Introducción a QoS Policing y Marcación en el Catalyst 3550

Contenido

Introducción

La función de regulación determina si el nivel de tráfico se encuentra dentro del perfil o contrato especificado, y le permite descartar el tráfico fuera de perfil o marcarlo a un valor diferente de punto de código de servicios diferenciados (DSCP). Esto aplica un nivel de servicio contratado.

DSCP es una medida del nivel de calidad de servicio (QoS) del paquete. Junto con DSCP, también se utilizan la precedencia IP y la Clase de servicio (CoS) para transmitir el nivel de QoS del paquete.

La regulación no debe confundirse con el modelado del tráfico, aunque ambos se aseguran de que el tráfico permanezca dentro del perfil o contrato.

La regulación de tráfico no almacena en búfer el tráfico, por lo que la regulación de tráfico no afecta al retraso de la transmisión. En lugar de almacenar en búfer los paquetes fuera de perfil, la regulación los descarta o los marca con diferentes niveles de QoS (reducción de DSCP).

El modelado del tráfico almacena en búfer el tráfico fuera del perfil y suaviza las ráfagas de tráfico, pero afecta la variación de demora y retraso. El modelado sólo se puede aplicar en la interfaz saliente, mientras que la regulación se puede aplicar tanto en la interfaz entrante como en la saliente.

El Catalyst 3550 admite la regulación tanto para las direcciones de entrada como de salida. No se admite el modelado de tráfico.

La marcación cambia el nivel de QoS del paquete según una política.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Versiones de hardware y de software

La regulación y la marcación en el Catalyst 3550 es compatible con todas las versiones de software. A continuación se muestra la guía de configuración más reciente. Consulte esta documentación para ver todas las funciones admitidas.

- Configuración de QoS

QoS Policing y Parámetros de Marcación

Para configurar la regulación, debe definir los mapas de política de QoS y aplicarlos a los puertos. Esto también se conoce como QoS basada en puerto.

Nota: Catalyst 3550 no soporta QoS basada en VLAN.

El regulador se define por parámetros de velocidad y ráfaga, así como por acciones para el tráfico fuera de perfil.

Se admiten estos dos tipos de reguladores:

- Agregado
- Individual

El regulador agregado actúa sobre el tráfico en todas las instancias donde se aplica. El regulador individual actúa por separado sobre el tráfico a través de cada instancia donde se aplica.

Nota: En el Catalyst 3550, el regulador agregado sólo puede aplicarse a diferentes clases de la misma política. No se admite la regulación de agregado en varias interfaces o políticas.

Por ejemplo, aplique el regulador de tráfico agregado para limitar el tráfico de clase customer1 y clase customer2 en el mismo policy-map a 1 Mbps. Tal regulador permite 1 Mbps de tráfico en la clase customer1 y customer2 juntos. Si aplica el regulador individual, el regulador limita el tráfico para la clase customer1 a 1 Mbps y para la clase customer2 a 1 Mbps. Por lo tanto, cada instancia del regulador de tráfico es independiente.

Esta tabla resume la acción de QoS sobre el paquete cuando se trata tanto por las políticas de ingreso como de egreso:

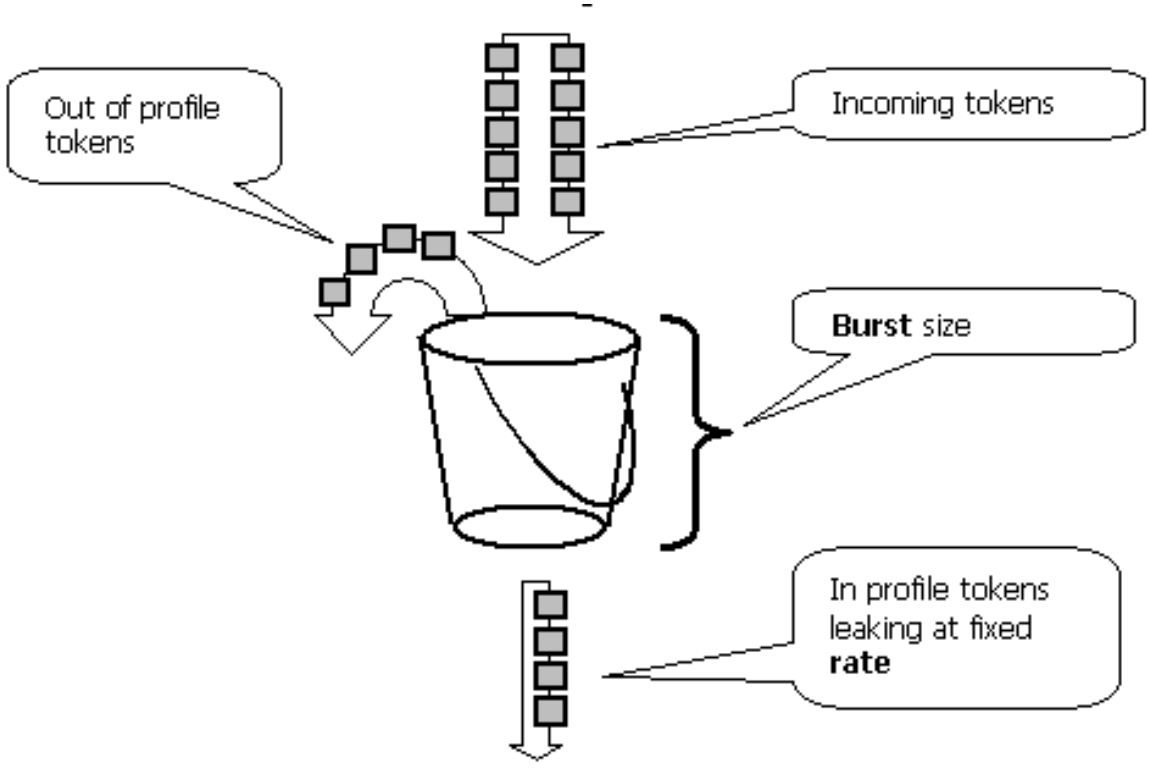
	Ingress policy			
Egress policy	Transmit	Drop	$Markdown_i$	$Mark_i$
Transmit	Transmit	Drop	$Markdown_i$	$Mark_i$
Drop	Drop	Drop	Drop	Drop
$Markdown_e$	$Markdown_e$	Drop	$Markdown_i$ then $Markdown_e$	$Mark_i$ then $Markdown_e$

Nota: Es posible marcar y reducir dentro de la misma clase de tráfico de la misma política. En tal caso, todo el tráfico para la clase en particular se marca primero. La regulación del tráfico y la reducción se producen en el tráfico ya marcado.

La regulación de QoS en el Catalyst 3550 cumple con este concepto de cubeta con fuga:

El número de tokens proporcionales a los tamaños de paquetes de tráfico entrante se colocan en una cubeta con ficha; el número de tokens es igual al tamaño del paquete. En un intervalo regular, se elimina de la cubeta un número definido de tokens derivado de la velocidad configurada. Si no hay lugar en la cubeta para acomodar un paquete entrante, el paquete se considera fuera de perfil y se descarta o se marca de acuerdo con la acción de regulación configurada.

Este concepto se muestra en este ejemplo:



Nota: El tráfico no se almacena en la memoria intermedia en la cubeta, ya que puede aparecer en

este ejemplo. El tráfico real no fluye a través de la cubeta; la cubeta sólo se utiliza para decidir si el paquete está en perfil o fuera de perfil.

Nota: La implementación del hardware de la regulación puede variar, pero funcionalmente sigue cumpliendo con este modelo.

