

运行 Cisco IOS 软件的 Catalyst 6500/6000 系列交换机的 QoS 分类和标记

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[术语](#)

[输入端口处理](#)

[交换引擎 \(PFC\)](#)

[在 Cisco IOS 软件版本 12.1\(12c\)E 及更高版本中配置服务策略对数据包进行分类或标记](#)

[在早于 Cisco IOS 软件版本 12.1\(12c\)E 的 Cisco IOS 软件版本中配置服务策略对数据包进行分类或标记](#)

[内部 DSCP 的四个可能的来源](#)

[内部 DSCP 如何被选择？](#)

[输出端口处理](#)

[附注和限制](#)

[默认 ACL](#)

[WS-X61xx、WS-X6248-xx、WS-X6224-xx 和 WS-X6348-xx 线路卡的限制](#)

[来自 Supervisor 引擎 1A/PFC 上的 MSFC1 或 MSFC2 的数据包](#)

[分类汇总](#)

[监控和验证配置](#)

[检查端口配置](#)

[检查定义类别](#)

[检查应用于接口的策略映射](#)

[案例分析示例](#)

[第 1 种情况：在边缘标记](#)

[第 2 种情况：只有千兆以太网接口的核心交换机的信任配置](#)

[相关信息](#)

简介

本文档将阐释在运行 Cisco IOS® 软件的 Cisco Catalyst 6500/6000 机箱中，在对数据包进行标记和分类的各个阶段所发生的事情。本文档对特殊情况 and 限制进行了说明，并提供了一些简单案例研究。

本文档未提供与 QoS 或标记有关的所有 Cisco IOS 软件命令的详尽列表。关于 Cisco IOS 软件命令行界面(CLI)的更多信息，参考[配置 PFC QoS](#)。

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以下硬件版本：

- 运行 Cisco IOS 软件并使用下列 Supervisor 引擎之一的 Catalyst 6500/6000 系列交换机：有策略特性卡(PFC)和多层交换机特性卡(MSFC)的 Supervisor 引擎 1A 带有 PFC 和 MSFC2 的 Supervisor 引擎 1A 带有 PFC2 和 MSFC2 的 Supervisor 引擎 2

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](#)。

术语

下面列出了本文档使用的术语：

- 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：交换机也会为每个数据包分配一个内部 DSCP (IP 或非 IP)。本文档的[内部 DSCP 的四个可能来源](#)部分详细说明了这种内部 DSCP 分配。
- IP 优先级 — IP 报头中的 ToS 字节的前三位。
- 业务类别(CoS) —能使用标记数据包在Layer2的唯一的字段(L2)。CoS 由以下任意三位组成：dot1q 数据包的 IEEE 802.1Q (dot1q) 标记中的三个 IEEE 802.1p (dot1p) 位。**注意：**默认情况下，Cisco 交换机不标记本地 VLAN 数据包。三个位呼叫“用户字段”—ISL封装的数据包的交换机间链路(ISL)报头的。**注意：**CoS 不存在于非 dot1q 或 ISL 数据包中。
- 分类 — 用于选择要标记的数据流的进程。
- 标记 — 在数据包中设置第 3 层 (L3) DSCP 值的进程。本文档扩大了标记的定义，纳入了 L2 CoS 值的设置。

Catalyst 6500/6000 系列交换机可以基于以下三个参数进行分类：

- DSCP
- IP 优先级
- Cos

Catalyst 6500/6000 系列交换机会在不同阶段执行分类和标记。下面就是不同位置所发生的事项：

- 输入端口 (入口专用集成电路 [ASIC])
- 交换引擎(PFC)
- 输出端口 (出口 ASIC)

输入端口处理

输入端口与分类相关的主要配置参数是端口的 trust 状态。系统的每个端口可以有如下 trust 状态之一：

- trust-ip-precedence
- trust-dscp
- trust-cos
-

要设置或更改端口的 trust 状态，请在接口模式下发出以下 Cisco IOS 软件命令：

```
6k(config-if)#mls qos trust ?
cos          cos keyword
dscp        dscp keyword
ip-precedence ip-precedence keyword
<cr>
```

注意：默认情况下，启用 QoS 时所有端口将处于 untrusted 状态。要在运行 Cisco IOS 软件的 Catalyst 6500 上启用 QoS，请在主配置模式下发出 **mls qos** 命令。

