Comprensión de QoS en switches de la familia Catalyst 6000

Contenido

- Introducción
- Definición de QoS Capa 2
- La necesidad de QoS en un switch
- Soporte del hardware para QoS en la familia Catalyst 6000
- Compatibilidad del software de la familia Catalyst 6000 para QoS
- Mecanismos de prioridad en IP y Ethernet
- Flujo de QoS en la familia Catalyst 6000
- Colas, memoria intermedia, umbrales y mapeos
- WRED o WRR
- Configuración del puerto ASIC basado en QoS en la familia Catalyst 6000
- Clasificación y regulación del tráfico con PFC
- Servidor de políticas abiertas común
- Información Relacionada

Introducción

Este documento explica las capacidades de la Calidad de servicio (QoS) disponibles en los switches de la familia Catalyst 6000. Este documento trata las funciones de configuración de QoS y proporciona ejemplos sobre cómo puede implementarse QoS.

Este documento no debe interpretarse como una guía de configuración. Se utilizan ejemplos de configuración en este documento para ayudar a explicar las funciones de QoS del hardware y el software de la familia Catalyst 6000. Si necesita referencias de sintaxis para las estructuras de comandos de QoS, consulte las siguientes guías de configuración y comandos para la familia Catalyst 6000:

- Catalyst 6500 Family Switches

Definición de QoS Capa 2

Mientras muchos creen que la calidad de servicio (QoS) en switches de Capa 2 (L2) simplemente consiste en priorizar las tramas Ethernet, no muchos se dan cuenta de que implica mucho más que eso. QoS L2 implica lo siguiente:

1. **Programación de la Cola de Entrada:** cuando la trama ingresa al puerto, puede ser asignada a una de un número de colas basadas en puerto antes de ser programadas a ser conmutadas a un puerto de salida. Habitualmente, se utilizan varias colas en los

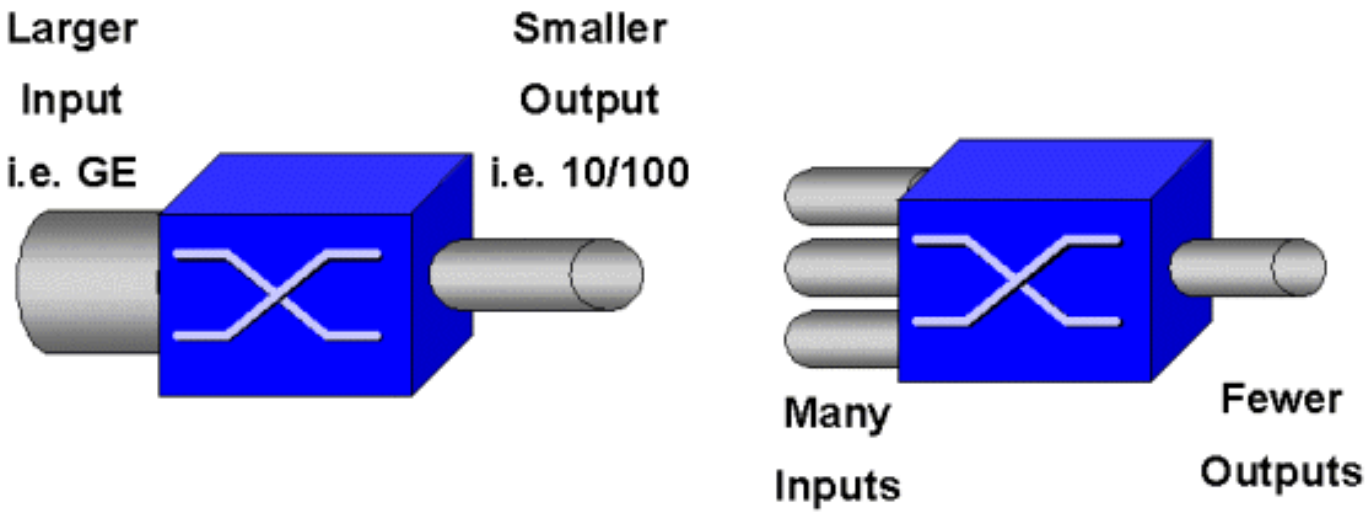
casos en que los distintos niveles de tráfico requieran diversos niveles de servicio; o bien, en los casos en que se deba mantener la latencia de switch al mínimo. Por ejemplo: los datos de voz y video basados en IP requieren una latencia reducida, por lo que es probable que se deban conmutar estos datos antes que otros como el Protocolo de Transferencia de Archivos (FTP), Web, correo electrónico, Telnet y demás.

2. **Clasificación:** el proceso de clasificación implica inspeccionar diferentes campos en el encabezado Ethernet L2, junto con los campos del encabezado IP (Capa 3 [L3]) y el encabezado de Protocolo de Control de Transmisión/Protocolo de Datagrama de Usuario (TCP/UDP) (Capa 4 [L4]) para ayudar a determinar el nivel de servicio que se aplicará a la trama cuando pase por el switch.
3. **Control de tráfico:** la regulación del tráfico es el proceso de inspección de una trama Ethernet para determinar si ha excedido un índice predefinido de tráfico en un determinado marco de tiempo (habitualmente, este marco de tiempo es una cifra fija interna del switch). Si dicha trama no condice con el perfil (es decir, forma parte de un flujo de datos que excede el límite predefinido), se la podrá eliminar; o bien, se podrá reducir el valor de Clase de Servicio (CoS).
4. **Reescritura:** el proceso de reescritura es la capacidad del switch para modificar la CoS en el encabezado de Ethernet o los bits del tipo de servicio (ToS) en el encabezado IPV4.
5. **Planificación de la cola de salida:** Luego del proceso de sobrescritura, el switch ubicará la trama de Ethernet en la cola de salida (egreso) apropiada para conmutar. El switch realizará la administración de la memoria intermedia en esta cola al asegurarse de no se desborde. Habitualmente, lo hará empleando un algoritmo Random Early Discard (RED), algoritmo mediante el cual se eliminan (descartan) tramas aleatorias de la cola. La RED ponderada (WRED) es un derivado de RED (la cual se usa en ciertos módulos de la familia Catalyst 6000) con la cual se examinan los valores de Clase de servicio (CoS) para determinar qué tramas serán eliminadas. Cuando las memorias intermedias alcanzan umbrales predeterminados, las tramas de menor prioridad por lo general se pierden dejando las tramas de mayor prioridad en la cola.

En este documento, se explican más detalladamente los mecanismos mencionados y cómo se relacionan con la familia Catalyst 6000 en las siguientes secciones.

La necesidad de QoS en un switch

Placas de interconexión enormes, millones de paquetes conmutados por segundo y switches sin bloqueo son sinónimos de muchos switches actuales. ¿Por qué es necesario QoS? La respuesta es que se debe a la congestión.



Un switch puede ser el más veloz del mundo, pero ante cualquiera de las dos situaciones que se muestran en la figura anterior, el switch se congestionará. Cuando eso suceda, y si no se han implementado funciones de administración de la congestión, se descartarán los paquetes. Cuando los paquetes se colocan, se producen las retransmisiones. Cuando se producen retransmisiones, se puede incrementar la carga de la red. En redes ya congestionadas, esto puede sumarse a problemas existentes de rendimiento y profundizar la disminución del rendimiento.

Con las redes convergentes, la administración de la congestión es aún más crítica. El tráfico sensible a la latencia como la voz y el video puede verse gravemente afectado en caso de demoras. El sólo hecho de agregar buffers a un switch tampoco aliviará necesariamente los problemas de congestión. El tráfico sensible a la latencia se debe conmutar lo más rápido posible. En primer lugar, se debe identificar a este tráfico importante mediante técnicas de clasificación y, posteriormente, implementar técnicas de administración de buffer para evitar que se descarte el tráfico de mayor prioridad durante una congestión. Finalmente, se deben incorporar técnicas de programación para conmutar paquetes importantes desde las colas lo más rápido posible. Como podrá leer en este documento, la familia Catalyst 6000 implementa todas estas técnicas, convirtiendo así al subsistema de QoS en uno de los más completos de la industria actual.

Todas las técnicas de QoS descritas en la sección anterior se estudiarán con mayor detalle a lo largo de este documento.

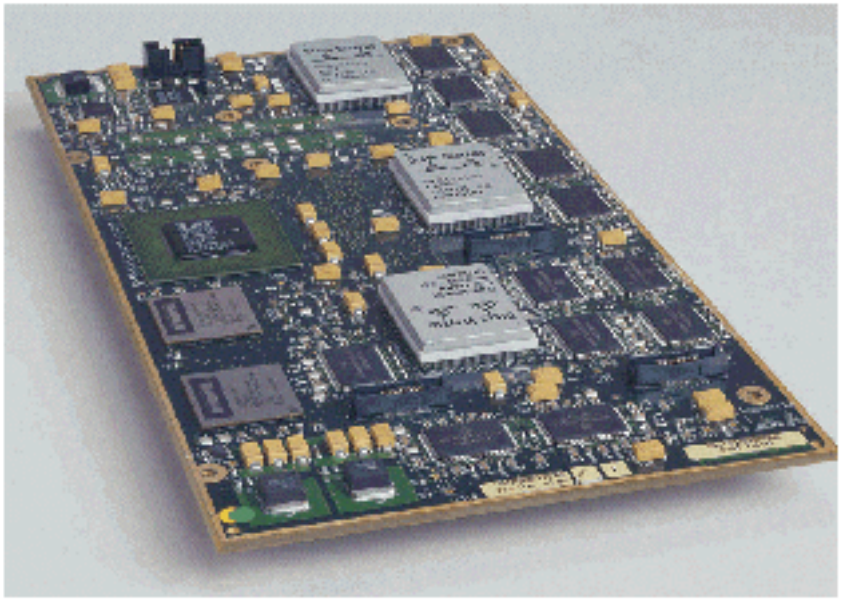
Soporte del hardware para QoS en la familia Catalyst 6000

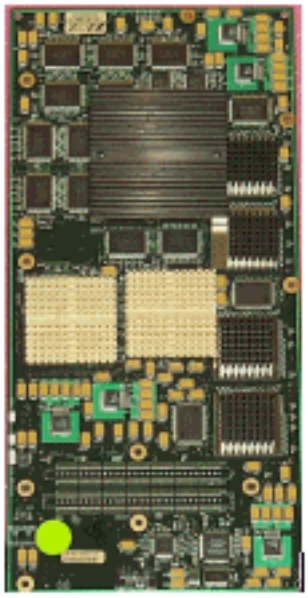
Para lograr compatibilidad con QoS en la familia Catalyst 6000, es necesario contar con cierto soporte de hardware. El hardware de soporte para QoS incluye: Multilayer Switch Feature Card (MSFC), Policy Feature Card (PFC) y Port Application Specific Integrated Circuits (ASIC) en las propias tarjetas de línea. En este documento no se exploran las capacidades de Calidad de servicio (QoS) de la MSFC sino las capacidades de Calidad de servicio (QoS) del PFC y los ASIC en las tarjetas de línea.

PFC

La PFC versión 1 es una tarjeta secundaria que se coloca sobre en el Supervisor I (SupI) y el Supervisor IA (SupIA) de la familia Catalyst 6000. La PFC2 es una nueva versión de la PFC1 y se incluye con el nuevo Supervisor II (SupII) y con algunos ASIC recientemente incorporados. Pese

a que tanto la PFC1 como la PFC2 son conocidas principalmente por su aceleración de hardware de conmutación L3, QoS es uno de sus propósitos adicionales. Las PFC se muestran a continuación.





Aunque las PFC 1 y PFC2 son básicamente iguales, presentan algunas diferencias en la funcionalidad de la Calidad de servicio (QoS). Concretamente, la PFC2 añade lo siguiente:

1. La capacidad para derribar la política de QoS a una Tarjeta de envío distribuido (DFC).

2. Decisiones políticas son sutilmente diferentes. Tanto la PFC1 como la PFC2 son compatibles con la regulación normal mediante la cual se descartan o reducen tramas si una política añadida o de microflujo devuelve una decisión fuera del perfil. Sin embargo, la PFC2 añade compatibilidad para una velocidad excesiva, lo que le indica se pueden tomar decisiones regulatorias a un segundo nivel de regulación.

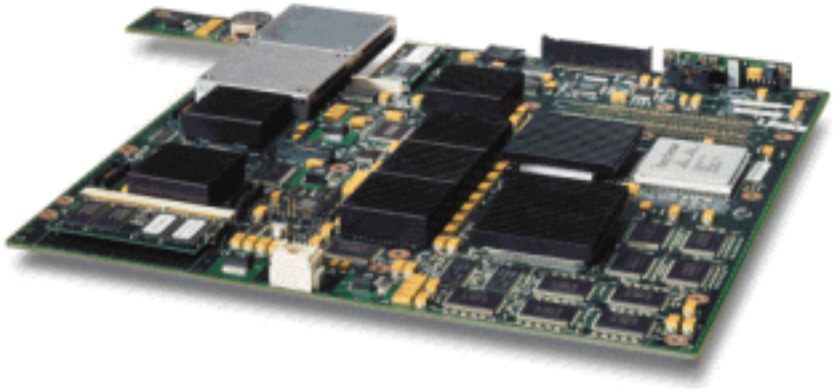
Cuando se define un regulador de velocidad excesiva, se pueden descartar o reducir los paquetes cuando exceden el límite. Si se establece un nivel de regulación de exceso, se utiliza el mapeo de DSCP de exceso para reemplazar el valor DSCP original con un valor reducido. Si sólo se establece un nivel de regulación normal, se utiliza el mapeo DSCP normal. El nivel de regulación de exceso tendrá prioridad para seleccionar reglas de mapeo cuando se establezcan ambos

niveles de regulación.

Es importante mencionar que las funciones QoS descritas en este documento y ejecutadas por los ASIC mencionados lograron excelentes niveles de rendimiento. El rendimiento de QoS en una familia base Catalyst 6000 (sin módulo de switch fabric) da como resultado 15 MPPS. Se pueden lograr mayores niveles de rendimiento en materia de QoS si se utilizan DFC.

DFC

La DFC puede asociarse al WS-X6516-GBIC como una opción. Sin embargo, es una pieza estándar en la tarjeta WS-X6816-GBIC. También puede ser compatible en otras tarjetas de línea de trama del futuro, como la recientemente presentada tarjeta de línea 10/100 (WS-X6548-RJ45) de trama, la tarjeta de línea RJ21 (WS-X6548-RJ21) de trama y la tarjeta de línea 100FX (WS-X6524-MM-FX). A continuación se muestra el DFC.



La DFC permite que la tarjeta de línea con trama (conectada por barra cruzada) ejecute la conmutación local. Para lograrlo, también debe ser compatible con cualquier regulación QoS que se haya definido para el switch. El administrador no puede configurar directamente el DFC; más bien, se encuentra bajo el control de la MSFC/PFC maestra en el supervisor activo. La PFC principal transferirá una tabla Forwarding Information Base (FIB) que, a su vez, le entrega a la DFC sus tablas de reenvío L2 y L3. Además transferirá una copia de las regulaciones QoS para que también resulten locales a la tarjeta de línea. Posteriormente, las decisiones de conmutación local podrán hacer referencia a la copia local de cualquier regulación QoS brindando así velocidades de procesamiento QoS de hardware y mayores niveles de rendimiento mediante la conmutación distribuida.

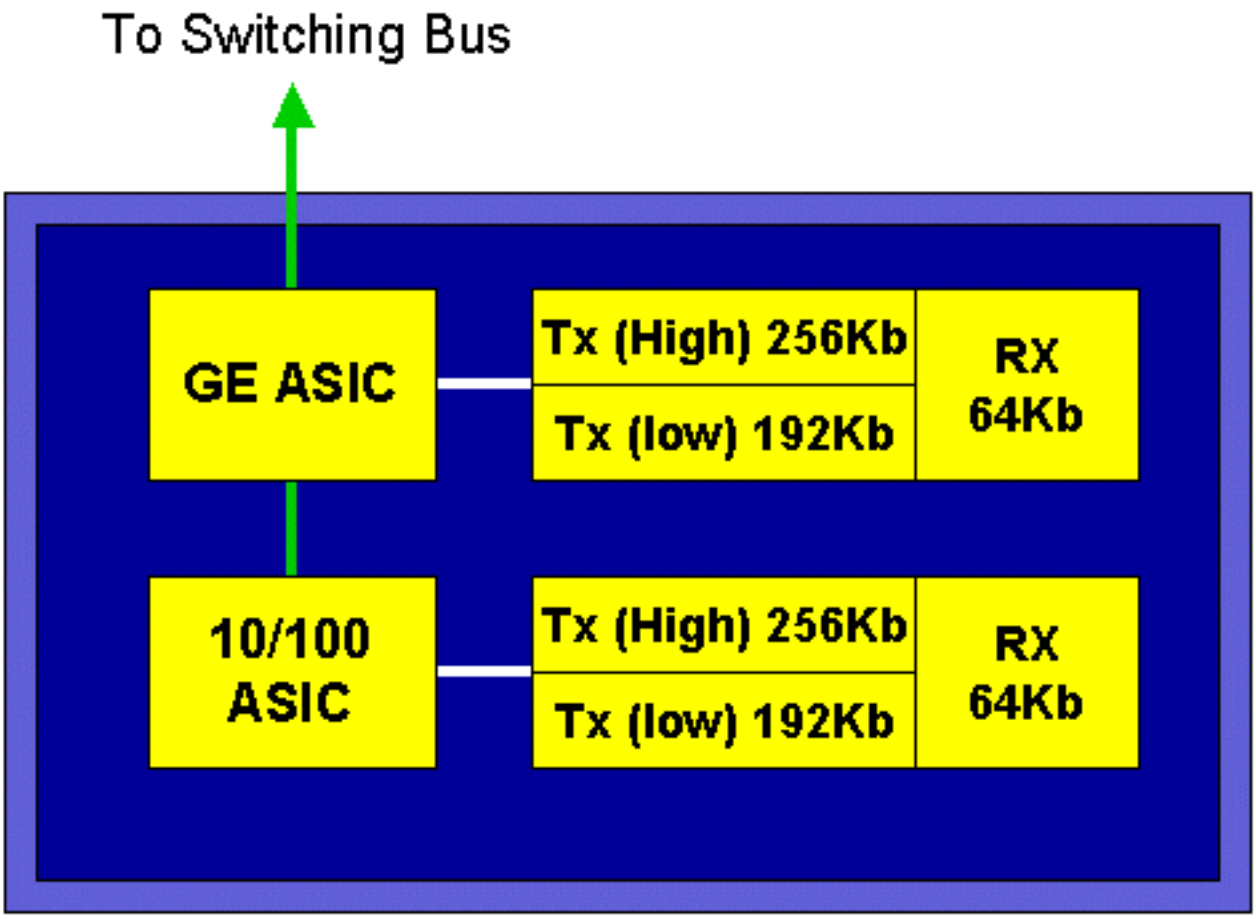
ASIC Basados en Puertos

Para completar la imagen de hardware, cada una de las tarjetas de línea implementa un número de ASIC. Aquellos ASIC implementan las colas, el almacenamiento en memoria intermedia y los umbrales utilizados para el almacenamiento temporal de tramas a medida que éstas transitan por el switch. En las tarjetas 10/100, se utiliza una combinación de ASIC para proporcionar los 48 puertos 10/100.