Estos parámetros controlan el funcionamiento de la regulación:

- **Velocidad**: define cuántos tokens se quitan en cada intervalo. Esto fija de manera eficaz la velocidad de tráfico ordenado. Todo el tráfico por debajo de la velocidad se considera en el perfil. Las velocidades admitidas oscilan entre 8 Kbps y 2 Gbps, y aumentan en 8 Kbps.
- **Intervalo**: define la frecuencia con la que los tokens se quitan de la cubeta. El intervalo se fija en 0,125 milisegundos (o 8000 veces por segundo). No se puede cambiar este intervalo.
- **Ráfaga**: define la cantidad máxima de tokens que la cubeta puede contener en cualquier momento. Las ráfagas admitidas oscilan entre 8000 bytes y 2000000 bytes, y aumentan en 64 bytes.

Nota: Aunque las cadenas de ayuda de la línea de comandos muestran un gran rango de valores, la opción de velocidad-bps no puede exceder la velocidad de puerto configurada y la opción de byte de ráfaga no puede exceder los 200000 bytes. Si ingresa un valor mayor, el switch rechaza el mapa de política cuando lo conecta a una interfaz.

Para mantener la velocidad de tráfico especificada, la ráfaga debe ser no menor que la suma de esta ecuación:

```
Burstmin (bits) = Rate (bps) / 8000 (1/sec)
```

Por ejemplo, calcule el valor mínimo de ráfaga para mantener una velocidad de 1 Mbps. La velocidad se define como 1000 Kbps, por lo que la ráfaga mínima necesaria es la suma de esta ecuación:

```
1000 (Kbps) / 8000 (1/sec) =125 (bits)
```

El tamaño mínimo de ráfaga soportada es de 8000 bytes, que es superior a la ráfaga mínima calculada.

Nota: Debido a la granularidad de la regulación del hardware, la velocidad exacta y la ráfaga se redondean al valor admitido más cercano.

Cuando configura la velocidad de ráfaga, debe tener en cuenta que algunos protocolos implementan mecanismos que reaccionan a la pérdida de paquetes. Por ejemplo, el protocolo de control de transmisión (TCP) reduce la ventana a la mitad para cada paquete perdido. Esto causa un efecto "diente de la vista" en el tráfico TCP cuando el TCP intenta acelerar a la velocidad de línea y el regulador lo controla. Si se calcula la velocidad promedio del tráfico de los dientes de la sierra, esta velocidad es mucho menor que la velocidad controlada. Sin embargo, puede aumentar la ráfaga para lograr una mejor utilización. Un buen comienzo es configurar la ráfaga en el doble de la cantidad de tráfico enviado con la velocidad deseada durante el tiempo de ida y vuelta (RTT de TCP). Si se desconoce RTT, puede duplicar el valor del parámetro de ráfaga.

Por la misma razón, no se recomienda comparar la operación del regulador por tráfico orientado a la conexión. Este escenario generalmente muestra un rendimiento inferior al permitido por el regulador de tráfico.

El tráfico sin conexión también puede reaccionar a la regulación de tráfico de forma diferente. Por ejemplo, el sistema de archivos de red (NFS) utiliza bloques, que podrían consistir en más de un paquete de protocolo de datagramas de usuario (UDP). Un paquete descartado puede activar la retransmisión de muchos paquetes, incluso de todo el bloque.

Este ejemplo calcula la ráfaga para una sesión TCP con una velocidad de regulación de tráfico de 64 Kbps y dado que el TCP RTT es de 0,05 segundos:

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

En este ejemplo, `<burst>` es para una sesión TCP. Amplíe esta cifra para calcular el promedio del número esperado de sesiones que viajan a través del regulador de tráfico.

Nota: Este es sólo un ejemplo, en cada caso se necesita evaluar los requisitos y el comportamiento del tráfico y las aplicaciones en comparación con los recursos disponibles para elegir los parámetros de regulación.

