了解 Catalyst 6000 系列交换机的服务质量

目录

简介

本文档介绍了 Catalyst 6000 系列交换机中提供的服务质量 (QoS) 功能。本文档涉及 QoS 配置功能，并提供了一些示例说明如何实现 QoS。

本文档并不意味着是一份配置指南。整个文档借助配置示例来帮助说明 Catalyst 6000 系列硬件和软件的 QoS 功能。有关 QoS 命令结构的语法参考，请参阅适用于 Catalyst 6000 系列的以下配置和命令指南：

- Catalyst 6500系列交换机

定义第二层 QoS

许多人都可能认为第 2 层 (L2) 交换机中的 QoS 仅仅与确定以太网帧的优先级有关，而很少有人意识到它涉及更多内容。L2 QoS 涉及以下内容：

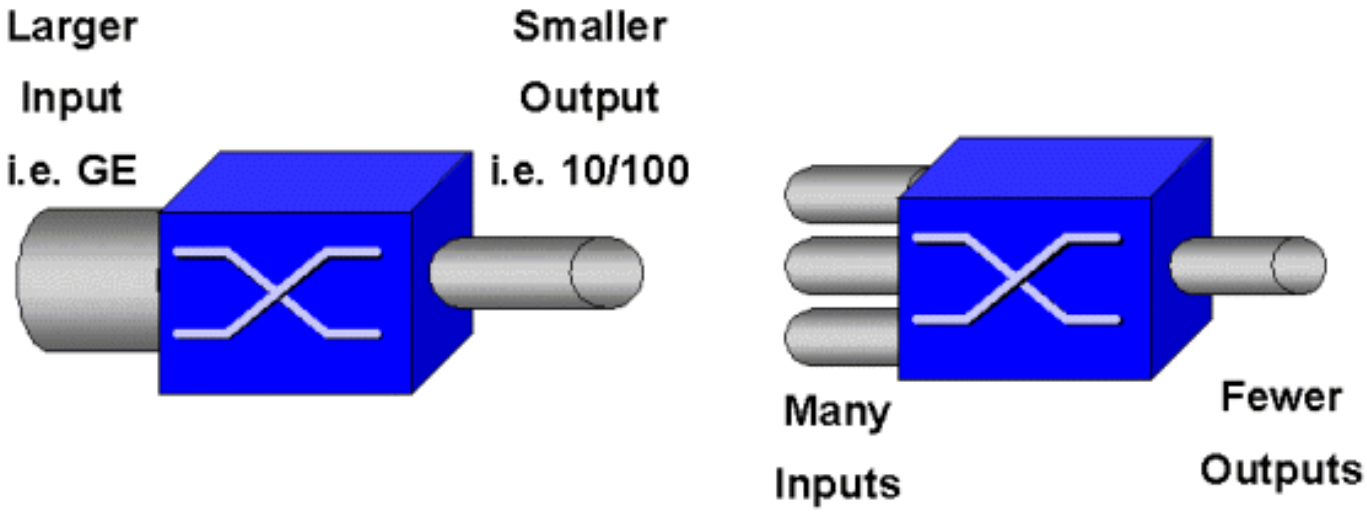
1. **输入队列安排：**当帧进入端口时，可以先将它指定给其中一个基于端口的队列，然后再安排将它交换到输出端口。通常，在以下情况下可使用多个队列：不同的流量需要不同的服务级别，或交换机延迟必须保持最小值。例如， IP根据视频，并且语音数据要求低延时，那么那里可能在需要在交换其他数据之前交换此数据例如文件传输协议(FTP)，Web，电子邮件， Telnet，等等。

2. **分类：**分类进程在以太网L2报头介入检查不同的字段，与IP报头的(第3层(L3))字段一起并且传输控制协议/用户数据报协议(TCP/UDP)报头(Layer4 (L4))在确定将应用到帧作为它的级别的协助服务传输交换机。
3. **修正：**管制是检查以太网帧在某个时间段（通常，此时间段是交换机内部的一个固定数字）内是否超过预定义的流量速率的过程。如果该帧超出预约带宽(即它是数据流的一部分超出预定义的速率限额)，可以或者丢弃或业务类别(CoS)值可以标下来。
4. **重写：**重写进程是交换机的能力修改Cos在以太网报头或服务类型(ToS)位IPv4报头的。
5. **输出队列安排：**在重写过程后，交换机就会将以太网帧放在相应的出站（输出）队列中进行交换。交换机将通过确保缓冲区不会溢出来对此队列进行缓冲区管理。它将通过使用随机早期丢弃(RED)算法典型地执行此，藉以随机的帧从队列删除(丢弃)。加权 RED (WRED) 是 RED 的一种衍生算法（供 Catalyst 6000 系列中的某些模块使用），该算法通过检查 CoS 值确定要丢弃的帧。当缓冲区达到预定义的阈值时，优先级低的帧通常会被丢弃，而优先级高的帧保留在队列中。

本文档的后面部分将更详细地介绍上面的每种机制，并说明这些机制如何与 Catalyst 6000 系列相关。

交换机对 QoS 的需要

当前，巨大的背板、每秒交换数百万的数据包，以及非阻塞交换机都是许多交换机的代名词。为什么还需要 QoS？答案是由于拥塞。



即使是世界上最快的交换机，在上图中所示的任一场景下，也会出现拥塞。出现拥塞时，如果拥塞管理功能未运行，数据包将被丢弃。当数据包被丢弃时，就会进行重新传输，而重新传输可能会增加网络负载。如果网络中已出现拥塞，现有性能问题就会更严重，并且有可能进一步降低性能。

对于收敛网络，拥塞管理更为重要。如果出现延迟，则对延迟敏感的流量（如语音和视频）会受到严重影响。仅仅在交换机中增加更多缓冲区也不一定能够缓解拥塞问题。必须尽快交换对延迟敏感

的流量。首先，您需要通过分类技术标识此重要流量，然后实现缓冲区管理技术，以避免拥塞期间优先级较高的流量被丢弃。最后，您需要结合安排技术，尽快交换队列中的重要数据包。正如本文档所述，Catalyst 6000 系列可实现所有这些技术，这使得其 QoS 子系统成为如今业界最全面的子系统之一。

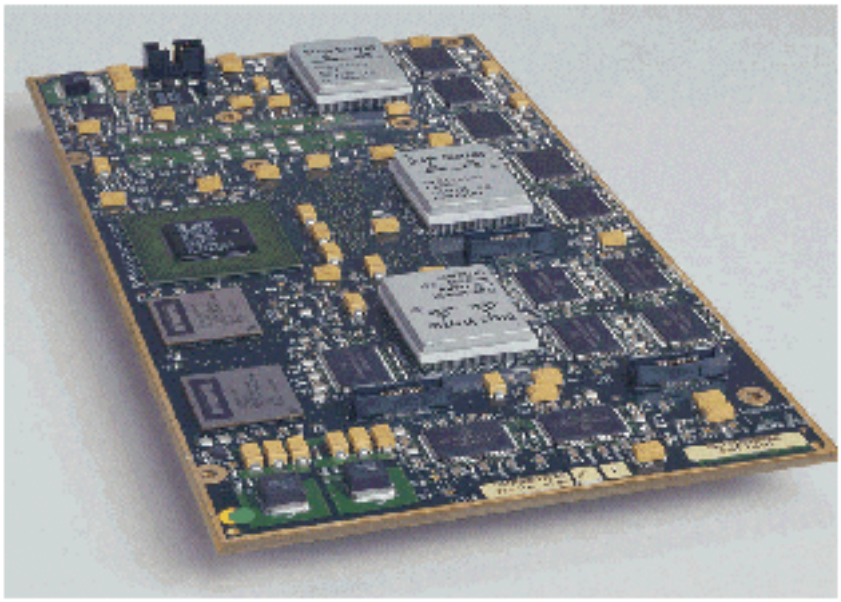
本文档将更详细地论述前面部分中介绍的所有 QoS 技术。

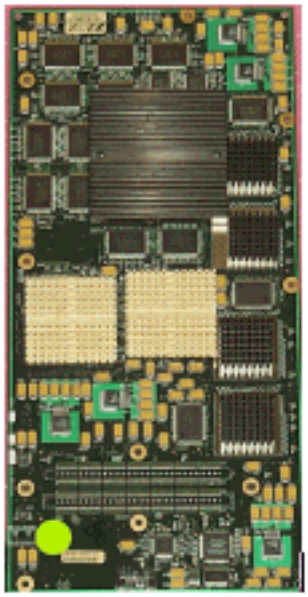
Catalyst 6000 系列中对 QoS 的硬件支持

要支持 Catalyst 6000 系列中的 QoS，需要提供一些硬件支持。支持QoS的硬件包括多层交换机特性卡(MSFC)、策略特性卡(PFC)和波尔特特殊用途的集成电路(ASIC)在线卡。本文档将不探讨 MSFC 的 QoS 功能，而是会重点关注板卡上的 PFC 和 ASIC 的 QoS 功能。

PFC

PFC 版本 1 是 Catalyst 6000 系列的 Supervisor I (SupI) 和 Supervisor IA (SupIA) 上的一个子卡。PFC2 是 PFC1 的重新开发，随新的 Supervisor II (SupII) 和一些新的板载 ASIC 一起提供。虽然 PFC1 和 PFC2 主要以其 L3 交换的硬件加速而闻名，但 QoS 是它们的另一个其他用途。PFC 如下所示：





虽然 PFC1 和 PFC2 基本上相同，但在 QoS 功能方面有一些差别。也就是说，PFC2 中增加了以下功能：

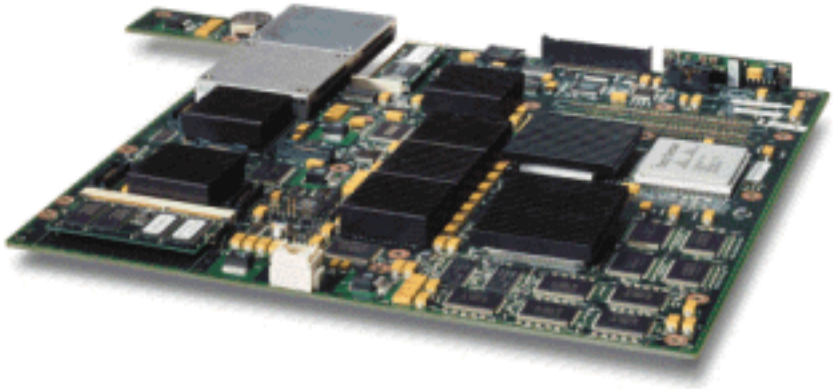
1. 能力增加QoS策略到分布式转发卡(DFC)。
2. 管制决策稍有不同。PFC1 和 PFC2 都支持正常管制，即，当聚合或微流策略返回超出配置规定决策时，就会将帧丢弃或降级。但是，PFC2 增加了对超额速率的支持；超额速率表示另一种管制级别，达到该级别时可以执行相应的策略操作。

定义了超额速率监察器时，如果数据包超过超额速率，就会将其丢弃或降级。如果设置了超额管制级别，将使用超额 DSCP 映射将原始 DSCP 值替换为降级后的值。如果只设置了正常管制级别，则会使用正常 DSCP 映射。如果同时设置了这两个管制级别，超额管制级别将可优先选择映射规则。

务必注意，本文档中介绍的由提及的 ASIC 执行的 QoS 功能会产生高级别性能。基本 Catalyst 6000 系列（没有交换矩阵模块）中的 QoS 性能产生 15 MPPS。如果使用 DFC，则 QoS 性能可以提高更多。

DFC

可以将 DFC 作为一个选件附加到 WS-X6516-GBIC。但是，在 WS-X6816-GBIC 卡上，DFC 是一个标准固定装置。DFC 在将来的其他结构板卡上也受支持，这些板卡包括最近推出的结构 10/100 (WS-X6548-RJ45) 板卡、结构 RJ21 板卡 (WS-X6548-RJ21) 和 100FX 板卡 (WS-X6524-MM-FX)。DFC 如下所示：



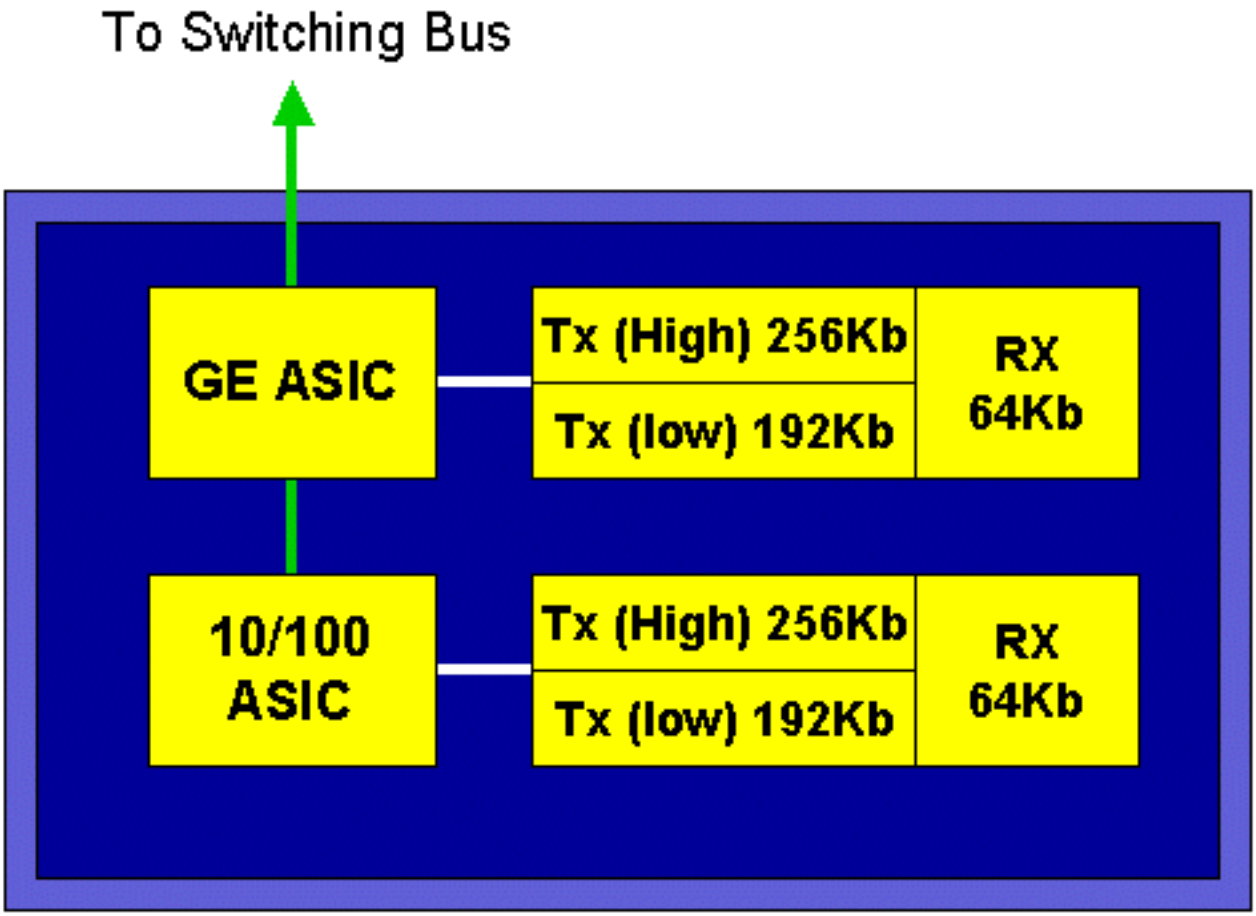
DFC 允许结构（交叉相连的）板卡执行本地交换。为此，它还必须支持对交换机定义的所有 QoS 策略。管理员不能直接配置 DFC；相反，DFC 受活动 Supervisor 上的主 MSFC/PFC 控制。主要的PFC将增加转发信息库(FIB)表，给DFC其L2和L3转发表。它还会下推 QoS 策略的副本，以便这些策略对板卡也是本地策略。接下来，本地交换决策可以参考任何 QoS 策略的本地副本，从而通过分布式交换提供硬件 QoS 处理速度并产生更高级别的性能。

基于端口的 ASIC

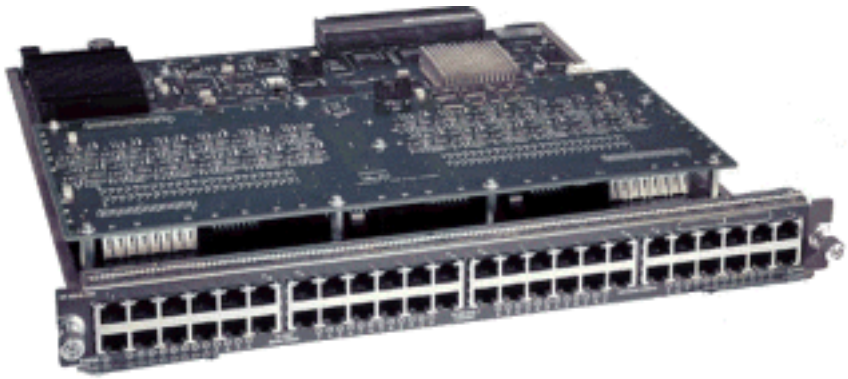
要完成硬件图片，每个板卡都需要实现一定数目的 ASIC。这些 ASIC 将实现用于在帧通过交换机时临时存储这些帧的队列、缓冲区和阈值。在 10/100 卡上，ASIC 的组合用于提供 48 个 10/100 端口。