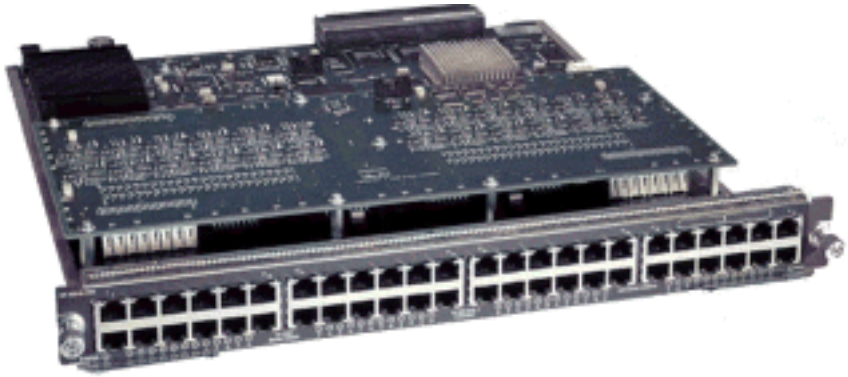
Tarjetas de Línea 10/100 Originales (WS-X6348-RJ45)

Los ASIC 10/100 proveen una serie de colas de Recepción (Rx) y Transmisión (TX) para cada puerto 10/100. El ASIC brinda 128 K de almacenamiento en memoria intermedia por cada puente 10/100 puertos. Consulte las notas de la versión para conocer los detalles acerca de qué almacenamiento en buffer por puerto se encuentra disponible en cada tarjeta de línea. Cada

puerto de esta tarjeta de línea es compatible con una cola Rx y dos colas TX, denominadas alta y baja. Esto se ilustra en el diagrama que figura a continuación.



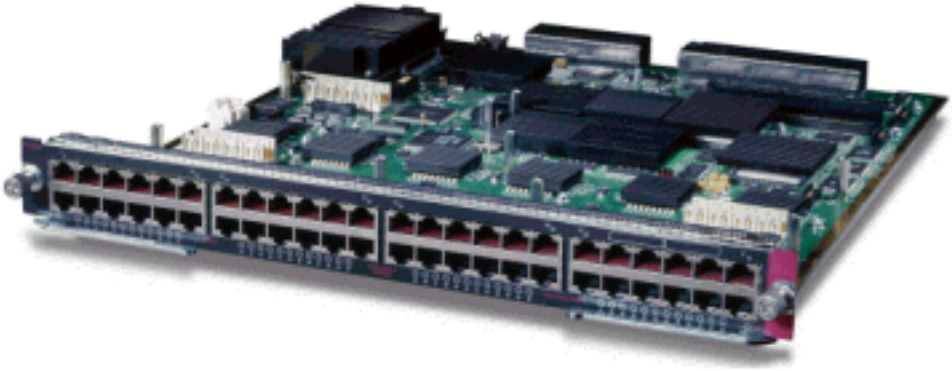
En el diagrama anterior, cada ASIC 10/100 proporciona conexión a 12 puertos 10/100. En el caso de cada puerto 10/100, se proporcionan buffers de 128 K. Los 128 K de buffers se dividen entre cada una de las tres colas. Las figuras que se muestran en la cola anterior no son las predeterminadas aunque son una representación de lo que podría configurarse. La cola Rx única obtiene 16 K y la memoria restante (112 K) está dividida entre dos colas Tx. De forma predeterminada (en CatOS), la cola alta recibe el 20 por ciento de este espacio y la cola baja recibe el 80 por ciento. En Catalyst IOS, la norma predeterminada es darle el 10 por ciento a la cola alta y el 90 por ciento a la cola baja.



Si bien la tarjeta proporciona almacenamiento en buffer de dos etapas, sólo el almacenamiento en buffer basado en ASIC 10/100 se puede manipular durante la configuración de QoS.

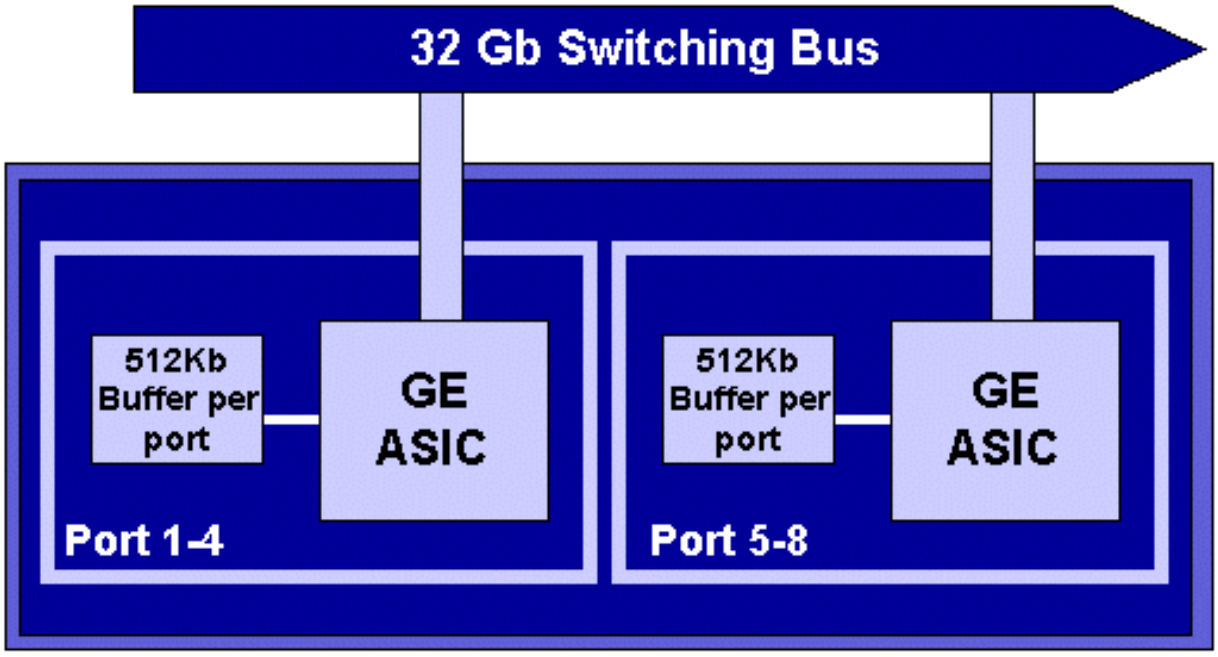
Tarjetas de Línea 10/100 (WS-X6548-RJ45) de Trama

Los nuevos ASIC 10/100, proveen unas series de colas Rx y TX para cada puerto 10/100. Los ASIC proporcionan un pool compartido de memoria disponible en todos los puertos 10/100. Consulte las notas de la versión para conocer los detalles acerca de qué almacenamiento en buffer por puerto se encuentra disponible en cada tarjeta de línea. Cada puerto de esta tarjeta de línea es compatible con dos colas Rx y tres colas TX. Una cola Rx y una cola TX quedan señaladas como cola de prioridad absoluta. Esto actúa como una cola de latencia baja, lo cual es ideal para el tráfico sensible a la latencia como la Voz a través del tráfico IP (VoIP).

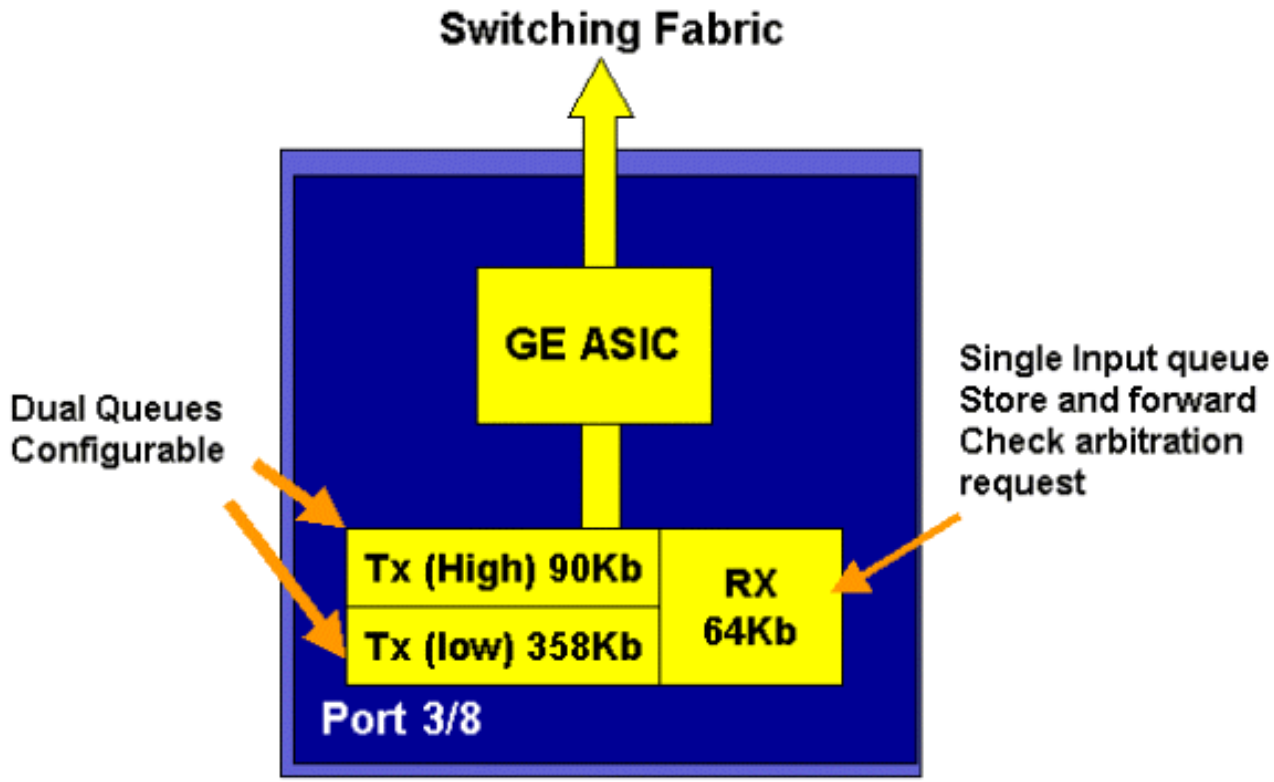


Tarjetas de Línea GE (WS-X6408A, WS-X6516, WS-X6816)

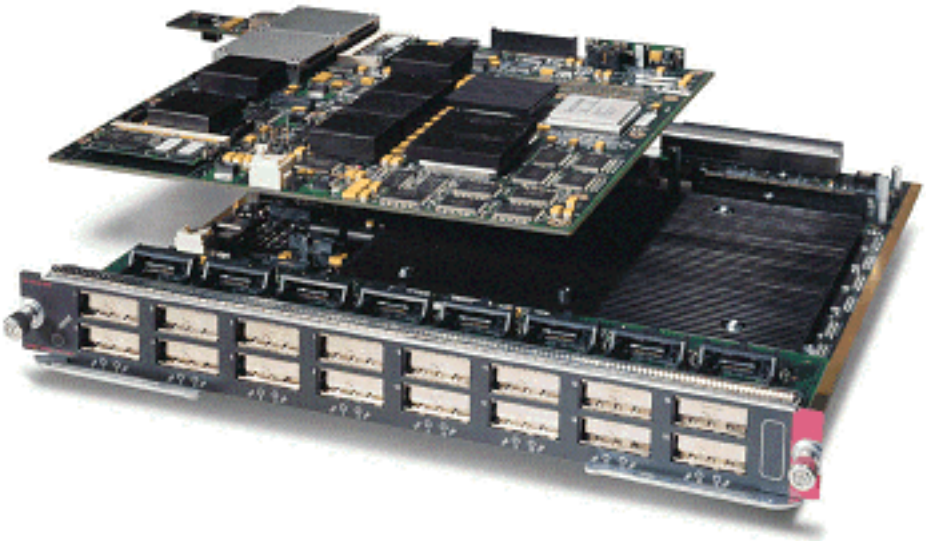
En el caso de tarjetas de línea GE, el ASIC proporciona 512 K de almacenamiento en buffer por puerto. En el diagrama que figura a continuación, se muestra una representación de la tarjeta de línea GE de ocho puertos.



Al igual que con los puertos 10/100, cada puerto GE tiene tres colas, una Rx y dos TX. Este es el valor predeterminado en la tarjeta de línea WS-X6408-GBIC y se muestra en el siguiente diagrama.



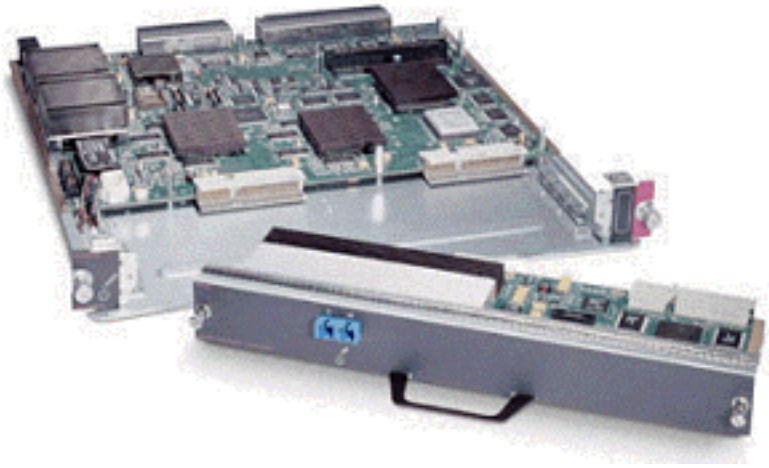
En las tarjetas de línea GE más nuevas de 16 puertos, los puertos GBIC en el SupIA y SupII, y la tarjeta GE WS-X64048-GBIC de 8 puertos, se proveen dos colas adicionales de Prioridad estricta (SP). Se asigna una cola de estricta prioridad se asigna como cola de Rx y la otra, como cola de TX. Esta cola SP se utiliza principalmente para colocar en cola el tráfico sensible a la latencia como la voz. Con la cola SP, todos los datos colocados en esta cola serán procesados antes que los datos en las colas alta y baja. Sólo cuando la cola SP esté vacía se efectuará el servicio de las colas alta y baja.



Tarjetas de Línea 10 GE (WS-X6502-10GE)

En el segundo semestre del año 2001, Cisco presentó un grupo de tarjetas de línea 10 GE con un puerto de 10 GE por tarjeta de línea. Este módulo necesita una ranura del chasis 6000. La tarjeta de línea 10 GE es compatible con QoS. En el caso del puerto 10 GE, proporciona dos colas Rx y tres colas TX. Una cola Rx y una cola TX quedan señaladas como cola SP. También se

proporciona almacenamiento en buffer, llegando a un total de 256 K de almacenamiento en buffer Rx y a 64 MB de almacenamiento en buffer TX. Este puerto implementa una estructura de cola 1p1q8t para el lado Rx y una estructura de cola 1p2q1t para el lado Tx. Las estructuras de colas se detallan más adelante en este documento.



Resumen del Hardware QoS para la Familia Catalyst 6000

Los componentes de hardware que ejecutan las funciones de QoS anteriormente señaladas en la familia Catalyst 6000 se detallan en la tabla que figura a continuación.

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

Compatibilidad del software de la familia Catalyst 6000 para QoS

La familia Catalyst 6000 es compatible con dos sistemas operativos. La plataforma de software original, CatOS se originó de la base de códigos utilizada en la plataforma de Catalyst 5000. Más recientemente, Cisco introdujo Integrated Cisco IOS ® (Native Mode) (anteriormente conocido como Native IOS), que utiliza una base de código derivada del Cisco Router IOS. Ambas plataformas de OS (CatOS e Integrated Cisco IOS [Modo Nativo]) implementan software de soporte para habilitar QoS en la plataforma de la familia de switches Catalyst 6000 empleando el hardware descrito en las secciones anteriores.

Nota: Este documento utiliza ejemplos de configuración de ambas plataformas OS.

Mecanismos de prioridad en IP y Ethernet

En el caso de cualquier servicio de QoS que se aplique a datos, debe existir una forma de etiquetar o priorizar un paquete IP o una trama Ethernet. Se utilizan los campos ToS y CoS para lograr este objetivo.