La acción de regulación puede ser descartar el paquete o cambiar el DSCP del paquete (reducción). Para reducir el paquete, se debe modificar un mapa DSCP controlado. Un mapa DSCP controlado por defecto señala el paquete al mismo DSCP. Por lo tanto, no se produce ninguna reducción.

Los paquetes se pueden enviar fuera de orden cuando un paquete fuera de perfil se marca a un DSCP asignado a una cola de salida diferente a la DSCP original. Si el orden de los paquetes es importante, reduzca los paquetes fuera de perfil al DSCP asignado a la misma cola de salida que los paquetes dentro del perfil.

Políticas y características de marcación soportados por Catalyst 3550

Esta tabla proporciona un resumen de las funciones relacionadas con la regulación y el marcado soportadas por el Catalyst 3550, desglosado por dirección:

	Direction	
Feature	Ingress	Egress
Individual policers	Yes, totally 128 for GE and 8 for FE including ingress aggregate policers	Yes, totally 8 including egress aggregate policers
Aggregate policers	Yes, totally 128 for GE and 8 for FE including ingress individual policers	Yes, totally 8 including egress individual policers
Marking	Yes	No
Policer Markdown	Yes	Yes
Match with ACL	Yes	No
Match DSCP	Yes	Yes
Match IP precedence	Yes	No
Match COS	Yes, for non-IP traffic	No
Trust DSCP	Yes	No
Trust COS	Yes	No
Trust IP precedence	Yes	No

Se admite una instrucción match por class-map. Estas son sentencias de coincidencia válidas para la política de ingreso:

- match access-group
- match ip dscp
- match ip precedence

Nota: En el Catalyst 3550, el comando **match interface** no se soporta y sólo se permite un comando match en un class-map. Por lo tanto, es difícil clasificar todo el tráfico que llega a través de una interfaz y controlar todo el tráfico con un solo regulador. Vea la sección Cómo clasificar todo el tráfico de interfaz con un único regulador de este documento.

Esta es la sentencia de coincidencia válida para la política de egreso:

- match ip dscp

Estas son acciones de política válidas para la política de ingreso:

- vigilancia
- set ip dscp (mark)
- set ip precedence (mark)
- trust dscp
- trust ip-precedence
- trust cos

Esta tabla muestra la matriz de políticas de QoS de ingreso admitida:

Trust I/F	Match DSCP[1]	Match ACL	Trust Class[2]	Set DSCP[3]	Police	Result
						Traffic is assigned default QOS level of the port (0 by default)
√						QOS level of incoming traffic is preserved, according to what is trusted
	√		√		√	IP Traffic is matched by DSCP and then trusted then policed, excess traffic dropped or marked down
	√		√			IP Traffic is matched by DSCP/IP precedence and its QOS level is preserved
	√			√		IP Traffic is matched by DSCP/IP precedence then marked
	√			√	√	IP Traffic is matched by DSCP/IP precedence then marked then policed
		√	√		√	Traffic is matched by access list, QOS level of the matched traffic is preserved, then traffic is policed
		√	√			Traffic is matched by access list and its QOS level is preserved according to what is trusted
		√		√	√	Traffic is matched by access list then marked and then policed
		√		√		Traffic is matched by ACL then marked with specified DSCP/IP precedence
		MAC ACL w/COS	√			Match non-IP traffic by MAC EtherType and COS and preserve QOS level
		MAC ACL w/COS	√		√	Match non-IP IP traffic by MAC EtherType and COS and preserve QOS level then police
		MAC ACL w/COS		√		Match non-IP IP traffic by MAC EtherType and COS then mark matched traffic
		MAC ACL W/COS		√	√	Match non-IP IP traffic by MAC EtherType and COS then mark and then police

1. Esta opción también cubre la precedencia IP de coincidencia.
2. Esta opción cubre la confianza en CoS, precedencia IP y DSCP.
3. Esta opción también cubre la configuración de la precedencia IP.

Esta es la acción de política válida para la política de egreso:

- vigilancia

Esta tabla muestra la matriz de políticas de QoS de salida admitida:

Match DSCP	Police	Result
		Traffic is sent out with COS and IP precedence according to QOS maps and internal DSCP after ingress QOS processing
√	√	Traffic is matched by DSCP and policed

La marcación permite que el nivel de QoS del paquete cambie en función de la clasificación o regulación. La clasificación divide el tráfico en diferentes clases para el procesamiento de QoS basado en los criterios definidos.

El procesamiento de QoS se basa en el DSCP interno; la medida del nivel de QoS del paquete. El DSCP interno se deriva según la configuración de confianza. El sistema admite CoS de confianza, DSCP, precedencia IP e interfaces no confiables. Trust especifica el campo del cual se deriva el DSCP interno para cada paquete, de la siguiente manera:

- Al confiar en el CoS, el nivel de QoS se deriva del encabezado de capa 2 (L2) del protocolo de enlace entre switches (ISL) o del paquete encapsulado 802.1Q.
- Al confiar en la precedencia DSCP o IP, el sistema deriva el nivel QoS del campo de precedencia DSCP o IP del paquete en consecuencia.

Confiar en el CoS sólo es significativo en las interfaces de trunking, y confiar en el DSCP (o precedencia IP) tiene sentido sólo para los paquetes IP.

Cuando una interfaz no es de confianza, el DSCP interno se deriva del CoS predeterminado configurable para la interfaz correspondiente. Este es el estado predeterminado cuando se habilita QoS. Si no se configura ningún CoS predeterminado, el valor predeterminado es cero.

Una vez que se determina el DSCP interno, se puede cambiar marcando y controlando, o retener.

Después de que el paquete se someta al procesamiento de QoS, sus campos de nivel de QoS (dentro del campo IP/DSCP para IP y dentro del encabezado ISL/802.1Q, si los hubiera) se actualizan desde el DSCP interno. Existen estos mapas especiales de QoS relevantes para la regulación:

- **DSCP-to-Policed DSCP**: se utiliza para derivar el DSCP controlado cuando se reduce el paquete.
- **DSCP-to-CoS**: se utiliza para derivar el nivel de CoS del DSCP interno para actualizar el encabezado ISL/802.1Q del paquete saliente.
- **CoS-to-DSCP**: se utiliza para derivar el DSCP interno de la CoS entrante (encabezado ISL/802.1Q) cuando la interfaz está en el modo CoS de confianza.

Estas son importantes consideraciones específicas de la implementación:

- La política de servicio de ingreso no se puede asociar a la interfaz cuando la interfaz se configura para confiar en cualquiera de las métricas de QoS, como CoS/DSCP o precedencia IP. Para que coincida en la precedencia DSCP/IP y la regulación de entrada, debe configurar la confianza para la clase particular dentro de la política, no en la interfaz. Para marcar según la precedencia DSCP/IP, no se debe configurar ninguna confianza.
- Sólo el tráfico IPv4 sin opciones de IP y la encapsulación de la Agencia de Proyectos de Investigación Avanzada (ARPA) Ethernet II se considera tráfico IP desde el punto de vista del

hardware y de la QoS. El resto del tráfico se considera que no es de IP, incluida la IP con opciones, como IP encapsulada de protocolo de acceso de subred (SNAP) e IPv6.
- Para los paquetes que no son de IP, "match access group" es el único método de clasificación porque no puede coincidir con DSCP para el tráfico que no es de IP. Para ello, se utiliza una lista de acceso (ACL) de control de acceso a los medios (MAC); los paquetes se pueden comparar según la dirección MAC de origen, la dirección MAC de destino y EtherType. No es posible hacer coincidir el tráfico IP con la ACL MAC, ya que el switch hace una distinción entre tráfico IP y tráfico no IP.

