# Supervisión de QoS y marca con los Supervisores Engine basados en el IOS del Catalyst 4000/4500

## Contenido



## Introducción

La función de regulación determina si el nivel de tráfico se encuentra dentro del perfil especificado (contrato). La función de regulación del tráfico permite tanto la eliminación del tráfico fuera de perfil como la reducción del tráfico hasta un valor distinto de Punto de código de servicios diferenciados (DSCP) a fin de hacer cumplir el nivel de servicio contratado. DSCP es una medida del nivel de calidad de servicio (QoS) del paquete. Junto con DSCP, la precedencia IP y la clase de servicio (CoS) también se utilizan para transmitir el nivel QoS del paquete.

El policing no se debe confundir con el modelado de tráfico, aunque ambos se aseguren de que el tráfico permanezca dentro del perfil (contrato). La regulación de tráfico no almacena el tráfico en memoria temporal, de modo que el retardo de la transmisión no se ve afectado. En lugar de almacenar los paquetes fuera de perfil en la memoria intermedia, la política aplicada los perderá o los marcará con un nivel de QoS diferente (marcación DSCP). El modelado de tráfico mitiga el tráfico fuera de perfil y alisa las ráfagas de tráfico, pero afecta al retardo y a la variación de retraso. El shaping se puede aplicar solamente en una interfaz saliente, mientras que la vigilancia se puede aplicar en ambas interfaces entrante y saliente.

El Catalyst 4000/4500 con el Supervisor Engine 3, 4 y 2+ (SE3, SE4, SE2+ de ahora en adelante en este documento) soporta el policing en entrante y las direcciones de salida. El modelado de tráfico también se soporta, no obstante este documento tratará solamente de las Políticas y marcado. El marcado es un proceso de cambio del nivel del paquete QoS según una política.

## prerrequisitos

## Requisitos

No hay requisitos específicos para este documento.

## Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

# QoS Policing y Parámetros de Marcación

La regulación se configura definiendo correspondencias de políticas QoS y aplicándolas a los puertos (QoS basadas en puertos) o a VLAN (QoS basadas en VLAN). El regulador se define por parámetros de velocidad y de ráfaga y también por acciones para tráfico dentro y fuera del perfil.

Existen dos tipos de reguladores del tráfico admitidos: agregado y por interfaz. Cada vigilante puede aplicarse a diversos puertos o redes VLAN.

El vigilante global actúa sobre el tráfico a lo largo de todas las VLAN o todos los puertos aplicados. Por ejemplo, aplicamos al vigilante global para limitar el tráfico del Trivial File Transfer Protocol (TFTP) al 1 Mbps en los VLA N 1 y 3. Tal policer permitirá el 1 Mbps del tráfico TFTP en los VLA N 1 y 3 junto. Si aplicamos un regulador para cada interfaz, éste limitará el tráfico TFTP en las VLAN 1 y 3 a 1 Mbps cada una.

**Nota:** Si se aplica la regulación de ingreso y la de egreso al paquete, se actuará según la decisión más grave. Es decir, si el regulador de ingreso especifica para caer el paquete y el regulador de egreso especifica para marcar el paquete abajo, el paquete será caído. La Tabla 1 sintetiza la acción de QoS sobre el paquete cuando se le aplican ambas políticas de ingreso y egreso.

**Tabla 1:** Acción de QoS según la política de ingreso y egreso

| | **Ingress policy** | | | |
|---|---|---|---|---|
| **Egress policy** | **Transmit** | **Drop** | **Markdown$_i$** | **Mark$_i$** |
| **Transmit** | Transmit | Drop | Markdown$_i$ | Mark$_i$ |
| **Drop** | Drop | Drop | Drop | Drop |
| **Markdown$_e$** | Markdown$_e$ | Drop | Markdown$_e$ | Markdown$_e$ |
| **Mark$_e$** | Mark$_e$ | Drop | Mark$_e$ | Mark$_e$ |