原始 10/100 板卡 (WS-X6348-RJ45)

10/100 ASIC为每10/100端口提供一系列的接收(Rx)和Transmit(Tx)队列。ASIC 为每个 10/100 端口提供 128 K 缓冲区。有关每个板卡上的每个端口可用的缓冲区的详细信息，请参阅发行版注释。此板卡上的每个端口都支持一个 Rx 队列和两个 TX 队列（表示为高和低），如下图所示：



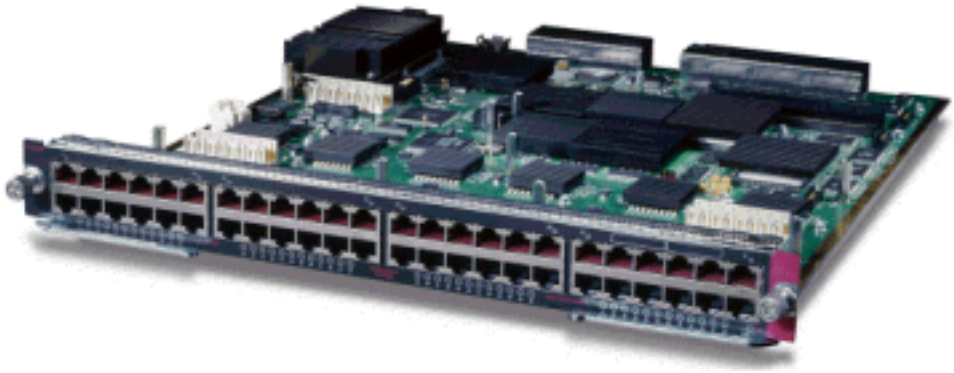
在上图中，每个 10/100 ASIC 为 12 个 10/100 端口提供一个分支点。对于每个 10/100 端口，提供 128 K 缓冲区。这 128 K 缓冲区在三个队列之间分配。但是，上面的队列中显示的数字不是默认值，它们表示可以配置的值。单个 Rx 队列获得 16 K，其余存储空间 (112 K) 在两个 Tx 队列之间分配。默认情况下（在 CatOS 中），高优先级队列获得此空间的 20%，低优先级队列获得 80%。在 Catalyst IOS 中，默认情况是为高优先级队列提供 10% 的空间，为低优先级队列提供 90% 的空间。



虽然该板卡提供两阶段缓冲，但在配置 QoS 期间，只能控制基于 10/100 ASIC 的缓冲。

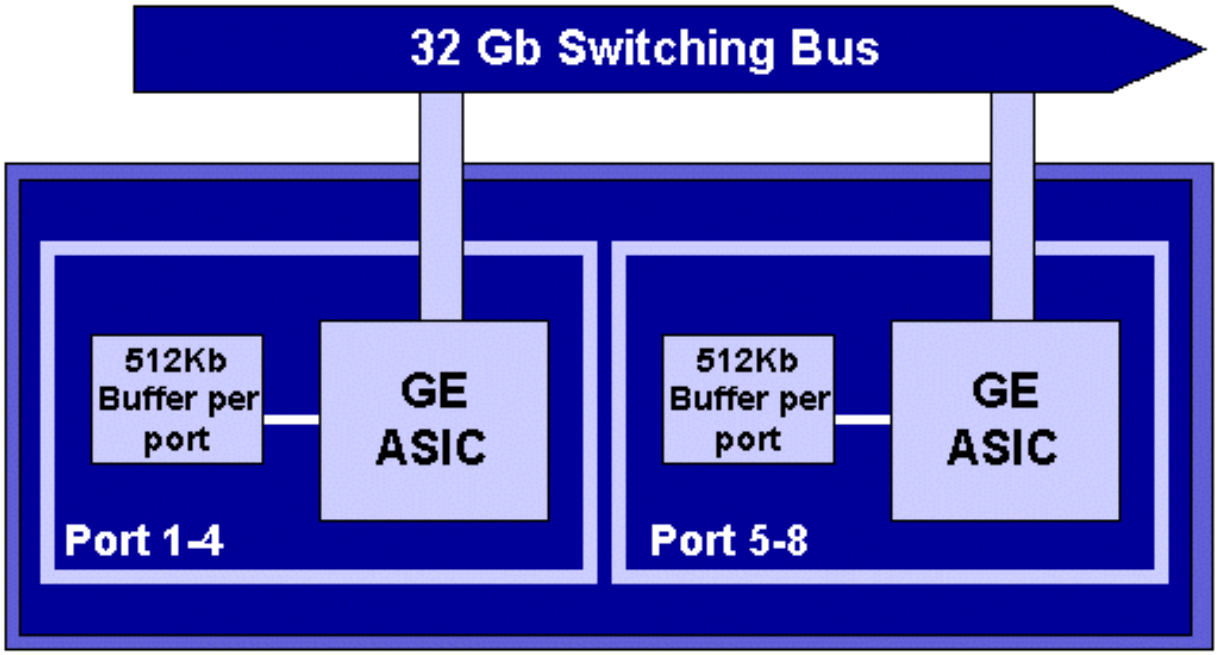
结构 10/100 板卡 (WS-X6548-RJ45)

新的 10/100 ASIC 为每个 10/100 端口提供一系列 Rx 和 TX 队列。ASIC 提供 10/100 端口可用的共享内存池。有关每个板卡上的每个端口可用的缓冲区的详细信息，请参阅发行版注释。此板卡上的每个端口都支持两个 Rx 队列和三个 TX 队列。一个 Rx 队列和一个 TX 队列均被表示为绝对优先级队列。此队列充当低延迟队列，适用于对延迟敏感的流量，如 IP 语音 (VoIP) 流量。

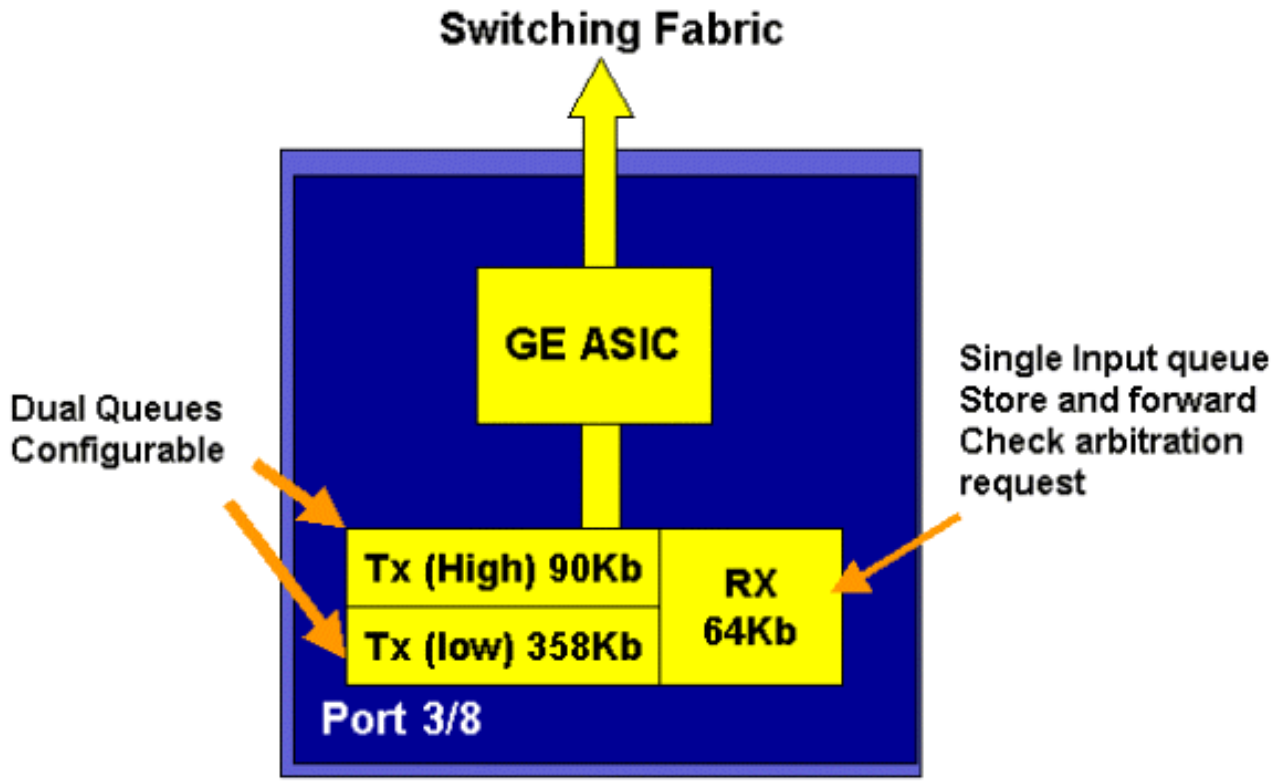


GE 板卡（WS-X6408A、WS-X6516 和 WS-X6816）

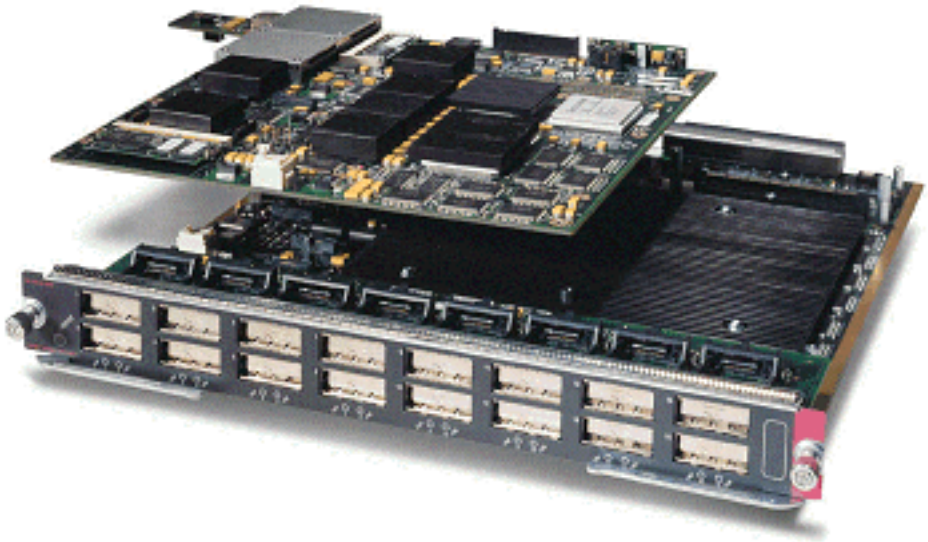
对于 GE 板卡，ASIC 为每个端口提供 512 K 缓冲区。下图显示了一个八端口 GE 板卡的表示。



与 10/100 端口一样，每个 GE 端口有三个队列：一个 Rx 队列和两个 TX 队列。下图显示的是 WS-X6408-GBIC 板卡上的默认值。

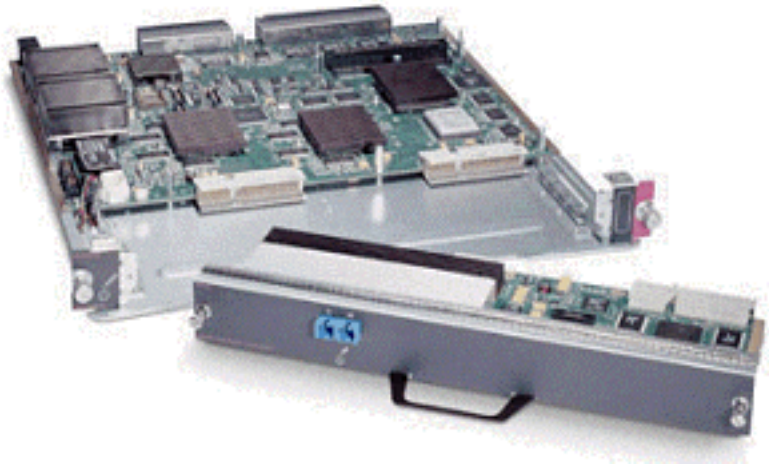


在更新的线路16端口GE卡，两个额外的严格优先级(SP)队列提供SupIA和SupII的GBIC端口和WS-X6408A-GBIC 8端口GE卡。一个 SP 队列被指定为 Rx 队列，而另一个 SP 队列被指定为 TX 队列。此 SP 队列主要用于对延迟敏感的流量（如语音）进行排队。对于 SP 队列，此队列中的所有数据将在高优先级队列和低优先级队列中的数据之前处理。仅当 SP 队列为空时，才会处理高优先级队列和低优先级队列。



10 GE 板卡 (WS-X6502-10GE)

在 2001 年下半年，Cisco 推出了一组 10 GE 板卡，每个板卡提供一个 10 GE 端口。此模块采用 6000 机箱中的一个插槽。10 GE 板卡支持 QoS。对于 10 GE 端口，它提供两个 Rx 队列和三个 TX 队列。一个 Rx 队列和一个 TX 队列均被指定为 SP 队列。同样为此端口提供了缓冲区，总共提供 256 K 的 Rx 缓冲区和 64 MB 的 TX 缓冲区。此端口对于 Rx 端实施 1p1q8t 队列结构，而对于 TX 端实施 1p2q1t 队列结构。本文档后面部分将对队列结构进行详细介绍。



Catalyst 6000 系列 QoS 硬件汇总

下表详细介绍了执行 Catalyst 6000 系列中的上述 QoS 功能的硬件组件。

QoS Process	Catalyst 6500 Component that performs function
Input Scheduling	Performed by port ASIC's L2 only with or without the PFC
Classification	Performed by Supervisor or PFC L2 only is done by Supervisor L2/3 is done by PFC
Policing	Done by PFC via L3 forwarding Engine
Packet Re-write	Done by port ASIC's L2/L3 based on classification done in point 2 above
Output Scheduling	Done by port ASIC's L2/L3 based on classification done in point 2 above

Catalyst 6000 系列软件对 QoS 的支持

Catalyst 6000 系列支持两种操作系统。原始软件平台 CatOS 是根据 Catalyst 5000 平台上使用的代码库创建的。最近，Cisco 推出了集成 Cisco IOS ®（本地模式）（以前称为 Native IOS），它使用源自 Cisco 路由器 IOS 的代码库。两OS平台(CatOS和集成Cisco IOS)实现软件支持启用在Catalyst 6000交换机系列平台的QoS使用在前面部分描述的硬件。

注意：本文档使用这两个 OS 平台的配置示例。

IP 和以太网中的优先级机制

对于要应用于数据的任何 QoS 服务，必须有一种方法标记 IP 数据包或以太网帧或者确定它们的优先级。ToS 和 CoS 字段就用于实现此目的。

Tos

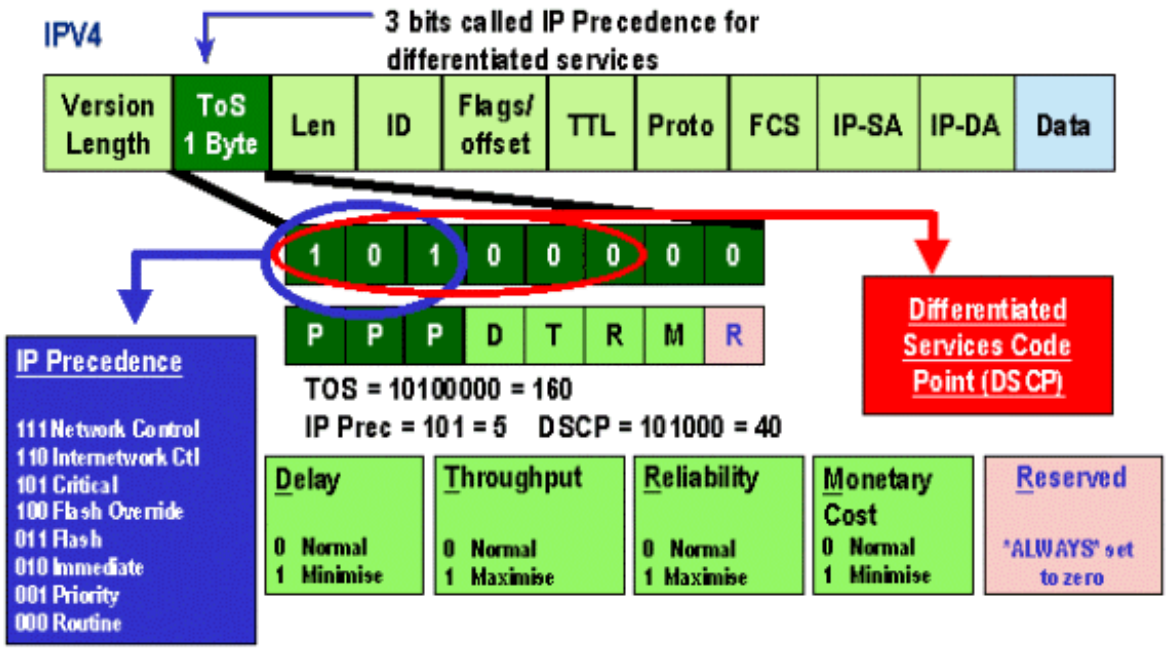
ToS 是 IPV4 报头中存在的一个 1 字节字段。ToS 字段包含 8 位，其中前 3 位用于指示 IP 数据包的优先级。这前 3 位称为 IP 优先级位。这些位可以设置为 0 到 7 之间的任意数字，其中 0 为最低