在输入端口级别，您还可以为每个端口应用一个默认 CoS。示例如下：

```
6k(config-if)#mls qos cos cos-value
```

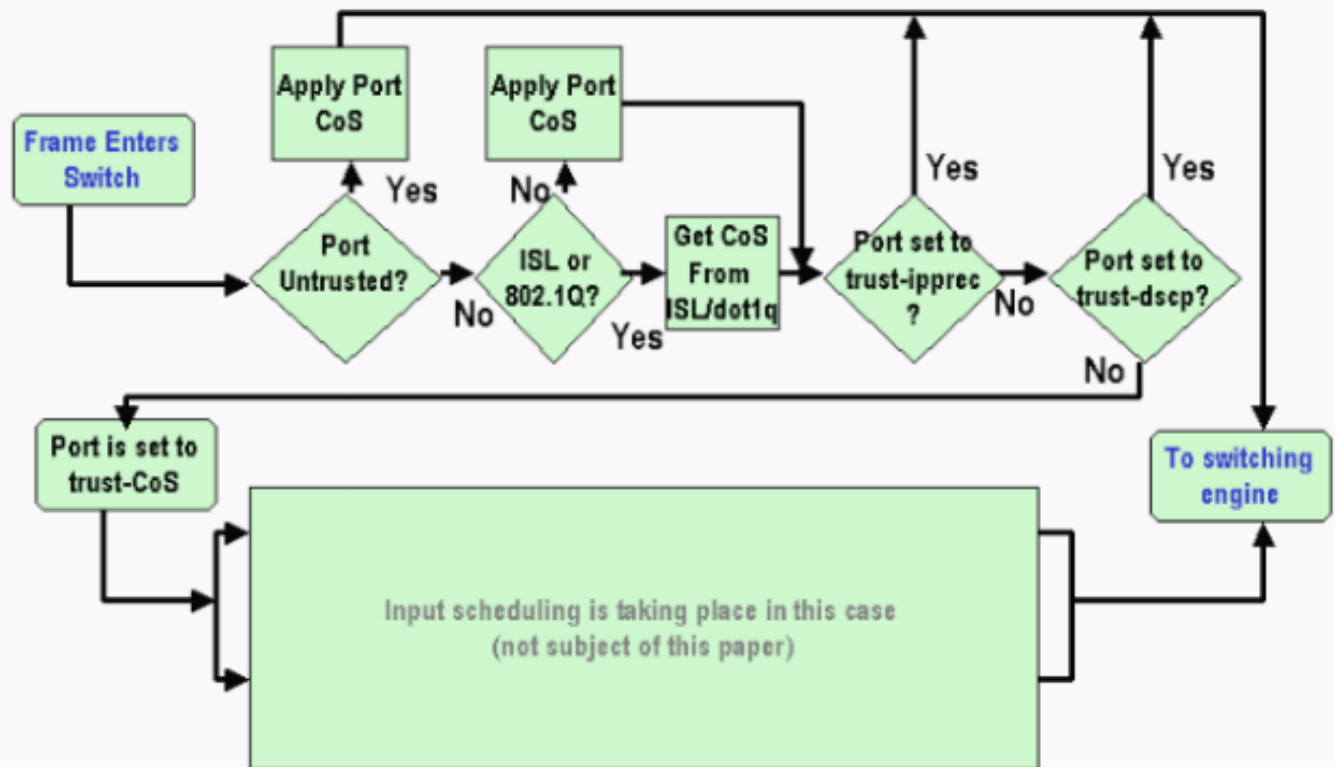
该默认 CoS 适用于所有数据包，例如 IP 和互联网分组交换 (IPX)。您可以将默认 CoS 应用于任何物理端口。

如果端口处于 untrusted 状态，可以使用端口默认 CoS 来标记帧并将报头传递给交换引擎 (PFC)。如果端口设置为其中一种 trust 状态，请执行以下两个选项之一：

- 如果帧没有收到 CoS (dot1q 或 ISL) ，则应用默认端口 CoS。
- 对于 dot1q 和 ISL 帧，原样保留 CoS。

然后，将帧传递给交换引擎。

下面的示例揭示了输入分类和标记。该示例显示了如何将内部 CoS 分配给每个帧：



注意：如该示例所示，每个帧都分配了一个内部 CoS。分配是基于收到的 CoS 或默认端口 CoS 进行的。内部 CoS 包含未携带任何实际 CoS 的无标记帧。内部 CoS 写入在专用数据包报头中（称为数据总线报头），并通过数据总线发送给交换引擎。

交换引擎 (PFC)

当报头到达交换引擎时，交换引擎增强地址识别逻辑(EARL)分配每成帧内部DSCP。该内部 DSCP 是在帧流经交换机时由 PFC 分配给帧的内部优先级。这不是 IP 版本 4 (IPv4) 报头中的 DSCP。内部 DSCP 是从现有 CoS 或 ToS 设置中导出的，用于在帧退出交换机时重置 CoS 或 ToS。该内部 DSCP 将分配给由 PFC 交换或路由的所有帧，包括非 IP 帧。

此部分将探讨如何为接口分配服务策略以便进行标记。其中还会探讨内部 DSCP 的最终设置，这取决于端口的 trust 状态以及所应用的服务策略。

在 Cisco IOS 软件版本 12.1(12c)E 及更高版本中配置服务策略对数据包进行分类或标记

要配置服务策略，请完成以下步骤：

1. 配置访问控制表(ACL)定义您要考虑的流量。可以对 ACL 进行编号或命名；Catalyst 6500/6000 支持扩展 ACL。发出 **access-list xxx** Cisco IOS 软件命令，如下例所示

```
:(config)#access-list 101 permit ip any host 10.1.1.1
```
2. 配置数据流类别（类别映射）以根据所定义的 ACL 或收到的 DSCP 来匹配数据流。发出 **class-map** Cisco IOS 软件命令。PFC Qos 不支持为每个类别映射提供一个以上的匹配语句。此外，PFC Qos 只支持下列匹配语句：**match ip access-group****match ip dscp****match ip precedence****match protocol****注意：match protocol**命令启用使用基于网络的应用程序识别 (NBAR)匹配流量。**注意：**在这些选项中，只支持使用 **match ip dscp** 和 **match ip precedence**

语句。但是，这些语句对于数据包的标记或分类却没有任何用处。您可以使用这些语句，例如，为与特定 DSCP 匹配的所有数据包制定策略。不过，该操作不在本文的讨论范围之内。

```
(config)#class-map class-name
```

```
(config-cmap)#match {access-group | input-interface | ip dscp} 注意： 下面的示例只显示了 match 命令的三个选项。但是您可以在此命令提示符下配置很多选项。注意： 根据流入的数据包，只会采用此 match 命令的其中一个选项进行条件匹配，而忽略其他选项。示例如下：
```

```
class-map match-any TEST
  match access-group 101
```

```
class-map match-all TEST2
  match ip precedence 6
```

3. 配置一个策略映射为先前定义类别应用一个策略。该策略映射包含：一个名称一组类别语句对于每个类别语句，需要为该类别采取的操作PFC1 和 PFC2 QoS 支持下列操作：**trust dscp trust ip precedence trust cos** Cisco IOS 软件版本 12.1(12c)E1 及更高版本中的 **set ip dscp** Cisco IOS 软件版本 12.1(12c)E1 及更高版本中的 **set ip precedence police** **注意：** 此操作不在本文的讨论范围之内。(config)#policy-map policy-name

```
(config-pmap)#class class-name
(config-pmap-c)#{police | set ip dscp}
```

注意： 此示例只显示了两个选项，但是您可以在 (config-pmap-c)# 命令提示符下配置很多选项。示例如下：

```
policy-map test_policy
  class TEST
    trust ip precedence
  class TEST2
    set ip dscp 16
```

4. 配置一个服务策略输入将先前定义的策略映射应用于一个或多个接口。**注意：** 您能附加服务策略到物理接口或到交换的虚拟接口(SVI)或VLAN接口。如果将服务策略应用于 VLAN 接口，则唯一使用此服务策略的端口是属于该 VLAN 并为基于 VLAN 的 QoS 配置的端口。如果没有为基于 VLAN 的 QoS 设置该端口，该端口仍将使用默认的基于端口的 QoS 并只会查看应用于物理接口的服务策略。下面的示例将服务策略 test_policy 应用于千兆以太网端口

```
1/1 : (config) interface gigabitethernet 1/1
(config-if)#service-policy input test_policy
```

下面的示例将服务策略 test_policy 应用于 VLAN 10 中具有基于 VLAN 的 QoS 配置的所有端

```
口 : (config) interface gigabitethernet 1/2
```

```
(config-if)#switchport mode access
(config-if)#switchport access vlan 10
(config-if)#mls qos vlan-based
(config-if)#exit
(config-if)#interface vlan 10
```

```
(config-if)#service-policy input test_policy
```

注意： 如果跳过类别的特定定义并将 ACL 直接与策略映射中的定义相关联，则可以合并此过程中的步骤 2 和步骤 3。在下面的示例中，在配置策略映射之前没有定义类别 TEST

police，该类别是在策略映射中定义的：(config)#policy-map policy-name

```
(config-pmap)#class class_name {access-group acl_index_or_name | dscp dscp_1 [dscp_2
[dscp_N]] | precedence ipp_1 [ipp_2 [ipp_N]]}
```

```
!--- Note: This command should be on one line.
```

```
policy-map TEST
class TEST police access-group 101
```

[在早于 Cisco IOS 软件版本 12.1\(12c\)E 的 Cisco IOS 软件版本中配置服务策略对数据包进行分类或标记](#)

在早于 Cisco IOS 软件版本 12.1(12c)E1 的 Cisco IOS 软件版本中，不能在策略映射中使用 set ip

dscp 或 **set ip precedence** 操作。因此，标记某个类别所定义的特定数据流的唯一方法就是使用非常高的速率配置监视器。例如，该速率应当至少是端口的线路速率，或是某种足够高的速率以使所有数据流都能够应用监视器。然后，使用 **set-dscp-transmit xx** 作为遵从操作。请按照下列步骤操作来设置此配置：

1. 配置 ACL 以定义要关注的数据流。可以对 ACL 进行编号或命名；Catalyst 6500/6000 支持扩展 ACL。发出 **access-list xxx** Cisco IOS 软件命令，如下例所示：

```
(config)#access-list 101
permit ip any host 10.1.1.1
```

2. 配置数据流类别（类别映射）以根据所定义的 ACL 或收到的 DSCP 来匹配数据流。发出 **class-map** Cisco IOS 软件命令。PFC QoS 不支持为每个类别映射提供一个以上的匹配语句。此外，PFC QoS 只支持下列匹配语句：**match ip access-group****match ip dscp****match ip precedence****match protocol****注意**：**match protocol** 命令允许使用 NBAR 来匹配数据流。**注意**：在这些语句中，只支持使用 **match ip dscp** 和 **match ip precedence** 语句。但是，这些语句对于数据包的标记或分类却没有任何用处。您可以使用这些语句，例如，为与特定 DSCP 匹配的所有数据包制定策略。不过，该操作不在本文的讨论范围之内。

```
(config)#class-map
class-name
(config-cmap)#match {access-group | input-interface | ip dscp}
```

注意：下面的示例只显示了 **match** 命令的三个选项。但是您可以在此命令提示符下配置很多选项。示例如下：

```
class-map match-any TEST
  match access-group 101
```

```
class-map match-all TEST2
  match ip precedence 6
```

3. 配置一个策略映射为先前定义的类别应用一个策略。该策略映射包含：一个名称一组类别语句对于每个类别语句，需要为该类别采取的操作PFC1 和 PFC2 QoS 支持下列操作：**trust dscp****trust ip precedence****trust cos****police**因为不支持使用 **set ip dscp** 和 **set ip precedence** 操作，所以必须使用 **police** 语句。由于您实际上并不希望对数据流应用策略，而只是要标记它，因而可以使用一个定义为允许所有数据流的监视器。因此，可以使用一个较大的速率和突发流量来配置监视器。例如，可以使用所允许的最大速率和突发流量来配置监视器。示例如下：

```
policy-map test_policy
  class TEST
    trust ip precedence
  class TEST2
    police 4000000000 31250000 conform-action
    set-dscp-transmit 16 exceed-action policed-dscp-transmit
```