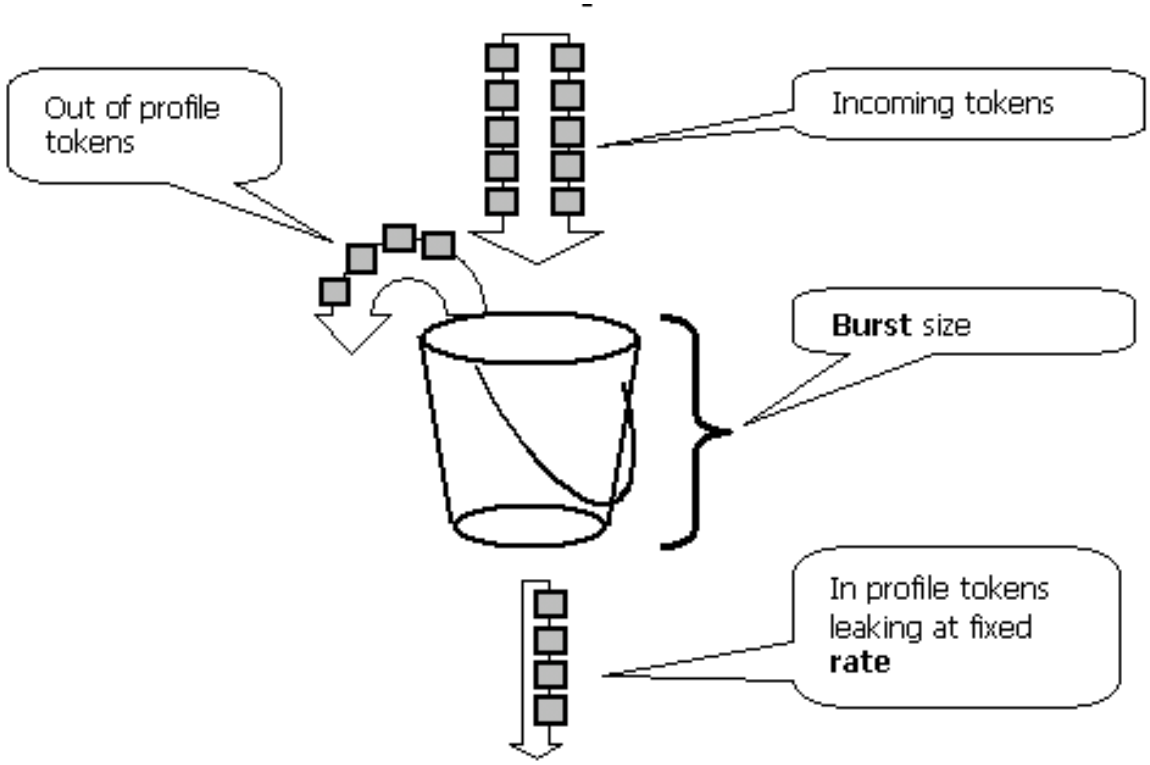
Se implementa el Catalyst 4000 SE3, SE4, hardware de calidad de servicio SE2+ de una manera tal que el marcado real del paquete ocurra después del regulador de egreso. Esto significa que si bien la política de ingreso remarca el paquete (mediante la marcación del supervisor o la marcación regular), la política de egreso aún verá a los paquetes marcados con el nivel de QoS original. La política de egreso verá el paquete como si la política de ingreso no lo hubiese marcado. Esto significa el siguiente:

- La marcación de egreso invalida a la marcación de ingreso.
- La política de egreso no puede coincidir con los niveles QoS modificados por la marcación de ingreso.

Otras repercusiones importantes son las siguientes:

- No es posible marcar y rebajar dentro de la misma clase de tráfico en la misma política.
- Los vigilantes globales son por-dirección. Es decir, si aplican a un vigilante global al ingreso y a la salida, habrá dos vigilantes globales, uno en la entrada y uno en la salida.
- Cuando un vigilante global es aplicado dentro de la directiva a los VLA N y a la interfaz física, habrá con eficacia dos vigilantes globales - uno para las interfaces VLAN y otro para las interfaces físicas. Actualmente no es posible vigilar las interfaces VLAN y las interfaces físicas juntas en totalización.