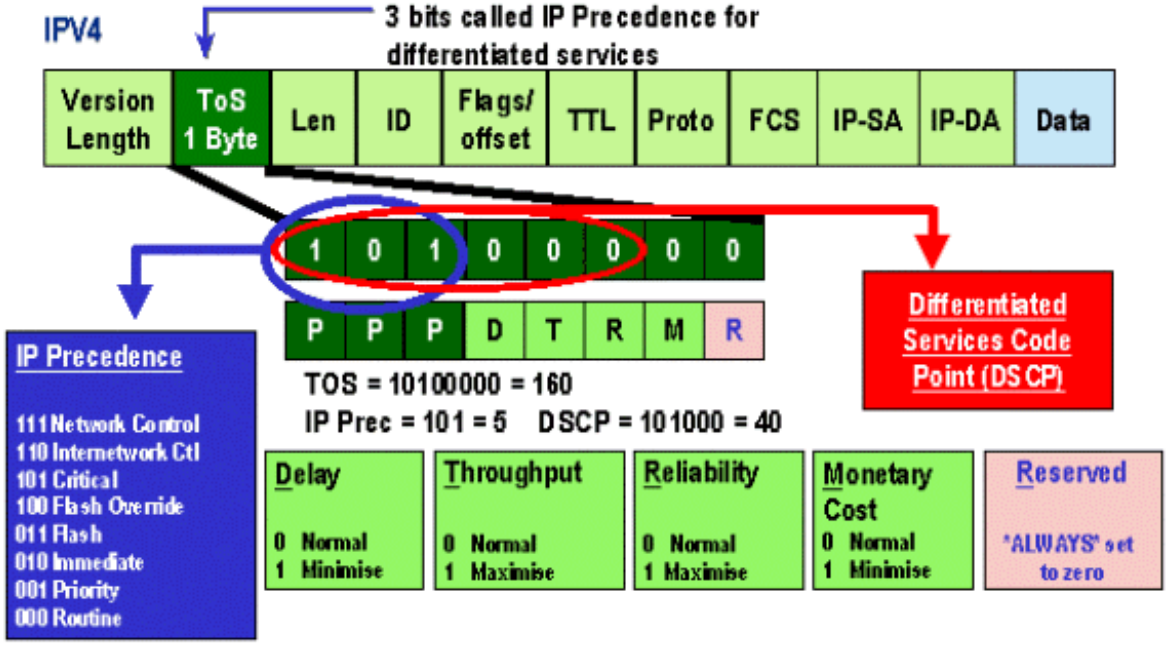
ToS

ToS es un campo de un byte existente en un encabezado IPV4. El campo ToS consta de ocho bits, de los cuales los tres primeros bits se utilizan para indicar la prioridad del paquete IP. Estos tres primeros bits son conocidos como bits de precedencia IP. Estos bits pueden configurarse de cero a siete: cero representa la prioridad más baja y siete, la más alta. Desde hace varios años está disponible el soporte para la configuración de la precedencia de IP en el IOS. El soporte para reiniciar la precedencia de IP puede llevarse a cabo a través de la MSFC o la PFC (independiente de la MSFC). La configuración de confianza de no confiable también puede borrar cualquier configuración de precedencia IP en una trama entrante.

Los valores que pueden configurarse para la precedencia de IP son los siguientes:

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

El diagrama a continuación es una representación de los bits de precedencia IP en el encabezado ToS. Los tres Bits más importantes (MIB) se interpretan como los bits de precedencia IP.



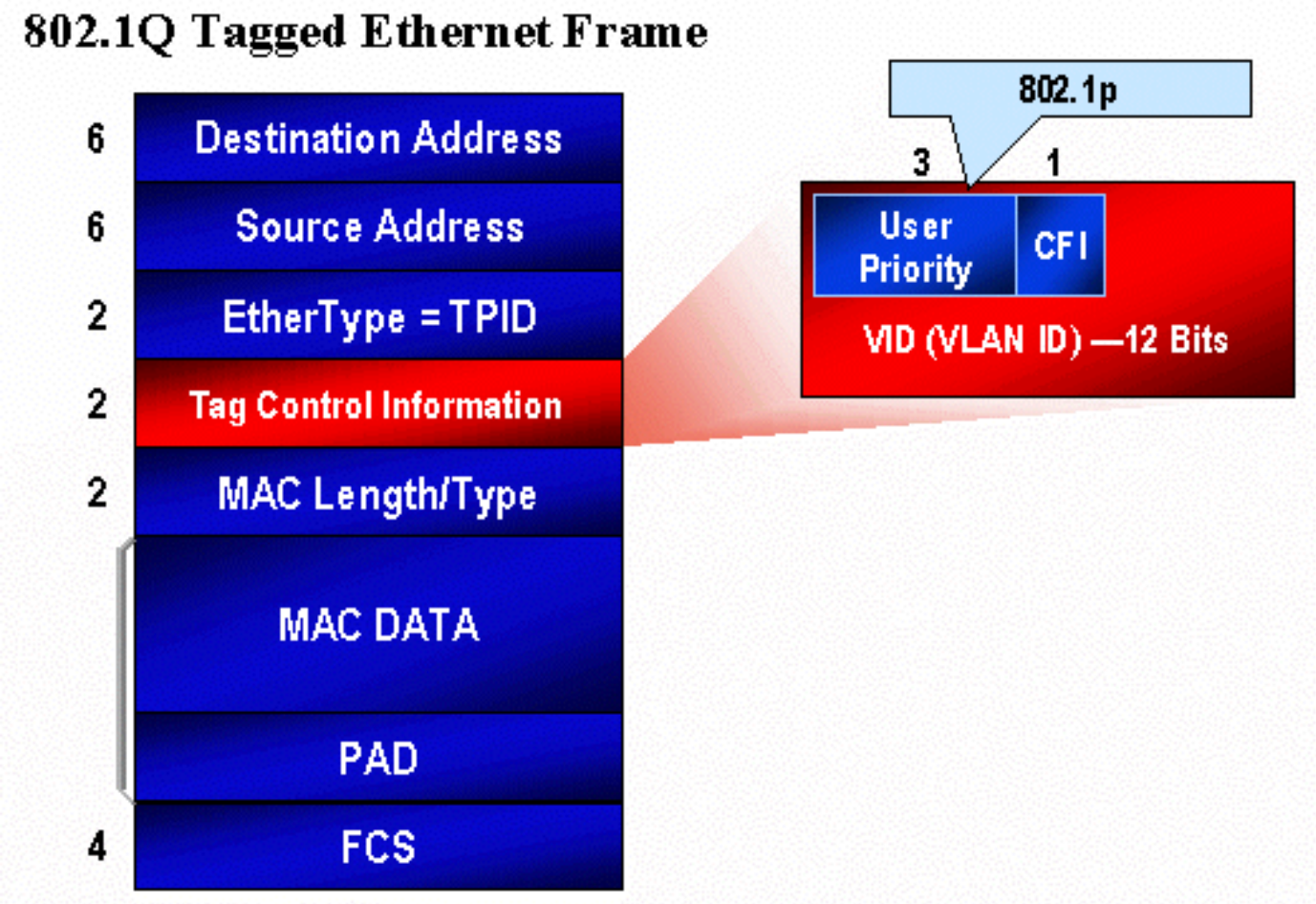
Más recientemente, se expandió el uso del campo ToS para abarcar a los seis MSB, conocidos como DSCP. DSCP genera 64 valores de prioridad (dos a la sexta) que se pueden asignar al paquete IP.

Catalyst 6000 family puede manipular el ToS. Esto puede lograrse utilizando la PFC y/o la MSFC. Cuando una trama ingrese al switch, se le asignará un valor DSCP. Este valor DSCP es usado internamente en el switch para asignar niveles de servicio (políticas QoS) definidas por el administrador. El DSCP puede ya existir en una trama y se puede usar, o el DSCP se puede derivar desde CoS existente, precedencia IP o DSCP en la trama (el puerto debe ser confiable). Se utiliza un mapa interno del switch para derivar DSCP. Con 8 valores de precedencia IP/CoS posibles y 64 valores DSCP posibles, el mapa predeterminado hará un mapeo de CoS/IPPrec 0 a DSCP 0, de CoS/IPPrec 1 a DSCP 7, de CoS/IPPrec 2 a DSCP 15, etc. Estos mapeos predeterminados pueden ser anulados por el administrador. Cuando la trama está programada para el puerto de salida, se puede volver a escribir la CoS y el valor DSCP se utiliza para obtener una nueva CoS.

CoS

CoS hace referencia a tres bits en un encabezado ISL, o bien en un encabezado 802.1Q, que se utilizan para indicar la prioridad de la trama Ethernet cuando atraviesa una red conmutada. A los propósitos de este documento, sólo haremos referencia al uso del encabezado 802.1Q. Los bits CoS en el encabezado 802.1Q son normalmente conocidos como bits 802.1p. No debe sorprendernos que existan tres bits CoS que coinciden con el número de bits utilizado para la precedencia IP. En muchas redes y con el objetivo de conservar QoS de principio a fin, es posible que un paquete atraviese los dominios L2 y L3. Para mantener la QoS, la ToS puede ser correlacionada con la CoS, y la CoS puede ser correlacionada con la ToS.

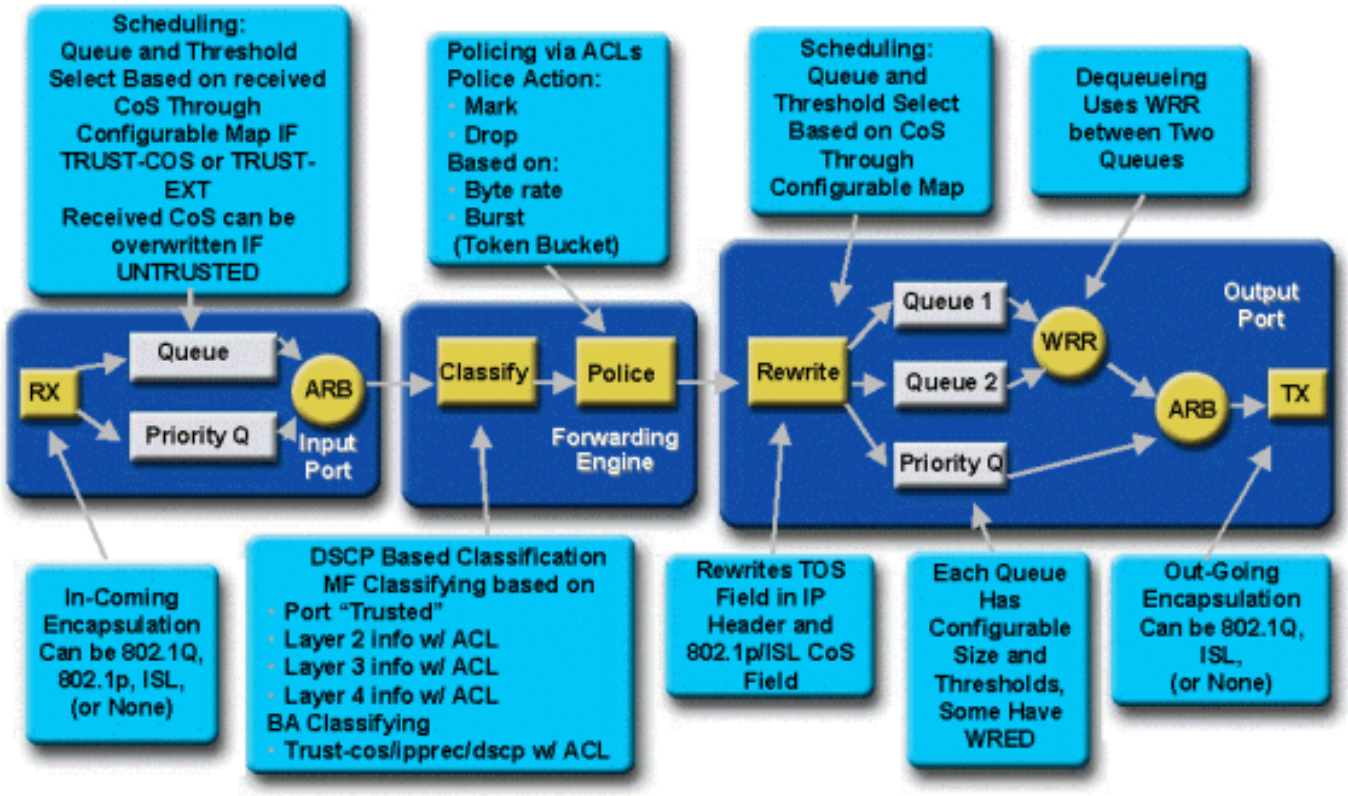
El siguiente diagrama es una trama Ethernet con etiqueta con un campo 802.1Q que consiste de un Ethertype de dos bytes y una etiqueta de dos bytes. Dentro de la etiqueta de dos bytes se encuentran los bits de prioridad del usuario (conocidos como 802.1p).



Flujo de QoS en la familia Catalyst 6000

La QoS en la familia de switches Catalyst 6000 constituye la implementación más completa de QoS efectuada en la totalidad de los switches Cisco Catalyst actuales. En las siguientes secciones se describe cómo se aplican los diversos procesos QoS a una trama cuando atraviesa el switch.

Anteriormente en este documento se aclaró que los switches L2 y L3 pueden ofrecer una buena cantidad de elementos QoS. Aquellos elementos son la clasificación, la programación de la cola de entrada, la regulación del tráfico, la reescritura y la programación de la cola de salida. La diferencia con la familia Catalyst 6000 es que estos elementos de QoS son aplicados por un motor L2 que conoce los detalles de L3 y L4, así como también sólo la información del encabezado de L2. El siguiente diagrama resume cómo la familia Catalyst 6000 implementa estos elementos.



Ingresa una trama al switch y es procesada inicialmente por el ASIC de puerto que recibió la trama. La ubicará en una cola Rx. Dependiendo de la tarjeta de línea de la familia Catalyst 6000, habrá una o dos colas Rx.

El puerto ASIC utilizará los bits de clase de servicio (CoS) como indicador de la cola en la que se ubicará la trama (si hay varias colas de entrada). Si el puerto se clasifica como no confiable, el ASIC de puerto puede sobreescribir los bits CoS existentes en base a un valor predeterminado.

La trama se pasa al motor de reenvío L2/L3 (PFC), que clasificará y, opcionalmente, controlará (límite de velocidad) la trama. La clasificación es el proceso que consiste en asignarle un valor DSCP a la trama; dicho valor será utilizado en forma interna por el switch para procesar la trama. El DSCP será derivado de una de las siguientes opciones:

1. Un valor DSCP existente, configurado antes de que la trama ingrese al switch.

2. Los bits de precedencia IP recibidos ya configurados en el encabezado IPV4. Dado que existen 64 valores de DSCP y sólo ocho valores de precedencia IP, el administrador configurará una asignación que es utilizada por el switch para derivar DSCP. Los mapeos predeterminados están listos para ser usados, en caso de que el administrador no configure otros mapas.
3. Los bits de CoS recibidos ya están configurados antes de que la trama ingrese al switch. En forma similar que con la precedencia IP, hay un máximo de ocho valores CoS, los cuales deben ser correlacionados cada uno con uno de los valores 64 DSCP. Se puede configurar este mapa, o el switch puede usar el mapa que tenga predeterminado.
4. Configurado para la trama mediante el valor predeterminado de DSCP asignado típicamente a través de una entrada de la lista de control de accesos (ACL).

Una vez asignado un valor DSCP a la trama, se aplica la regulación (límite de velocidad) del tráfico, en caso de existir una configuración de regulación. La regulación del tráfico limitará el flujo de datos a través de la PFC al descartar o marcar el tráfico que no encaje en el perfil. El concepto de falta de coincidencia con el perfil se utiliza para indicar que el tráfico ha excedido un límite

definido por el administrador como la cantidad de bits por segundo que enviará la PFC. El tráfico fuera de perfil puede perderse o el valor CoS resultar marcado. El PFC1 y el PFC2 actualmente son compatibles sólo con la regulación de entrada (limitación de velocidad). El soporte para políticas de entrada y salida estará disponible con la versión de un nuevo PFC.

Posteriormente, la PFC pasará la trama al puerto de egreso para que la procese. En este momento, se invoca un proceso de reescritura para modificar los valores CoS en la trama y el valor ToS en el encabezado IPV4. Esto se deriva del DSCP interno. La trama luego será colocada en una cola de transmisión según su valor CoS, lista para ser transmitida. Mientras la trama esté en la cola, el puerto ASIC monitoreará las memorias intermedias e implementará WRED para evitar que se desborden. Luego, se utiliza un algoritmo de programación WRR para programar y transmitir tramas desde el puerto de egreso.

Cada una de las siguientes secciones estudiará este flujo más detalladamente y ofrecerá ejemplos de configuración para cada uno de los pasos descritos anteriormente.

Colas, memorias intermedias, umbrales y mapeos

Antes de describir la configuración de QoS en detalle, es necesario explicar ciertos términos para garantizar que comprenda por completo las capacidades de configuración de QoS del switch.

Colas

Cada uno de los puertos del switch cuenta con una serie de colas de entrada y salida que se utilizan como áreas de almacenamiento temporal de datos. Las tarjetas de línea de la familia Catalyst 6000 implementan diferentes cantidades de colas para cada puerto. Generalmente, las colas se implementan en ASIC de hardware para cada puerto. En las tarjetas de la línea familiar Catalyst 6000 de primera generación, la configuración típica era una cola de entrada y dos colas de salida. En tarjetas de línea más nuevas (10/100 y GE), ASIC implementa un conjunto adicional de dos colas (una de entrada y una de salida) que permite contar con dos colas de entrada y tres colas de salida. Estas dos colas extras son colas SP especiales usadas para el tráfico susceptible a la latencia tal como VoIP. Se atienden en un estilo de SP. Es decir, si una trama llega a la cola SP, la planificación de tramas de las colas inferiores deja de procesar la trama en la cola SP. Sólo cuando la cola de SP está vacía se reanudará la programación de paquetes desde cola(s) inferior(es).

Cuando una trama llega a un puerto (para entrada o salida) en momentos de congestión, se ubicará dentro de una cola. La decisión con respecto a en qué cola está ubicada la trama, generalmente estará basada en el valor CoS en el encabezado Ethernet de la trama entrante.