4. 配置一个服务策略输入将先前定义的策略映射应用于一个或多个接口。**注意**：服务策略可以应用于物理接口、SVI 或 VLAN 接口。如果将服务策略应用于 VLAN 接口，则唯一使用此服务策略的端口是属于该 VLAN 并为基于 VLAN 的 QoS 配置的端口。如果没有为基于 VLAN 的 QoS 设置该端口，该端口仍将使用默认的基于端口的 QoS 并只会查看应用于物理接口的服务策略。下面的示例将服务策略 **test_policy** 应用于千兆以太网端口 1/1：

```
(config) interface
gigabitethernet 1/1
```

```
(config-if)#service-policy input test_policy
```

下面的示例将服务策略 **test_policy** 应用于 VLAN 10 中具有基于 VLAN 的 QoS 配置的所有端口：

```
(config) interface gigabitethernet 1/2
```

```
(config-if)#switchport mode access
(config-if)#switchport access vlan 10
(config-if)#mls qos vlan-based
(config-if)#exit
(config-if)#interface vlan 10
(config-if)#service-policy input test_policy
```

[内部 DSCP 的四个可能的来源](#)

内部 DSCP 是从下列各项之一中导出的：

1. 收到的现有 DSCP 值，这是在帧进入交换机之前设置的例如，**trust dscp**。
2. IPv4 报头中已经设置的所收到的 IP 优先级位由于有 64 个 DSCP 值但只有 8 个 IP 优先级值，因此管理员需要配置一个交换机用来导出 DSCP 的映射。如果管理员未配置映射，将使用默认映射。例如，**trust ip precedence**。
3. 在帧进入交换机之前已经设置的并存储在数据总线报头中的所收到的 CoS 位，或者，如果传入的帧中没有 CoS，则会从传入端口的默认 CoS 中导出对于 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。管理员可以配置该映射，或者，交换机可以使用已经设置好的默认映射。
4. 服务策略可以将内部 DSCP 设置为特定值。

对于此列表中的编号 2 和 3，默认情况下静态映射如下所示：

- 对于 CoS 到 DSCP 映射，所导出的 DSCP 等于 CoS 的八倍。
- 对于 IP 优先级到 DSCP 映射，所导出的 DSCP 等于 IP 优先级的八倍。

您可以发出以下命令以覆盖和验证此静态映射：

- **mls qos map ip-prec-dscp dscp_1 dscp_2 dscp_3 dscp_4 dscp_5 dscp_6 dscp_7 dscp_8**
- **mls qos map cos-dscp dscp_1 dscp_2 dscp_3 dscp_4 dscp_5 dscp_6 dscp_7 dscp_8**

对应于 CoS (或 IP 优先级) 的映射的第一个 DSCP 值为 0。CoS (或 IP 优先级) 的第二个值为 1，以此类推。例如，以下命令将更改映射以使 CoS 0 映射到 DSCP 0，CoS 1 映射到 DSCP 8，等等：

```
Cat65(config)#mls qos map cos-dscp 0 8 16 26 32 46 48 54
Cat65#show mls qos maps
CoS-dscp map:
cos:      0 1 2 3 4 5 6 7
-----
dscp:     0 8 16 26 32 46 48 54
```