El policing en el Catalyst 4000 SE3, SE4, SE2+ cumple con el concepto de contador dinámico, pues el modelo abajo ilustra. Las fichas correspondientes a los paquetes de tráfico entrante son ubicadas en una cubeta (# de fichas = tamaño del paquete). Periódicamente, se elimina un número definido de tokens (que provienen de la velocidad configurada) del sector de almacenamiento. Si no hay lugar en el bloque de memoria para acomodar un paquete entrante, el paquete se considera fuera de perfil y es suprimido o marcado para su eliminación, de acuerdo con la acción de regulación de tráfico configurada.




Cabe observar que el tráfico no se almacena en el bloque de memoria, como podría entenderse por el modelo que se muestra arriba. El tráfico real ahora circula a través de la cubeta. El compartimiento se utiliza solamente para decidir a si el paquete es en perfil o fuera de perfil.

Observe que implementación de hardware exacta del policing podría ser diferente, cumple funcionalmente al modelo antedicho.

Los siguientes parámetros controlan la operación de regulación de tráfico:

- La tarifa define cuántos tokens se quitan en cada intervalo. Esto fija de manera eficaz la velocidad de tráfico ordenado. Todo tráfico por debajo de la velocidad se considera dentro del perfil.
- El intervalo define con qué frecuencia los tokens son eliminados del bloque de memoria. El intervalo establecido es de 16 nanosegundos (16 seg * 10-9). No puede cambiarse el intervalo.

- La ráfaga define la cantidad máxima de fichas que la cubeta puede contener.

Refiera a las Políticas y marcado que comparan en la sección de los Supervisores Engine basados en el IOS del Catalyst 6000 y del Catalyst 4000/4500 en el extremo de este documento para las diferencias en la explosión entre el Catalyst 6000 y el Catalyst 4000 SE3, SE4, SE2+.

El supervisor asegura que, si se examina cualquier período de tiempo (de cero a infinito), el supervisor no permitirá más de

```
<rate> * <period> + <burst-bytes> + <1 packet> bytes
```

del tráfico a través del vigilante durante este período.

El Catalyst 4000 SE3, SE4, hardware de calidad de servicio SE2+ tiene cierto granularity para el policing. De acuerdo con la velocidad configurada, la desviación máxima de la velocidad es 1.5% de ella.

Al configurar la velocidad de ráfaga, usted necesita tener en cuenta que algunos protocolos (tales como TCP) implementen los mecanismos de control de flujo que reaccionan en la pérdida del paquete. Por ejemplo, el TCP reduce la ventana por la mitad para cada paquete perdido. Cuando está limpiada a una cierta velocidad, la utilización de link eficaz será más baja que la velocidad configurada. Uno puede aumentar la explosión para alcanzar una mejor utilización. Un buen comienzo para tal tráfico sería fijar la explosión para ser igual dos veces a la cantidad de tráfico enviada con la velocidad deseada durante el Round-Trip Time (RTT). Por la misma razón, no es recomendado para evaluar la operación de regulador de tráfico por el tráfico orientado a la conexión, pues mostrará generalmente el menor rendimiento que permitido por el policer.

**Nota:** Tal vez, el tráfico sin conexión también reaccione de diferente manera ante la regulación. Por ejemplo, el Sistema de archivos de la red (NFS) usa bloques que podrían consistir en más de un paquete de Protocolo de datagrama del usuario (UDP). Un paquete caído pudo accionar muchos paquetes (bloque entero) que se retransmitirán.