En el egreso se empleará un algoritmo de programación para vaciar la cola TX (salida). WRR es la técnica que se utiliza para lograrlo. Para cada cola, se utiliza un ordenamiento para determinar cuántos datos se vaciarán de la cola antes de pasar a la cola siguiente. El ordenamiento asignado por el administrador es un número de 1 a 255, el cual se asigna a cada cola TX.

Buffers

A cada cola se le asigna una cierta cantidad de espacio en buffer para guardar datos en forma transitoria. La memoria reside en el puerto ASIC y está dividida y asignada teniendo en cuenta cada puerto. Para cada puerto GE, ASIC GE asigna 512 K de espacio de buffer. En el caso de los puertos 10/100, el ASIC de puerto reserva 64 K o 128 K (según la tarjeta de línea) de espacio en buffer por puerto. Este espacio de memoria intermedia es dividido entre la cola Rx (ingreso) y las colas TX (egreso).

Umbrales

Un aspecto de la transmisión normal de datos es que si se pierde un paquete, ese paquete será retransmitido (flujos TCP). En momentos de congestión, esto se puede añadir a la carga de la red y podría hacer que los buffers se desborden aun más. Como un medio para garantizar que los buffers no se desborden, el switch de la familia Catalyst 6000 emplea algunas técnicas para evitar que eso suceda.

Los umbrales son niveles imaginarios asignados por el switch (o por el administrador) que definen puntos de utilización de recursos en los que el algoritmo de administración de congestiones puede comenzar a descartar datos de la cola. En los puertos family de Catalyst 6000, hay cuatro umbrales que están asociados con las colas de entrada. Se suele disponer de dos umbrales asociados con colas de salida.

Estos umbrales también fueron implementados, en el contexto del QoS, con el objeto de asignar tramas con diferentes prioridades a estos umbrales. Cuando el buffer comienza a llenarse y se superan los umbrales, el administrador puede asignar diferentes prioridades a diferentes umbrales que le indican al switch qué tramas se deben descartar cuando se excede un umbral.

Asignaciones

En las secciones sobre colas y umbrales anteriores, se mencionó que el valor CoS en la trama Ethernet se utiliza para determinar en qué cola se debe colocar la trama y en qué punto de la acumulación de información del buffer se puede descartar una trama. Éste es el propósito de las correspondencias.

Cuando se ha configurado la calidad de servicio (QoS) en la familia de switches Catalyst 6000, se habilitan los mapeos predeterminados, los cuales definen lo siguiente:

- en qué umbrales son pasibles de desconexión las tramas con valores CoS específicos
- en qué cola se ubica una trama (en base a su valor CoS)

Mientras existan los mapeos predeterminados, el administrador puede anularlos. Existen mapeos para:

- Valores CoS en una trama entrante a un valor DSCP
- Valores de precedencia IP en una trama entrante a un valor DSCP
- Valores DSCP a un valor CoS para una trama saliente
- Valores CoS a umbrales de descarte en colas de recepción
- Valores CoS a umbrales de descarte en colas de transmisión
- Valores de reducción DSCP para tramas que excedan las sentencias de regulación de tráfico
- Valores CoS a una trama con una dirección MAC de destino específica

WRED y WRR

WRED y WRR son dos residentes de algoritmos sumamente poderosos en la familia del Catalyst 6000. Tanto WRED como WRR utilizan una etiqueta de prioridad (CoS) dentro de una trama Ethernet para proporcionar una administración de buffer y una programación de salida mejoradas. B

WRED

WRED es un algoritmo de administración de buffer empelado por la familia Catalyst 6000 para minimizar el impacto que se genera al descartar tráfico de alta prioridad en momentos de congestión. WRED se basa en el algoritmo RED.

Para poder comprender RED y WRED, vuelva a leer el concepto de administración de flujo TCP. La administración de flujo garantiza que el remitente TCP no sobrecargue la red. El algoritmo de inicio lento TCP forma parte de su solución. Determina que, cuando se inicia un flujo, se envíe un solo paquete antes de aguardar la confirmación de recepción. Luego se envían dos paquetes antes de recibir el ACK, y se incrementa gradualmente el número de paquetes enviados antes de recibir cada ACK. Este proceso se reiterará hasta que el flujo alcance un nivel de transmisión (es decir, que se envíen *x* cantidad de paquetes) que la red pueda administrar sin que la carga genere una congestión. En caso de registrarse una congestión, el algoritmo de inicio lento reducirá el tamaño de la ventana (es decir, la cantidad de paquetes que se envían antes de aguardar una confirmación de recepción), disminuyendo así el rendimiento general de esa sesión TCP (flujo).

RED controlará una cola cuando comience a llenarse. Una vez que se exceda un umbral determinado, se comenzará a descartar paquetes en forma aleatoria. No se presta atención a flujos específicos; más bien, se descartarán los paquetes aleatorios. Estos paquetes podrían provenir de flujos de prioridad alta o baja. Los paquetes descartados pueden ser parte de un flujo único o de varios flujos TCP. En caso de que varios flujos se vean afectados, como se describió anteriormente, se puede generar un impacto considerable en cada tamaño de ventana de flujo.

A diferencia de RED, WRED no es aleatorio cuando las tramas se pierden. WRED tiene en cuenta la prioridad de las tramas (en el caso de la familia de Catalyst 6000, utiliza el valor CoS). Con la WRED, el administrador asigna tramas con ciertos valores de la Clase de servicio (CoS) a umbrales específicos. Una vez que se exceden estos umbrales, las tramas con valores de clase de servicio (CoS) que se mapean con estos valores pueden ser eliminados. Otras tramas con valores de CoS asignadas a los umbrales mayores se mantienen en la cola. Este proceso permite que se conserven intactos flujos de prioridad más elevada al mantener sus mayores tamaños de ventana intactos y al minimizar la latencia involucrada en la transmisión de paquetes del remitente al receptor.

¿Cómo determinar si su tarjeta de línea es compatible con WRED? Ejecute el siguiente comando. En la salida, busque la sección que indica la compatibilidad con WRED en ese puerto.

```
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)
```

En caso de que WRED no se encuentre disponible en un puerto, el puerto empleará un método de liberación de cola como administración de buffer. La liberación de cola, como su nombre lo indica, simplemente libera las estructuras una vez que las memorias intermedias se han utilizado completamente.

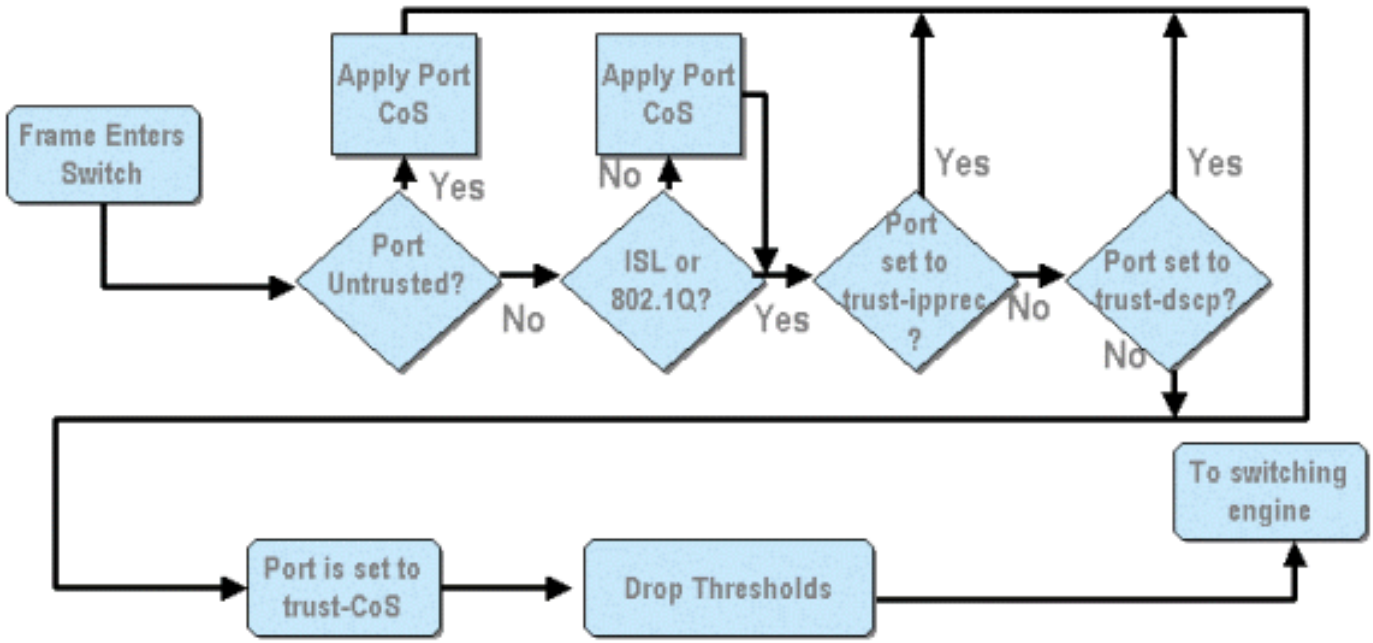
WRR

WRR se utiliza para programar tráfico de egreso desde colas TX. Un algoritmo de ordenamiento cíclico alternará entre colas TX enviando una cantidad equivalente de paquetes desde cada cola antes de pasar a la cola siguiente. El aspecto ponderado de WRR permite que el algoritmo de programación inspeccione una carga asignada a la cola. Esto permite acceso de colas definidas a más del ancho de banda. El algoritmo de programación WRR vaciará más datos de las colas identificadas que de otras colas y, por consiguiente, proporcionará una polarización para las colas designadas.

La configuración para WRR y otros aspectos de lo anteriormente descrito se explican en las siguientes secciones.

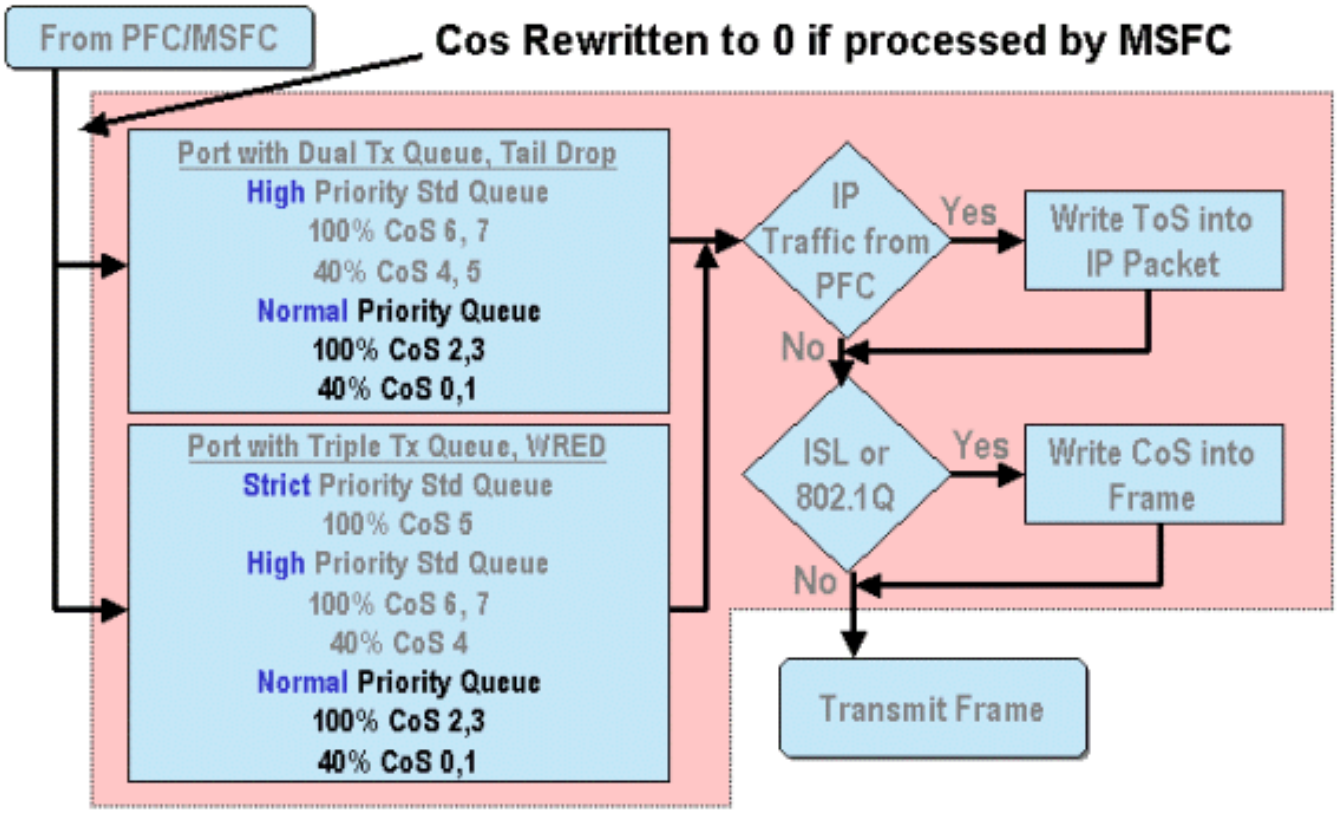
Configuración del puerto ASIC basado en QoS en la familia Catalyst 6000

La configuración de QoS les ordena al ASIC de puerto o a la PFC que ejecuten una acción QoS. En las siguientes secciones se examinará la configuración de Calidad de servicio (QoS) para estos dos procesos. En el ASIC de puertos, la configuración de la calidad de servicio (QoS) afecta al flujo de tráfico entrante y saliente.



En el diagrama anterior, se puede ver que se aplican los siguientes procesos de configuración de QoS:

1. estados de confianza de los puertos
2. aplicación de CoS (Clase de servicio) basada en puerto
3. asignación de umbral de caída Rx
4 CoS a mapas de umbral de descarte RX



Cuando se procesa una trama ya sea por el MSFC o el PCF, pasa al puerto de salida ASIC para continuar su procesamiento. Cualquier trama procesada por el MSFC reiniciará sus valores CoS a cero. Esto debe ser tenido en cuenta para el procesamiento de la Calidad del servicio (QoS) en

los puertos de salida.

El diagrama anterior muestra el procesamiento QoS que realizó el ASIC de puerto para el tráfico saliente. Algunos de los procesos invocados en un procesamiento QoS de salida incluyen lo siguiente:

1. Asignaciones de eliminación de cola de TX y umbrales de WRED
2. CoS a eliminación de cola TX y mapas WRED

Además, en el diagrama anterior no se muestra el proceso de reasignación del CoS para la trama de salida utilizando un mapa DSCP a CoS.

Las siguientes secciones estudian con más detalle las capacidades de configuración de QoS de los ASIC basados en puerto.

Nota: Resulta importante aclarar que cuando se invocan comandos QoS utilizando CatOS, los mismos se aplican normalmente a todos los puertos con el tipo de cola específico. Por ejemplo: si un umbral de descarte WRED se aplica a puertos con tipo de cola 1p2q2t, este umbral de descarte WRED se aplicará a todos los puertos en todas las tarjetas de línea que admitan este tipo de cola. Con el IOS Cat, los comandos QoS (Calidad de servicio) se aplican generalmente en el nivel de interfaz.

Activación de QoS

Antes de poder efectuar cualquier configuración QoS en la familia Catalyst 6000, se deberá habilitar QoS en el switch. Esto se logra ejecutando el siguiente comando:

CatOS

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

Integrated Cisco IOS (Modo Nativo)

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

Cuando se habilita QoS en la familia Catalyst 6000, el switch configurará una serie de valores predeterminados de QoS para el switch. Estos valores incluyen las siguientes configuraciones:

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

Puertos confiables y no confiables

Cualquier puerto dado de la familia Catalyst 6000 puede configurarse como confiable o NO confiable. El estado de confianza del puerto establece como se marcará, clasificará y programará la trama cuando atraviese el switch. De forma predeterminada, todos los puertos están en estado no confiable.

Puertos no confiables (Configuración predeterminada para puertos)

En caso de que el puerto esté configurado como puerto no confiable, una trama que ingrese inicialmente al puerto tendrá su valor de CoS y ToS restaurado por el puerto ASIC a cero. Esto significa que la trama proporcionará el servicio de prioridad inferior en su trayecto a través del switch.

Como alternativa, el administrador puede reiniciar el valor CoS de cualquier trama Ethernet que ingrese a un puerto no confiable a un valor predeterminado. Se analizarán configuraciones de este tipo en una sección posterior.

La configuración del puerto como no confiable le indicará al switch que no ejecute ningún mecanismo para evitar la congestión. La prevención de congestión es el método utilizado para descartar tramas basadas en sus valores CoS una vez que éstos excedieron los umbrales definidos para esa cola. Todas las tramas que ingresan a este puerto tendrán la misma probabilidad de ser eliminadas una vez que el buffer alcance el 100 por ciento de su capacidad.

En CatOS, un puerto 10/100 o un puerto GE puede configurarse como no confiable ejecutando el siguiente comando:

CatOS

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

Este comando posiciona al puerto 16 del módulo 3 en el estado de desconfianza.

Nota: En el caso de Integrated Cisco IOS (Modo Nativo), el software actualmente sólo admite configuración de confianza para puertos GE.

Integrated Cisco IOS (Modo Nativo)

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

En el ejemplo anterior, ingresamos la configuración de la interfaz y aplicamos la forma **no** del comando para configurar el puerto como no confiable porque es IOS.

Puertos confiables

Ocasionalmente, las tramas Ethernet que ingresan a un switch tendrán una configuración CoS o ToS que el administrador quiere que el switch mantenga cuando la trama atraviese el switch. Para este tráfico, el administrador puede configurar el estado de confianza de un puerto donde ingresa ese tráfico al switch como confiable.

Como se mencionó anteriormente, el switch utiliza un valor DSCP internamente para asignar un nivel predeterminado de servicio a esa trama. Cuando una trama ingresa a un puerto confiable, el administrador puede configurar el puerto para buscar en cualquiera de los CoS existentes, IP de precedencia, o valor de DSCP para configurar el valor DSCP interno. Como alternativa, el administrador puede configurar un DSCP predeterminado para cada paquete que ingrese al puerto.