优先级，而 7 为最高优先级。许多年来 IOS 中一直支持设置 IP 优先级。MSFC 或 PFC（独立于 MSFC）可以实现对重置 IP 优先级的支持。如果信任设置为不信任，则也可以清除传入帧上的任何 IP 优先级设置。

可以设置的 IP 优先级值如下：

IP Precedence bits	IP Precedence Value
000	Routine
001	Priority
010	Intermediate
011	Flash
100	Flash Override
101	Critical
110	Internetwork Control
111	Network Control

下图是 ToS 报头中 IP 优先级位的表示。三最重要的位(MSB)解释作为IP优先级位。



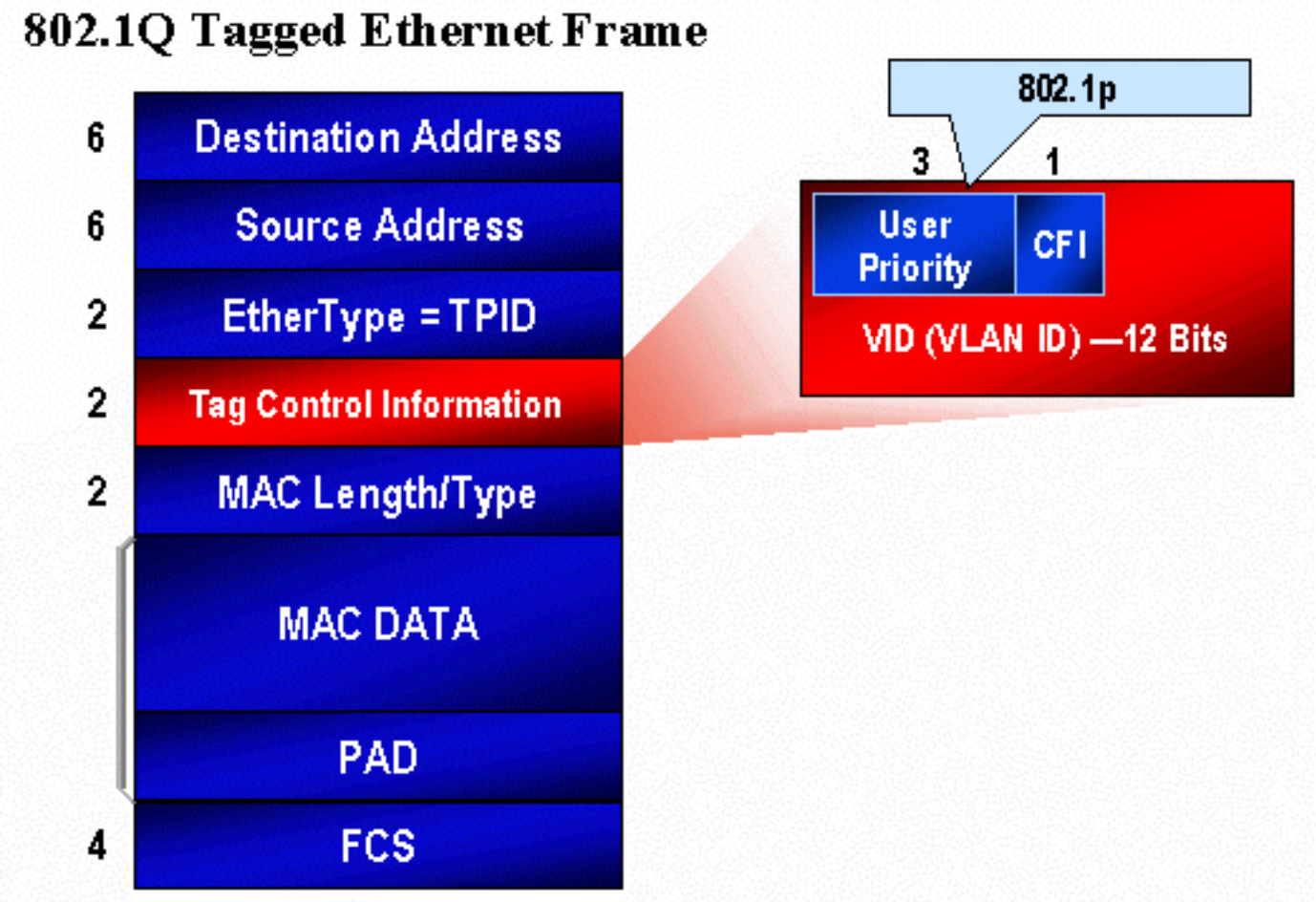
最近，ToS 字段的使用已扩展为包括 6 个 MSB，称为 DSCP。DSCP 导致可以将 64 个优先级值（2 的 6 次方）指定给 IP 数据包。

Catalyst 6000 系列可以处理 ToS。这可以通过使用 PFC 和/或 MSFC 来实现。当帧进入交换机时，将为它指定一个 DSCP 值。此 DSCP 值在交换机内部用于指定管理员定义的服务级别（QoS 策略）。DSCP 可以已存在于帧中并可以使用，或者可以根据帧中的现有 CoS、IP 优先级或 DSCP 来生成 DSCP（如果端口受信任）。交换机内部使用映射来生成 DSCP。对于 8 个可能的 CoS/IP 优先级值和 64 个可能的 DSCP 值，默认映射会将 CoS/IPPrec 0 映射到 DSCP 0、将 CoS/IPPrec 1 映射到 DSCP 7，将 CoS/IPPrec 2 映射到 DSCP 15，依此类推。管理员可以覆盖这些默认映射。当帧被安排到出站端口时，可以重写 CoS 并使用 DSCP 值来生成新的 CoS。

Cos

CoS 指的是 ISL 报头或 802.1Q 报头中的三位，用于指示通过交换网络的以太网帧的优先级。出于本文档的目的，我们只涉及使用 802.1Q 报头。802.1Q 报头中的 CoS 位通常称为 802.1p 位。毫不奇怪，有三个 CoS 位，这与用于 IP 优先级的位数匹配。在许多网络中，为了端到端地维持 QoS，数据包可以通过 L2 和 L3 域。为了维持 QoS，可以将 ToS 映射到 CoS，并可以将 CoS 映射到 ToS。

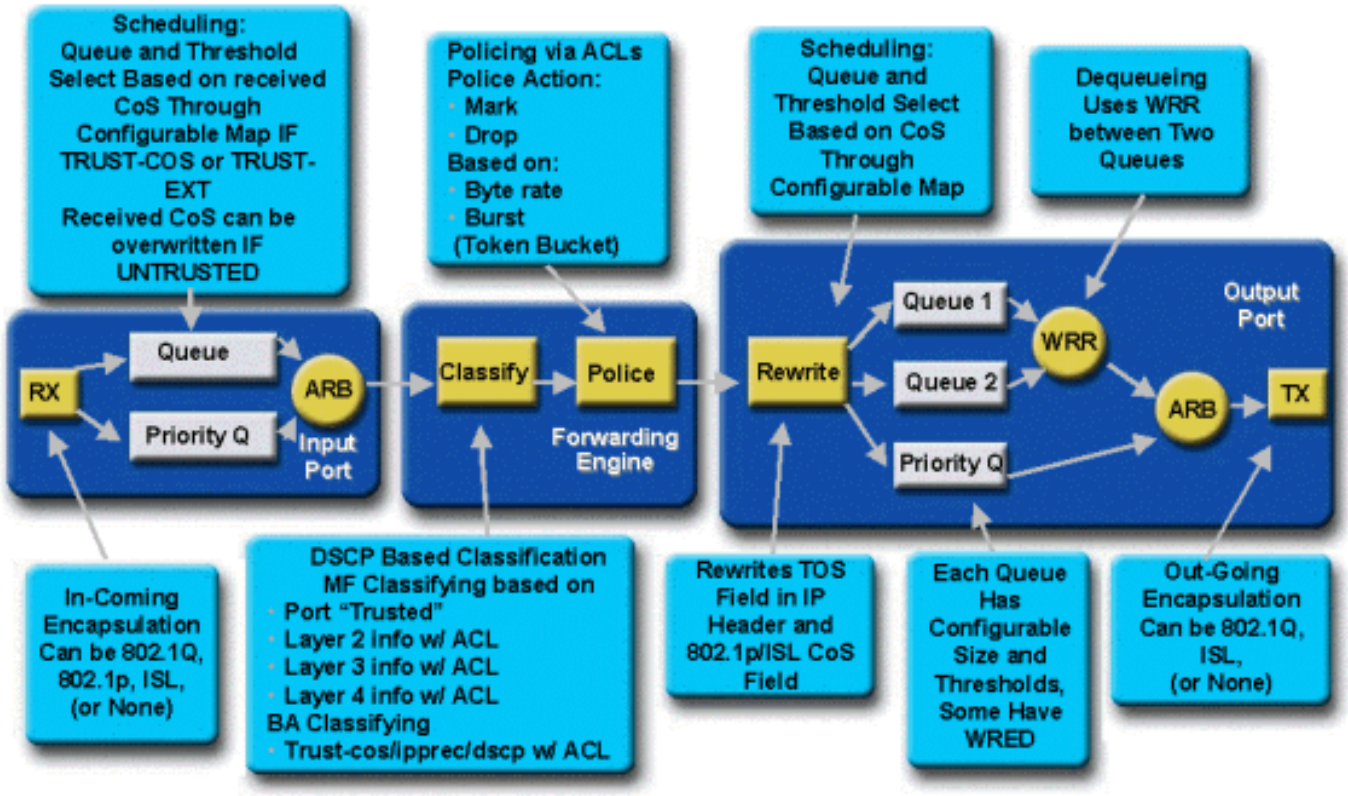
下图是一个使用 802.1Q 字段标记的以太网帧，该帧包含一个 2 字节以太网类型和一个 2 字节标记。该 2 字节标记中是用户优先级位（称为 802.1p）。



Catalyst 6000 系列中的 QoS 流

Catalyst 6000 系列中的 QoS 是当前所有 Cisco Catalyst 交换机中最全面的 QoS 实施。下面各部分介绍如何将各种 QoS 过程应用于通过交换机的帧。

在本文档的前面部分中，已说明许多 L2 和 L3 交换机可以提供一些 QoS 元素。这些元素为分类、输入队列安排、管制、重写和输出队列安排。与 Catalyst 6000 系列的不同之处在于这些 QoS 元素由深入了解 L3 和 L4 详细信息以及只了解 L2 报头信息的 L2 引擎应用。下图总结了 Catalyst 6000 系列如何实现这些元素。



当帧进入交换机时，最初由接收帧的端口 ASIC 处理。端口 ASIC 将帧放入 Rx 队列中。将有一个或两个 Rx 队列，这取决于 Catalyst 6000 系列板卡。

端口 ASIC 将使用 CoS 位作为指示符，确定要将帧放入的队列（如果有多个输入队列）。如果端口被分类为不信任，则端口 ASIC 可以根据预定义的值覆盖现有 CoS 位。

然后，帧被传递给 L2/L3 转发引擎 (PFC)，PFC 将对帧进行分类并可选择进行管制（速率限制）。分类是为帧指定 DSCP 值的过程，该值由交换机内部用于处理帧。将根据以下任一值生成 DSCP：

1. 在帧进入交换机之前设置的现有 DSCP 值
2. IPV4 报头中已设置的接收到的 IP 优先级位。由于有 64 个 DSCP 值，但只有 8 个 IP 优先级值，因此管理员将配置交换机用来生成 DSCP 的映射。如果管理员不配置映射，则默认映射必须已存在。
3. 在帧进入交换机之前已设置的接收到的 CoS 位。与 IP 优先级类似，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存在的默认映射。
4. 为帧设置通过使用DSCP默认值虽则典型地分配访问控制表(ACL)条目。

为帧指定 DSCP 值后，如果存在管制配置，则会应用管制（速率限制）。管制会通过丢弃或降级超出配置规定的流量，限制通过 PFC 的数据流。超出配置规定是一个术语，用于指示流量超过了管理员定义为 PFC 每秒将发送的位数的限制。超出配置规定的流量可能被丢弃，或者 CoS 值可能降级。PFC1 和 PFC2 当前只支持输入管制（速率限制）。发布新 PFC 时将提供对输入和输出管制的支持。

然后，PFC 将帧传递给输出端口进行处理。此时，将调用重写过程修改帧中的 CoS 值以及 IPV4 报头中的 ToS 值。这是根据内部 DSCP 生成的。然后，根据帧的 CoS 值将帧放入传输队列中，准备进行传输。当帧位于队列中时，端口 ASIC 将监视缓冲区并实施 WRED 以避免缓冲区溢出。然后，使用 WRR 安排算法来安排并通过输出端口传输帧。

下面每部分将更详细地探讨此流程，并提供上面介绍的每个步骤的配置示例。

队列、缓冲区、阈值和映射

在详细介绍 QoS 配置之前，必须进一步解释一些术语，以确保您真正了解交换机的 QoS 配置功能。

队列

交换机上的每个端口都有一系列输入和输出队列，用作数据的临时存储区域。Catalyst 6000 系列板卡对每个端口实现不同数目的队列。通常在硬件 ASIC 中实现每个端口的队列。在第一代 Catalyst 6000 系列板卡上，典型配置为一个输入队列和两个输出队列。在较新的板卡（10/100 和 GE）上，ASIC 实现一组额外的队列（共两个队列，一个输入队列和一个输出队列），从而导致两个输入队列和三个输出队列。这两个额外的队列是特殊的 SP 队列，用于对延迟敏感的流量（如 VoIP）。它们将以 SP 方式处理。也就是说，如果帧到达 SP 队列，将停止安排优先级较低的队列中的帧，以处理 SP 队列中的帧。仅当 SP 队列为空时，才会重新开始安排优先级较低的队列中的数据包。

如果在拥塞时帧到达某个端口（用于输入或输出），则该帧将被放入队列中。通常根据传入帧的以太网报头中的 CoS 值决定将帧放入哪个队列中。

输出时，将使用安排算法清空 TX（输出）队列。WRR 就是可实现此目的的一种算法。对于每个队列，权重用于指示在移到下一个队列之前将从当前队列中清空多少数据。管理员指定的权重是 1 到 255 之间的一个数字，将为每个 TX 队列都指定权重。

缓冲区

每个队列都分配有一定数量的缓冲区空间，用于存储传输数据。端口 ASIC 上的缓冲区空间是内存，它按每个端口进行划分和分配。对于每个 GE 端口，GE ASIC 分配 512 K 缓冲区空间。对于 10/100 端口，端口 ASIC 为每个端口保留 64 K 或 128 K（取决于板卡）缓冲区空间。然后，此缓冲区空间将在 Rx（输入）队列和 TX（输出）队列之间分配。

阈值

正常数据传输的一个方面是，如果一个数据包被丢弃，则会导致重新传输该数据包（TCP 流）。出现拥塞时，这可能会增加网络负载，并可能导致缓冲区溢出更多。作为一种确保缓冲区不溢出的方法，Catalyst 6000 系列交换机使用许多技术来避免缓冲区溢出。

阈值是交换机（或管理员)指定的定义利用率点的虚假级别，到达这些点时，拥塞管理算法将开始丢弃队列中的数据。在 Catalyst 6000 系列端口上，通常有 4 个与输入队列关联的阈值。通常有 2 个与输出队列关联的阈值。

这些阈值也部署在 QoS 的上下文中，作为将具有不同优先级的帧指定给这些阈值的方法。当缓冲区开始变满并且超过阈值时，管理员可以将不同的优先级映射到不同的阈值，以指示交换机在超过阈值时应丢弃哪些帧。

映射

在上面的队列和阈值部分中，已说明以太网帧中的 CoS 值用于确定要将帧放入的队列，以及确定当缓冲区的剩余空间为多少时就可以丢弃帧。这就是映射的目的。

在 Catalyst 6000 系列上配置 QoS 时，会启用默认映射，默认映射定义以下内容：

- 达到哪些阈值就可以丢弃具有特定 CoS 值的帧
- 将帧放入的队列（根据其 CoS 值）

虽然存在默认映射，但管理员可以覆盖这些默认映射。以下项之间存在映射：

- 传入帧中的 CoS 值到 DSCP 值

- 传入帧中的 IP 优先级值到 DSCP 值
- DSCP 值到传出帧中的 CoS 值
- CoS 值到接收队列中的丢弃阈值
- CoS 值到传输队列中的丢弃阈值
- 超出管制声明的帧中的 DSCP 降级值
- CoS 值到具有特定目标 MAC 地址的帧

WRED 和 WRR

WRED 和 WRR 是 Catalyst 6000 系列上功能非常强大的两种算法。WRED 和 WRR 都使用以太网帧中的优先级标记 (CoS) 来提供增强的缓冲区管理和出站安排。B

WRED

WRED 是一种缓冲区管理算法，Catalyst 6000 系列使用它使拥塞时丢弃高优先级流量所产生的影响降到最小。WRED 基于 RED 算法。

要了解 RED 和 WRED，请重新访问 TCP 流管理的概念。流管理确保 TCP 发送方不会使网络过载。TCP 慢启动算法是解决此问题的解决方案的一部分。它规定当流开始时，将发送一个数据包，然后等待确认。然后，在收到 ACK 之前发送两个数据包，并逐渐增加收到每个 ACK 之前发送的数据包数目。这种情况将持续到流达到网络可以处理且负载不会导致拥塞的传输级别（即，发送 *x* 个数据包）为止。如果出现拥塞，慢启动算法将减小窗口大小（即，等待确认前发送的数据包的数目），从而降低该 TCP 会话（流）的整体性能。

当队列开始变满时，RED 就会监视该队列。一旦超过某个阈值，就会开始随机丢弃数据包。不会考虑特定流；而是丢弃任意的数据包。这些数据包可能来自高优先级流或低优先级流。丢弃的数据包可能属于单个流或多个 TCP 流。如果如上所述有多个流受到影响，这将会对每个流窗口大小产生很大影响。

与 RED 不同，WRED 不随机丢弃帧。WRED 会考虑帧的优先级（对于 Catalyst 6000 系列，WRED 使用 CoS 值）。对于 WRED，管理员会将包含某些 CoS 值的帧指定给特定阈值。一旦超过这些阈值，就可以丢弃其 CoS 值映射到这些阈值的帧。CoS 值指定给较大阈值的其他帧将保留在队列中。此过程允许较高优先级的流保持完整，这使得其较大的窗口大小保持完整，并使从发送方到接收方获得数据包过程中涉及的延迟最小。

如何知道板卡是否支持 WRED？可以发出以下命令。然后，检查输出中是否存在表明该端口支持 WRED 的部分。

```
Console> show qos info config 2/1
QoS setting in NVRAM:
QoS is enabled
Port 2/1 has 2 transmit queue with 2 drop thresholds (2q2t).
Port 2/1 has 1 receive queue with 4 drop thresholds (1q4t).
Interface type:vlan-based
ACL attached:
The qos trust type is set to untrusted.
```

```
Default CoS = 0
Queue and Threshold Mapping:
Queue Threshold CoS
----- --------- ---------------
1     1         0 1
1     2         2 3
2     1         4 5
2     2         6 7
Rx drop thresholds:
Rx drop thresholds are disabled for untrusted ports.
Queue #  Thresholds - percentage (abs values)
-------  ---------------------------------
1        50% 60% 80% 100%
TX drop thresholds:
Queue #  Thresholds - percentage (abs values)
-------  ---------------------------------
1        40% 100%
2        40% 100%
TX WRED thresholds:
WRED feature is not supported for this port_type.
!-- Look for this. Queue Sizes: Queue # Sizes - percentage (abs values) ------- ----------------
--------------------- 1 80% 2 20% WRR Configuration of ports with speed 1000MBPS: Queue # Ratios
(abs values) ------- ---------------------------------- 1 100 2 255 Console> (enable)
```

如果某个端口上不能使用 WRED，该端口将使用尾部丢弃缓冲区管理方法。顾名思义，尾部丢弃是指当缓冲区被充分利用时就丢弃传入的帧。

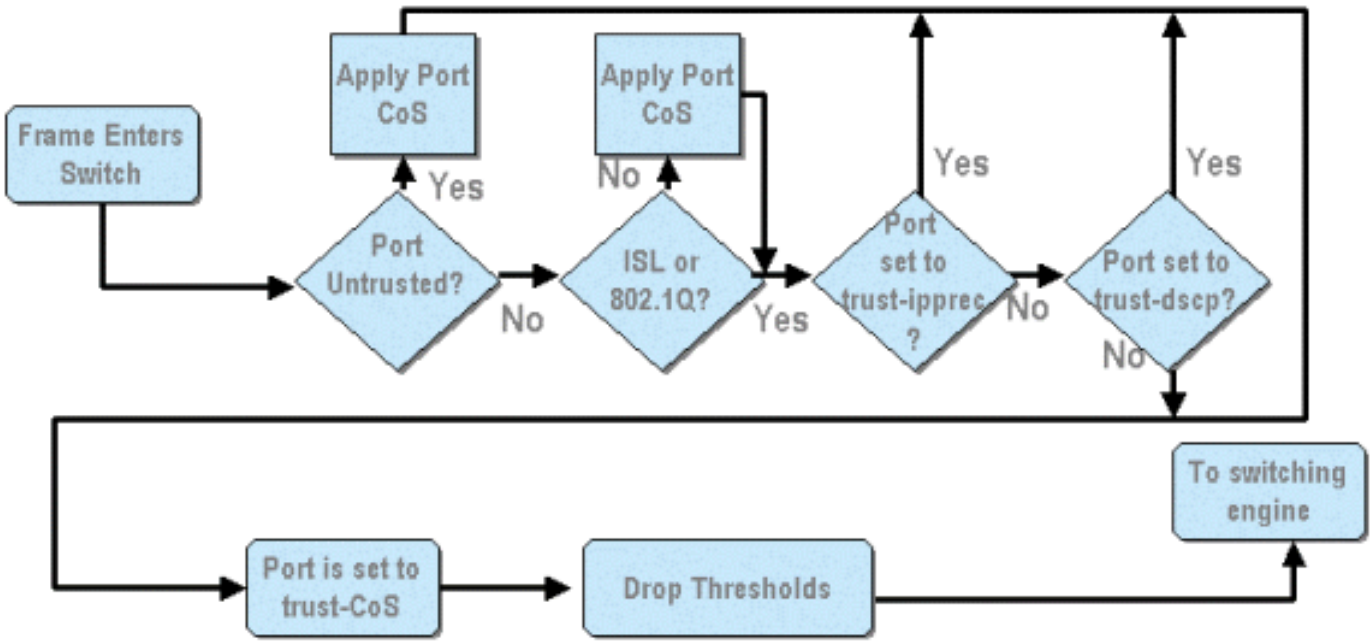
WRR

WRR 用于安排 TX 队列中的输出流量。普通的循环算法将在 TX 队列之间切换，并且在移到下一个队列之前，发送每个队列中相同数目的数据包。WRR 的加权特性允许安排算法检查分配给队列的权重。这样就允许规定的队列使用更多带宽。WRR 安排算法从标识的队列中清空的数据要多于从其他队列中清空的数据，这就对指定队列产生偏见。

下面部分中将解释 WRR 的配置以及上面所介绍的内容的其他方面。

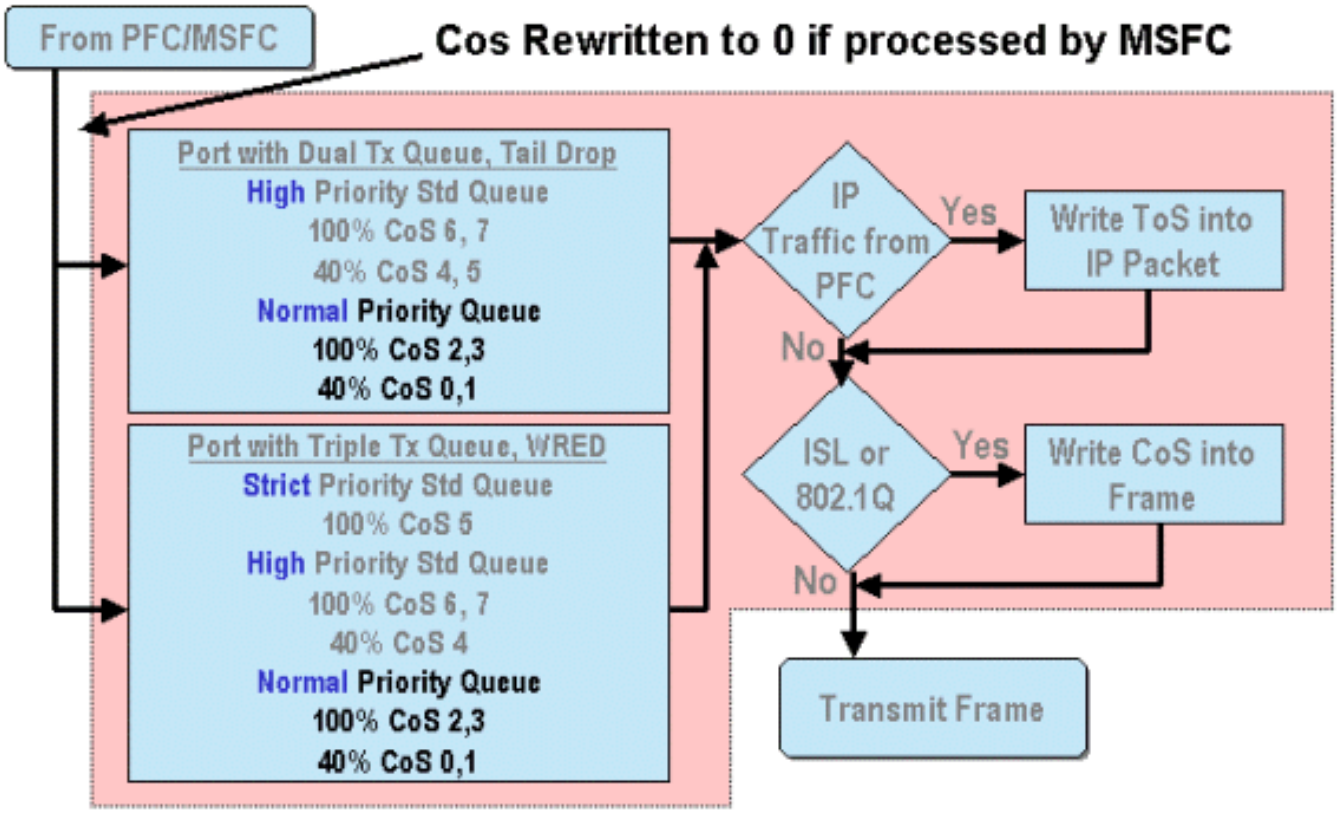
在 Catalyst 6000 系列上配置基于 QoS 的端口 ASIC

QoS 配置指示端口 ASIC 或 PFC 执行 QoS 操作。下面部分将说明这两个过程的 QoS 配置。在端口 ASIC 上，QoS 配置同时影响入站和出站数据流。



从上图中，我们可以看到以下 QoS 配置过程适用：

1. 端口的信任状态
2. 应用基于端口的 CoS
3. Rx 丢弃阈值指定
4 CoS 到 Rx 丢弃阈值映射



当帧由 MSFC 或 PFC 处理时，它将被传递到出站端口 ASIC 以进行进一步处理。MSFC 处理的任何帧的 CoS 值都会重置为零。对于出站端口上的 QoS 处理，需要考虑到这一点。

上图显示端口 ASIC 对出站流量执行的 QoS 处理。进行出站 QoS 处理时调用的一些过程包括：

1. TX 尾部丢弃和 WRED 阈值指定

2. CoS 到 TX 尾部丢弃和 WRED 映射

此外，上图中未显示使用 DSCP 到 CoS 映射将 CoS 重新指定给出站帧的过程。

下面部分更详细地说明了基于端口的 ASIC 的 QoS 配置功能。

注意：需要注意的一个要点是，当使用 CatOS 调用 QoS 命令时，这些命令通常应用于具有指定队列类型的所有端口。例如，如果将 WRED 丢弃阈值应用于队列类型为 1p2q2t 的端口，则此 WRED 丢弃阈值将应用于支持此队列类型的所有板卡上的所有端口。使用 Cat IOS 时，通常在接口级别应用 QoS 命令。

启用 QoS

在 Catalyst 6000 系列上进行任何 QOS 配置之前，必须首先在交换机上启用 QoS。可发出以下命令来启用 QoS：

CatOS

```
Console> (enable) set qos enable
!-- QoS is enabled. Console> (enable)
```

集成 Cisco IOS（本地模式）

```
Cat6500(config)# mls qos
```

在 Catalyst 6000 系列中启用 QoS 后，交换机将设置一系列的 QoS 默认值。这些默认值包括以下设置：

QoS Feature	Default setting
Trust state of each port	Un-trusted
Receive Queue drop threshold percentages	Threshold 1 – 50% Threshold 2 – 60% Threshold 3 – 80% Threshold 4 – 100%
Transmit Queue drop threshold percentages	Low priority queue threshold 1 – 80% Low priority queue threshold 2 – 100% High priority queue threshold 1 – 80% High priority queue threshold 2 – 100%
CoS value to Drop threshold mapping	Receive queue 1/drop threshold 1: CoS 0 and 1 Transmit queue 1/drop threshold 1: CoS 0 and 1 Receive queue 1/drop threshold 2: CoS 2 and 3 Transmit queue 1/drop threshold 2: CoS 2 and 3 Receive queue 1/drop threshold 3: CoS 4 and 5 Transmit queue 2/drop threshold 1: CoS 4 and 5 Receive queue 1/drop threshold 4: CoS 6 and 7

	Transmit queue 2/drop threshold 2: CoS 6 and 7
CoS to DSCP Mapping (DSCP set from CoS value)	CoS 0 = DSCP 0 CoS 1 = DSCP 8 CoS 2 = DSCP 16 CoS 3 = DSCP 24 CoS 4 = DSCP 32 CoS 5 = DSCP 40 CoS 6 = DSCP 48 CoS 7 = DSCP 56
IP Precedence to DSCP Map (DSCP set from IP Precedence value)	IP precedence 0 = DSCP 0 IP precedence 1 = DSCP 8 IP precedence 2 = DSCP 16 IP precedence 3 = DSCP 24 IP precedence 4 = DSCP 32 IP precedence 5 = DSCP 40 IP precedence 6 = DSCP 48 IP precedence 7 = DSCP 56
DSCP to CoS map (CoS set from DSCP values)	DSCP 0-7 = CoS 0 DSCP 8-15 = CoS 1 DSCP 16-23 = CoS 2 DSCP 24-31 = CoS 3 DSCP 32-39 = CoS 4 DSCP 40-47 = CoS 5 DSCP 48-55 = CoS 6 DSCP 56-63 = CoS 7

信任和不信任的端口

可以将 Catalyst 6000 系列上的任何给定端口配置为信任或不信任。端口的信任状态规定当帧通过交换机时如何标记、分类和安排帧。默认情况下，所有端口都处于不信任状态。

不信任的端口（端口的默认设置）

如果端口配置为不信任的端口，则端口 ASIC 会将最初进入该端口的帧的 CoS 和 ToS 值重置为零。这意味着该帧在其通过交换机的路径上被给予最低优先级的服务。

或者，管理员可以将进入不信任端口的任何以太网帧的 CoS 值重置为预先确定的值。此配置将在后面部分中讨论。

将端口设置为不信任将指示交换机不执行任何拥塞避免。拥塞避免是用于在帧的 CoS 值超过为该队列定义的阈值时根据其 CoS 值丢弃帧的方法。一旦缓冲区达到 100%，进入此端口的所有帧被丢弃的机会都相同。

在 CatOS 中，可发出以下命令将 10/100 或 GE 端口配置为不信任：

CatOS

```
Console> (enable) set port qos 3/16 trust untrusted
!-- Port 3/16 qos set to untrusted. Console> (enable)
```

此命令将模块 3 上的端口 16 设置为不信任状态。

注意：对于集成 Cisco IOS（本地模式），软件当前只支持将 GE 端口设置为信任状态。

集成 Cisco IOS（本地模式）

```
Cat6500(config)# interface gigabitethernet 1/1
Cat6500(config-if)# no mls qos trust
```

在上面的示例中，由于是 IOS，因此输入了接口配置并应用 **no** 形式的命令将端口设置为不信任。

信任的端口

有时，对于进入交换机且具有 CoS 或 ToS 设置的以太网帧，管理员会希望交换机在该帧通过交换机时保持其设置。对于此流量，管理员可以将该流量通过其进入交换机的端口的信任状态设置为信任。

如前面所述，交换机内部使用 DSCP 值将预先确定的服务级别指定给该帧。当帧进入信任端口时，管理员可以配置该端口以查看现有 CoS、IP 优先级或 DSCP 值来设置内部 DSCP 值。或者，管理员可以对进入该端口的每个数据包设置预定义的 DSCP。

可发出以下命令将端口的信任状态设置为信任：

CatOS

```
Console> (enable) set port qos 3/16 trust trust-cos
!-- Port 3/16 qos set to trust-COs Console> (enable)
```

此命令适用于 WS-X6548-RJ45 板卡，它将端口 3/16 的信任状态设置为信任。交换机将使用传入帧中设置的 CoS 值来设置内部 DSCP。可以根据交换机上启用 QoS 时创建的默认映射生成 DSCP，也可以根据管理员定义的映射生成 DSCP。管理员也可以使用 trust-dscp 或 trust-ipprec 关键字来代替 trust-COs 关键字。

在以前的 10/100 板卡（WS-X6348-RJ45 和 WS-X6248-RJ45）上，需要发出 **set qos acl** 命令来设置端口信任。在此命令中，可以由 **set qos acl** 命令的一个子参数指定信任状态。不支持在这些板卡的端口上设置信任 CoS，如下图所示：

```
Console> (enable) set port qos 4/1 trust trust-COs
Trust type trust-COs not supported on this port.
!-- Trust-COs not supported, use acl instead. Rx thresholds are enabled on port 4/1. !-- Need to
turn on input queue scheduling. Port 4/1 qos set to untrusted. !-- Trust-COs not supported, so
port is set to untrusted.
```

上面的命令说明需要启用输入队列安排。因此，对于 WS-X6248-RJ45 和 WS-X6348-RJ45 板卡上的 10/100 端口，虽然设置信任状态必须使用 ACL，但仍必须配置 **set port qos x/y trust trust-COs** 命令。

对于集成 Cisco IOS（本地模式），可以在新的 WS-X6548-RJ45 板卡上的 GE 接口和 10/100 端口上执行信任设置。

集成 Cisco IOS（本地模式）

```
Cat6500(config)# interface gigabitethernet 5/4
Cat6500(config-if)# mls qos trust ip-precedence
Cat6500(config-if)#
```

本示例将 GE 端口 5/4 的信任状态设置为信任。帧的 IP 优先级值将用于生成 DSCP 值。

输入分类和设置基于端口的 CoS

在以太网帧进入交换机端口时，如果符合以下两个条件之一，则可以更改以太网帧的 CoS：

1. 端口被配置为不信任，或者
2. 以太网帧尚未设置现有 CoS 值

如果您要重新配置传入以太网帧的 CoS，则应该发出以下命令：

CatOS

```
Console> (enable) set port qos 3/16 cos 3
!-- Port 3/16 qos set to 3. Console> (enable)
```

当未标记的帧到达时，或者端口被设置为不信任时，此命令将进入模块 3 上端口 16 的以太网帧的 CoS 设置为值 3。

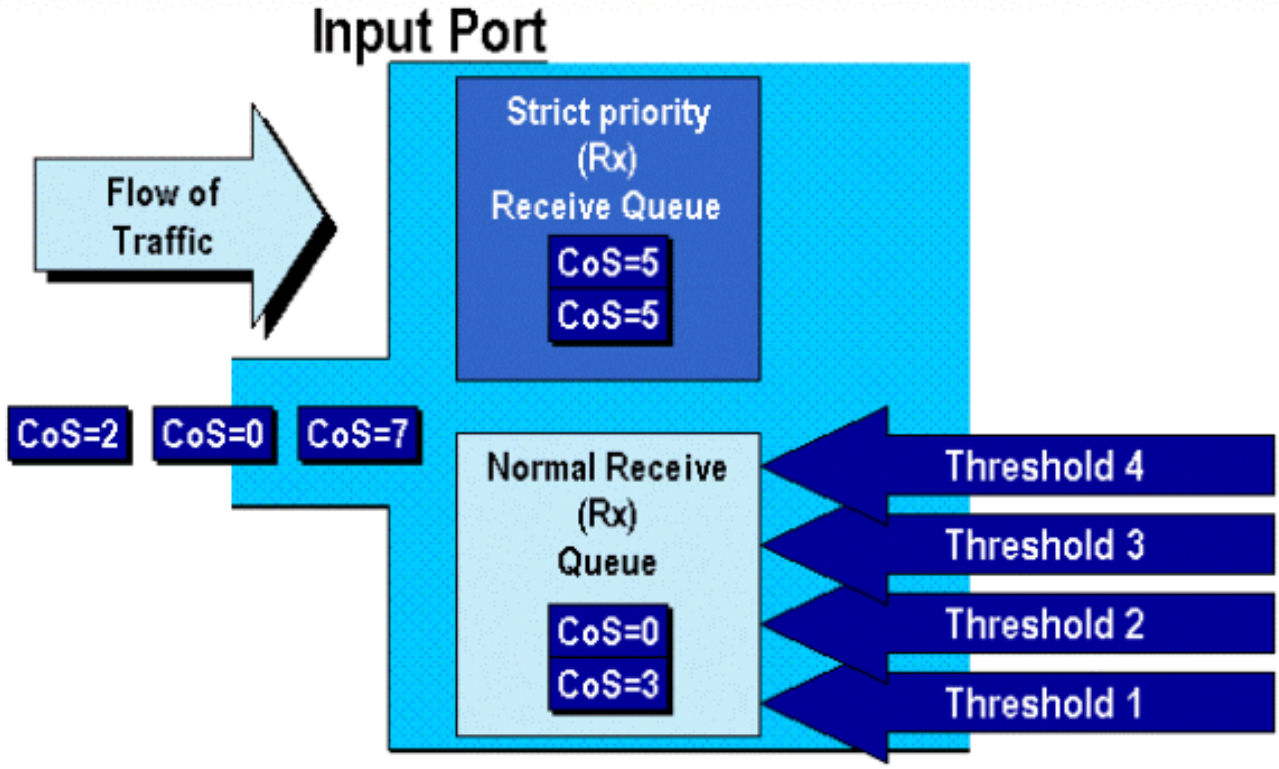
集成 Cisco IOS（本地模式）

```
Cat6500(config)# interface fastethernet 5/13
Cat6500(config-if)# mls qos COs 4
Cat6500(config-if)#
```

当未标记的帧到达时，或者端口被设置为不信任时，此命令将进入模块 5 上端口 13 的以太网帧的 CoS 设置为值 4。

配置 Rx 丢弃阈值

在帧进入交换机端口时，帧将被放入 Rx 队列中。为了避免缓冲区溢出，端口 ASIC 在每个 Rx 队列上设置 4 个阈值，并在超过这些阈值时使用它们来标识可以丢弃的帧。在超过阈值时，端口 ASIC 将使用帧设置的 CoS 值来标识可以丢弃的帧。当出现拥塞时，此功能允许具有较高优先级的帧在缓冲区中保留更长时间。



如上图所示，帧到达并被放入队列中。当队列开始变满时，端口 ASIC 将监视阈值。超过阈值后，将随机丢弃队列中具有管理员所标识的 CoS 值的帧。1q4t 队列（位于 WS-X6248-RJ45 和 WS-X6348-RJ45 板卡上）的默认阈值映射如下所示：

- 阈值 1 设置为 50%，且 CoS 值 0 和 1 映射到此阈值
- 阈值 2 设置为 60%，且 CoS 值 2 和 3 映射到此阈值
- 阈值 3 设置为 80%，且 CoS 值 4 和 5 映射到此阈值
- 阈值 4 设置为 100%，且 CoS 值 6 和 7 映射到此阈值

对于 1P1q4t（位于 GE 端口上）队列，默认映射如下所示：

- 阈值 1 设置为 50%，且 CoS 值 0 和 1 映射到此阈值
- 阈值 2 设置为 60%，且 CoS 值 2 和 3 映射到此阈值
- 阈值 3 设置为 80%，且 CoS 值 4 映射到此阈值
- 阈值 4 设置为 100%，且 CoS 值 6 和 7 映射到此阈值
- CoS 值 5 映射到严格优先级队列

对于 1p1q0t（位于 WS-X6548-RJ45 板卡的 10/100 端口上），默认映射如下所示：

- CoS 值为 5 的帧进入 SP Rx 队列（队列 2），其中只有当 SP 接收队列缓冲区达到 100% 满时，交换机才会丢弃传入的帧。
- CoS 值为 0、1、2、3、4、6 或 7 的帧进入标准 Rx 队列。当 Rx 队列缓冲区达到 100% 满时，交换机就丢弃传入的帧。

管理员可以更改这些丢弃阈值。此外，还可以更改映射到每个阈值的默认 CoS 值。不同的板卡实现不同的 Rx 队列实施。队列类型的汇总如下所示。

CatOS

```
Console> (enable) set qos drop-threshold 1q4t rx queue 1 20 40 75 100
!-- Rx drop thresholds for queue 1 set at 20%, 40%, 75%, and 100%. Console> (enable)
```

此命令将具有 1 个队列和 4 个阈值（表示为 1q4t）的所有输入端口的接收丢弃阈值设置为 20%、40%、75% 和 100%。

集成 Cisco IOS（本地模式）中发出的命令如下所示。

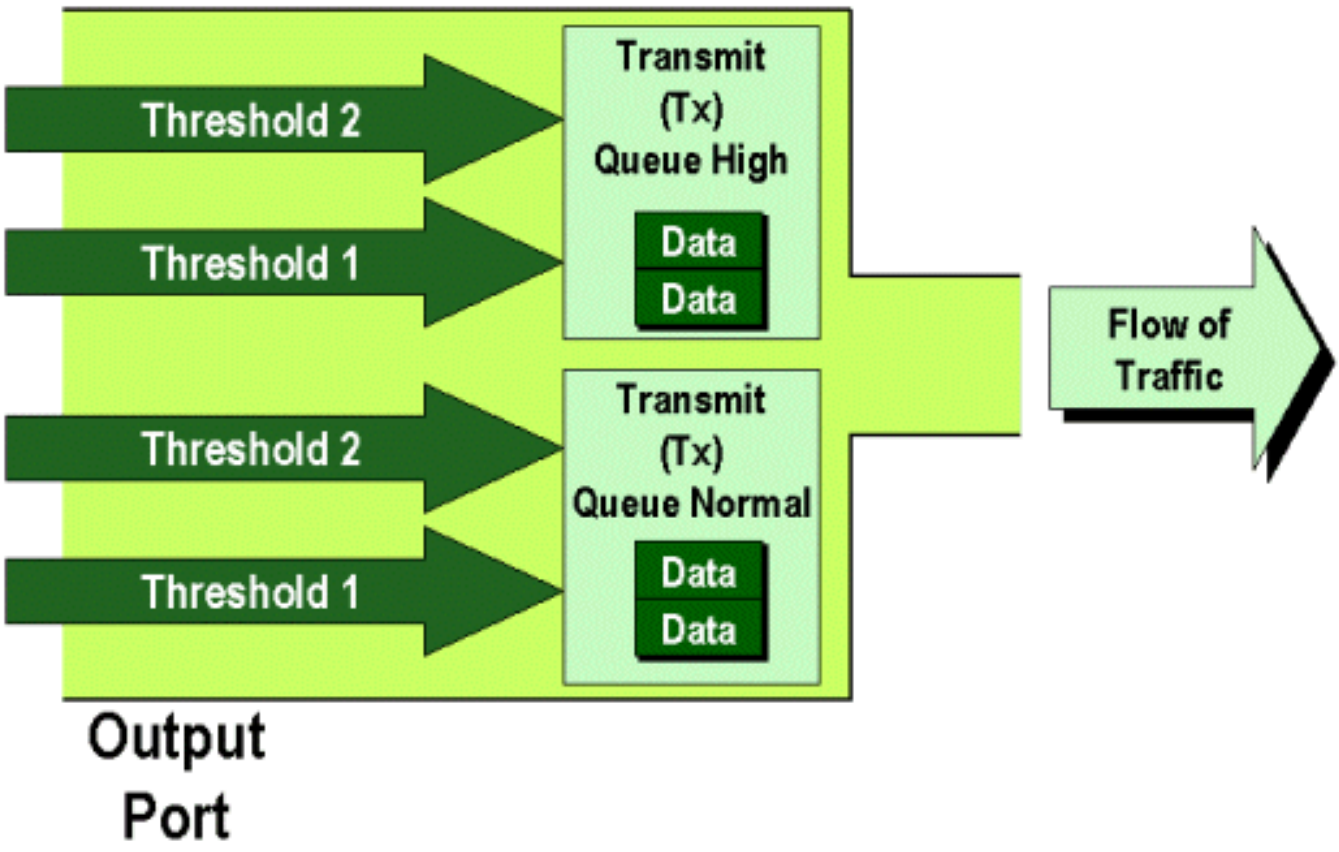
集成 Cisco IOS（本地模式）

```
Cat6500(config-if)# wrr-queue threshold 1 40 50
Cat6500(config-if)# wrr-queue threshold 2 60 100

!-- Configures the 4 thresholds for a 1q4t rx queue and. Cat6500(config-if)# rcv-queue threshold
1 60 75 85 100

!-- Configures for a 1p1q4t rx queue, which applies to !-- the new WS-X6548-RJ45 10/100 line
card.
```

管理员必须启用 Rx 丢弃阈值。目前应使用 **set port qos x/y trust trust-COs** 命令激活 Rx 丢弃阈值（其中 *x* 是模块号，而 y 是该模块上的端口）。

配置 Tx 丢弃阈值

在输出端口上，该端口将有两个 TX 阈值用作拥塞避免机制的一部分，并且具有队列 1 和队列 2。队列 1 表示为标准低优先级队列，而队列 2 表示为标准高优先级队列。根据所使用的板卡，它们将使用尾部丢弃或 WRED 阈值管理算法。这两种算法都对每个 TX 队列使用两个阈值。



管理员可以按如下所示手动设置这些阈值：

CatOS

```
Console> (enable) set qos drop-threshold 2q2t TX queue 1 40 100
!-- TX drop thresholds for queue 1 set at 40% and 100%. Console> (enable)
```

此命令将具有 2 个队列和 2 个阈值（表示为 2q2t）的所有输出端口的队列 1 的 TX 丢弃阈值设置为 40% 和 100%。

```
Console> (enable) set qos wred 1p2q2t TX queue 1  60 100
!-- WRED thresholds for queue 1 set at 60% 100% on all WRED-capable 1p2q2t ports. Console>
(enable)
```

此命令将具有 1 个 SP 队列、2 个普通队列和 2 个阈值（表示为 1p2q2t）的所有输出端口的队列 1 的 WRED 丢弃阈值设置为 60% 和 100%。队列 1 定义为普通低优先级队列，并且具有最低优先级。队列 2 是普通高优先级队列，并且其优先级高于队列 1 的优先级。队列 3 是 SP 队列，它优先于该端口上的所有其他队列进行处理。

集成 Cisco IOS（本地模式）中发出的等价命令如下所示：

集成 Cisco IOS（本地模式）

```
Cat6500(config-if)# wrr-queue random-detect max-threshold  1 40 100
Cat6500(config-if)#
```

此命令将 1p2q2t 端口的队列 1 的 WRED 丢弃阈值设置为 40%（作为阈值 1 (TX)）和 100%（作为阈值 2 (TX)）。

在集成 Cisco IOS（本地模式）中也可以根据需要需要禁用 WRED。可以使用 **n** 形式的命令来禁用 WRED。以下是禁用 WRED 的一个示例：

集成 Cisco IOS（本地模式）

```
Cat6500(config-if)# no wrr-queue random-detect queue_id
```

将 MAC 地址映射到 CoS 值

除了根据全局端口定义设置 CoS 外，交换机还允许管理员根据目标 MAC 地址和 VLAN ID 设置 CoS 值。这就允许使用预先确定的 CoS 值标记发往特定目标的帧。可发出以下命令来进行此配置：

CatOS

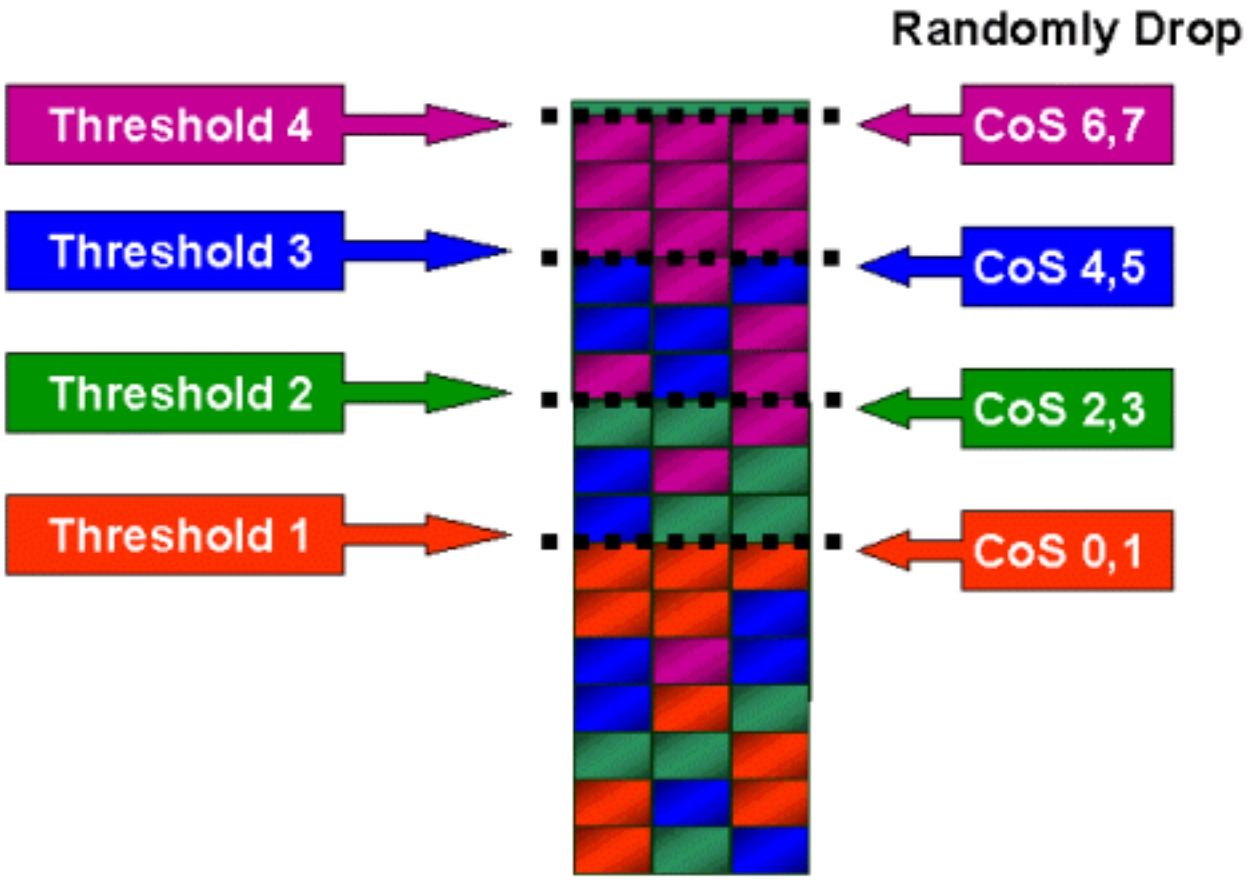
```
Console> (enable) set qos Mac-COs 00-00-0c-33-2a-4e 200 5
!-- COs 5 is assigned to 00-00-0c-33-2a-4e VLAN 200. Console> (enable)
```

此命令将来自 VLAN 200 且其 MAC 地址为 00-00-0c-33-2a-4e 的任何帧的 CoS 设置为 5。

集成 Cisco IOS（本地模式）中没有等价的命令。这是因为此命令只有在没有 PFC 时才受支持，而集成 Cisco IOS（本地模式）的运行需要 PFC。

将 CoS 映射到阈值

配置阈值后，管理员可以将 CoS 值指定给这些阈值，以便在超过阈值时，可以丢弃具有特定 CoS 值的帧。通常，管理员将低优先级帧指定给较小的阈值，这样在出现拥塞时可以将高优先级流量保留在队列中。



上图显示具有 4 个阈值的输入队列，并显示如何将 CoS 值指定给每个阈值。

以下输出显示如何将 CoS 值映射到阈值：

CatOS

```
Console> (enable) set qos map 2q2t 1 1 COs 0 1
!-- QoS TX priority queue and threshold mapped to COs successfully. Console> (enable)
```

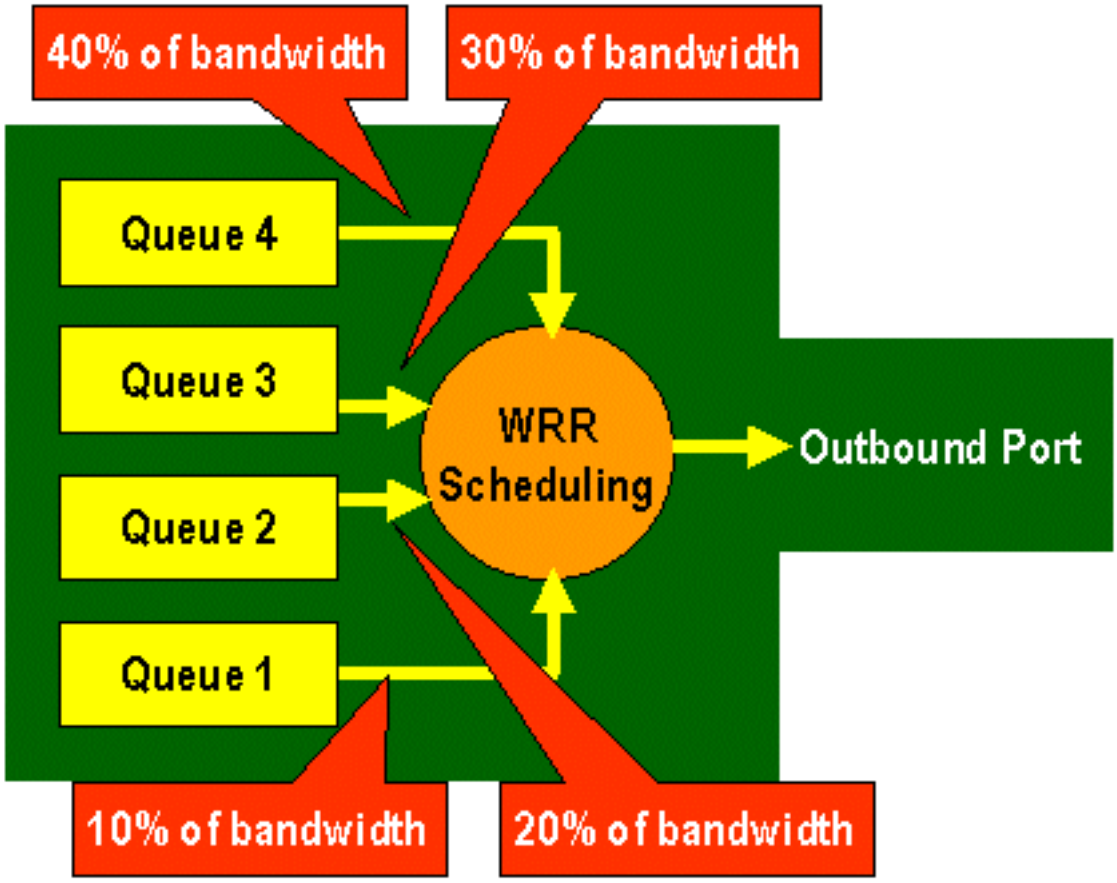
此命令将 CoS 值 0 和 1 指定给队列 1 的阈值 1。集成 Cisco IOS（本地模式）中的等价命令如下所示：

集成 Cisco IOS（本地模式）

```
Cat6500(config-if)# wrr-queue COs-map  1  1  0  1
Cat6500(config-if)#
```

配置 Tx 队列的带宽

当帧放入在输出队列中时，将使用输出安排算法传输帧。输出调度程序进程使用 WRR 传输输出队列中的帧。根据所使用的板卡硬件，每个端口有 2 个、3 个或 4 个传输队列。



在 WS-X6248 和 WS-X6348 板卡（使用 2q2t 队列结构）上，WRR 机制使用 2 个 TX 队列进行安排。在 WS-X6548 板卡（使用 1p3q1t 队列结构）上，有 4 个 TX 队列。在这 4 个 TX 队列中，有 3 个 TX 队列由 WRR 算法处理（最后一个 TX 队列是 SP 队列）。在 GE 板卡上，有 3 个 TX 队列（使用 1p2q2t 队列结构）；其中一个队列是 SP 队列，因此 WRR 算法仅处理 2 个 TX 队列。

通常，管理员会为 TX 队列指定一个权重。WRR 的工作方式是在转至下一个队列之前，查看指定给端口队列的权重，交换机内部使用权重来决定要传输的流量数目。指定给每个端口队列的权重值可以是 1 到 255 之间的一个任意数字。

CatOS

```
Console> (enable) set qos wrr 2q2t 40 80
!-- QoS wrr ratio set successfully. Console> (enable)
```

此命令将权重值 40 指定给队列 1，并将权重值 80 指定给队列 2。这有效地说明指定给这两个队列的带宽比率为 2:1 (80:40 = 2:1)。此命令在具有两个队列和两个阈值的所有端口上生效。

集成 Cisco IOS（本地模式）中发出的等价命令如下所示：

集成 Cisco IOS（本地模式）

```
Cat6500(config-if)# wrr-queue bandwidth 1 3
Cat6500(config-if)#
```

以上命令表示两个队列之间的比率为 3:1。您将注意到此命令的 Cat IOS 版本仅适用于特定接口。

DSCP 到 CoS 映射

当帧放入到输出端口中时，端口 ASIC 将使用指定的 CoS 执行拥塞避免（即 WRED），并且还使用 CoS 来确定帧的安排（即，传输帧）。此时，交换机将使用默认映射来获取指定的 DSCP 值并将该 DSCP 值映射回到一个 CoS 值。此表中显示了此默认映射。

或者，管理员可以创建交换机用来获取指定的内部 DSCP 值的映射，并为帧创建新的 CoS 值。下面以示例形式显示了如何使用 CatOS 和集成 Cisco IOS（本地模式）来实现此目的。

CatOS

```
Console> (enable) set qos dscp-cos--map 20-30:5 10-15:3 45-52:7
!-- QoS dscp-cos-map set successfully. Console> (enable)
```

以上命令将 DSCP 值 20 到 30 映射到 CoS 值 5、将 DSCP 值 10 到 15 映射到 CoS 值 3，并将 DSCP 值 45 到 52 映射到 CoS 值 7。所有其他 DSCP 值都使用交换机上启用 QoS 时创建的默认映射。

集成 Cisco IOS（本地模式）中发出的等价命令如下所示：

集成 Cisco IOS（本地模式）

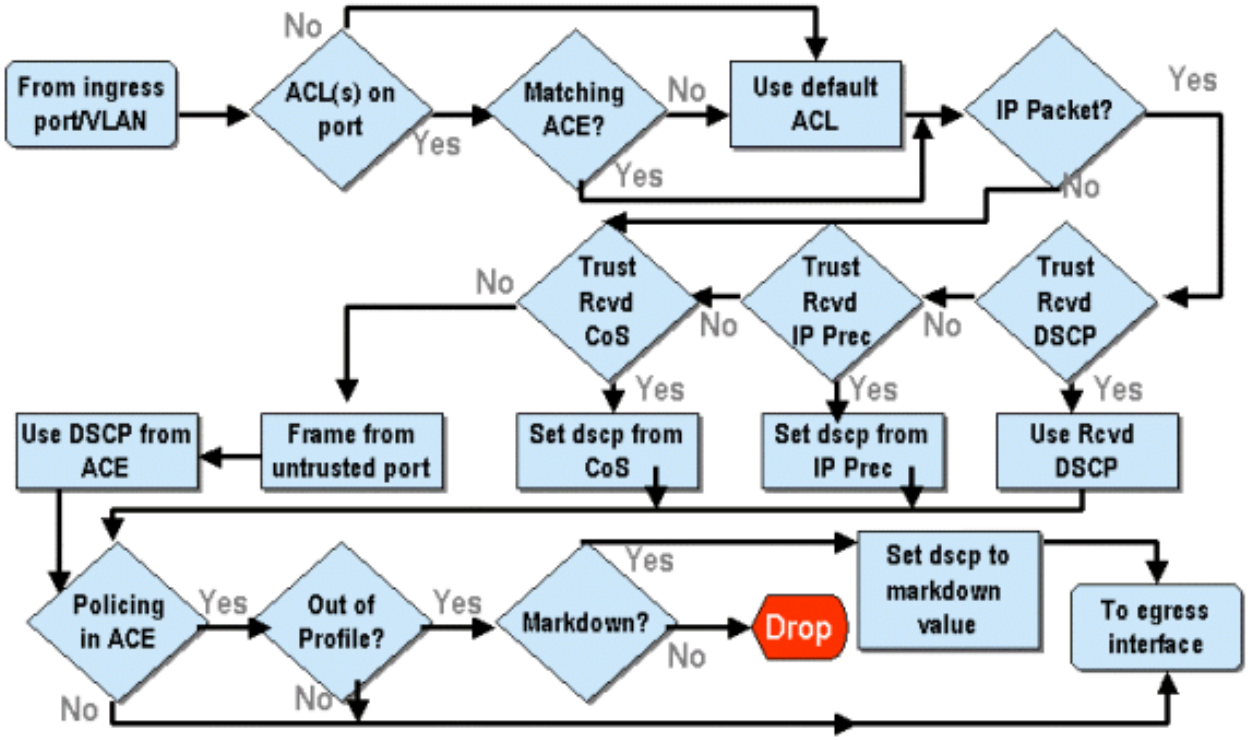
```
Cat6500(config)# mls qos map dscp-cos 20 30 40 50 52 10 1 to 3
Cat6500(config)#
```

此命令将 DSCP 值 20、30、40、50、52、10 和 1 映射到 CoS 值 3。

PFC 的分类和策略

PFC 支持对帧进行分类和管制。分类可以使用 ACL 指定（标记）具有优先级 (DSCP) 的传入帧。管制允许将数据流限制在一定数量的带宽。

下面部分将从 CatOS 和集成 Cisco IOS（本地模式）OS 平台的角度介绍 PFC 上的这些功能。下图显示了 PFC 应用的过程：



配置使用 CatOS 的 Catalyst 6000 系列的策略

管制功能分为两个部分，一部分用于 CatOS，另一部分用于集成 Cisco IOS（本地模式）。这两个部分都产生相同的最终结果，但用不同的方式配置和实现。

修正

PFC 支持对传入交换机的流量进行速率限制（管制）的能力，并且可以将数据流减少到预定义的限制。超过该限制的流量可能被丢弃，或者帧中的 DSCP 值降级为一个较小的值。

PFC1 或 PFC2 中当前不支持输出（出口）速率限制。计划于 2002 年下半年推出的 PFC 的新修订版中将增加此支持，该修订版会支持输出（出口）管制。

CatOS 和新的集成 Cisco IOS（本地模式）中都支持管制，但这些功能的配置极不相同。下面部分将介绍这两个 OS 平台中的管制配置。

聚合和微流 (CatOS)

聚合和微流是用于定义 PFC 执行的管制范围的术语。

微流定义单个流的管制。流是由会话定义的，它具有唯一的 SA/DA MAC 地址、SA/DA IP 地址和 TCP/UDP 端口号。对于通过 VLAN 中的端口发起的每个新流，可以使用微流来限制交换机接收到的该流的数据量。在微流定义中，对于超过规定的速率限制的数据包，可以将它们丢弃，也可以将其 DSCP 值降级。

与微流类似，聚合也可用来限制流量的速率。但是，聚合速率适用于与指定 QoS ACL 匹配的端口或 VLAN 上的所有入站流量。您能观看聚合作为匹配在访问控制项(ACE)的配置文件累计数据流的管制。

聚合和微流都会定义交换机可以接受的流量数量。可以同时将聚合和微流指定给端口或 VLAN。

定义微流时，最多可以定义 63 个微流和 1023 个聚合。

访问控制条目和 QoS ACL (CatOS)

QoS ACL 包括一个 ACE 列表，并定义了一组 PFC 用于处理传入帧的 QoS 规则。ACE类似于路由器访问控制列表(RACL)。ACE 定义传入帧的分类、标记和管制标准。如果传入帧符合 ACE 中设置的标准，则 QoS 引擎将处理该帧（按 ACE 所认为的那样)。

所有 QoS 处理都在硬件中完成，因此启用 QoS 管制不会影响交换机的性能。

PFC2 当前支持多达 500 个 ACL，并且这些 ACL 最多可以包括 32000 个 ACE（总计）。实际 ACE 数目取决于 PFC 中定义的其他服务和可用的存储空间。

可以定义三种类型的 ACE。它们是 IP、IPX 和 MAC。IP 和 IPX ACE 均会检查 L3 报头信息，而基于 MAC 的 ACE 只检查 L2 报头信息。此外还应注意，MAC ACE 仅适用于非 IP 和非 IPX 流量。

创建管制规则

创建管制规则的过程包括创建聚合（或微流），然后将该聚会（或微流）映射到 ACE。

例如，如果要求将端口 5/3 上所有传入的 IP 流量限制为最多 20 MB，则必须配置上面提到的两个步骤。

首先，本示例请求限制所有传入的 IP 流量。这意味着必须定义聚合监察器。此命令示例可能如下：

```
Console> (enable) set qos policer aggregate test-flow rate 20000 burst 13 policed-dscp
!-- Hardware programming in progress !-- QoS policer for aggregate test-flow created
successfully. Console> (enable)
```

创建了一个称为 test-flow 的聚合。它将速率定义为 20000 KBPS (20 MBPS)，将突发定义为 13。policed-dscp 关键字指示超过此策略的所有数据的 DSCP 值都要降级，如 DSCP 降级映射（存在默认降级映射，或者可由管理员修改降级映射）中所指定的那样。可使用 drop 关键字代替 policed-dscp 关键字。drop 关键字将丢弃所有超出配置规定的流量（位于指定的突发值外的流量）。

管制工具采用漏令牌桶方案，在该方案中，您可定义一个突发（在给定（固定）时间间隔内每秒将收到的数据量（以位计）），然后定义速率（一秒内从该桶中清空的数据量）。溢出此桶的所有数据都将被丢弃或使其 DSCP 降级。上面提到的给定时间段（或间隔）为 0.00025 秒（1/4000 秒），它是固定的（也就是说，您无法使用任何配置命令更改此数字）。

上面示例中的数字 13 表示桶每 1/4000 秒最多接受 13,000 位数据。这与52 MB关连每秒钟(13K * (1/0.00025)或13K * 4000)。您必须始终确保配置的突发大于或等于发送出数据的速率。也就是说，突发应大于或等于您在给定时间段内要传输的最小数据量。如果突发生成的数字小于您所指定的速率，则速率限制将等于突发。也就是说，如果定义的速率为 20 MBPS，而突发的计算结果为 15MBPS，则速率只能为 15MBPS。接下来您可能要问为什么是 13？请记住，突发定义令牌桶的深度，换句话说，就是每 1/4000 秒用于接收传入数据的桶的深度。因此，突发可以是大于或等于 20 MBPS 的到达数据速率所支持的任意数字。可用于速率限制 20MB 的最小突发为 20000/4000 = 5。

处理监察器时，管制算法最初用全部令牌填满令牌桶。令牌数等于突发值。因此，如果突发值为 13，则桶中的令牌数等于 13,000。对于每 1/4000 秒，管制算法将发送出的数据量等于定义的速率除以 4000。发送的每个数据位（二进制数字）都将消耗桶中的一个令牌。时间间隔结束时，管制算法会使桶中重新装满一组新的令牌。放回的令牌数定义为速率/4000。请结合上面的示例理解以下命令：

```
Console> (enable) set qos policer aggregate test-flow rate 20000 burst 13
```

假定这是一个 100 MBPS 端口，并且正在以 100 MBPS 速率向该端口中持续发送流。我们知道这等于传入速率为每秒 100,000,000 位。此处的参数是速率为 20000 且突发为 13。在时间间隔 t0，桶中装满了全部令牌（13,000 个）。在时间间隔 t0，第一组数据到达端口。对于此时间间隔

，到达速率将为每秒 100,000,000/4000 = 25,000 位。由于令牌桶的深度仅为 13,000 个令牌，因此，在此时间间隔内到达端口的 25,000 位中，只有 13,000 位能够被发送，12,000 位将被丢弃。

指定的速率定义转发速率为每秒 20,000,000 位，这相当于每个 1/4000 秒时间间隔发送 5,000 位。发送的每 5,000 位将消耗 5,000 个令牌。在时间间隔 T1，另外 25,000 位数据到达，但桶丢弃 12,000 位。桶中重新装满令牌，其数目定义为速率/4000（等于 5,000 个新令牌）。然后，算法发送出下一组补充数据（即另外 5,000 位数据，这将消耗另外 5,000 个令牌），并在每个时间间隔都如此。

本质上，超过桶深度（定义的突发）的所有传入数据都被丢弃。发送数据后留下的数据（与规定的速率匹配）也被丢弃，从而为下一组到达的数据腾出空间。不完整数据包是指在时间间隔内未完全接收的数据包，这种数据包不会被丢弃，而是保留到端口中完全接收该数据包为止。

此突发数字假定数据流是持续的。但是，在现实世界的网络中，数据不是持续的，并且数据流由 TCP 窗口大小确定，而 TCP 窗口大小将 TCP 确认合并到传输序列中。要考虑 TCP 窗口大小的问题，建议使突发值增大一倍。在上面的示例中，建议的值 13 实际上被配置为 26。

另一个要明确的要点是，在时间间隔 0（即，管制周期的开始），令牌桶中装满了令牌。

现在，必须将此聚合策略合并到 QoS ACE 中。ACE 用于制定规范以便将一组标准与传入帧匹配。请考虑以下示例。您要将上面定义的聚合应用于所有 IP 流量，尤其是来自子网 10.5.x.x 且发送到子网 203.100.45.x 的流量。ACE 看起来如下所示：

```
Console> (enable) set qos acl ip test-acl trust-dscp aggregate test-flow tcp 10.5.0.0
203.100.45.0
!-- Test-acl editbuffer modified. Issue the commit command to apply changes.
Console> (enable)
```

上面的命令创建了一个 IP ACE（使用 **set qos acl ip** 命令表示），现在该 IP ACE 与称为 test-acl 的 QoS ACL 关联。创建的与 ACL test-acl 关联的后续 ACE 将附加到 ACE 列表的末尾。该 ACE 条目与聚合 test-flow 关联。此策略将应用于源子网为 10.5.0.0 且目标子网为 203.100.45.0 的所有 TCP 流。

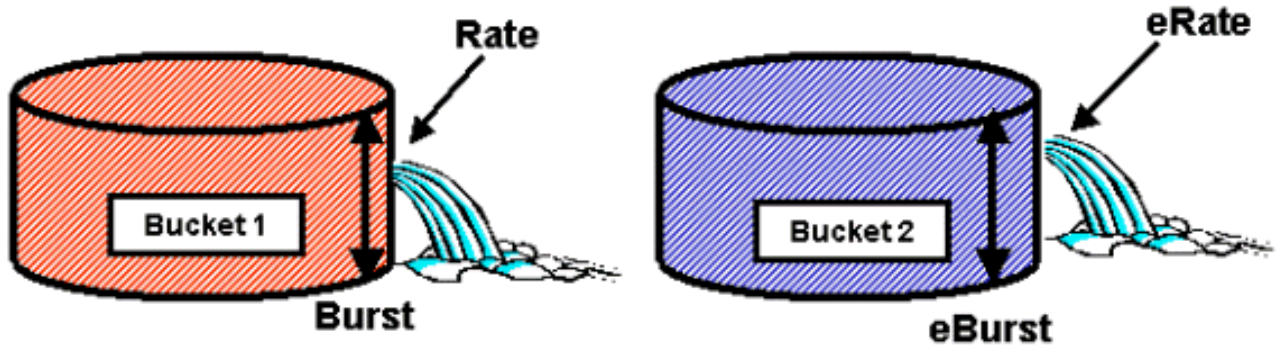
ACL（和关联的 ACE）将提供非常精细的、可供管理员使用的配置灵活性。ACL 可以包含一个或多个 ACE，并且可以使用源和/或目标地址以及 L4 端口值来标识需要管制的特定流。

但是，在实际进行任何管制之前，必须将 ACL 映射到物理端口或 VLAN。

PFC2 管制决策

对于 PFC2，CatOS 7.1 和 CatOS 7.2 中进行了一处更改，即引入了双漏桶算法进行管制。此新算法增加了以下两个新级别：

1. **普通管制级别：**这等同于第一个桶，它定义两个参数 burst 和 rate，burst 用于指定桶的深度，而 rate 用于指定发送桶中的数据时应采用的速率。
2. **超额管制级别：**这等同于第二个桶，它定义两个参数 eburst 和 erate，eburst 用于指定桶的深度，而 erate 用于指定发送桶中的数据时应采用的速率。



此过程的工作方式是数据开始填满第一个桶。PFC2 接受小于或等于第一个桶的深度（burst 值）的传入数据流。可以将从第一个桶中溢出的数据降级，并将它们传递到第二个桶。第二个桶可以接受第一个桶中溢出的传入速率小于或等于 eburst 值的数据。第二个桶中的数据将采用 erate 参数减去 rate 参数所定义的速率进行发送。从第二个桶中溢出的数据也可以被降级或丢弃。

以下是一个双漏桶监察器的示例：

```
Console> (enable) set qos policer aggregate AGG1 rate 10000 policed-dscp erate 12000 drop burst
13 eburst 13
```

本示例在适当的位置设置一个称为 AGG1 的聚合，其流量速率超过 10 MBPS，并且将根据管制的 DSCP 映射进行降级。根据 drop 关键字，超过 erate（设置为 12 MBPS）的流量将被丢弃。

将聚合监察器应用于支持 DFC 的模块

应注意，由于 Catalyst 6000 系列使用集中转发引擎 (PFC) 转发流量的方式，可以在非 DFC 板卡上应用聚合监察器。通过使用中央转发引擎，可以记录给定 VLAN 的流量统计信息。可以使用此过程将聚合监察器应用于 VLAN。

但是，在支持 DFC 的板卡上，转发决策被分发给该板卡。DFC 只知道其紧邻的板卡上的端口，而不知道其他板卡上的流量移动。为此，如果将聚合监察器应用于在多个 DFC 模块间具有成员端口的 VLAN，则监察器可能会生成不一致的结果。这是因为 DFC 只能记录本地端口统计信息，而不考虑其他板卡上的端口统计信息。由于此原因，如果聚合监察器已应用于在支持 DFC 的板卡上具有成员端口的 VLAN，则该监察器会导致 DFC 对流量进行管制，使流量不超过仅针对 DFC 板卡上的 VLAN 端口的规定限制。

DSCP 降级映射 (CatOS)

定义监察器以降级超出配置规定的流量而不是将其丢弃时，可以使用 DSCP 降级映射。超出配置规定的流量定义为超过定义的突发设置的流量。

启用 QoS 时，将设置默认 DSCP 降级映射。本文档前面部分的此表中列出了此默认降级映射。命令行界面(CLI)允许管理员通过发出**set qos policed-dscp-map命令**修改默认减价映射。此命令示例如下：

```
Cat6500(config)# set qos policed-dscp-map 20-25:7 33-38:3
```

本示例修改 policed DSCP 映射，将 DSCP 值 20 到 25 将降级为 DSCP 值 7，且 DSCP 值 33 到 38 将降级为 DSCP 值 3。

将策略映射到 VLAN 和端口 (CatOS)

构建 ACL 后，必须将它映射到端口或 VLAN 以便该 ACL 生效。

许多不了解的人感兴趣的一个命令是使所有 QoS 基于端口的默认 QoS 设置。如果将聚合（或微流）应用于 VLAN，则除非已将端口配置为基于 VLAN 的 QoS，否则聚合（或微流）不会在该端口上生效。

```
Console> (enable) set port qos 2/5-10 vlan-based
!-- Hardware programming in progress  !-- QoS interface is set to vlan-based for ports 2/5-10.
Console> (enable)
```

将基于端口的 QoS 更改为基于 VLAN 的 QoS 会立即分离指定给该端口的所有 ACL，并将任何基于 VLAN 的 ACL 指定给该端口。

发出以下命令可以将 ACL 映射到端口（或 VLAN）：

```
Console> (enable) set qos acl map test-acl 3/5
!-- Hardware programming in progress  !-- ACL test-acl is attached to port 3/5. Console>
(enable) Console> (enable) set qos acl map test-acl 18
!-- Hardware programming in progress  !-- ACL test-acl is attached to VLAN 18. Console> (enable)
```

在将 ACL 映射到端口（或 VLAN）后，还要将 ACL 提交到硬件，然后该 ACL 才会生效。这将在下一部分中进行说明。此时，ACL 位于内存中的临时编辑缓冲区中。在此缓冲区中时，可以修改 ACL。

如果要删除编辑缓冲区中的任何未提交的 ACL，可以发出 **rollback** 命令。此命令本质上将从编辑缓冲区中删除 ACL。

```
Console> (enable) rollback qos acl test-acl
!-- Rollback for QoS ACL test-acl is successful. Console> (enable)
```

提交 ACL (CatOS)

要应用（上面）定义的 QoS ACL，必须将 ACL 提交到硬件。提交过程将临时缓冲区中的 ACL 复制到 PFC 硬件。当 QoS ACL 中定义的策略位于 PFC 内存中后，就可以将该策略应用于与 ACE 匹配的所有流量。

为了便于配置，大多数管理员发出 **commit all** 命令。但是，您可以提交当前位于编辑缓冲区中的特定 ACL（许多 ACL 中的一个）。以下是一个 commit 命令的示例：

```
Console> (enable) commit qos acl test-acl
!-- Hardware programming in progress  !-- ACL test-acl is committed to hardware. Console>
(enable)
```

如果要从端口（或 VLAN）中删除 ACL，则需要发出以下命令清除使 ACL 与该端口（或 VLAN）关联的映射：

```
Console> (enable) clear qos acl map test-acl 3/5
!-- Hardware programming in progress  !-- ACL test-acl is detached from port 3/5.
Console>(enable)
```

配置使用集成 Cisco IOS（本地模式）的 Catalyst 6000 系列的策略

集成 Cisco IOS（本地模式）支持管制。但是，配置和实施管制功能是使用策略映射实现的。每个策略映射都由多个策略类构成，并且可以对不同类型的数据流定义这些策略类。

进行过滤时，策略映射类使用基于 IOS 的 ACL 和类匹配语句来标识要管制的流量。标识出流量后，策略类就可以使用聚合和微流监察器将管制策略应用于这些匹配的流量。

下面部分更详细地说明如何在集成 Cisco IOS（本地模式）中配置管制。

聚合和微流（集成 Cisco IOS（本地模式））

聚合和微流是用于定义 PFC 执行的管制范围的术语。与 CatOS 类似，聚合和微流同样可以在集成 Cisco IOS（本地模式）中使用。

微流定义单个流的管制。流是由会话定义的，它具有唯一的 SA/DA MAC 地址、SA/DA IP 地址和 TCP/UDP 端口号。对于通过 VLAN 中的端口发起的每个新流，可以使用微流来限制交换机接收到的该流的数据量。在微流定义中，对于超过规定的速率限制的数据包，可以将它们丢弃，也可以将其 DSCP 值降级。可以使用策略映射类中包括的 police flow 命令应用微流。

要在集成 Cisco IOS（本地模式）中启用微流管制，必须在交换机上全局启用微流管制。这可以通过发出以下命令来实现：

```
Cat6500(config)# mls qos flow-policing
```

此外，还可以将微流管制应用于桥接的流量，这种流量不是在第三层交换的。要使交换机支持对桥接流量进行微流管制，请发出以下命令：

```
Cat6500(config)# mls qos bridged
```

此命令还支持对多播流量进行微流管制。如果需要将微流监察器应用于多播流量，则必须启用此命令（**mls qos bridged**）。

与微流类似，聚合也可用来限制流量的速率。但是，聚合速率适用于与指定 QoS ACL 匹配的端口或 VLAN 上的所有入站流量。可以将聚合视为对与定义的流量配置文件匹配的累积流量的管制。

在集成 Cisco IOS（本地模式）中可以定义两种形式的聚合，如下所示：

- 每接口聚合监察器
- 指定的聚合监察器

通过发出策略映射类中的 **police** 命令，可以将每接口聚合应用于单独的接口。这些映射类可以应用于多个接口，但监察器单独管制每个接口。指定的聚合适用于一组端口，并以渐增方式管制通过所有接口的流量。通过发出 **mls qos aggregate policer** 命令可以应用指定的聚合。

定义微流时，最多可以定义 63 个微流和 1023 个聚合。

创建管制规则（集成 Cisco IOS（本地模式））

创建管制规则的过程包括通过策略映射创建聚合（或微流），然后将该策略映射附加到接口。

请考虑为 CatOS 创建的相同示例。要求是将端口 5/3 上的所有传入 IP 流量限制为最大 20 MBPS。

首先，必须创建策略映射。创建一个名为 limit-traffic 的策略映射。其实现过程如下：

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)#
```

您立即就会注意到交换机提示符更改了，以反映您正处于创建映射类的配置模式。请记住，一个策略映射可以包含多个类。每个类都包含一组单独的、可应用于不同数据流的策略操作。

我们将创建一个流量类，用于专门将传入流量限制为 20 MBPS。此类的名称为 limit-to-20。如下所示：

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20
Cat6500(config-pmap-c)#
```

此时提示符再次更改，以反映您现在处于映射类配置过程中（提示符末尾显示 -c）。如果要应用速率限制以与特定传入流量匹配，则可以配置 ACL 并将它应用于类名。如果要对源自网络 10.10.1.x 的流量应用 20 MBPS 限制，请发出以下 ACL：

```
Cat6500(config)# access-list 101 permit ip 10.10.1.0  0.0.0.255 any
```

可以按如下所示将此 ACL 添加到类名：

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20 access-group 101
Cat6500(config-pmap-c)#
```

定义类映射后，现在就可以对该类定义单独的监察器。您可以创建聚合（使用 police 关键字）或微流（使用 police flow 关键字）。按如下所示创建聚合：

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20 access-group 101
Cat6500(config-pmap-c)# police 20000000 13000 confirm-action transmit exceed-action drop
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

上面的 class 语句（police 命令）设置速率限制为 20000 k (20 MBPS)，且突发为 52 MBPS (13000 x 4000 = 52MB)。如果流量与配置文件匹配，且在规定的限制内，则操作是通过 confirm-action 语句设置为传输符合配置规定的流量。如果流量超出配置规定（在本示例中，超过 20 MB 限制），则设置 exceed-action 语句以丢弃该流量（在本示例中，丢弃所有超过 20 MB 的流量）。

配置微流时，将执行类似的操作。如果要将进入某个端口且与给定类映射匹配的所有流的速率限制为每个流 200 K，则该流的配置将类似于以下配置：

```
Cat6500(config)# mls qos flow-policing
Cat6500(config)# policy-map limit-each-flow
Cat6500(config-pmap)# class limit-to-200
Cat6500(config-pmap-c)# police flow 200000 13000 confirm-action transmit exceed-action drop
```

```
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
```

DSCP 降级映射

定义监察器以降级超出配置规定的流量而不是将其丢弃时，可以使用 DSCP 降级映射。超出配置规定的流量定义为超过定义的突发设置的流量。

启用 QoS 时，将建立默认 DSCP 降级映射。此表中列出了此默认降级映射。管理员可以通过 CLI 发出 **set qos policed-dscp-map** 命令来修改默认降级映射。此命令示例如下：

```
Cat6500(config)#

mls qos map policed-dscp normal-burst 32 to 16
```

本示例定义对默认 policed dscp 映射的修改，将 DSCP 值 32 降级为 DSCP 值 16。对于定义了此监察器的端口，如果具有此 DSCP 值的任何传入数据是超过规定突发的数据块的一部分，则此传入数据的 DSCP 值将降级为 16。

将策略映射到 VLAN 和端口（集成 Cisco IOS（本地模式））

构建某策略后，必须将它映射到端口或 VLAN，才能使该策略生效。与 CatOS 中的提交过程不同，集成 Cisco IOS（本地模式）中没有等价的过程。当策略映射到接口时，该策略就会生效。要将上面的策略映射到接口，请发出以下命令：

```
Cat6500(config)# interface fastethernet 3/5
Cat6500(config-if)# service-policy input limit-traffic
```

如果策略已映射到 VLAN，则对于 VLAN 中要应用 VLAN 策略的每个端口，您必须发出 **mls qos vlan-based** 命令通知接口 QoS 是基于 VLAN 的。

```
Cat6500(config)# interface fastethernet 3/5
Cat6500(config-if)# mls qos vlan-based
Cat6500(config-if)# exit
Cat6500(config)# interface vlan 100
Cat6500(config-if)# service-policy input limit-traffic
```

假定接口 3/5 是 VLAN 100 的一部分，则已应用于 VLAN 100 的策略 limit-traffic 也会应用于接口 3/5。

配置使用 CatOS 的 Catalyst 6000 系列的分类

PFC 中支持使用可以查看 L2、L3 和 L4 报头信息的 ACL 对数据进行分类。对于 SupI 或 IA（不包含 PFC），分类限于对端口使用 trust 关键字。

下面部分介绍 PFC 用来在 CatOS 中进行分类的 QoS 配置组件。

CoS 到 DSCP 映射 (CatOS)

在帧进入交换机时，交换机将为该帧设置 DSCP 值。如果端口处于信任状态，并且管理员已使用 trust-COs 关键字，则帧中设置的 CoS 值将用于确定为该帧设置的 DSCP 值。如前面所述，当帧通

过交换机时，交换机可以根据内部 DSCP 值为该帧指定服务级别。

此关键字在某些较早的 10/100 模块（WS-X6248 和 WS-X6348）上不受支持。对于这些模块，建议使用 ACL 来应用传入数据的 CoS 设置。

启用 QoS 时，交换机会创建默认映射。此映射用于标识将根据 CoS 值设置的 DSCP 值。本文档前面部分的此表中列出了这些映射。或者，管理员也可以设置唯一的映射。此命令示例如下：

```
Console> (enable) set qos cos-dscp-map 20 30 1 43 63 12 13 8
!-- QoS cos-dscp-map set successfully. Console> (enable)
```

上面的命令设置以下映射：

Cos	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

虽然现实网络中很可能不会使用上面的映射，但其目的旨在告诉您使用此命令产生的结果。

IP 优先级到 DSCP 映射 (CatOS)

与 CoS 到 DSCP 映射类似，帧可以根据传入数据包的 IP 优先级设置确定 DSCP 值。这种情况只有在管理员将端口设置为信任，且已使用 trust-ipprec 关键字时才会发生。

启用 QoS 时，交换机会创建默认映射。此文档前面部分的此表中引用了此映射。此映射用于标识将根据 IP 优先级值设置的 DSCP 值。或者，管理员也可以设置唯一的映射。此命令示例如下：

```
Console> (enable) set qos ipprec-dscp-map 20 30 1 43 63 12 13 8
!-- QoS ipprec-dscp-map set successfully. Console> (enable)
```

上面的命令设置以下映射：

IP 优先级	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

虽然现实网络中很可能不会使用上面的映射，但其目的旨在告诉您使用此命令产生的结果。

分类 (CatOS)

当帧传递到 PFC 进行处理时，将对该帧执行分类过程。PFC 将使用预配置的 ACL（或默认 ACL）为该帧指定 DSCP 值。在 ACE 中，可以使用四个关键字中的一个来指定 DSCP 值。这些关键字如下：

1. TRUST-DSCP（仅适用于 IP ACL）
2. TRUST-IPPREC（仅适用于 IP ACL）
3. TRUST-COS（适用于除 PFC2 上的 IPX 和 MAC 外的所有 ACL）
4. DSCP

TRUST-DSCP 关键字假定到达 PFC 中的帧在进入交换机之前已设置了 DSCP 值。交换机将维护此 DSCP 值。

使用 TRUST-IPPREC 时，PFC 将根据 ToS 字段中现有的 IP 优先级值生成 DSCP 值。然后，PFC 将使用 IP 优先级到 DSCP 映射指定正确的 DSCP。交换机上启用 QoS 时，会创建默认映射。或者，可以使用管理员创建的映射来生成 DSCP 值。

与 TRUST-IPPREC 类似，TRUS-COS 关键字指示 PFC 根据帧报头中的 CoS 生成 DSCP 值。PFC 也可以使用 CoS 到 DSCP 映射（可以是默认映射或管理员指定的映射）来生成 DSCP 值。

当来自不信任的端口的帧到达时，可以使用 DSCP 关键字。这对于生成 DSCP 来说是一种有趣的情形。此时，可以使用在 set qos acl 语句中配置的 DSCP 来生成 DSCP。但是，此时还可以使用 ACL 并根据 ACE 中设置的分类标准来生成流量的 DSCP。这意味着，可以使用 ACE 中的分类标准来标识流量，这些分类标准包括 IP 源和目标地址、TCP/UDP 端口号、ICMP 代码、IGMP 类型、IPX 网络和协议号、MAC 源和目标地址，以太网类型（仅适用于非 IP 和非 IPX 流量）等。这就是说，可以配置 ACE，以便将特定 DSCP 值指定给基于 FTP 流量的 HTTP 流量。

请看下例：

```
Console> (enable) set port qos 3/5 trust untrusted
```

将端口设置为不信任将指示 PFC 使用 ACE 生成帧的 DSCP。如果为 ACE 配置了分类标准，则可以使用不同优先级对来自该端口的各个流进行分类。以下 ACE 说明了这点：

```
Console> (enable) set qos acl ip abc dscp 32 tcp any any eq http
Console> (enable) set qos acl ip ABC dscp 16 tcp any any eq ftp
```

在本示例中，有两条 ACE 语句。第一条 ACE 语句标识端口号为 80 (80 = HTTP) 的任何 TCP 流（关键字 any 用于标识源和目标流量），将为这种流量指定 DSCP 值 32。第二条 ACE 语句标识来自任何主机，且要发送到 TCP 端口号为 21 (FTP) 的任何主机的流量，将为这种流量指定 DSCP 值 16。

配置使用集成 Cisco IOS（本地模式）的 Catalyst 6000 系列的分类

下面部分介绍用于支持使用集成 Cisco IOS（本地模式）的 PFC 上的分类的 QoS 配置组件。

CoS 到 DSCP 映射（集成 Cisco IOS（本地模式））

在帧进入交换机时，交换机将为该帧设置 DSCP 值。如果端口处于信任状态，并且管理员已使用 mls qos trust-COs 关键字（在 WS-X6548 板卡的 GE 端口或 10/100 端口上），则帧中设置的 CoS 值将用于确定为该帧设置的 DSCP 值。如前面所述，当帧通过交换机时，交换机可以根据内部 DSCP 值为该帧指定服务级别。

启用 QoS 时，交换机会创建默认映射。有关默认设置，请参阅此表。此映射用于标识将根据 CoS 值设置的 DSCP 值。或者，管理员也可以设置唯一的映射。此命令示例如下：

```
Cat6500(config)# mls qos map cos-dscp 20 30 1 43 63 12 13 8
Cat6500(config)#
```

上面的命令设置以下映射：

Cos	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

虽然现实网络中很可能不会使用上面的映射，但其目的旨在告诉您使用此命令产生的结果。

IP 优先级到 DSCP 映射（集成 Cisco IOS（本地模式））

与 CoS 到 DSCP 映射类似，帧可以根据传入数据包的 IP 优先级设置确定 DSCP 值。这种情况只有在管理员将端口设置为信任，且已使用 mls qos trust-ipprec 关键字时才会发生。仅 WS-X6548 板卡上的 GE 端口和 10/100 端口支持此关键字。对于 WS-X6348 和 WS-X6248 板卡上的 10/100 端口，应使用 ACL 为传入数据指定 IP 优先级信任。

启用 QoS 时，交换机会创建默认映射。有关默认设置，请参阅此表。此映射用于标识将根据 IP 优先级值设置的 DSCP 值。或者，管理员也可以设置唯一的映射。此命令示例如下：

```
Cat6500(config)# mls qos map ip-prec-dscp 20 30 1 43 63 12 13 8
Cat6500(config)#
```

上面的命令设置以下映射：

IP 优先级	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

虽然现实网络中很可能不会使用上面的映射，但其目的旨在告诉您使用此命令产生的结果。

分类（集成 Cisco IOS（本地模式））

当帧传递到 PFC 时，可以执行分类过程为传入帧指定新的优先级。此处的注意事项是：只有当帧来自不受信任的端口，或者帧已分类为不受信任时，上述操作才能执行。

策略映射类操作可用于：

1. TRUST COS
2. TRUST IP-PRECEDENCE
3. TRUST DSCP
4. NO TRUST

TRUST DSCP 关键字假定到达 PFC 中的帧在进入交换机之前已设置 DSCP 值。交换机将维护此 DSCP 值。

使用 TRUST IP-PRECEDENCE 时，PFC 将根据 ToS 字段中现有的 IP 优先级值生成 DSCP 值。然后，PFC 将使用 IP 优先级到 DSCP 映射指定正确的 DSCP。交换机上启用 QoS 时，会创建默认映射。或者，可以使用管理员创建的映射来生成 DSCP 值。

与 TRUST IP-PRECEDENCE 类似，TRUST COs 关键字指示 PFC 根据帧报头中的 CoS 生成 DSCP 值。PFC 也可以使用 CoS 到 DSCP 映射（可以是默认映射或管理员指定的映射）来生成 DSCP 值。

以下是根据现有优先级（DSCP、IP 优先级或 CoS）生成 DSCP 的示例：

```
Cat6500(config)# policy-map assign-dscp-value
Cat6500(config-pmap)# class test
Cat6500(config-pmap-c)# trust COs
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

上面的类映射根据以太网报头中的 CoS 生成 DSCP 值。

当来自不信任的端口的帧到达时，将使用 NO TRUST 形式的关键字。这样帧就可以在管制过程中指定 DSCP 值。

以下示例说明如何使用下面的策略定义将新的优先级 (DSCP) 指定给进入 PFC 的不同流。

```
Cat6500(config)# access-list 102 permit tcp any any eq http
Cat6500(config)# policy-map new-dscp-for-flow
Cat6500(config-pmap)# class test access-group 102
Cat6500(config-pmap-c)# no trust
Cat6500(config-pmap-c)# police 1000 1 confirm-action set-dscp-transmit 24  Cat6500(config-pmap-
c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

上面的示例显示以下内容：

1. 正创建的 ACL 用于标识进入端口的 http 流。
2. 一个称为 new-dscp-for-flow 的策略映射。
3. 一个称为 test 的类映射，它使用访问列表 102 来标识此类映射将对其执行操作的流量。
4. 类映射 test 将传入帧的信任状态设置为不信任，并为该流指定 DSCP 值 24。
5. 此类映射还将所有 http 流的总大小限制为最大值 1 MB。

通用开放策略服务器 (COPS)

COPS 是一种协议，它使得 Catalyst 6000 系列可以从远程主机配置 QoS。目前，只有在使用 CatOS 时 COPS 才受支持，并且 COPS 是 QoS 的 intserv 体系结构的一部分。使用集成 Cisco IOS（本地模式）时目前不支持 COPS（自本文档的日期起）。虽然 COPS 协议将 QoS 配置信息携带到交换机，但它不是 QoS 配置信息的来源。使用 COPS 协议需要一个外部 QoS 管理器托管交换机的 QoS 配置。外部 QoS 管理器使用 COPS 协议开始将这些配置下推到交换机。思科的QoS Policy Manager (QPM)是外部QoS管理器的示例。

本文档的意图不是说明 QPM 的工作，而是通过使用 QPM 说明交换机支持外部 QoS 配置所需的配置。

COPS 配置

默认情况下，COPS 支持已禁用。要在交换机上使用 COPS，必须将其启用。这可以通过发出以下命令来实现：

```
Console> (enable) set qos policy-source cops
!-- QoS policy source for the switch set to COPS. Console> (enable)
```

执行此命令时，将从 COPS 服务器获取某些默认 QoS 配置值。这些默认 QoS 配置值包括：

1. CoS 到队列映射
2. 指定的输入和输出队列阈值
3. 指定的 WRR 带宽
4. 任何聚合和微流策略
5. 用于输出流量的 DSCP 到 CoS 映射
6. ACL
7. 指定的默认端口 CoS

使用 COPS 执行 QoS 配置时，一定要了解这些配置的应用方式是不同的。将使用 COPS 来配置端口 ASIC，而不是直接配置端口。端口 ASIC 通常控制一组端口，因此 COPS 配置将同时应用于许多端口。

配置的端口 ASIC 是 GE ASIC。在 GE 板卡上，每个 GE 有四个端口（端口 1-4、5-8、9-12 和 13-16）。在这些板卡上，COPS 配置将影响每组端口。在 10/100 板卡上（正如本文前面部分所讨论的那样），有两组 ASIC，即 GE ASIC 和 10/100 ASIC。每四个 10/100 ASIC 就存在一个 GE ASIC。每个 10/100 ASIC 支持 12 个 10/100 端口。COPS 将配置 GE ASIC。因此，通过 COPS 对 10/100 板卡应用 QoS 配置时，该配置将应用于所有 48 个 10/100 端口。

发出 **set qos policy-source cops** 命令启用 COPS 支持时，通过 COPS 应用的 QoS 配置将应用于交换机机箱中的所有 ASIC。可以将 COPS 配置应用于特定 ASIC。这可以使用以下命令完成：

```
Console> (enable) set port qos 5/4 policy-source cops
!-- QoS policy source set to COPS for port (s) 5/1-4. Console> (enable)
```

通过应用上面的命令，您可以看到此命令是在 GE 模块上发出的，因为有四个端口受此命令影响。

策略决策点服务器和域名

策略决策点服务器(PDPS)是外部Policy Manager过去常常存储增加到交换机的QoS配置细节。如果交换机上启用了 COPS，则必须使用将 QoS 配置详细信息提供给交换机的外部管理器的 IP 地址来配置交换机。这类似于在启用了 SNMP 时定义 SNMP 管理器的 IP 地址。

可使用以下命令标识外部 PDPS：

```
Console> (enable) set cops server 192.168.1.1 primary
!-- 192.168.1.1 is added to the COPS diff-serv server table as primary server. !-- 192.168.1.1
is added to the COPS rsvp server table as primary server. Console> (enable)
```

上面的命令将设备 192.168.1.1 标识为主决策点服务器。

当交换机与 PDPS 通信时，交换机必须属于 PDPS 上定义的域。PDPS 只与属于其定义的域的交换机通信，因此必须配置交换机以标识它所属的 COPS 域。这可以通过发出以下命令来实现：

```
Console> (enable) set cops domain name remote-cat6k
!-- Domain name set to remote-cat6k. Console> (enable)
```

上面的命令显示交换机被配置为域 remote-cat6k 的一部分。应在 QPM 中定义此域，并且应将交换机添加到此域。

相关信息

- 交换机产品支持
- LAN 交换技术支持
- 技术支持和文档 - Cisco Systems