Por ejemplo, lo que sigue es un cálculo de la explosión para una sesión TCP, con una velocidad de tráfico ordenado de 64 kbps y de un TCP RTT de 0.05 segundos:

```
<burst> = 2* <RTT> * <rate> = 2 * 0.05 [sec] * 64000/8 [bytes/sec] = 800 [bytes]
```

**Nota:** el **<burst>** está para una sesión TCP, así que debe ser escalado para hacer un promedio del número esperado de sesiones que van vía el policer. Esto es sólo un ejemplo, por lo tanto, en cada es necesario evaluar los requerimientos y el compartimiento del tráfico/aplicación con relación a los recursos disponibles a fin de poder determinar los parámetros de regulación.

La acción de regulación es suprimir el paquete (supresión) o cambiar el DSCP del paquete (marcado). A fin de marcar el paquete, la correspondencia DSCP regulada deberá modificarse. El DSCP limpiado valor por defecto comenta el paquete al mismo DSCP, es decir, ninguna marca abajo ocurre.

**Nota:** Los paquetes podrían ser enviados como defectuosos cuando un paquete fuera de perfil es marcado a un DSCP a una cola de salida diferente que el DSCP original. Por este motivo, si el ordenar de los paquetes es importante, se recomienda para marcar abajo de los paquetes fuera de perfil al DSCP asociado a la misma cola de salida que los paquetes del en perfil.

## Las características Políticas y marcadas soportaron en Supervisores Engine basados en el IOS del Catalyst 4000/4500

El ingreso (interfaz entrante) y el policing de la salida (interfaz saliente) se soportan en el Catalyst 4000 SE3, SE4, SE2+. El switch admite 1024 reguladores de tráfico de ingreso y 1024 de egreso. Dos ingresos y dos reguladores de egreso son utilizados por el sistema para el comportamiento predeterminado del ninguno-policing.

Observe que cuando el vigilante global es aplicado dentro de la directiva a un VLA N y a una interfaz física, un adicional entrada del regulador de tráfico del hardware se utiliza. Actualmente no es posible vigilar las interfaces VLAN y las interfaces físicas juntas en totalización. Eso puede modificarse en futuras versiones del software.

Todas las versiones de software incluyen el soporte para limpiar. El Catalyst 4000 soporta la declaración de coincidencia válida hasta 8 por la clase, y hasta 8 clases se soportan por el directiva-mapa. Las declaraciones de coincidencia válida son como sigue:

- match access-group
- match ip dscp
- match ip precedence
- haga juego ningunos

**Nota:** Para los paquetes V4 que no son IP, la sentencia match ip dscp es la única manera de clasificación siempre que los paquetes estén entrando a puertos de enlace troncal que confían en la CoS. No se deje confundir por la palabra clave ip del comando match ip dscp; debido a que el DSCP interno coincide, esto se aplica a todos los paquetes, no sólo a IP. Cuando un puerto es configurado a trust CoS, el último es extraído desde la trama L2 (802.1Q o indicado de ISL) y convertido a DSCP interno usando un CoS a un asociador QoS del DSCP. Este valor DSCP interno puede entonces compararse en la política utilizando match ip dscp.

Las acciones de política válida son como sigue:

- vigilancia
- set ip dscp
- set ip precedence
- trust dscp
- trust cos

La marcación permite cambiar el nivel de QoS del paquete sobre la base de clasificación o regulación de tráfico. La clasificación parte el tráfico en diversas clases para el proceso de QoS basado en los criterios definidos. Para hacer juego la Prioridad IP o el DSCP, la interfaz entrante correspondiente se debe fijar al modo de confianza. El Switch soporta confiar en el CoS, confiando en el DSCP, y las interfaces no confiables. La confianza especifica el campo del que se derivará el nivel de QoS del paquete.

Al confiar en la Clase de servicio (CoS), el nivel de Calidad de servicio (QoS) va a derivar del encabezador L2 del paquete encapsulado ISL u 802.1Q. Al confiar en el DSCP, el Switch derivará el QoS llano del campo DSCP del paquete. Confiar en la Clase de servicio (CoS) es de utilidad para interfaces troncales y confiar en DSCP es válido sólo para paquetes IP V4.

Cuando una interfaz no es confiable (éste es el estado predeterminado si la Calidad de servicio [QoS] está habilitada), se obtendrá la DSCP interna de la CoS o DSCP configurable predeterminada para la interfaz correspondiente. Si no se configura ningún CoS o DSCP predeterminado, el valor predeterminado será cero (0). Una vez que se determine el nivel de QoS original del paquete, se asigna un DSCP interno. El DSCP interno se puede conservar o cambiar mediante su marcado o regulación.

Después de que el paquete es sometido al procesamiento de QoS, los campos de niveles de QoS (en el campo IP DSCP de IP y en el encabezado ISL/802.1Q, si hay alguno) serán actualizados desde el DSCP interno.

Hay mapas especiales usados para convertir las métricas QoS confiables del paquete en DSCP interno y viceversa. Estas correspondencias son como sigue:

- DSCP DSCP limpiado; utilizado para derivar el DSCP vigilado durante la marcación del paquete.
- DSCP a CoS: se usa para derivar el nivel de la clase de servicio (CoS) desde el DSCP interno para actualizar el encabezado ISL/802.1Q del paquete de salida.
- CoS to DSCP: usado para derivar DSCP interno desde el servicio CoS entrante (ISL/802.1Q header) cuando la interfaz está en modo trust CoS.

Tenga en cuenta que cuando una interfaz está en modo de la Clase de servicio (CoS) de confianza, la CoS saliente siempre será igual a la CoS entrante. Esto es específico a la implementación de Calidad de servicio(QoS) en el Catalyst 4000 SE3, SE4, SE2+.

## Configuración y control de tráfico

Configurar el policing en el IOS implica los pasos siguientes:

1. Definición de la regulación de tráfico.
2. Definición de criterios de selección de tráfico para el establecimiento de políticas.
3. Definiendo la servicio-directiva usando la clase y la aplicación de un policer a una clase especificada.
4. Aplicación de una política de servicio a un puerto o a una VLAN.

Evalúe el siguiente ejemplo: Hay un generador de tráfico asociado al puerto 5/14 que envía ~17 Mbps del tráfico UDP con un destino del puerto 111. Deseamos que este tráfico se reduzca a 1Mbps y que se descarte el tráfico excesivo.

```
! enable qos
qos
! define policer, for rate and burst values, see 'policing parameters
qos aggregate-policer pol_1mbps 1mbps 1000 conform-action transmit
exceed-action
drop
! define ACL to select traffic
access-list 111 permit udp any any eq 111
! define traffic class to be policed
class-map match-all cl_test
match access-group 111
! define QoS policy, attach policer to traffic class
policy-map po_test
class cl_test
police aggregate pol_1mbps
! apply QoS policy to an interface
interface FastEthernet5/14
switchport access vlan 2
! switch qos to vlan-based mode on this port
qos vlan-based
! apply QoS policy to an interface
interface Vlan 2
service-policy output po_test
!
```

Tenga en cuenta que cuando un puerto está en el modo QoS basado en VLAN, pero no se aplica ninguna política de servicio a la VLAN correspondiente, el switch seguirá la política de servicio (si la hay) que se aplica en un puerto físico. Esto proporciona una mayor flexibilidad para combinar QoS basados en VLAN y en puertos.

Existen dos tipos de reguladores del tráfico admitidos: agregado con nombre y por interfaz. Un regulador agregado nombrado regulará el tráfico combinado de todas las interfaces a las cuales es aplicado. El ejemplo anterior usaba un regulador de tráfico designado. El regulador de tráfico por interfaz, a diferencia del regulador de tráfico designado, controlará el tráfico de forma individual en cada interfaz en la que se aplique. Se define un vigilante por interfaz dentro de la configuración de correspondencia de políticas. Considere el siguiente ejemplo con un regulador global por interfaz.

```
! enable qos
qos
! define traffic class to be policed
class-map match-all cl_test2
match ip precedence 3 4
! define QoS policy, attach policer to traffic class
policy-map po_test2
class cl_test2
! per-interface policer is defined inside the policy map
police 512k 1000 conform-action transmit exceed-action drop
interface FastEthernet5/14
switchport
! set port to trust DSCP - need this to be able to match to incoming IP precedence
qos trust dscp
! switch to port-based qos mode
no qos vlan-based
! apply QoS policy to an interface
service-policy input po_test2
```