La configuración del estado de seguridad de un puerto para que sea seguro se puede lograr

ejecutando el siguiente comando.

CatOS

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

Este comando corresponde a la tarjeta de línea WS-X6548-RJ45 y establece el estado de confianza del puerto 3/16 como “de confianza”. El switch usará el valor de clase de servicio (CoS) que se configuró en la trama entrante para configurar el DSCP interno. El DSCP podrá provenir de cualquier mapa predeterminado que fuese creado cuando se habilitó QoS en el switch o, como alternativa, de un mapa definido por el administrador. En lugar de la palabra clave trust-CoS, el administrador también puede utilizar las palabras clave trust-dscp o trust-ipprec.

En las tarjetas de línea 10/100 anteriores (WS-X6348-RJ45 y WS-X6248-RJ45), debe configurarse la confianza del puerto ejecutando el comando set qos acl. En este comando, un estado de confianza puede asignarse utilizando un subparámetro del comando **set qos acl**. Como se muestra a continuación, no se admite la configuración de CoS en puertos, en estas tarjetas de línea.

```
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.
```

El comando anteriormente mencionado indica que resulta necesario habilitar la programación de cola de salida. Por lo tanto, para puertos 10/100 en las tarjetas de línea WS-X6248-RJ45 y WS-X6348-RJ45, el comando set port qos x/y trust trust-COs debe seguir configurado, aunque para configurar los estados de confianza deba utilizarse la ACL.

Con Integrated Cisco IOS (Modo Nativo), la configuración se puede ejecutar sobre una interfaz GE y puertos 10/100 en la nueva tarjeta de línea WS-X6548-RJ45.

Integrated Cisco IOS (Modo Nativo)

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

Este ejemplo configura el estado de confianza trust del puerto GE de 5/4 a confiable. El valor de precedencia IP de la trama se usará para obtener el valor de DSCP.

Clasificación de Entrada y Configuración de Puertos Basada en CoS

Cuando ingresa a un puerto del switch, una trama Ethernet puede modificar su valor CoS si cumple con alguno de los dos criterios siguientes:

1. el puerto está configurado como no confiable, o

2. la trama Ethernet no posee un valor CoS existente configurado

Si desea volver a configurar el CoS de una trama Ethernet entrante, deberá ejecutar el siguiente comando:

CatOS

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

Este comando configura los CO de tramas Ethernet entrantes en el puerto 16 del módulo 3 a un valor de 3 cuando llega una trama sin marcar o si el puerto está configurado como no confiable.

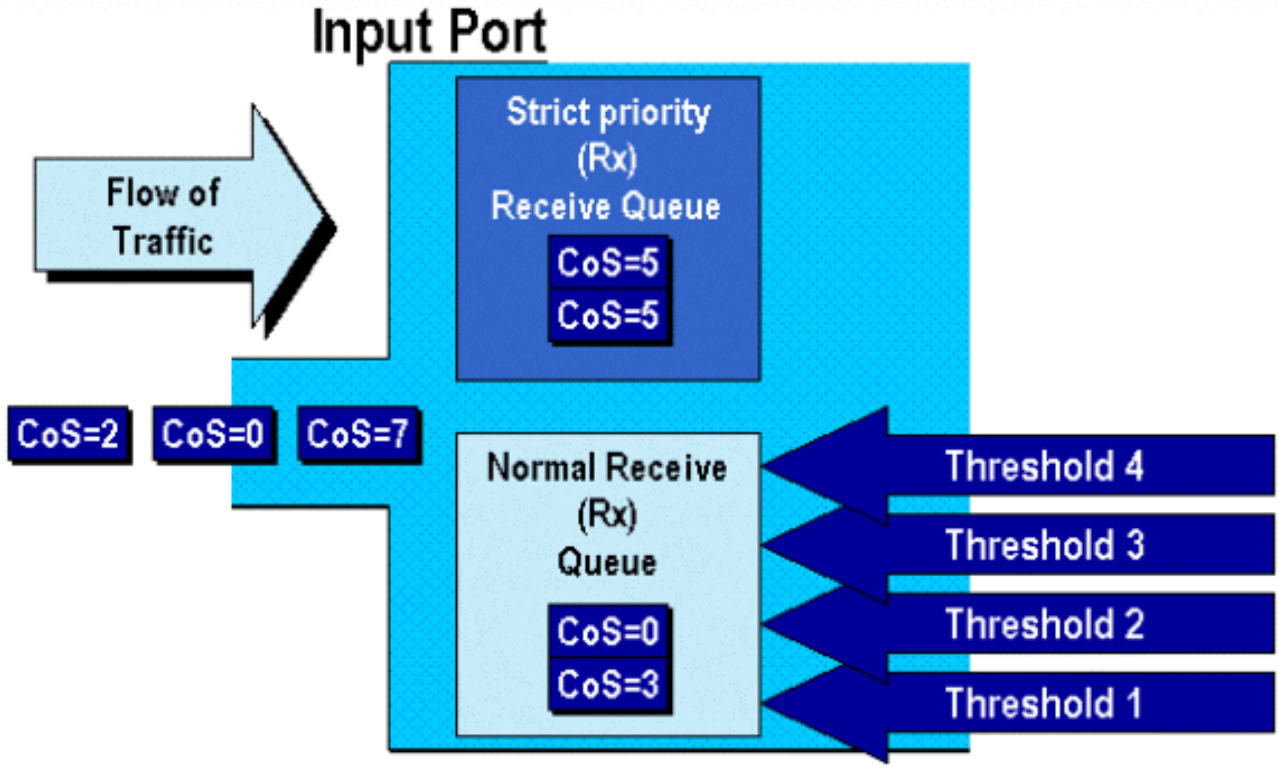
Integrated Cisco IOS (Modo Nativo)

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

Este comando configura los CO de tramas Ethernet entrantes en el puerto 13 en el módulo 5 a un valor de 4 cuando llega una trama sin marcar o si el puerto está configurado como no confiable.

Configure los umbrales de caída RX

Durante el ingreso al puerto del switch, la trama se colocará en una cola Rx. Para evitar los desbordamientos de la memoria intermedia, el puerto ASIC implementa cuatro umbrales en cada cola Rx y los usa para identificar las tramas que pueden ser descargadas una vez que se han excedido estos umbrales. El puerto ASIC utilizará las tramas establecidas como valor COs para identificar cuáles pueden dejar de transmitirse cuando se exceda el umbral. Esta capacidad permite que las tramas de mayor prioridad se mantengan en el búfer por un mayor tiempo cuando ocurre una congestión.



Como se muestra en el diagrama anterior, las tramas ingresan y se ubican en la cola. Cuando la cola comienza a llenarse, los umbrales son monitoreados por el ASIC de puerto. Cuando se pasa un umbral, las tramas con valores CO identificadas por el administrador se descartan al azar de la cola. Los mapeos de umbral predeterminados para una cola 1q4t (en las tarjetas de línea WS-X6248-RJ45 y WS-X6348-RJ45) son así:

- el umbral 1 se establece en 50% y los valores de CoS 0 y 1 se asignan a este umbral
- el umbral 2 se establece en 60% y los valores CO 2 y 3 se asignan a este umbral
- el umbral 3 se establece en 80% y los valores CO 4 y 5 se asignan a este umbral
- threshold 4 is set to 100% and COs values 6 and 7 are mapped to this threshold (el umbral 4 está configurado en 100% y valores COs 6 y 7 están correlacionados con este umbral)

En el caso de una cola 1P1q4t (que se encuentra en puertos GE), los mapeos predeterminados son los siguientes:

- el umbral 1 se establece en 50% y los valores de CoS 0 y 1 se asignan a este umbral
- el umbral 2 se establece en 60% y los valores CO 2 y 3 se asignan a este umbral
- el umbral 3 se establece en 80% y los valores CO 4 se asignan a este umbral
- threshold 4 is set to 100% and COs values 6 and 7 are mapped to this threshold (el umbral 4 está configurado en 100% y valores COs 6 y 7 están correlacionados con este umbral)
- El Valor CoS de 5 se mapea a la cola de prioridad estricta

En el caso de una cola 1p1q0t (que se encuentra en puertos 10/100 en la tarjetas de línea WS-X6548-RJ45), los mapeos predeterminados son los siguientes:

- Tramas con CoS 5 van a la cola SP Rx (cola 2), donde el switch elimina las tramas entrantes sólo cuando el buffer de cola recibida SP está completo al 100 por ciento.
- Tramas con CoS 0, 1, 2, 3, 4, 6 o 7 van a la cola RX estándar. El switch descarta las tramas entrantes cuando el buffer de cola Rx se encuentra completo al 100 por ciento.

Este umbral de caídas puede ser modificado por el administrador. Además, los valores CoS

predeterminados que se mapean a cada umbral también se pueden modificar. Diferentes tarjetas de línea aplican implementaciones de cola RX diferentes. A continuación se muestra un resumen de los tipos de cola.

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)
```

Este comando configura los umbrales de pérdida de recepción de todos los puertos de entrada con una cola y cuatro umbrales (indica 1q4t) en 20%, 40%, 75% y 100%.

A continuación se muestra el comando ejecutado en el IOS de Cisco Integrado (modo nativo).

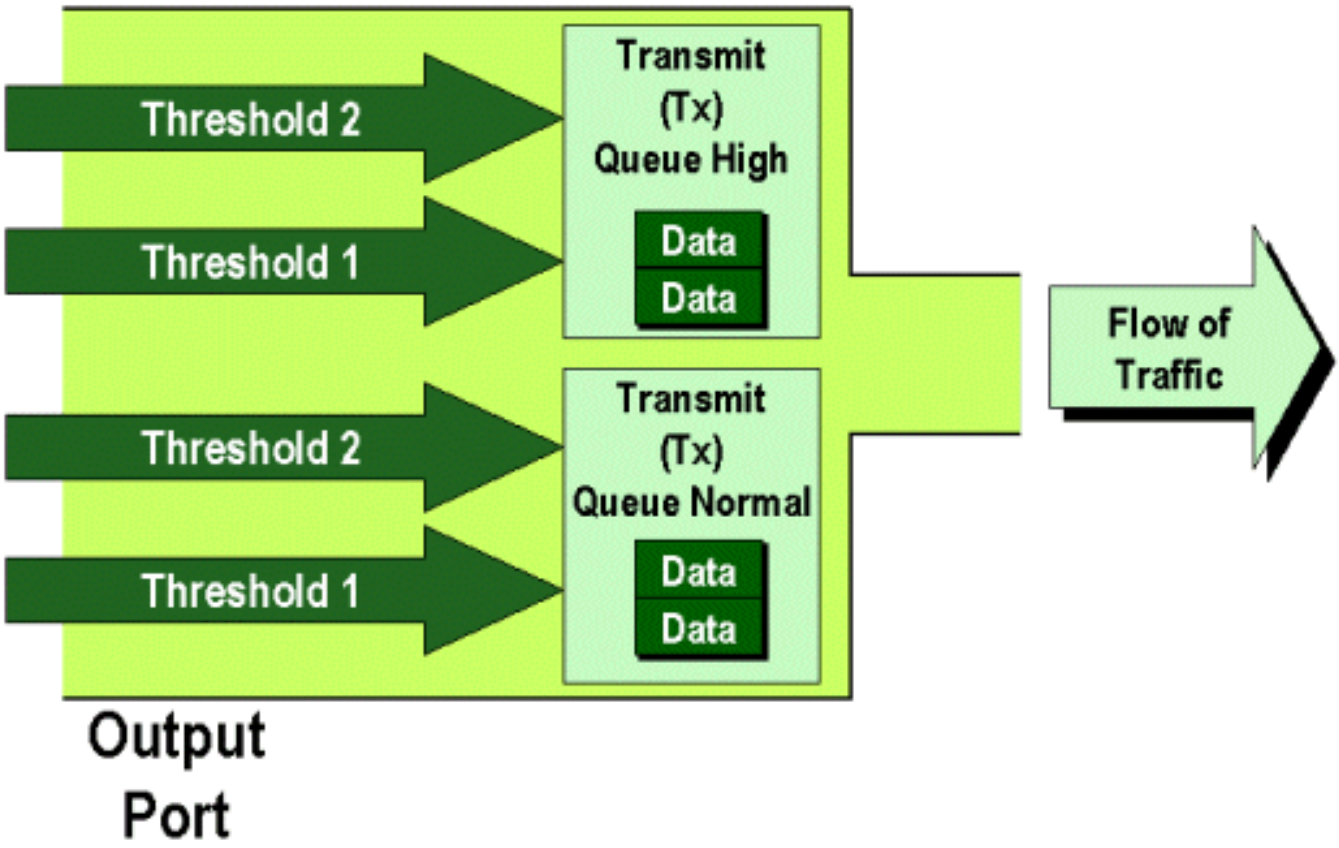
Integrated Cisco IOS (Modo Nativo)

```
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.
```

El administrador puede habilitar el umbral de caídas Rx. Actualmente, se debería emplear el comando **set port qos x/y trust trust-COs** para activar los umbrales de descarte Rx (donde *x* es el número de módulo e *y* es el puerto de ese módulo).

Configuración de los umbrales de caída TX

En un puerto de salida, el puerto tendrá dos umbrales TX que se utilizan como parte del mecanismo de prevención de congestión, la cola 1 y la cola 2. La cola 1 se denota como la cola de baja prioridad estándar y la cola 2 se denota como la cola de alta prioridad estándar. Dependiendo de la tarjeta de línea utilizada, emplearán un algoritmo de eliminación de cola o un algoritmo WRED de administración de descarte. Ambos algoritmos emplean dos umbrales para cada cola TX.



El administrador puede configurar manualmente los umbrales de la siguiente manera:

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)
```