Configuración y supervisión de políticas

Estos pasos son necesarios para configurar la regulación del tráfico en Cisco IOS:

1. Definir un regulador (para los reguladores de agregado)
2. Definir criterios para seleccionar el tráfico para la regulación
3. Definir un mapa de clase para seleccionar el tráfico utilizando criterios definidos
4. Definir una política de servicio mediante la clase y aplicar un regulador a la clase especificada
5. Aplicar una política de servicio a un puerto

Se admiten estos dos tipos de reguladores:

- Agregado nombrado
- Individual

El regulador de tráfico agregado designado controla el tráfico combinado de todas las clases dentro de la misma política a donde se aplica. No se admite el control agregado en diferentes interfaces.

Nota: El regulador agregado no se puede aplicar a más de una política. Si es así, se muestra este mensaje de error:

```
QoS: Cannot allocate policer for policy map <policy name>
```

Tenga en cuenta este ejemplo:

Hay un generador de tráfico conectado al puerto GigabitEthernet0/3 que envía aproximadamente 17 Mbps de tráfico UDP con el puerto de destino 111. También hay tráfico TCP del puerto 20. Desea que estos dos flujos de tráfico se controlen hasta 1 Mbps y que se descarte el tráfico excesivo. Este ejemplo muestra cómo se hace esto:

```
!--- Globally enables QoS. mls qos !--- Defines the QoS policer, sets the burst !--- to 16000
for better TCP performance. mls qos aggregate-policer pol_1mbps 1000000 16000 exceed-action drop
!--- Defines the ACLs to select traffic. access-list 123 permit udp any any eq 111
access-list 145 permit tcp any eq 20 any
!--- Defines the traffic classes to be policed. class-map match-all cl_udp111 match access-group
123
class-map match-all cl_tcp20
  match access-group 145
!--- Defines the QoS policy, and attaches !--- the policer to the traffic classes. policy-map
po_test
  class cl_udp111
```

```
    police aggregate pol_1mbps
  class cl_tcp20
    police aggregate pol_1mbps
!--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport switchport
access vlan 2 service-policy input po_test
!
```

En el primer ejemplo se utilizó el regulador agregado designado. El regulador individual, a diferencia del regulador designado, controla el tráfico por separado en cada clase donde se aplica. El regulador individual se define dentro de la configuración del policy map. En este ejemplo, dos clases de tráfico son controladas por dos reguladores de tráfico individuales; cl_udp111 se controla a 1 Mbps por ráfaga de 8K, y cl_tcp20 se controla a 512 Kbps por ráfaga de 32K:

```
!--- Globally enables QoS. mls qos !--- Defines the ACLs to select traffic. access-list 123
permit udp any any eq 111
access-list 145 permit tcp any eq 20 any
!--- Defines the traffic classes to be policed. class-map match-all cl_udp111
  match access-group 123
class-map match-all cl_tcp20
  match access-group 145
!--- Defines QoS policy, and creates and attaches !--- the policers to the traffic classes.
policy-map po_test2
  class cl_udp111
    police 1000000 8000 exceed-action drop
  class cl_tcp20
    police 512000 32000 exceed-action drop
!--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport switchport
access vlan 2 service-policy input po_test2
```

Este comando se utiliza para monitorear la operación de regulación:

```
cat3550#show mls qos interface g0/3 statistics
GigabitEthernet0/3
Ingress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
Others: 267718     0          267717     0          0
Egress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
Others: 590877        n/a        n/a      266303     0

WRED drop counts:
  qid  thresh1    thresh2   FreeQ
   1 : 0          0         1024
   2 : 0          0         1024
   3 : 0          0         8
   4 : 0          0         1024
```

Nota: De forma predeterminada, no hay estadísticas por DSCP. El Catalyst 3550 admite una recopilación de estadísticas por interfaz y por dirección para hasta ocho valores DSCP diferentes. Esto se configura cuando ejecuta el comando **mls qos monitor**. Para monitorear las estadísticas para los DSCP 8, 16, 24 y 32, debe ejecutar este comando **per-interface**:

```
cat3550(config-if)#mls qos monitor dscp 8 16 24 32
```