Utilizan al siguiente comando de monitorear el funcionamiento de establecimiento de políticas:

```
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400026 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166067574 bytes Exceed: 5268602114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400138 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166088574 bytes Exceed: 5268693114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
```

El contador próximo a class-map cuenta el número de paquetes que coinciden con la clase correspondiente.

Sea consciente de las consideraciones específicas de la implementación siguiente:

- El contador de paquetes por clase no es por interfaz. Esto es, cuenta todos los paquetes que coinciden con la clase en todas las interfaces en las que esta clase se aplica dentro de la política de servicio.
- El policers no mantiene a los contadores de paquetes, sólo soportan a los contadores de bytes.
- No hay un comando específico para verificar la velocidad de tráfico saliente u ofrecido por regulador de tráfico.
- Los contadores se ponen al día en una base periódica. Si ejecuta el comando anterior repetidamente en rápida sucesión, los contadores aún podrían aparecer en algún momento.

## Marcación de configuración y control

La marcación de la configuración involucra los siguientes pasos:

1. Defina los criterios para clasificar el tráfico - lista de acceso, DSCP, precedencia de IP, entre otros.
2. Defina las clases de tráfico que se clasificarán usando los criterios definidos previamente.
3. Cree una correspondencia de políticas asociando acciones de marcación y/o acciones de regulación del tráfico con las clases definidas.
4. Configuración del modo de confianza en la interfaz(ces) correspondiente(s).
5. Aplique la correspondencia de políticas a una interfaz.

Considere el siguiente ejemplo donde quisiéramos que el tráfico entrante con la Prioridad IP 3 recibiera el puerto 777 de 192.168.196.3 UDP asociado a la Prioridad IP 6. Todo otro tráfico de precedencia IP 3 se controla debajo de 1 Mbps y el tráfico excedente se debe marcar debajo de precedencia IP 2.

```
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400026 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166067574 bytes Exceed: 5268602114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400138 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166088574 bytes Exceed: 5268693114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
```

Se utiliza el comando del **sh policy interface** de monitorear la marca. La salida de ejemplo y las consecuencias están documentadas en la configuración de la regulación del tráfico antes

mencionada.

## Comparar las Políticas y marcado en los Supervisores Engine basados en el IOS del Catalyst 6000 y del Catalyst 4000/4500

| Feature | Catalyst6000 | Catalyst4000 SE3 |
|---|---|---|
| Egress QoS policies | Not supported by Supervisor 1A and Superviso r2 hardware. | Supported. |
| Burst policing parameter calculation | Burst should be at least the same size as maximum frame supposed to pass via policer and no less then rate/interval, with the interval being 250 microseconds | No such restriction. |
| QoS policing L2 & L3 | By default, microflow policing is only enabled for L3 on the sup1a and is not enabled at all for Supervisor 2. A CLI command is available to enable it for L2 on sup1a and L2 & L3 for sup2. Aggregate policing for sup1a & Supervisor 2 is enabled by default for L2 & L3. | Always. |
| Egress CoS | Always derived from internal DSCP using DSCP to CoS QoS map. | If the ingress port is in trust CoS mode, the egress CoS will be the same as the ingress CoS. Otherwise, it will be derived from the internal DSCP. |
| Microflow policing | Supported. | Not supported. |
| QoS behavior when port is in VLAN-based QoS mode, but no policy is applied to the VLAN. | No policy applied. | Fallback to port-based QoS. Will apply policy attached to port. |

## Información Relacionada

- Información y configuración de QoS
- Soporte Técnico - Cisco Systems