Este comando configura los umbrales de descarte TX para la cola 1 para todos los puertos de salida con dos colas y dos umbrales (indica 2q2t) al 40% y al 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)
```

Este comando configura los umbrales de caída de WRED para la cola 1 para todos los puertos de salida con una cola SP, dos colas normales y dos umbrales (denota 1p2q2t) al 60% y el 100%. La cola 1 se define como la cola de prioridad baja normal y posee la prioridad más baja. La cola 2 es la cola normal de alta prioridad y tiene una prioridad más alta que la cola 1. La cola 3 es la cola SP y se mantiene por delante de todas las demás colas en ese puerto.

Abajo se muestra el comando equivalente emitido en el IOS de Cisco Integrado (modo nativo).

Integrated Cisco IOS (Modo Nativo)

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

Esto configura los umbrales de caída de WRED para un puerto 1p2q2t en la cola 1 hasta 40% para el umbral 1 (TX) y 100% para el umbral 2 (TX).

Puede también desactivarse el WRED si se lo requiere en el IOS integrado de Cisco (Modo nativo). El método utilizado para realizar esto es usar la forma **n"** del comando. A continuación, se muestra un ejemplo de deshabilitación de WRED:

Integrated Cisco IOS (Modo Nativo)

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

Mapeo de Dirección MAC a Valores CoS

Además de configurar COs en base a una definición de puerto global, el switch permite al administrador establecer valores COs basados en la dirección MAC de destino y el ID de VLAN. Esto permite que las tramas destinadas a destinos específicos se etiqueten con un valor CoS predeterminado. Esta configuración puede lograrse emitiendo el siguiente comando:

CatOS

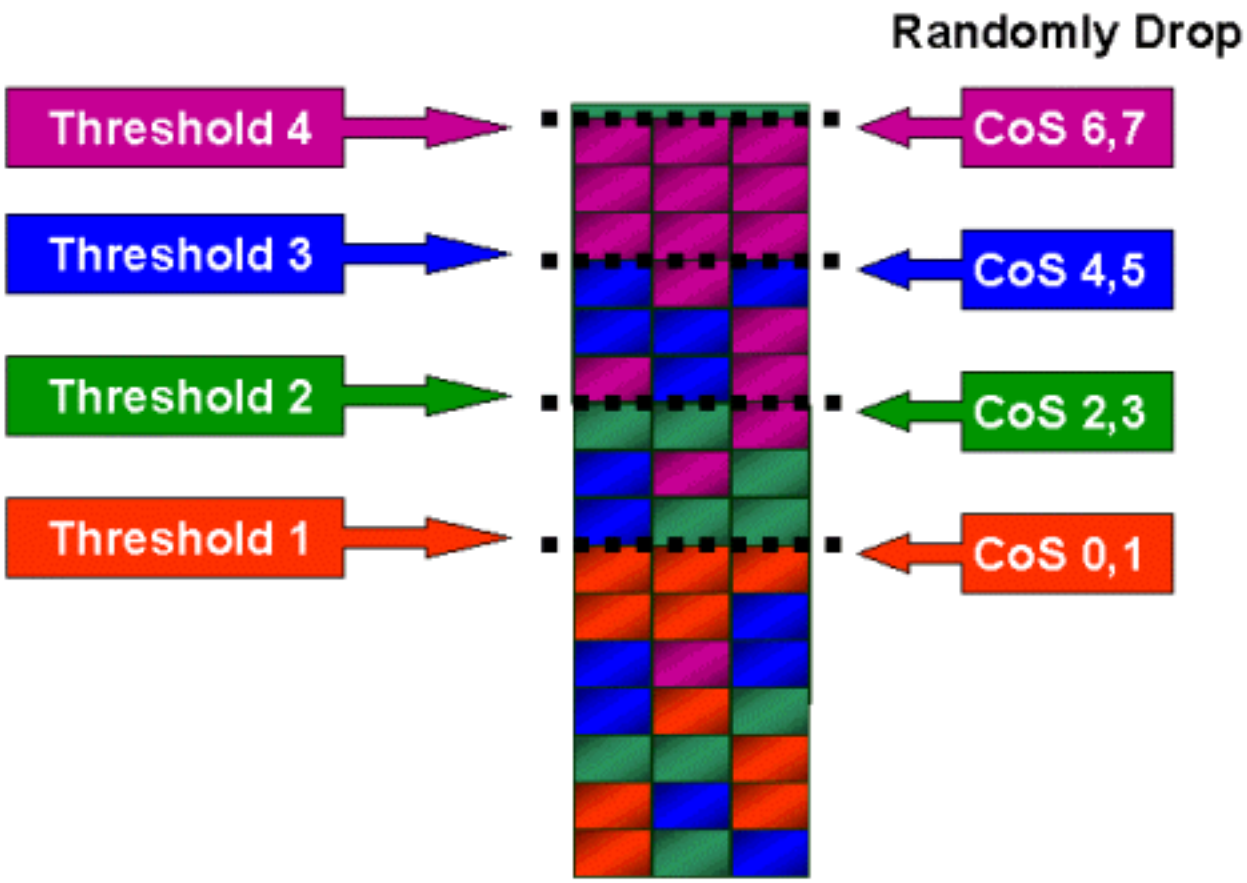
```
Console> (enable) set qos Mac-COs 00-00-0c-33-2a-4e 200 5
!-- COs 5 is assigned to 00-00-0c-33-2a-4e VLAN 200. Console> (enable)
```

Este comando configura un CoS de 5 para cualquier trama cuya dirección MAC de destino es 00-00-0c-33-2a-4e que provenía de VLAN 200.

No hay un comando equivalente en Integrated Cisco IOS (Modo Nativo). Esto es debido a que este comando sólo se admite cuando ningún PFC está presente y el Integrated Cisco IOS (Modo nativo) requiere un PFC para funcionar.

Mapeo de CoS a Umbrales

Una vez configurados los umbrales, el administrador puede entonces asignar valores CoS a estos umbrales para que, cuando se exceda el umbral, las tramas con valores CoS específicos pueda descartarse. Por lo general, el administrador asignará tramas de menor prioridad a los umbrales más bajos, a fin de mantener un tráfico de mayor prioridad en la cola en caso de que se produzca congestión.



La figura anterior muestra una cola de entrada con cuatro umbrales y también, cómo se asignaron los valores COs a cada umbral.

El siguiente resultado muestra cómo los valores CO pueden ser mapeados a umbrales:

CatOS

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

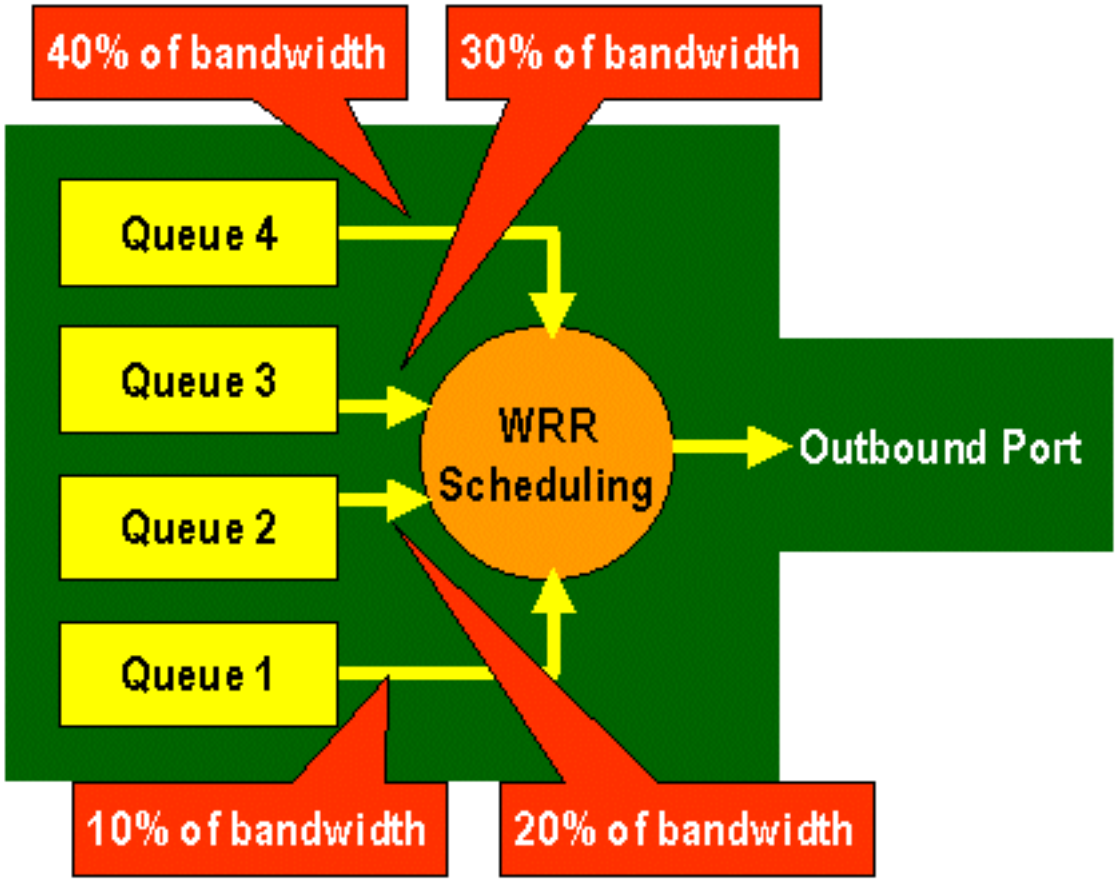
Este comando asigna valores CoS de 0 y 1 a la cola 1, umbral 1. A continuación se muestra el comando equivalente en Integrated Cisco IOS (Native Mode).

Integrated Cisco IOS (Modo Nativo)

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

Configure el ancho de banda en colas TX.

Cuando se coloca una trama en una cola de salida, ésta será transmitida utilizando un algoritmo de planificación de salida. El proceso programador de resultado usa WRR para transmitir tramas desde las colas de resultados. Dependiendo del hardware de tarjeta de línea utilizado, puede haber dos, tres o cuatro colas de transmisión por puerto.



En las tarjetas de línea WS-X6248 y WS-X6348 (con estructuras de cola 2q2t), el mecanismo WRR utiliza dos colas TX para la programación. En las tarjetas de línea WS-X6548 (con una estructura de cola 1p3q1t) hay cuatro colas TX. De estas cuatro colas TX, tres colas TX son atendidas por el algoritmo WRR (la última cola TX es una cola SP). En las tarjetas de línea GE, hay tres colas TX (usando una estructura de cola 1p2q2t); una de estas colas es una cola SP, por lo que el algoritmo WRR sólo presta servicio a dos colas TX.

Generalmente, el administrador asignará un peso a la cola TX. WRR funciona mirando el peso asignado a la cola de puerto, utilizada internamente por el switch para determinar cuánto tráfico será transmitido antes de seguir por la siguiente cola. Se puede asignar un valor de ponderación entre 1 y 255 a cada una de las colas de puerto.

CatOS

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

Este comando asigna un peso de 40 a la cola 1 y 80 a la cola 2. Esto significa efectivamente una relación de dos a uno (80 a 40 = 2 a 1) del ancho de banda asignado entre las dos colas. Este comando tiene efecto en todos los puertos con dos colas y dos umbrales en los puertos.

Abajo se muestra el comando equivalente emitido en el IOS de Cisco Integrado (modo nativo).

Integrated Cisco IOS (Modo Nativo)

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

```
Cat6500(config-if)#
```

El anterior representa una relación de tres a uno entre las dos colas. Notará que la versión Cat IOS de este comando sólo se aplica a una interfaz específica.

Mapeo de DSCP a CoS

Cuando la trama es ubicada en el puerto de egreso, el ASIC del puerto usará las CO asignadas para evitar la congestión (es decir, WRED) y también para determinar la programación de la trama (es decir, la transmisión de la misma). En este momento, el switch utilizará el mapa predeterminado para tomar el DSCP y mapa asignados de regreso a un valor CoS. En esta tabla se muestra este mapa predeterminado.

Como alternativa, el administrador puede crear un mapa que será utilizado por el switch para tomar el DSCP internos asignado y crear un nuevo valor CoS para la trama. A continuación se muestran ejemplos de cómo se utilizaría CatOS e Integrated Cisco IOS (Modo Nativo) para lograr esto.

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)
```

El comando anterior mapea los valores DSCP de 20 a 30 a un valor CoS de 5, los valores DSCP de 10 a 15 a un CO de 3 y los valores DSCP de 45 a 52 a un valor CoS de 7. Todos los demás valores DSCP utilizan el mapa predeterminado creado cuando se habilitó QoS en el switch.

Abajo se muestra el comando equivalente emitido en el IOS de Cisco Integrado (modo nativo).

Integrated Cisco IOS (Modo Nativo)

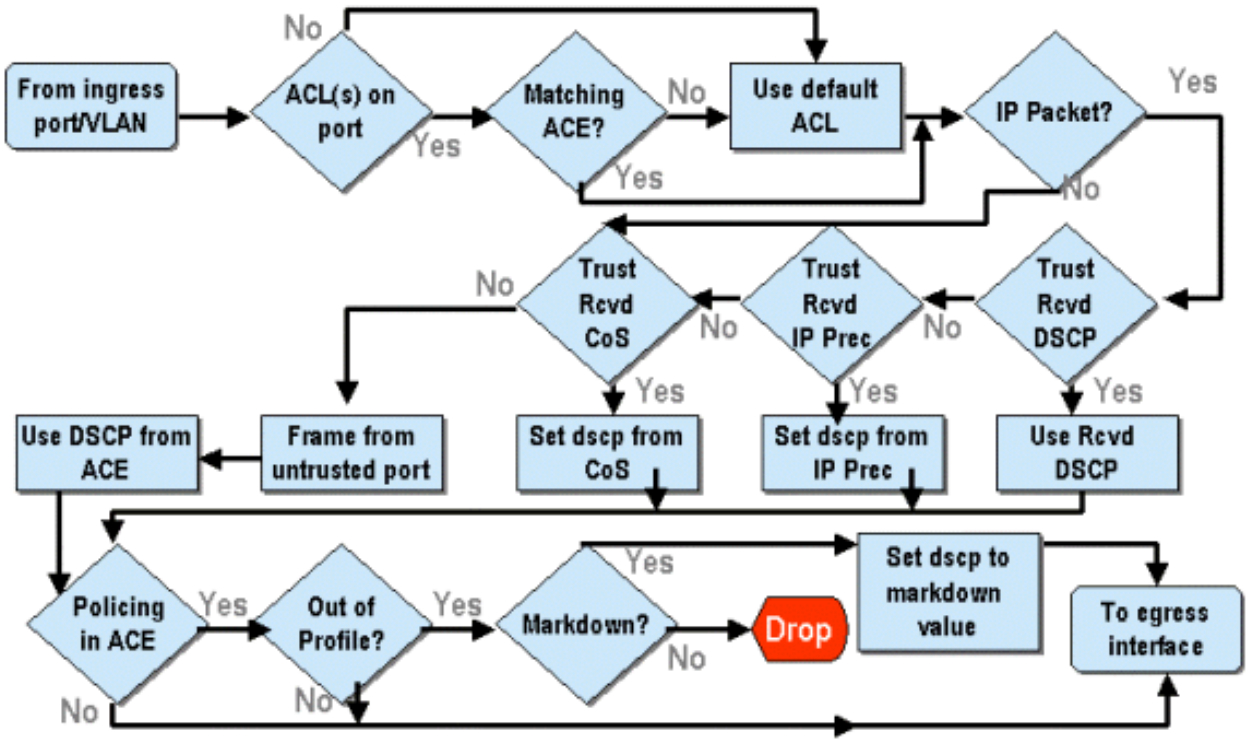
```
Cat6500(config)# mls qos map dscp-cos 20 30 40 50 52 10 1 to 3
Cat6500(config)#
```

Esto configura los valores de DSCP de 20, 30, 40, 50, 52, 10 y 1 a un valor CO de 3.

Clasificación y regulación del tráfico con PFC

La PFC es compatible con la clasificación y regulación del tráfico de tramas. La clasificación puede utilizar una ACL para asignar (marcar) una trama entrante como de alta prioridad (DSCP). La regulación del tráfico permite que un flujo de tráfico quede limitado a una cifra exacta de ancho de banda.

En las siguientes secciones se describirán estas capacidades de la PFC desde la perspectiva de las plataformas CatOS y la Integrated Cisco IOS (Modo Nativo). En el siguiente diagrama se muestra el proceso aplicado por la PFC:



Configuración de Regulación del Tráfico en la Familia Catalyst 6000 con CatOS

La función de regulación se subdivide en dos secciones, una para CatOS y otra para el IOS de Cisco Integrado (modo nativo). Ambas logran el mismo resultado final, pero se configuran e implementan de formas diferentes.

Control de tráfico

La PFC admite la capacidad de limitar (o regular) la velocidad del tráfico entrante al switch y puede reducir el flujo de tráfico a un límite predeterminado. El tráfico que exceda de ese límite puede ser eliminado o tener el valor DSCP en la trama rebajado hacia un valor inferior.

Actualmente, la función de limitación de velocidad de salida (egreso) no es compatible ni en PFC1 ni en PFC2. Esta función se añadirá en una versión de la PFC prevista para el segundo semestre de 2002 que sí será compatible con la regulación del tráfico de salida (egreso).

La regulación del tráfico es compatible tanto con CatOS como con el nuevo Integrated Cisco IOS (Modo Nativo), aunque la configuración de estas funciones es muy diferente. Las siguientes secciones describirán la configuración de la regulación en ambas plataformas OS.

Agregados y Microflujos (CatOS)

Agregados y Microflujos son los términos empleados para definir el alcance de la regulación del tráfico que ejecuta la PFC.

Un microflujo define la regulación del tráfico de un único flujo. Un flujo es definido por una sesión con una única dirección MAC SA/DA, dirección IP SA/DA y números de puerto TCP/UDP. Para cada nuevo flujo que se inicie a través de un puerto de una VLAN, se puede emplear el microflujo para limitar la cantidad de datos que recibe el switch para dicho flujo. En la definición del microflujo, los paquetes que excedan el límite de velocidad prescripto se podrán descartar o hacer que se reduzca su valor DSCP.

Del mismo modo que un microflujo, un agregado puede utilizarse para limitar la velocidad del

tráfico. Sin embargo, la velocidad del agregado se aplica al tráfico saliente en un puerto o VLAN que coincide con una ACL de QoS especificada. Puede ver al agregado como la regulación de tráfico acumulativo que coincide con el perfil en la Access Control Entry (ACE).

Tanto el agregado como el microflujo definen la cantidad de tráfico que se puede aceptar en un switch. Se puede asignar tanto un agregado como un microflujo en forma simultánea a un puerto o VLAN.

Cuando define los microflujos, puede definir hasta 63 microflujos y 1023 agregados.

Access Control Entries y ACL de QoS (CatOS)

Una ACL de QoS está conformada por una lista de ACE que definen un conjunto de reglas QoS que utiliza la PFC para procesar tramas entrantes. Las ACE son similares a una Router Access Control List (RACL). El ACE define los criterios de clasificación, de marcado y las políticas para una trama entrante. En caso de que una trama entrante coincida con los criterios establecidos en la ACE, el motor QoS procesará la trama (según lo determine la ACE).

Todo el procesamiento de QoS se ejecuta en el hardware; por lo tanto, habilitar la regulación del tráfico QoS no ejerce impacto alguno en el rendimiento del switch.

Actualmente, la PFC2 admite un máximo de 500 ACL y esas ACL pueden estar conformadas por un máximo de 32000 ACE (en total). Las cantidades reales de ACE dependerán de otros servicios definidos y de la memoria disponible en la PFC.

Existen tres tipos de Ace que se pueden definir. Ellos son IP, IPX y MAC. Las ACE IP e IPX inspeccionan la información del encabezado L3, mientras que las ACE basadas en MAC sólo inspeccionan la información del encabezado L2. También se debe aclarar que las ACE MAC sólo se pueden aplicar a tráfico que no sea IP ni IPX.

Creación de Reglas de Regulación del Tráfico

El proceso para crear una regla de regulación del tráfico implica crear un agregado (o microflujo) y, posteriormente, mapear dicho agregado (o microflujo) a una ACE.

Si, por ejemplo, el requisito fuese limitar todo el tráfico IP entrante al puerto 5/3 a un máximo de 20 MB, se deben configurar los dos pasos mencionados anteriormente.

En primer lugar, el ejemplo exige que se limite todo el tráfico IP entrante. Esto significa que debe definirse un regulador de agrupamientos. Un ejemplo podría verse de la siguiente manera:

```
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)
```

Hemos creado un regulador integral llamado test-flow (Flujo de prueba). Define una velocidad de 20000 KBPS (20 MBPS) y una ráfaga de 13. La palabra clave policed-dscp indica que cualquier dato que exceda esta política tendrá su valor DSCP marcado como se especifica en un mapa de reducción DSCP (existe uno predeterminado o el administrador puede modificarlo). Una alternativa al uso de la palabra clave policed-dscp es utilizar la palabra clave drop. La palabra calve drop simplemente perderá todo el tráfico fuera del perfil (tráfico que cae fuera del valor de ráfaga asignado).

La función de regulación trabaja en un esquema de cubeta con ficha dinámico en el que se define

una ráfaga (definida como la cantidad de datos en bits por segundo que aceptará en un intervalo de tiempo determinado (fijo)) y luego, la velocidad (que es la cantidad de datos que se vaciarán de la cubeta en un segundo). Cualquier dato que desborde a ésta se descarta o reduce su DSCP. El período de tiempo (o intervalo) mencionado anteriormente es de 0.00025 segundos (o 1/4000 de segundo) y es fijo (es decir, no se pude utilizar comando de configuración alguno para cambiar este número).

