机以及使用以下Supervisor引擎之一有效：

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

但是，所有示例命令已在运行软件版本6.3的SUP1A/PFC的Catalyst 6506上尝试。

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

以下是本文档中使用的术语列表：

- 差分服务代码点(DSCP):IP报头中服务类型(ToS)字节的前六位。DSCP 只存在于 IP 数据包中。**注意：**您还为每个数据包（IP或非IP）分配内部DSCP，本文档稍后将详细介绍此内部DSCP分配。
- IP 优先级:IP报头中ToS字节的前三位。
- 服务类别(CoS):第2层(L2)上唯一可用于标记数据包的字段。 它包含以下三位中的任一位：IEEE dot1q数据包的dot1q标记中的三个dot1p位。交换机间链路(ISL)报头中ISL封装数据包的三位称为“用户字段”。非dot1q或ISL数据包中不存在CoS。
- 分类：用于选择要标记的流量的过程。
- 标记：在数据包中设置第3层(L3)DSCP值的过程。在本文档中，标记的定义扩展为包括设置L2 CoS值。

Catalyst 6000系列交换机能够根据以下三个参数进行分类：

- DSCP
- IP 优先级
- CoS

Catalyst 6000系列交换机正在不同位置进行分类和标记。以下是这些不同位置发生的情况：

- 输入端口(入口专用集成电路(ASIC))
- 交换引擎(策略功能卡(PFC))
- 输出端口（出口 ASIC）

启用 QoS

默认情况下，Catalyst 6000交换机上禁用QoS。QoS可以通过发出CatOS命令set qos enable**来启用**。

禁用QoS时，交换机不会进行分类或标记，因此，每个数据包离开交换机时都具有进入交换机时的DSCP/IP优先级。

输入端口处理

入口端口的主要配置参数（与分类相关）是端口的信任状态。系统的每个端口都可以具有以下信任状态之一：

- trust-ip-precedence
- trust-dscp
- trust-cos
- 不可信

本节的其余部分介绍端口信任状态如何影响数据包的最终分类。可以使用以下CatOS命令设置或更改端口信任状态：

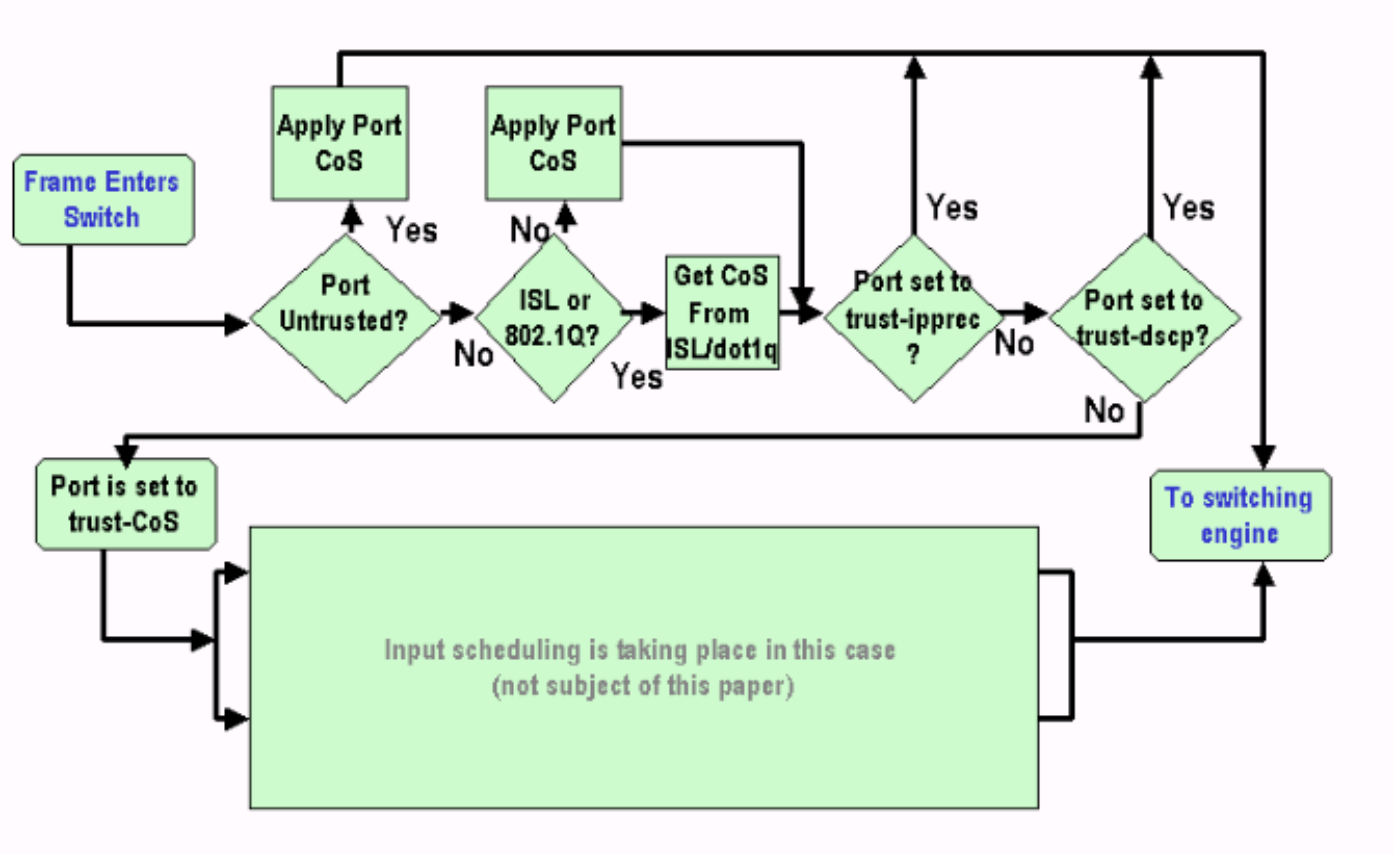
set port qos mod/*port trust* {untrusted | trust-cos | trust-ipprec | trust-dscp }