内部 DSCP 如何选择？

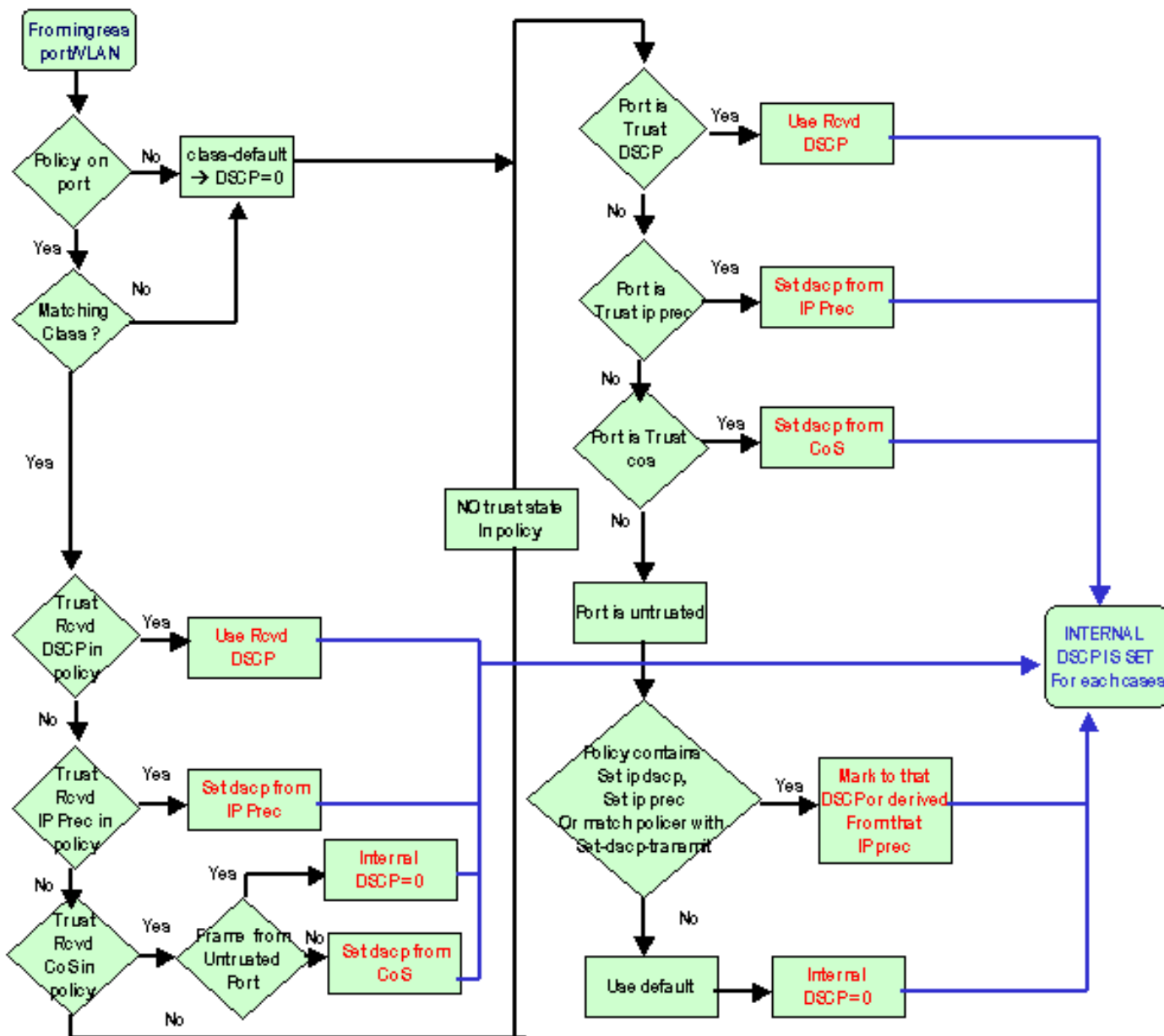
内部 DSCP 是基于下列参数选择的：

- 应用于数据包的 QoS 策略映射由以下规则确定：如果没有服务策略应用于传入端口或 VLAN，则使用默认操作。**注意**：此默认操作将内部 DSCP 设置为 0。如果有服务策略应用于传入端口或 VLAN，并且数据流与该策略所定义的其中一个类别匹配，则使用此条目。如果有服务策略应用于传入端口或 VLAN，并且数据流不与该策略所定义的其中一个类别相匹配，则使用默认设置。
- 端口的 trust 状态和策略映射的操作当端口具有一个特定 trust 状态和一个带有特定标记的策略 (同时的信任操作) 时，将适用以下规则：仅当端口处于 untrusted 状态时，才会应用 **set ip dscp** 命令或在策略映射中为每个监视器定义的 DSCP。如果端口具有 trust 状态，将使用该 trust 状态导出内部 DSCP。端口的 trust 状态始终优先于 **set ip dscp** 命令。策略映射中的 **trust xx** 命令优先于端口的 trust 状态。如果端口和策略包含不同的 trust 状态，则会考虑来自策略映射的 trust 状态。

因此，内部 DSCP 将取决于下列因素：

- 端口的 trust 状态
- 应用于端口的服务策略 (使用 ACL)
- 默认策略映射**注意**：默认设置会将 DSCP 重置为 0。
- ACL 是基于 VLAN 还是基于端口

下图概要描述了如何基于配置来选择内部 DSCP :



PFC 也能够制定策略。这可能会最终导致内部 DSCP 降级。有关策略的详细信息，请参阅 [Catalyst 6500/6000 系列交换机上的 QoS 策略](#)。

输出端口处理

您不能通过在输出端口级别采取任何措施来更改分类。请根据下列规则标记数据包：

- 如果数据包是 IPv4 数据包，请复制交换引擎分配给 IPv4 报头的 ToS 字节的内部 DSCP。
- 如果为 ISL 或 dot1q 封装配置了输出端口，请使用从内部 DSCP 导出的 CoS。复制 ISL 或 dot1q 帧中的 CoS。

注意： CoS 是根据静态映射从内部 DSCP 导出的。请发出以下命令以配置静态映射：

```
Router(config)#mls qos map dscp-cos dscp1 [dscp2 [dscp3 [dscp4 [dscp5 [dscp6 [dscp7 [dscp8]]]]]] to cos_value
!--- Note: This command should be on one line.
```

这里显示的是默认配置。默认情况下，CoS 是 DSCP 除以 8 的整数部分。请发出以下命令以查看

和验证映射：

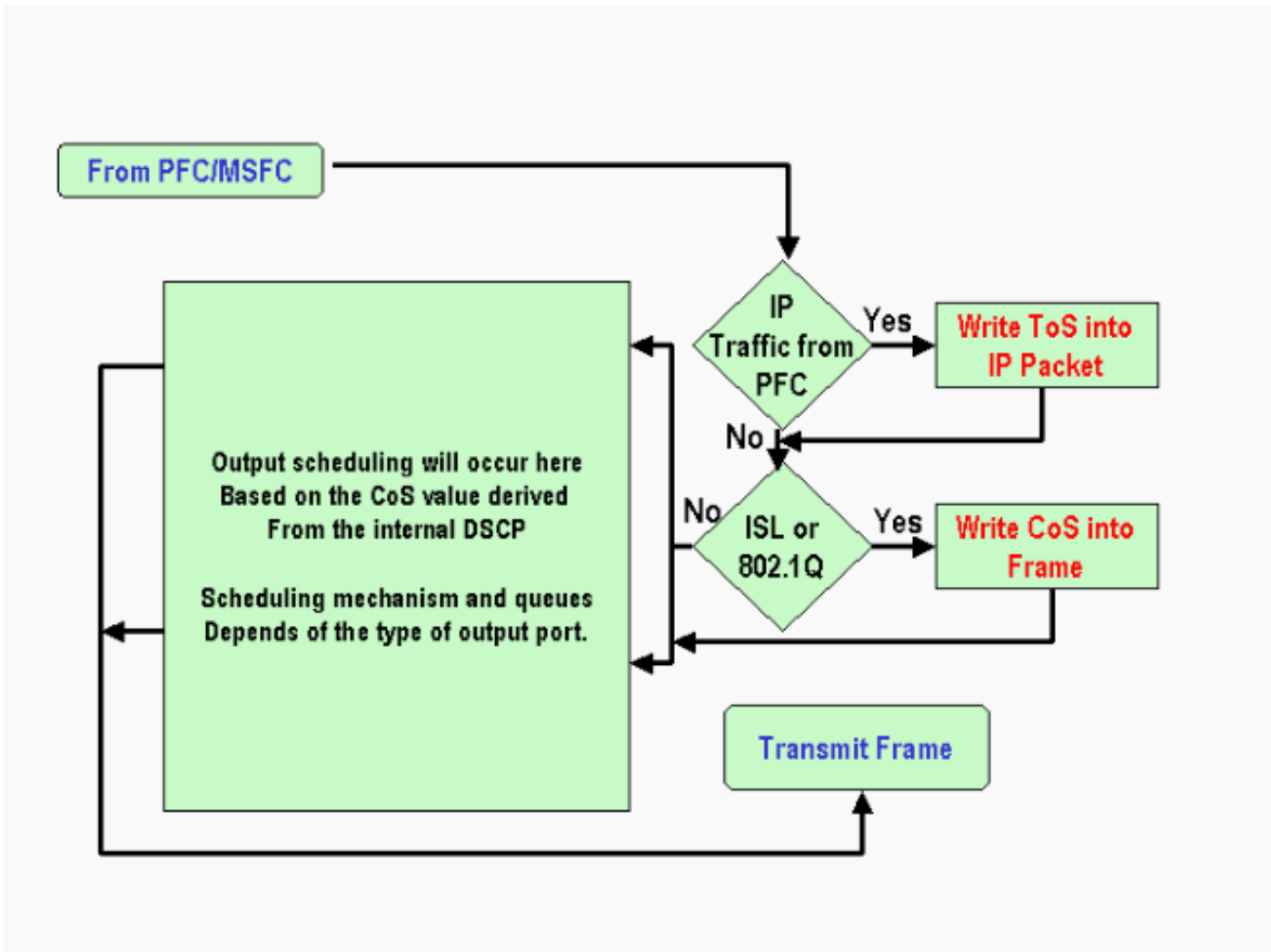
```
cat6k#show mls qos maps
...
Dscp-cos map:                                     (dscp= d1d2)
d1 :  d2 0  1  2  3  4  5  6  7  8  9
-----
0 :   00 00 00 00 00 00 00 00 01 01
1 :   01 01 01 01 01 01 02 02 02 02
2 :   02 02 02 02 03 03 03 03 03 03
3 :   03 03 04 04 04 04 04 04 04 04
4 :   05 05 05 05 05 05 05 05 06 06
5 :   06 06 06 06 06 06 07 07 07 07
6 :   07 07 07 07
```

要更改此映射，请在常规配置模式下发出以下配置命令：

```
mls qos map dscp-cos 0 1 2 3 4 5 6 7 to 0
mls qos map dscp-cos 8 9 10 11 12 13 14 15 to 1
mls qos map dscp-cos 16 17 18 19 20 21 22 23 to 2
...
```

当 DSCP 写入到 IP 报头中并且从 DSCP 中导出 CoS 后，数据包将基于 CoS 发送至输出调度的其中一个输出队列。即使数据包不是 dot1q 或 ISL，也会发生这种情况。有关输出队列调度的详细信息，请参阅[运行 Cisco IOS 系统软件的 Catalyst 6500/6000 系列交换机上的 QoS 输出调度](#)。

下图概要描述了与输出端口中的标记相关的数据包的处理方式：



[附注和限制](#)

[默认 ACL](#)

默认 ACL 使用“dscp 0”作为分类关键字。如果启用了 QoS，则通过不可信端口进入交换机且未能符合某个服务策略条目的所有数据流都将标记一个 DSCP 0。当前，不能在 Cisco IOS 软件中更改默认 ACL。

注意：在 Catalyst OS (CatOS) 软件中，可以配置和更改此默认行为。有关详细信息，请参阅[运行 CatOS 软件的 Catalyst 6500/6000 系列交换机上的 QoS 分类和标记](#)中的[默认 ACL](#)部分。

[WS-X61xx、WS-X6248-xx、WS-X6224-xx 和 WS-X6348-xx 线路卡的限制](#)

本部分只涉及下列板卡：

- WS-X6224-100FX-MT：Catalyst 6000 24 端口 100 FX 多模式
- 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 100 FX，增强 QoS，MT
- WS-X6324-100FX-SM：Catalyst 6000 24 端口 100 FX，增强 QoS，MT
- WS-X6348-RJ-45：Catalyst 6000 48 端口 10/100，增强 QoS
- 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 QoS，内联电源
- WS-X6148-RJ21V：Catalyst 6500 48 端口 10/100 内联电源
- WS-X6148-RJ45V：Catalyst 6500 48 端口 10/100 内联电源