El número 13 del ejemplo anterior representa una cubeta que aceptará 13,000 bits de datos cada 1/4000 de segundo. Esto equivale a 52 MB por segundo (13K * [1 / 0.00025] o 13K * 4000). Siempre debe asegurarse de que la ráfaga esté configurada para ser igual o mayor que la velocidad a la que desea enviar los datos. En otras palabras, la ráfaga debe ser mayor o igual a la cantidad mínima de datos que desea transmitir durante un período determinado de tiempo. Si la ráfaga posee un valor inferior al que ha especificado como su velocidad, el límite de velocidad equivaldrá a la ráfaga. En otras palabras, si define una velocidad de 20 MBPS y una ráfaga calculada a 15MBPS, su velocidad sólo puede llegar a 15MBPS. La próxima pregunta que posiblemente haría es: ¿Por qué 13? Recordar que la ráfaga define la profundidad de la mencionada cubeta (sector de un archivo en disco), o en otras palabras, la profundidad de la cubeta que se utiliza para recibir los datos entrantes cada 1/4000ma de segundo. Entonces, la ráfaga podría ser cualquier número compatible con una velocidad de datos de llegada mayor o igual a 20 MB por segundo. La ráfaga mínima que uno puede usar para un límite de velocidad de 20MB es 20000/4000 = 5.

Cuando se procesa el regulador, el algoritmo de regulación de tráfico comienza completando la cubeta con fichas con un complemento de fichas completo. La cantidad de símbolos es igual al valor de ráfaga. Por lo tanto, si el valor de ráfaga es 13, el número de tokens en la cubeta es igual a 13 000. Por cada 1/4000 de segundo, el algoritmo de regulación de tráfico enviará una cantidad de datos igual a la velocidad definida dividida por 4000. Por cada bit (dígito binario) de datos enviados, consume un token de la cubeta. Al final del intervalo, se reemplazará la cubeta con un nuevo conjunto de token. El número de tokens al que reemplaza se define por la velocidad / 4000. Tenga en cuenta el ejemplo anterior para comprender lo siguiente:

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

Suponga éste es un puerto de 100 MBPS y que estamos enviando datos en un flujo constante de 100 MBPS al puerto. Sabemos que esto equivaldrá a una velocidad de entrada de 100,000,000 bits por segundo. Los parámetros aquí son una tasa de 20000 y una ráfaga de 13. En el intervalo de tiempo t0, hay un complemento completo de tokens en la cubeta (que es de 13.000). En un intervalo de tiempo t0, ingresará el primer conjunto de datos al puerto. Para este intervalo de tiempo, la velocidad de llegada será 100,000,000 / 4000 = 25,000 bits por segundo. Como nuestra cubeta de token sólo posee una profundidad de 13,000 token, sólo 13,000 bits de los 25,000 bits que ingresaron al puerto en este intervalo pueden ser enviados y 12,000 bits son descartados.

La velocidad especificada define una velocidad de reenvío de 20,000,000 bits por segundo, que equivale a 5,000 bits enviados por intervalo de 1/4000 de segundo. Por cada 5,000 bits enviados, se consumen 5,000 token. En un intervalo T1, llegan otros 25,000 bits de datos, pero la cubeta descarta 12,000 bits. Se recarga la cubeta con fichas definidas como velocidad / 4000 (equivale a 5,000 fichas nuevas). El algoritmo luego envía el siguiente complemento de datos que equivale a otros 5000 bits de datos (esto consume otros 5000 tokens) y así para cada intervalo.

Esencialmente, se descarta cualquier dato entrante que exceda la profundidad de la cubeta (definido como ráfaga). Los datos restantes luego de haber enviado datos (en coincidencia con la velocidad indicada) también se descartan, dejando así espacio para el siguiente juego de datos entrantes. Un paquete incompleto es uno que no ha sido recibido por completo dentro del intervalo de tiempo; no se lo descarta sino que se conserva hasta que se recibe completamente

en el puerto.

Este número de ráfaga asume un flujo de tráfico constante. Sin embargo, en las redes del mundo real, los datos no son constantes y el flujo es determinado por los tamaños de la ventana TCP, que incorpora confirmaciones de recepción TCP en la secuencia de transmisión. Para tener en cuenta los problemas de tamaño de las ventanas TCP, se recomienda duplicar el valor de ráfaga. En el ejemplo anterior, el valor sugerido de 13 realmente podría configurarse en 26.

Otro punto importante para tener en cuenta es que a intervalo de tiempo 0 (es decir, al comienzo del ciclo de regulación), la cubeta con ficha está llena de Tokens.

Esta política general debe ser incorporada a un QoS ACE. En una ACE, se hacen especificaciones para hacer coincidir un conjunto de criterios a una trama entrante. Evalúe el siguiente ejemplo: Quiere aplicar el agregado definido arriba a todo tráfico IP, pero específicamente para el tráfico originado desde subred 10.5.x.x y destinado para subred 203.100.45.x. La ACE se vería de la siguiente manera:

```
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)
```

El comando anterior ha creado un ACE de IP (denotado por el uso del comando set qos acl ip), que ahora se asocia a una ACL de QoS llamada test-acl. Las ACE posteriores que se crean y se asocian con test-acl de la ACL se agregan al final de la lista de ACE. La entrada ACE tiene el flujo de pruebas total asociado a la misma. A cualquier TCP que fluye con una subred de origen de 10.5.0.0 y una subred destino de 203.100.45.0 se le aplicará esta política de regulación del tráfico.

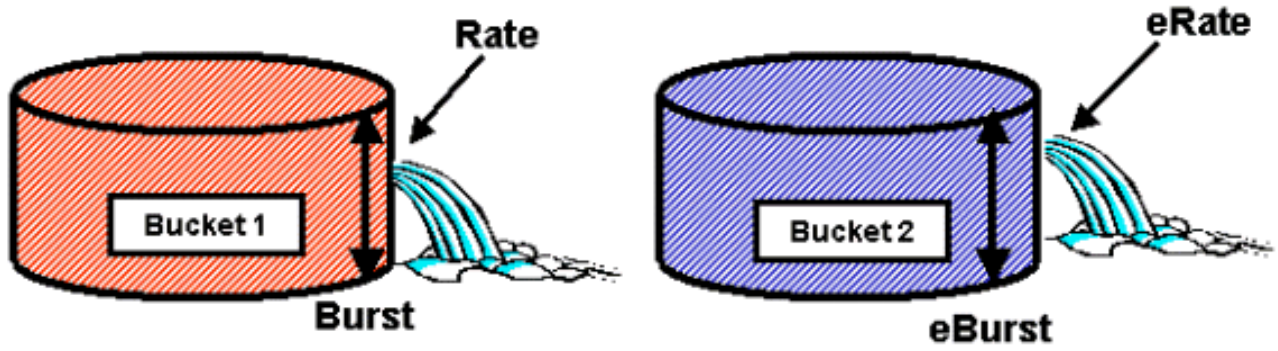
Las ACL (y las ACE asociadas) proporcionan un nivel muy granular de flexibilidad de configuración que puede utilizar el administrador. Una ACL puede estar conformada por una o más ACE, y se puede emplear la dirección de origen y/o destino, así como los valores del puerto L4, para identificar flujos particulares que requieran de regulación del tráfico.

Sin embargo, antes que se realice alguna regulación, se deberá mapear la ACL a un puerto físico o a una VLAN.

Decisiones de Regulación del Tráfico PFC2

En el caso de PFC2, se realizó un cambio en CatOS 7.1 y CatOS 7.2, que introdujo un algoritmo de cubeta dinámico dual para la regulación del tráfico. Con este nuevo algoritmo, se incorporan los siguientes dos nuevos niveles:

1. **Nivel de Regulación del Tráfico Normal:** esto se equipara con la primera cubeta y define parámetros que especifican la profundidad de la cubeta (ráfaga) y la velocidad de envío de los datos desde la cubeta (velocidad).
2. **Nivel de Regulación del Tráfico en Exceso:** equivale a una segunda cubeta y define parámetros que especifican la profundidad de la misma (e-ráfaga) y la velocidad a la que se deberían enviar los datos desde la cubeta (e-velocidad).



En este proceso los datos comienzan a llenar la primera cubeta. PFC2 acepta un flujo entrante de datos menor o igual a la profundidad (valor de ráfaga) de la primer cubeta. Los datos que desbordan la capacidad de la primera cubeta pueden ser reducidos y pasados a la segunda cubeta. La segunda cubeta puede aceptar una velocidad de datos entrantes que fluyen desde la cubeta uno a un valor inferior o igual al valor eburst. Los datos de la segunda cubeta se envían a una velocidad definida por el parámetro e-velocidad menos el parámetro velocidad. Los datos que desborden la segunda cubeta también se pueden reducir o descartar.

A continuación, se brinda un ejemplo de regulador de cubeta dinámico dual:

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

Este ejemplo establece en cambio un agregado llamado AGG1 con una velocidad de tráfico en exceso de 10 MBPS y será marcado de acuerdo con el mapa DSCP regulado. De acuerdo con la palabra clave drop (caída), se eliminará el tráfico que exceda la velocidad e (establecida en 12 MBPS).

Aplicación de Reguladores Agregados a Módulos Habilitados por DFC

Se debe aclarar que la aplicación de reguladores agregados en tarjetas de línea que no sean DFC se puede lograr gracias al modo en que la familia 6000 emplea un motor de reenvío centralizado (PFC) para reenviar el tráfico. La implementación de un motor de reenvío central permite llevar un registro de las estadísticas de tráfico de una VLAN determinada. Este proceso se puede utilizar para aplicar un regulador agregado a una VLAN.

En una tarjeta de línea habilitada por DFC, sin embargo, las decisiones de reenvío se distribuyen a esa tarjeta de línea. La DFC sólo reconocerá los puertos de su tarjeta de línea adyacente y no reconocerá el movimiento de tráfico de otras tarjetas de línea. Por este motivo, si se aplica un regulador agregado a una VLAN que cuenta con puertos miembros en diferentes módulos DFC, es posible que el regulador genere resultados inconsistentes. El motivo es que la DFC sólo puede llevar un registro de las estadísticas de puertos locales y no toma en cuenta las estadísticas de puertos de otras tarjetas de línea. Por esta razón, un regulador agregado aplicado a una VLAN con puertos miembro en una tarjeta de línea habilitada por DFC hará que la DFC regule el tráfico al límite de velocidad para puertos VLAN residentes sólo en la tarjeta de línea DFC.

Mapas de Reducción DSCP (CatOS)

Los mapas de reducción DSCP se utilizan cuando se define el regulador para reducir tráfico fuera de perfil en vez de descartarlo. El tráfico fuera de perfil se define como el tráfico que excede la configuración de ráfaga definida.

Se configura un mapa de reducción DSCP predeterminado cuando se habilita QoS. La correspondencia predeterminada de asignación de un valor inferior se detalla en esta tabla, más

arriba en el documento. La Interfaz de Línea de Comandos (CLI) permite que un administrador modifique el mapa de reducción predeterminado por medio del comando **set qos policed-dscp-map**. A continuación, se muestra un ejemplo

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

En este ejemplo se modifica el mapa DSCP regulado para reflejar que los valores DSCP 20 a 25 se reducirán a un valor DSCP de 7 y que los valores DSCP 33 a 38 se reducirán a un valor DSCP de 3.

Mapeo de Políticas de Regulación a VLAN y Puertos (CatOS)

Una vez que se construye una ACL, debe ser asignada a un puerto o a una VLAN para que esa ACL tenga vigencia.

Un comando interesante que pocos conocen es la configuración QoS predeterminada que hace que todo el proceso QoS se base en puertos. Si se aplica un agregado (o un microflujo) a una VLAN, sólo tendrá efecto sobre un puerto en caso de que dicho puerto haya sido configurado para QoS basada en VLAN.

```
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)
```

Al cambiar un proceso QoS basado en puerto a uno QoS basado en VLAN se separan automáticamente todas las ACL asignadas a ese puerto; además, se asigna cualquier ACL basada en VLAN a ese puerto.

El mapeo de la ACL a un puerto (o VLAN) se ejecuta mediante el siguiente comando:

```
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)
```

Incluso después de mapear la ACL a un puerto (o a una VLAN), la ACL sólo tendrá efecto cuando se asigne a hardware. Esto se describe en la siguiente sección. En este momento, la ACL reside en un buffer de edición temporario de la memoria. La ACL puede ser modificada mientras se encuentra en esta memoria intermedia.

Si desea retirar cualquier ACL no conectada que resida en el buffer de edición, deberá emplear el comando **rollback**. Este comando básicamente elimina la ACL de la memoria intermedia de edición.

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

Asignación de ACL (CatOS)

Para aplicar la ACL de QoS que definió (arriba), la ACL debe estar asignada a hardware. El proceso de asignación copia la ACL del buffer temporario al hardware de la PFC. Una vez que reside en la memoria PFC, la política definida en la ACL de QoS puede ser aplicada a todo el

tráfico que coincida con Aces

Para facilitar la configuración, la mayoría de los administradores ejecuta un comando **commit all**. Sin embargo, se puede asignar una ACL específica (entre muchas) que pudiera residir actualmente en el buffer de edición. A continuación, se muestra un ejemplo del comando de asignación.

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

Si desea retirar una ACL de un puerto (o de una VLAN), deberá limpiar el mapa que asocia dicha ACL a ese puerto (o VLAN) ejecutando el siguiente comando:

```
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)
```

Configurar la regulación del tráfico en la familia Catalyst 6000 con Cisco IOS integrado (modo nativo)

Integrated Cisco IOS (Modo Nativo) es compatible con la regulación del tráfico. Sin embargo, la configuración e implementación de la función de regulación del tráfico se logra empleando mapas de regulación. Cada mapa de regulación utiliza varias clases de políticas para conformar un mapa de regulación del tráfico; estas clases de políticas se pueden definir para diferentes tipos de flujos de tráfico.

Durante el filtrado, las clases de correspondencia de políticas utilizan ACL basados en el IOS e instrucciones de correspondencia de clases para identificar el tráfico que se debe controlar. Una vez que se identificó el tráfico, las clases de políticas pueden usar reguladores globales y de microflujo para aplicar las políticas de regulación a ese tráfico compatible.

Las siguientes secciones explican con más detalles la configuración de la regulación de IOS de Cisco integrado (Modo nativo).

Agregados y Microflujos (Integrated Cisco IOS [Modo Nativo])

Agregados y Microflujos son los términos empleados para definir el alcance de la regulación del tráfico que ejecuta la PFC. En forma similar a lo que sucede en CatOS, los agregados y microflujos también se utilizan en el IOS de Cisco integrado (modo nativo).

Un microflujo define la regulación del tráfico de un único flujo. Un flujo es definido por una sesión con una única dirección MAC SA/DA, dirección IP SA/DA y números de puerto TCP/UDP. Para cada nuevo flujo que se inicie a través de un puerto de una VLAN, se puede emplear el microflujo para limitar la cantidad de datos que recibe el switch para dicho flujo. En la definición del microflujo, los paquetes que excedan el límite de velocidad prescripto se podrán descartar o hacer que se reduzca su valor DSCP. Los microflujos se aplican empleando el comando de flujo de regulación que forma parte de una clase de mapa de regulación.

Para habilitar la regulación de microflujo en IOS de Cisco integrado (Modo nativo), se debe habilitar globalmente en el switch. Esto se puede lograr enviando el siguiente comando:

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

La regulación por microflujos también se puede aplicar al tráfico en puente, es decir, el tráfico que se conmuta mediante L3. Para permitir que el switch se compatible con la regulación de tráfico por microflujos en un tráfico en puente, ejecute el siguiente comando:

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

Este comando también habilita la regulación del tráfico por microflujos para tráfico multicast. En caso de que se necesite aplicarle un regulador por microflujo, se deberá habilitar este comando (**mls qos bridged**).

Del mismo modo que un microflujo, un agregado puede utilizarse para limitar la velocidad del tráfico. Sin embargo, la velocidad del agregado se aplica al tráfico saliente en un puerto o VLAN que coincide con una ACL de QoS especificada. Puede ver el total como la regulación del tráfico acumulado que coincide con un perfil de tráfico definido.

Existen dos formas de totales que pueden definirse en Cisco IOS integrado (modo nativo):

- reguladores de tráfico total por interfaz
- vigilantes globales designados

Los agregados por interfaz se aplican a una interfaz individual mediante el comando police dentro de una clase de correspondencia de políticas. Estas clases de mapas se pueden aplicar a varias interfaces, pero el vigilante controla cada interfaz por separado. Los agregados designados se aplican a un grupo de puertos y regulan el tráfico en todas las interfaces, en forma acumulativa. Los agregados designados se aplican ejecutando el comando **mls qos aggregate policer**.

Cuando define los microflujos, puede definir hasta 63 microflujos y 1023 agregados.

Creación de Reglas de Regulación del Tráfico (Integrated Cisco IOS [Modo Nativo])

El proceso para crear una regla de regulación del tráfico implica crear un agregado (o microflujo) a través de un mapa de regulación y, posteriormente, adjuntar ese mapa a una interfaz.

Analice el mismo ejemplo que se creó para CatOS. El requisito era limitar todo el tráfico IP entrante en el puerto 5/3 a un máximo de 20 MBPS.

Primero se debe crear un mapa de regulación. Cree un mapa llamado limit-traffic. Para ello, haga lo siguiente:

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

Notará inmediatamente que el mensaje del switch cambia para reflejar que se encuentra en modo de configuración para crear una clase de mapa. Recuerde que un mapa de políticas puede contener varias clases. Cada clase incluye un conjunto independiente de acciones de regulación que se pueden aplicar a diferentes flujos de tráfico.

Crearemos una clase de tráfico para limitar específicamente el tráfico entrante a 20 MBPS. Llamaremos a esta clase limit-to-20. Esto se muestra a continuación.