注意：默认情况下，启用QoS时，所有端口都处于不受信任状态。

在输入端口级别，您还可以按端口应用默认CoS，如以下示例所示：

set port qos mod/*port cos* cos *cos-value*

如果端口设置为不受信任状态，只需用端口默认CoS标记帧，然后将报头传递给交换引擎(PFC)。如果端口设置为信任状态之一，则应用默认端口CoS(如果帧没有接收到CoS（dot1q或ISL）)，或保持CoS原样（对于dot1q和ISL帧），然后将帧传递到交换引擎。输入分类在以下流程图中说明：



注意：如上面的流程图所示，每个帧将分配一个内部CoS（接收的CoS或默认端口CoS），包括不承载任何实际CoS的无标记帧。此内部CoS和接收的DSCP写入特殊数据包报头（称为数据总线报头），并通过数据总线发送到交换引擎。这种情况发生在入口线卡上，此时尚不清楚此内部CoS是否将携带到入口ASIC并插入到出站帧中。这取决于PFC的功能，下一节将进一步介绍。

交换引擎 (PFC)

报头到达交换引擎后，交换引擎编码地址识别逻辑(EARL)将为每个帧分配一个内部DSCP。此内部DSCP是PFC在帧传输交换机时分配给帧的内部优先级。这不是 IPv4 报头中的 DSCP。它源自现有CoS或ToS设置，用于在帧退出交换机时重置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将从以下其中一项派生：

1. 在进入交换机的帧之前设置的现有DSCP值。
2. 已在IPv4报头中设置接收的IP优先级位。因为有64个DSCP值，而且只有8个IP优先级值，所以管理员将配置交换机用于派生DSCP的映射。如果管理员未配置映射，则默认映射就位。
3. 收到的CoS位已在帧进入交换机之前设置，或者从传入端口的默认CoS设置（如果传入帧中没有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。可以配置此映射，或者交换机可以使用已有的默认映射。
4. 可以使用通常通过访问控制列表(ACL)条目分配的DSCP默认值为帧设置DSCP。

对于NOS2和3在上述列表中，使用的静态映射默认如下：

- DSCP派生等于CoS的八倍，用于CoS到DSCP的映射。
- DSCP派生等于IP优先级的8倍，用于IP优先级到DSCP映射。

通过发出以下命令，用户可以覆盖此静态映射：

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

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

与CoS（或IP优先级）的映射对应的DSCP的第一个值是“0”，CoS（或IP优先级）的第二个值是“1”，并以该模式继续。

内部 DSCP 的四个可能的来源中哪个将被使用？

本节介绍确定上述四个可能来源中哪一个将用于每个数据包的规则。这取决于以下参数：

1. 该数据包将应用什么QoS ACL?这由以下规则确定：**注意：**每个数据包都经过ACL条目。如果传入端口或VLAN上没有连接ACL，请应用默认ACL。如果有ACL连接到传入端口或VLAN，并且流量与ACL中的一个条目匹配，请使用此条目。如果有ACL连接到传入端口或VLAN，并且流量与ACL*中*的一个条目不匹配，则使用默认ACL。
2. 每个条目都包含一个分类关键字。以下是可能的关键字及其说明的列表：trust-ipprec:无论端口信任状态是什么，内部DSCP都将根据静态映射从收到的IP优先级派生。trust-dscp:无论端口信任状态是什么，内部DSCP都将从收到的DSCP派生。trust-cos:如果端口信任状态为可信(trust-cos、trust-dscp、trust-ipprec)，则根据静态映射从收到的CoS派生内部DSCP。 如果端口信任状态为trust-xx，则DSCP将根据相同的静态映射从默认端口CoS派生。dscp *xx*:内部DSCP将取决于以下传入端口信任状态：如果端口不可信，内部DSCP将设置为*xx*。如果端口为trust-dscp，则内部DSCP将是传入数据包中收到的DSCP。如果端口为trust-CoS，则内部DSCP将从收到的数据包的CoS派生。如果端口为trust-ipprec，则内部DSCP将从收到的数据包的IP优先级派生。
3. 每个QoS ACL都可应用于端口或VLAN，但需要考虑额外的配置参数；ACL 端口类型。可以将端口配置为基于 VLAN 或基于端口的端口。以下是两种配置类型的说明：配置为基于VLAN的端口只会查看应用于端口所属VLAN的ACL。如果端口上连接了ACL，则该ACL将被忽略，因为该端口上传入的数据包。如果属于VLAN的端口配置为基于端口，即使该VLAN附加了ACL，也不会考虑从该端口传入的流量。

以下是创建QoS ACL以标记IP流量的语法：

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

以下ACL将使用DSCP“40”标记指向主机1.1.1.1的所有IP流量，并将对所有其他IP流量使用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

创建ACL后，您需要将其映射到端口或VLAN，这可以通过发出以下命令来完成：

set qos acl map *acl_name* **[module/port | VLAN]**

默认情况下，ACL的每个端口都基于端口，因此，如果要将ACL附加到VLAN，则需要将此VLAN的端口配置为基于VLAN。这可以通过发出以下命令来完成：

设置基于端*口qos模*块/端口VLAN

还可以通过发出以下命令将其恢复为基于端口的模式：

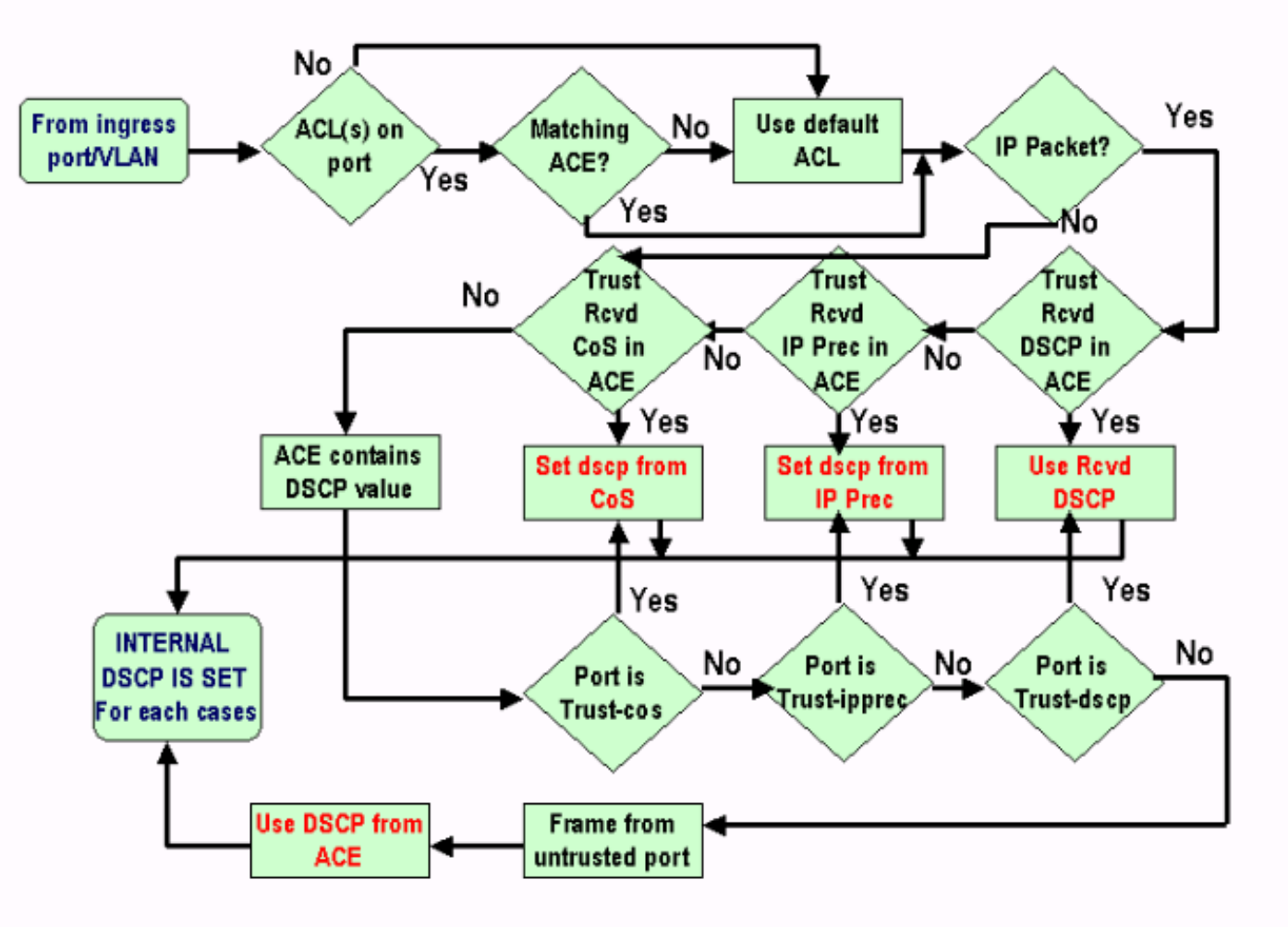
设置端口*qos模块/端口*基于端口

摘要:内部 DSCP 如何被选择？

内部DSCP取决于以下因素：

- 端口信任状态
- 连接到端口的ACL
- 默认 ACL
- ACL中基于VLAN或基于端口