这些板卡有一个限制。在端口级别，不能使用以下任何关键字来配置 trust 状态：

- trust-dscp
- trust-ipprec
- trust-cos

只能使用 untrusted 状态。在其中一个端口上配置 trust 状态的任何尝试都会导致显示以下警告消息之一：

```
Tank(config-if)#mls qos trust ?
  extend  extend keyword
Tank(config-if)#mls qos trust
% Incomplete command.
Tank(config-if)#mls qos trust cos
      ^
% Invalid input detected at '^' marker.
Tank(config-if)#mls qos trust ip-pre
      ^
% Invalid input detected at '^' marker.
```

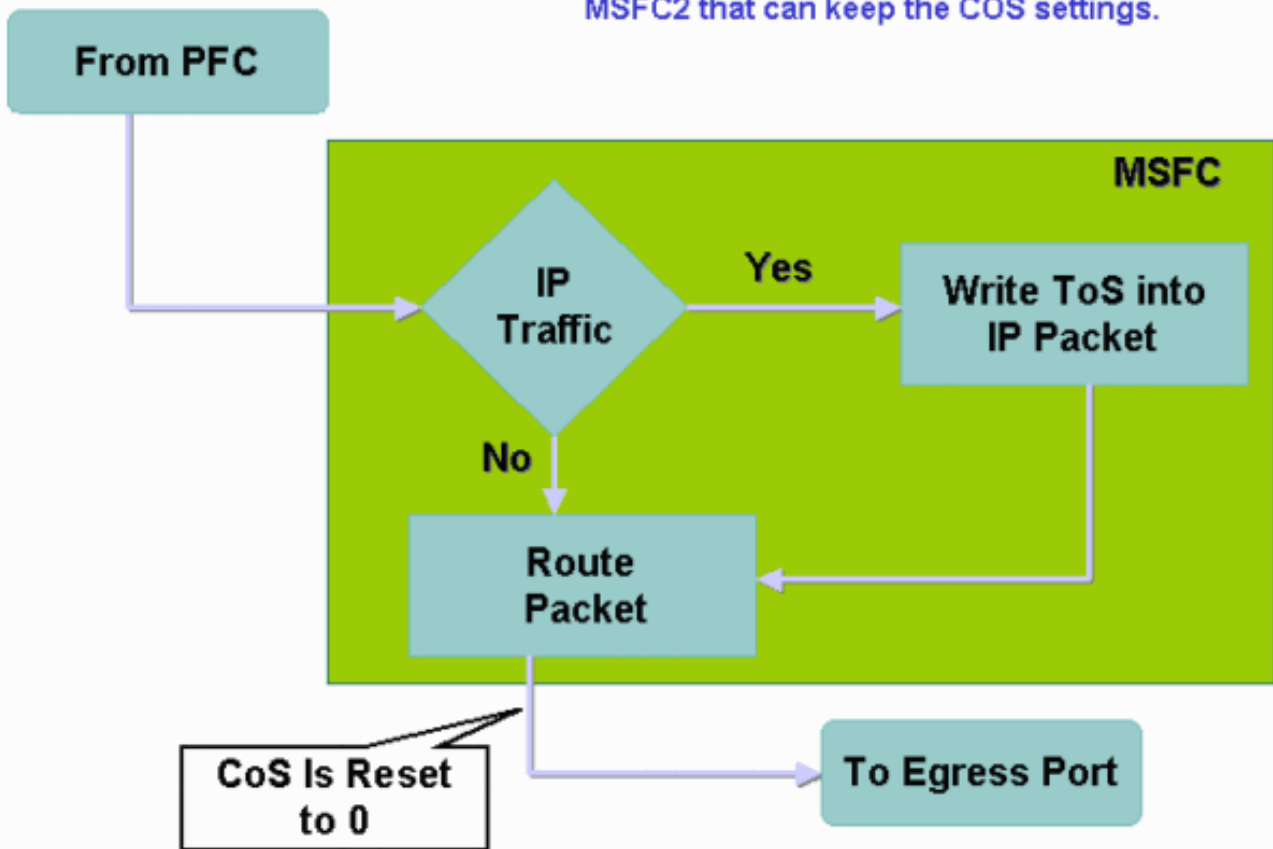
如果希望让可信帧进入这种板卡，必须向端口或 VLAN 应用服务策略。请使用本文档的[案例 1：在边缘标记](#)部分中的方法。

[来自 Supervisor 引擎 1/PFC 上的 MSFC1 或 MSFC2 的数据包](#)

来自 MSFC1 或 MSFC2 的所有数据包都有一个 CoS 0。数据包可以是软件路由的数据包或 MSFC

发出的数据包。这是 PFC 的一个限制，因为它会重置来自 MSFC 的所有数据包的 CoS。DSCP 和 IP 优先级仍会得以维护。PFC2 没有此限制。PFC2 的退出 CoS 与数据包的 IP 优先级是相等的。

This does not apply to the PFC2 or MSFC2 that can keep the COS settings.



分类汇总

以下各表显示了基于下列分类所得到的 DSCP：

- 传入端口 trust 状态
- 所应用的 ACL 中的分类关键字

下表为除 WS-X62xx 和 WS-X63xx 以外的所有端口提供了一个通用汇总：

策略映射关键字	set-ip-dscp xx 或 set-dscp-transmit xx	trust-dscp	trust-ipprec	trust-cos
端口信任状态				
不信任	xx ¹	Rx ² 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这是做一个新的标记的唯一方法帧。

² Rx =接收

下表为 WS-X61xx、WS-X62xx 和 WS-X63xx 端口提供了一个汇总：

策略映射关键字	set-ip-dscp xx 或 set-dscp-transmit xx	trust-dscp	trust-ipprec	trust-cos
端口信任状态				
不信任	xx	Rx DSCP	从 Rx ipprec 导出	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	不支持	不支持	不支持	不支持

监控和验证配置

检查端口配置

发出 **show queuing interface interface-id** 命令以验证端口设置和配置。

发出此命令时，可以验证下列分类参数以及其他参数：

- 是基于端口还是基于 VLAN
- trust 端口类型
- 应用于端口的 ACL

下面是此命令的输出示例。与分类相关的重要字段以粗体显示：

```
6500#show queuing interface gigabitethernet 3/2
Interface GigabitEthernet3/2 queuing strategy: Weighted Round-Robin
  Port QoS is enabled
  Trust state: trust COS
  Default COS is 0
  Transmit queues [type = 1p2q2t]:
```

该输出显示，此特定端口在端口级别上配置为 trust cos。并且默认端口的 CoS 为 0。

检查定义的类型

发出 **show class-map** 命令以检查所定义类别。示例如下：

```
Boris#show class-map
Class Map match-all test (id 3)
  Match access-group 112

Class Map match-any class-default (id 0)
  Match any
Class Map match-all voice (id 4)
```

检查应用于接口的策略映射

发出以下命令以检查在前面的命令中所应用和看到的策略映射：

- **show mls qos ip interface interface-id**
- **show policy-map interface interface-id**

下面是发出这些命令后的输出示例：

```
Boris#show mls qos ip gigabitethernet 1/1
[In] Default. [Out] Default.
QoS Summary [IP]: (* - shared aggregates, Mod - switch module)

Int Mod Dir Class-map DSCP AgId Trust FlId AgForward-Pk AgPoliced-k
-----
Gi1/1 1 In TEST 0 0* No 0 1242120099 0
```

注意： 您可以查看与分类相关的下列字段：

- **Class-map** - 表明哪个类别应用了此接口关联的服务策略。
- **Trust** - 表明该类别中的策略操作是否包含 **trust** 命令以及该类别中的可信内容。
- **DSCP** - 告诉为数据包传送押该类的您DSCP。

```
Tank#show policy-map interface fastethernet 4/4
```

```
FastEthernet4/4

service-policy input: TEST_aggre2

class-map: Test_marking (match-all)
  27315332 packets
  5 minute offered rate 25726 pps
  match: access-group 101
  police :
    10000000 bps 10000 limit 10000 extended limit
    aggregate-forwarded 20155529 packets action: transmit
    exceeded 7159803 packets action: drop
    aggregate-forward 19498 pps exceed 6926 pps
```

案例分析示例

下面提供了网络中可能出现的某些常见案例的配置示例。

第 1 种情况：在边缘标记

假设您要配置一台用作接入交换机的 Catalyst 6000。很多用户连接到该交换机的插槽 2，这是一个 WS-X6348 板卡 (10/100 Mbps)。用户可以发送：

- 常规数据流 - 该数据流始终位于 VLAN 100 中并且需要获得 DSCP 0。

- 来自 IP 电话的语音数据流 - 该数据流始终位于语音辅助 VLAN 101 中并且需要获得 DSCP 46。
- 关键任务应用程序数据流 - 该数据流也会进入 VLAN 100 并会被导向服务器 10.10.10.20。该数据流需要获得 DSCP 32。

应用程序不会对该数据流做任何标记。因此，请将端口设置为 untrusted 并配置一个特定 ACL 对数据流进行分类。一个 ACL 应用于 VLAN 100，一个 ACL 应用于 VLAN 101。您还需要将所有端口配置为基于 VLAN。下面是所获得的配置示例：

```
Boris(config)#mls qos
Boris(config)#interface range fastethernet 2/1-48
Boris(config-if)#mls qos vlan-based
Boris(config-if)#exit
Boris(config)#ip access-list extended Mission_critical
Boris(config-ext-nacl)#permit ip any host 10.10.10.20
Boris(config)#ip access-list extended Voice_traffic
Boris(config-ext-nacl)#permit ip any any
Boris(config)#class-map voice

Boris(config-cmap)#match access-group Voice_traffic
Boris(config)#class-map Critical

Boris(config-cmap)#match access-group Mission_critical
Boris(config)#policy-map Voice_vlan
Boris(config-pmap)#class voice
Boris(config-pmap-c)#set ip dscp 46
Boris(config)#policy-map Data_vlan
Boris(config-pmap)#class Critical
Boris(config-pmap-c)#set ip dscp 32
Boris(config)#interface vlan 100
Boris(config-if)#service-policy input Data_vlan
Boris(config)#interface vlan 101
Boris(config-if)#service-policy input Voice_vlan
```

[第 2 种情况：只有千兆以太网接口的核心交换机的信任配置](#)

假设您要配置一台核心 Catalyst 6000 交换机并且只在插槽 1 和插槽 2 中有一个千兆以太网接口。接入交换机之前已经正确标记了数据流。因此，您不需要进行任何重新标记。但是，您需要确保核心交换机信任传入 DSCP。这是一个比较简单的案例，因为所有端口都标记为 trust-dscp，这应当是足够的：

```
6k(config)#mls qos
6k(config)#interface range gigabitethernet 1/1-2 , gigabitethernet 2/1-2
6k(config-if)#mls qos trust dscp
```

[相关信息](#)

- [了解 Catalyst 6000 系列交换机的服务质量](#)
- [运行 CatOS 软件的 Catalyst 6500/6000 系列交换机上的 QoS 分类和标记](#)
- [LAN 产品支持](#)
- [LAN 交换技术支持](#)
- [技术支持和文档 - Cisco Systems](#)