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

El mensaje cambia nuevamente para reflejar que usted está ahora en la configuración de la clase correspondiente (que se muestra con el -c al final del mensaje). Si desea aplicar el límite de velocidad para que coincida con algún tráfico entrante específico, puede configurar una ACL y aplicarla al nombre de la clase. Si desea aplicar el límite de 20 MBPS al tráfico que proviene de una red 10.10.1.x, ejecute la siguiente ACL:

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

Puede añadir esta ACL al nombre de la clase de la siguiente manera:

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

Una vez que haya definido su class map (correspondencia de clase), puede definir ahora su individual polices para esa clase. Puede crear agregados (utilizando la clave de policía) o microflujos (utilizando la clave de flujo de policía). Cree el agregado tal como se indica a continuación.

```
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)#
```

La sentencia de clase anterior (comando police) establece un límite de velocidad de 20000 k (20 MBPS) con una ráfaga de 52 MBPS (13000 x 4000 = 52MB). Si el tráfico coincide con el perfil y se encuentra dentro del límite de velocidad, la acción que se deberá tomar es indicar que se transmita el tráfico que coincide con el perfil mediante la sentencia confirm-action. Si el tráfico no coincide con el perfil (es decir, en nuestro ejemplo anterior, el límite de 20 MB), se configura la sentencia exceed-action para descartar el tráfico (es decir, en nuestro ejemplo, se descarta todo tráfico que supere los 20 MB).

Al configurar un microflujo, se realiza una acción similar. Si deseamos limitar la velocidad de todos los flujos de un puerto que coincidieron con un mapa de clases determinado a 200 K cada uno, la configuración de dicho flujo deberá ser similar a la siguiente:

```
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
```

Mapas de Reducción DSCP

Los mapas de reducción DSCP se utilizan cuando se define el regulador para reducir tráfico fuera de perfil en vez de descartarlo. El tráfico fuera de perfil se define como el tráfico que excede la configuración de ráfaga definida.

Se establece un mapa de reducción DSCP predeterminado cuando se habilita QoS. Esta correspondencia reducida predeterminada está enumerada en la tabla. La CLI permite que un administrador modifique la correspondencia reducida predeterminada por medio del comando set qos policed-dscp-map. A continuación, se muestra un ejemplo

```
Cat6500(config)#

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

Este ejemplo define una modificación al mapa dscp predeterminado controlado que el valor DSCP de 32 se marcará a un valor DSCP de 16. Para un puerto con este regulador definido, cualquier dato entrante con este valor DSCP que forme parte de un bloque de datos que exceda la ráfaga declarada tendrá su valor DSCP marcado a 16.

Mapeo de Políticas de Regulación a VLAN y Puertos (Integrated Cisco IOS [Modo Nativo])

Una vez que se construye una política de regulación, se la debe mapear a un puerto o a una VLAN para que tenga vigencia. A diferencia del proceso de asignación de CatOS, no existe equivalente alguno en Integrated Cisco IOS (Modo Nativo). Cuando una política se asigna a una interfaz, dicha política entra en vigencia. Si desea mapear la política anterior a una interfaz, ejecute el siguiente comando:

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

Si se mapea una política a una VLAN, deberá informarle a la interfaz que QoS está basada en VLAN ejecutando el comando **mls qos vlan-based** para cada puerto de la VLAN en el que desee aplicar la política VLAN.

```
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
```

Suponiendo que la interfaz 3/5 era parte de VLAN 100, la política denominada limit-traffic que se aplicó a VLAN 100 también se aplicará a la interfaz 3/5.

Configuración de la Clasificación en la Familia Catalyst 6000 con CatOS

El PFC brinda soporte para la clasificación de datos utilizando ACL que pueden visualizar información de los encabezados de L2, L3 y L4. En el caso de SupI, o de IA (sin PFC), la clasificación se limita a emplear las palabras clave de trust (confianza) en los puertos.

La siguiente sección describe los componentes de la configuración de Calidad de servicio (QoS) usados por el PFC para la clasificación en el CatOS.

Mapeo de CoS a DSCP (CatOS)

Al ingresar al switch, una trama tendrá un valor DSCP establecido por el switch. Si el puerto se encuentra en estado no confiable y el administrador ha utilizado la palabra clave trust-CoS, se utilizará el valor CoS configurado en la trama para determinar el valor DSCP establecido para la trama. Tal como se mencionó anteriormente, el switch puede asignar niveles de servicio a la trama a medida que transita por el switch, en base al valor DSCP interno.

Esta palabra clave no es compatible en algunos de los módulos 10/100 más antiguos (WS-X6248 y WS-X6348). En el caso de esos módulos, se recomienda emplear ACL para aplicar la configuración de CoS para datos entrantes.

Cuando Qos está habilitado, el switch crea un mapa predeterminado. Este mapa se utiliza para identificar el valor DSCP que se establecerá basado en el valor de COs. Estos mapas ya se han incluido en esta tabla del documento. Como alternativa, el administrador puede configurar un mapa único. A continuación, se muestra un ejemplo

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

El comando anterior establece el siguiente mapa:

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

Aunque es poco probable que el mapa anterior se use en una red en la realidad, sirve para dar una idea de lo que puede lograrse mediante el uso de este comando.

Mapeo de Precedencia IP a DSCP (CatOS)

De manera similar a los CO para la correspondencia DSCP, una trama puede tener un valor DSCP determinado de la configuración de precedencia IP de los paquetes entrantes. Esto sólo ocurre si el administrador configura el puerto como confiable y si ha usado la palabra clave trust-ipprec.

Cuando Qos está habilitado, el switch crea un mapa predeterminado. Anteriormente en este documento, se hace referencia a este mapa dentro de esta tabla. Este mapa se utiliza para identificar el valor DSCP que será establecido de acuerdo con el valor de precedencia IP. Como alternativa, el administrador puede configurar un mapa único. A continuación, se muestra un ejemplo:

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

El comando anterior establece el siguiente mapa:

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

Aunque es poco probable que el mapa anterior se use en una red en la realidad, sirve para dar

una idea de lo que puede lograrse mediante el uso de este comando.

Clasificación (CatOS)

Cuando se pasa una trama a PFC para el procesamiento, el proceso de clasificación se lleva a cabo sobre la trama. Para asignarle un DSCP a la trama, el PFC usará una ACL pre-configurada (o predeterminada). Dentro del ACE, una de las cuatro palabras claves se usa para asignar un valor DSCP. Éstas son:

1. TRUST-DSCP (sólo IP ACL)
2. TRUST-IPPREC (IP ACL'=s únicamente)
3. TRUST-COS (todos los ACL excepto IPX y MAC en un PFC2)
4. DSCP

La palabra clave TRUST-DSCP asume que la trama que ingresa a la PFC ya posee un valor DSCP definido con anterioridad a su ingreso en el switch. El switch mantendrá este valor DSCP.

Con TRUST-IPPREC, la PFC derivará un valor DSCP a partir de un valor de precedencia IP existente que reside en el campo ToS. El PFC usará la precedencia IP de los mapas para asignar el DSCP correcto. Se crea un mapa predeterminado cuando se habilita QoS en el switch. Como alternativa, el administrador puede crear un mapa y emplearlo para derivar el valor DSCP.

De manera similar a TRUST-IPPREC, la palabra clave TRUS-COS le ordena al PFC que derive un valor DSCP a partir de los CO en el encabezado de la trama. También habrá un COs para la correspondencia DSCP (ya sea una predeterminada de un administrador asignado) para asistir a PFC en derivar el DSCP.

La palabra clave DSCP se utiliza cuando llega una trama de un puerto no confiable. Esto presenta una situación interesante para derivar el DSCP. En este momento, se utiliza el DSC configurado en la sentencia set qos acl para derivar DSCP. Sin embargo, también en este momento se pueden emplear las ACL para derivar DSCP para tráfico basado en los criterios de clasificación establecidos en la ACE. Esto significa que en una ACE, se pueden utilizar criterios de clasificación tales como la dirección IP de origen y destino, números de puerto TCP/UDP, códigos ICMP, tipo de IGMP, números de protocolo y red IPX, direcciones MAC de origen y destino, y Ethertypes (sólo para tráfico no IP y no IPX) a fin de identificar al tráfico. Esto quiere decir que se debe configurar una ACE para que asigne un valor DSCP específico para priorizar el tráfico HTTP respecto del tráfico FTP.

Tenga en cuenta el siguiente ejemplo:

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

La configuración de un puerto como no confiable instruirá al PFC para que use un ACE con el objeto de derivar el DSCP para la trama. Si se configura la ACE con criterios de clasificación, se podrán clasificar flujos individuales para ese puerto con diferentes prioridades. Las siguientes ACE ilustran esto:

```
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
```

En este ejemplo, tenemos dos sentencias ACE. El primero identifica cualquier flujo TCP (la palabra clave any se utiliza para identificar el tráfico de origen y de destino) cuyo número de

puerto es 80 (80 = HTTP) para que se le asigne un valor DSCP de 32. La segunda ACE identifica el tráfico originado en cualquier host y destinado a cualquier host cuyo número de puerto TCP es 21 (FTP). Se le asignará un valor DSCP de 16.

Configuración de clasificación en la familia Catalyst 6000 con Cisco IOS integrado (Modo nativo)

En la siguiente sección se describen los componentes de la configuración QoS empleados para admitir la clasificación en la PFC empleando Integrated Cisco IOS (Modo Nativo).

Mapeo de CoS a DSCP (Integrated Cisco IOS [Modo Nativo])

Al ingresar al switch, una trama tendrá un valor DSCP establecido por el switch. Si el puerto se encuentra en estado confiable y el administrador ha utilizado la palabra clave mls qos trust-CoS (en puertos GE o puertos 10/100 de las tarjetas de línea WS-X6548), se utilizará el valor CoS configurado en la trama para determinar el valor DSCP establecido para la trama. Tal como se mencionó anteriormente, el switch puede asignar niveles de servicio a la trama a medida que transita por el switch, en base al valor DSCP interno.

Cuando Qos está habilitado, el switch crea un mapa predeterminado. Consulte esta tabla para obtener información sobre la configuración predeterminada. Este mapa se utiliza para identificar el valor DSCP que se establecerá basado en el valor de COs. Como alternativa, el administrador puede configurar un mapa único. A continuación, se muestra un ejemplo

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

El comando anterior establece el siguiente mapa:

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

Aunque es poco probable que el mapa anterior se use en una red en la realidad, sirve para dar una idea de lo que puede lograrse mediante el uso de este comando.

Mapeo de Precedencia IP a DSCP (Integrated Cisco IOS [Modo Nativo])

De manera similar a los CO para la correspondencia DSCP, una trama puede tener un valor DSCP determinado de la configuración de precedencia IP de los paquetes entrantes. Esto sólo ocurre si el administrador configura el puerto en modo confiado y han usado la palabra clave mls qos trust-ipprec. Esta palabra clave sólo es admitida en puertos GE y puertos 10/100 en las tarjetas de línea WS-X6548. En el caso de puertos 10/100 o de las tarjetas de línea WS-X6348 y WS-X6248, se deberán utilizar ACL para asignar la confianza de precedencia IP a los datos entrantes.

Cuando Qos está habilitado, el switch crea un mapa predeterminado. Consulte esta tabla para obtener información sobre la configuración predeterminada. Este mapa se utiliza para identificar el valor DSCP que será establecido de acuerdo con el valor de precedencia IP. Como alternativa, el administrador puede configurar un mapa único. A continuación, se muestra un ejemplo

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

El comando anterior establece el siguiente mapa:

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

Aunque es poco probable que el mapa anterior se use en una red en la realidad, sirve para dar una idea de lo que puede lograrse mediante el uso de este comando.

Clasificación (Integrated Cisco IOS [Modo Nativo])

Cuando se pasa una trama al PFC, el proceso de clasificación se puede realizar para asignar una nueva prioridad a la trama entrante. La advertencia es que esto sólo puede lograrse cuando la trama proviene de un puerto no confiable o la trama se clasificó como no confiable.

Se puede utilizar una acción de clase de mapa de regulación para:

1. trust cos
2. TRUST IP-PRECEDENCE
3. TRUST DSCP
4. NO TRUST

La palabra clave TRUST DSCP asume que la trama de llegada al PFC ya posee un valor DSCP definido con anterioridad a su ingreso en el switch. El switch mantendrá este valor DSCP.

Con TRUST IP-PRECEDENCE (Precedencia IP confiable), el PFC derivará un valor DSCP desde un valor de precedencia IP existente que reside en el campo ToS. La PFC usará un mapa de precedencia IP a DSCP para asignar el DSCP correcto. Se crea un mapa predeterminado cuando se habilita QoS en el switch. Como alternativa, el administrador puede crear un mapa y emplearlo para derivar el valor DSCP.

De manera similar a TRUST IP-PRECEDENCE, la palabra clave TRUST CoS le ordena a la PFC que derive un valor DSCP a partir del valor CoS en el encabezado de la trama. También habrá un COs para la correspondencia DSCP (ya sea una predeterminada de un administrador asignado) para asistir a PFC en derivar el DSCP.

A continuación se incluye un ejemplo de derivación de DSCP a partir de una prioridad existente (DSCP, precedencia IP o CoS).

```
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)#
```

La clase correspondiente derivará el valor DSCP de las CO en el encabezado Ethernet.

Se utiliza la forma NO TRUST de la palabra clave cuando llega una trama de un puerto no confiable. Esto permite que se le asigne un valor DSCP a la trama durante el proceso de regulación del tráfico.

Analice el siguiente ejemplo en el que se muestra cómo se puede asignar una nueva prioridad

(DSCP) a diferentes flujos entrantes a la PFC empleando la siguiente definición de regulación.

```
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)#
```

El ejemplo anterior muestra lo siguiente:

1. Se crea una ACL para identificar flujos HTTP que ingresan al puerto.
2. Un mapa de regulación denominado new-dscp-for-flow.
3. Un mapa de clases (prueba de nombres) que utiliza la lista de acceso 102 para identificar el tráfico sobre el que ejecutará su acción el mapa de clases.
4. La prueba de mapa de clase configura el estado para la trama de ingreso de confiable a no confiable y le asigna un DSCP de 24 a ese flujo.
5. Este mapa de clases también limitará el agregado de todos los flujos HTTP a un máximo de 1MB.

Servidor de políticas abiertas comunes (COPS)

COPS es un protocolo que permite que la familia Catalyst 6000 configure un proceso QoS desde un host remoto. Actualmente, COPS sólo es compatible si se utiliza CatOS y si forma parte de la arquitectura intserv para QoS. Actualmente no hay soporte (a la fecha de este documento) para COPS cuando se utiliza IOS de Cisco integrado (modo nativo). Si bien el protocolo COPS contiene la información de configuración de calidad de servicio (QoS) para el switch, no es la fuente de información de configuración de QoS. El uso del protocolo COPS exige que un administrador externo de QoS incluya las configuraciones de QoS en el host para el switch. El administrador externo de QoS iniciará el push descendente de tales configuraciones al switch a través del protocolo COPS. QoS Policy Manager (QPM) de Cisco es un ejemplo de un Administrador externo de QoS.

Este documento no pretende explicar el funcionamiento del QPM sino mas bien la configuración necesaria en el switch para admitir configuraciones de QoS externas mediante el uso de QPM.

Configuración COPS.

De forma predeterminada, la compatibilidad con COPS se encuentra deshabilitada. Para poder utilizar COPS en el switch, se lo debe habilitar. Esto se puede lograr enviando el siguiente comando:

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

Al iniciarse este comando, se originarán ciertos valores QoS de configuración predeterminados desde el servidor COPS. Estos incluyen los siguientes:

1. Mapeos CoS a cola

2. Asignaciones de umbrales de colas de entrada y salida
3. Asignaciones de ancho de banda WRR
4. Cualquier política de regulación por agregados o microflujos
5. Mapas DSCP a CoS para tráfico de egreso
6. Listas de control de acceso (ACL)
7. Asignaciones de CoS de puerto predeterminadas

Cuando se realizan las configuraciones de QoS (Calidad de servicio) usando COPS, es importante comprender que la aplicación de estas configuraciones se realiza de manera diferente. COPS se utiliza para configurar el puerto ASIC más que para configurar los puertos directamente. El ASIC de puerto normalmente controla un grupo de puertos, por eso, la configuración COPS se asigna a una cantidad de puertos al mismo tiempo.

El puerto ASIC configurado es el ASIC GE. En las tarjetas de línea GE, hay cuatro puertos por cada GE (puertos 1-4, 5-8, 9-12, 13-16). En estas tarjetas de línea, la configuración de COPS afecta a cada grupo de puertos. En tarjetas de línea 10/100 (tal como ya se analizó en este documento), existen dos grupos de ASIC, GE y 10/100. Hay una ASIC GE por cada cuatro ASIC 10/100. Cada ASIC 10/100 admite 12 puertos 10/100. COPS configura la ASIC GE. En consecuencia, cuando se aplica la configuración de QoS a las tarjetas de línea 10/100 a través de COPS, la configuración se aplica a los 48 puertos 10/100.

Cuando se habilita el soporte COPS mediante la ejecución del comando set qos policy-source cops, se aplica la configuración de calidad de servicio (QoS) a través de COPS en todos los ASIC en el chasis del switch. Se puede aplicar la configuración COPS a ASIC específicas. Esto se puede lograr con el siguiente comando:

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

Puede ver en la aplicación del comando anterior que este comando fue ejecutado en un módulo GE ya que los cuatro puertos fueron impactados por el comando.

Servidores de Punto de Decisión de Regulación y Nombres de Dominio

Los Servidores del punto de decisión de políticas (PDPS) son los administradores de políticas externos usados para almacenar los detalles de configuración QoS enviados al switch. Si se habilita COPS en el switch, se debe configurar el switch con la dirección IP del administrador externo que proporcionará los detalles de la configuración QoS al switch. Esto es similar a lo que sucede cuando el SNMP está habilitado y la dirección IP del administrador de SNMP está definida.

El comando para identificar el PDPS externo se realice por medio de:

```
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)
```

El comando anterior identifica el dispositivo 192.168.1.1 como el servidor de punto de decisión primario.

Cuando el switch se comunica con el PDPS, debe ser parte de un dominio definido en el PDPS. El PDPS sólo se comunicará con los switches que forman parte de su dominio definido de manera que el switch sea configurado para identificar el dominio COPS al que pertenece. Esto se realiza

ejecutando el siguiente comando:

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

El comando anterior muestra el switch configurado como parte del dominio con el nombre remote-cat6k. Este dominio debería definirse en QPM y debería agregarse el switch a ese dominio.

Información Relacionada

- Soporte de Productos de Switches
- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems