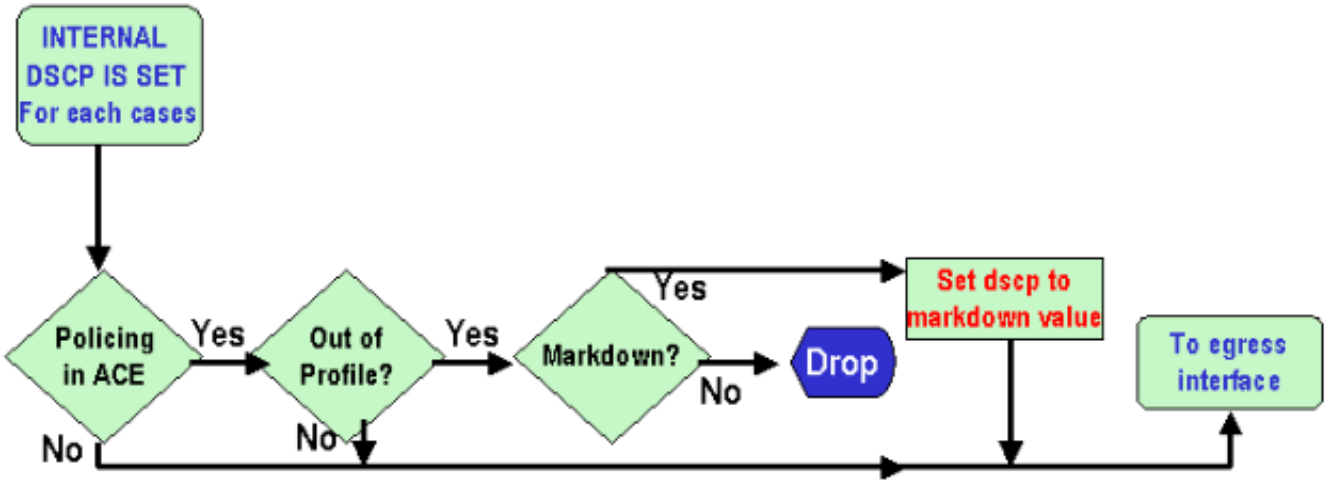
以下流程图总结了如何根据配置选择内部DSCP:



PFC 也能够制定策略。这可能最终导致内部DSCP的降级。有关管制的详细信息，请参阅以下文档：

- Catalyst 6000 上的 QoS 策略

以下流程图显示如何应用监察器：



输出端口处理

在出口端口级别无法更改分类，但在本节中，您将根据以下规则标记数据包：

- 如果数据包是IPv4数据包，请将交换引擎分配的内部DSCP复制到IPv4报头的ToS字节。
- 如果输出端口配置为ISL或dot1q封装，请使用从内部DSCP派生的CoS，并将其复制到ISL或dot1q帧中。

注意：CoS根据用户发出以下命令配置的静态DSCP派生自内部DSCP:

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

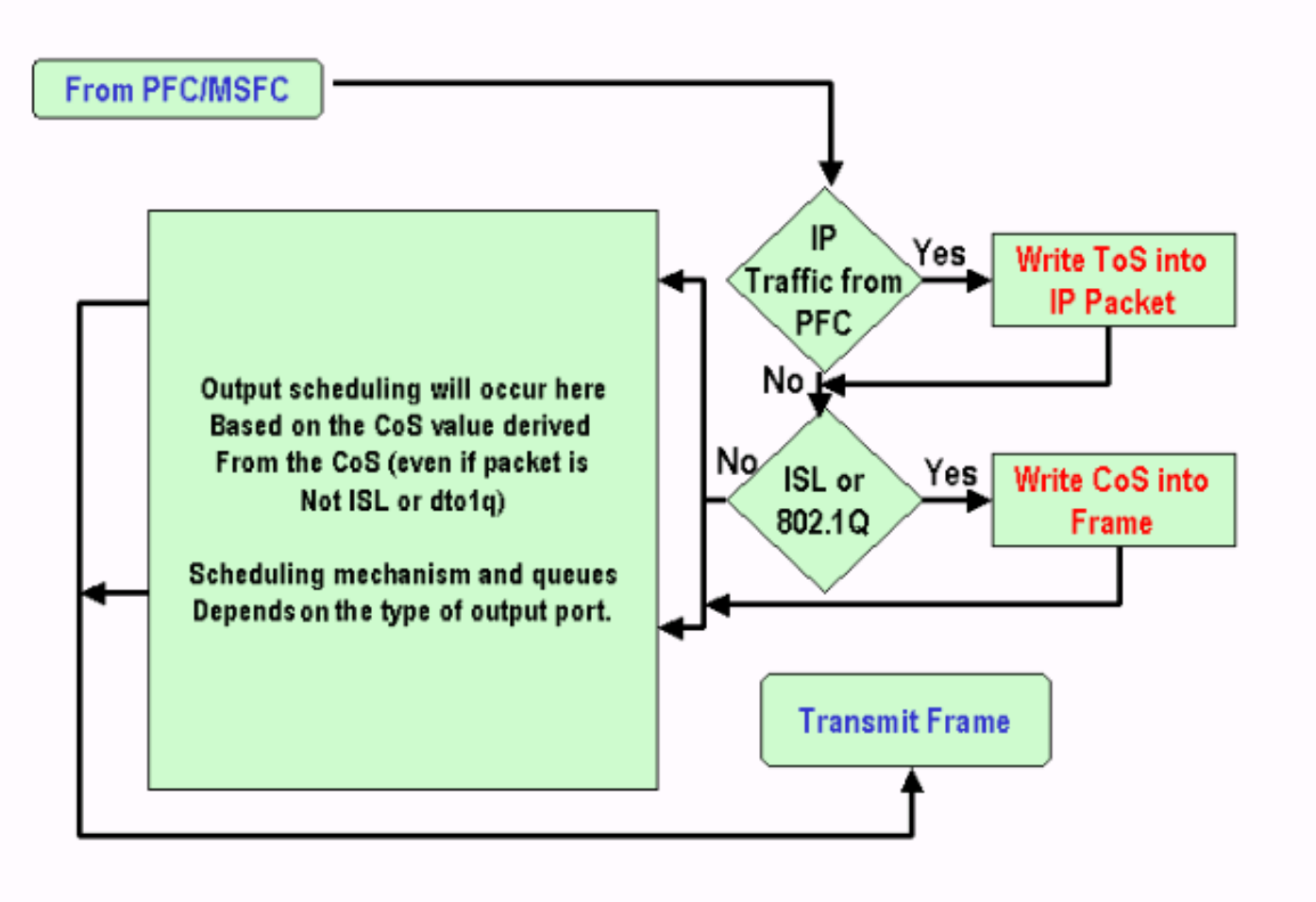
注意：以下是默认配置。默认情况下，CoS将是DSCP的整数部分除以八：

```
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IP报头，并且CoS从DSCP派生，数据包将根据其CoS（即使数据包不是dot1q或ISL）发送到输出队列之一以进行输出调度。 有关输出队列调度的详细信息，请参阅以下文档：

- Catalyst 6000系列交换机上的QoS:使用CatOS软件在带PFC或PFC 2的Catalyst 6000上执行输出调度

以下流程图总结了有关在输出端口中标记的数据包的处理：



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。这意味着，如果启用QoS，则通过不受信任端口进入交换机的所有流量都将标有DSCP“0”。您可以发出以下命令来检验IP的默认ACL:

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

也可以通过发出以下命令更改默认ACL:

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

ACL 条目限制中的 trust-cos

在条目中使用trust-CoS关键字时，还会显示其他限制。只有接收信任状态不不受信任时，才能信任条目中的CoS。尝试使用trust-CoS配置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.
```

此限制是之前在“输入端口处理”部分看到的结果。如该部分的流程图所示，如果端口不可信，则立即为帧分配默认端口CoS。因此，传入的CoS不会保留，也不会发送到交换引擎，从而导致即使使用特定ACL也无法信任CoS。

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

本节仅涉及以下线卡：

- WS-X6224-100FX-MT:CATALYST 6000 24端口100 FX多模
- 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端口100FX，增强型QOS，MT
- WS-X6324-100FX-SM:CATALYST 6000 24端口100FX，增强型QOS，MT
- WS-X6348-RJ-45:CATALYST 6000 48端口10/100，增强型QO
- WS-X6348-RJ21V:Catalyst 6000 48 端口 10/100，内联电源
- WS-X6348-RJ45V:CATALYST 6000 48端口10/100，增强型QOS，INLI NE电源

但是，这些线卡还有一些其他限制：

- 在端口级别，您不能trust-dscp或trust-ipprec。
- 在端口级别，如果端口信任状态为trust-CoS，则应用以下语句：输入调度的接收阈值已启用。此外，接收数据包中的CoS用于优先处理数据包以访问总线。CoS不受信任，并且不会用于派生内部DSCP，除非您还将该流量的ACL配置为trust-cos。此外，线卡在端口上信任cos还不够，您还需要为该流量使用带trust-cos的ACL。
- 如果端口信任状态不可信，则会进行正常标记（与标准情况一样）。 这取决于应用于流量的ACL。

任何尝试在这些端口之一上配置信任状态的行为都会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

下表显示按以下分类的结果DSCP:

- 传入端口信任状态。
- 所应用的 ACL 中的分类关键字.

除WS-X62xx和WS-X63xx外所有端口的通用表摘要

ACL关键字 端口信任状态	dscp xx	trust-dscp	trust-ipprec	trust-cos

不受信任	xx(1)	Rx DSCP	从 Rx ipprec 导出	0
trust-dscp	Rx-dscp	Rx DSCP	从 Rx ipprec 导出	从 Rx CoS 或端口 CoS 导出
trust-ipprec	从 Rx ipprec 导出	Rx DSCP	从 Rx ipprec 导出	从 Rx CoS 或端口 CoS 导出
trust-cos	从 Rx CoS 或端口 CoS 导出	Rx DSCP	从 Rx ipprec 导出	从 Rx CoS 或端口 CoS 导出

(1)这是对帧进行新标记的唯一方法。

WS-X62xx或WS-X63*xx*的表摘要

ACL关键字 **端口信任状态**	**dscp xx**	**trust-dscp**	**trust-ipprec**	**trust-cos**
不受信任	xx	Rx DSCP	从 Rx ipprec 导出	0
trust-dscp	Not Supported	Not Supported	Not Supported	Not Supported
trust-ipprec	Not Supported	Not Supported	Not Supported	Not Supported
trust-cos	xx	Rx DSCP	从 Rx ipprec 导出	从Rx CoS或端口CoS(2)派生

(2)这是保留来自62xx或63xx线卡的流量的传入CoS的唯一方法。

监视和确认配置

检查端口配置

端口设置和配置可以通过发出以下命令来验证：

show port qos module/*port*

通过发出此命令，除其他参数外，您还可以验证以下分类参数：

- 基于端口或基于VLAN
- 信任端口类型
- 连接到端口的ACL

以下是此命令输出的示例，其中突出显示了有关分类的重要字段：

```
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：对于每个字段，都有已配置的参数和运行时参数。将应用于数据包的参数是运行时参数。

检查 ACL

您可以发出以下命令，检查在以前命令中应用和看到的ACL:

show qos acl info runtime *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

以下示例是网络中可能出现的常见案例的配置示例。

第 1 种情况：在边缘标记

假设您正在配置Catalyst 6000作为接入交换机，该交换机有许多用户连接到插槽2，即WS-X6348线卡(10/100M)。 用户可以发送以下消息：

- 正常数据流量：这始终在VLAN 100中，需要获得DSCP“0”。
- 来自IP电话的语音流量：这始终在语音辅助VLAN 101中，需要获得DSCP“40”。
- 任务关键型应用流量：此流量也来自VLAN 100，并定向到服务器10.10.10.20。此流量需要获得DSCP“32”。

应用程序未标记任何此流量，因此您将使端口保持不受信任状态，并将配置特定ACL来对流量进行分类。VLAN 100将应用一个ACL，VLAN 101将应用一个ACL。您还需要将所有端口配置为基于VLAN。以下是结果配置的示例：

```
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：仅使用千兆接口信任核心

假设您配置的核心Catalyst 6000在插槽1和插槽2中仅具有千兆接口（机箱中不含62xx或63xx线卡）。 流量之前已被接入交换机正确标记，因此您无需重新标记，但需要确保您信任传入的DSCP。这是最简单的情况，因为所有端口都将标记为trust-dscp，并且应该足够：

```
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加权修改在机箱中使用62xx或63xx端口信任核心

假设您正在配置核心/分布设备，其中WS-X6416-GBIC线卡上有千兆链路（在插槽2中），WS-X6348线卡上有10/100链路（在插槽3中）。 您还需要信任所有传入流量，因为它之前在接入交换机级别进行了标记。由于您无法在6348线卡上信任dscp，因此在这种情况下，最简单的方法是保留所有端口为不受信任，并将默认ACL更改为trust-dscp，如以下示例所示：

```
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