Nota: El comando **mls qos monitor dscp 8 16 24 32** cambia la salida del comando **show mls qos**

int g0/3 statistics a esto:

```
cat3550#show mls qos interface g0/3 statistics
GigabitEthernet0/3
Ingress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
    8 : 0          0          675053785  0          0
    16: 1811748    0          0          0          0         ? per DSCP statistics
    24: 1227820404 15241073   0          0          0
    32: 0          0          539337294  0          0
Others: 1658208    0          1658208    0          0
Egress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
    8 : 675425886     n/a       n/a      0          0
    16: 0             n/a       n/a      0          0         ? per DSCP statistics
    24: 15239542      n/a       n/a      0          0
    32: 539289117     n/a       n/a      536486430  0
Others: 1983055       n/a       n/a      1649446    0

WRED drop counts:
  qid  thresh1    thresh2   FreeQ
   1 : 0          0         1024
   2 : 0          0         1024
   3 : 0          0         6
   4 : 0          0         1024
```

Esta es una descripción de los campos del ejemplo:

- **Entrante**: muestra cuántos paquetes llegan de cada dirección
- **NO_change**: muestra cuántos paquetes eran de confianza (como el nivel de QoS no cambiado)
- **Clasificado**: muestra cuántos paquetes se han asignado a este DSCP interno después de la clasificación
- **Regulado**: muestra cuántos paquetes fueron marcados por la regulación; DSCP se muestra antes de la reducción.
- **Descartado**: muestra cuántos paquetes fueron descartados por la regulación

Tenga en cuenta estas consideraciones específicas de la implementación:

- Si se configuran ocho valores DSCP cuando se ejecuta el comando **mls qos monitor**, el contador de otros que se ve al ejecutar el comando **show mls qos int statistics** podría mostrar información inadecuada.
- No hay un comando específico para verificar la velocidad de tráfico ofrecido o saliente por regulador.
- Dado que los contadores se recuperan del hardware secuencialmente, es posible que los contadores no se sumen correctamente. Por ejemplo, la cantidad de paquetes controlados, clasificados o descartados puede ser ligeramente diferente al número de paquetes entrantes.

Configuración y supervisión del marcado

Estos pasos son necesarios para configurar el marcado:

1. Definir los criterios para clasificar el tráfico
2. Definir las clases de tráfico que se van a clasificar con los criterios previamente definidos
3. Cree un mapa de políticas que adjunte acciones de marcado y de regulación de tráfico a las

clases definidas

4. Configure las interfaces correspondientes al modo de confianza
5. Aplique la correspondencia de políticas a una interfaz

En este ejemplo, desea que el tráfico IP entrante aloje 192.168.192.168 marcado con precedencia IP 6 y controlado hasta 1 Mbps; el exceso de tráfico debe reducirse a la precedencia IP 2:

```
!--- Globally enables QoS. mls qos !--- Defines the ACLs to select traffic. access-list 167
permit ip any host 192.168.192.168
!--- Defines the traffic class. class-map match-all cl_2host
  match access-group 167
!--- Defines QoS policy, and creates and attaches !--- the policers to the traffic classes.
policy-map po_test3
  class cl_2host
!--- Marks all the class traffic with the IP precedence 6. set ip precedence 6
!--- Polices down to 1 Mbps and marks down according to the QoS map. police 1000000 8000 exceed-
action policed-dscp-transmit
!--- Modifies the policed DSCP QoS map, so the !--- traffic is marked down from IP precedence 6
to 2. !--- In terms of DSCP, this is from 48 to 16 (DSCP=IPprec x8). mls qos map policed-dscp 48
to 16 !--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport
switchport access vlan 2 service-policy input po_test3
```

Se ejecuta el mismo comando **show mls qos interface statistics** para monitorear el marcado. La salida de muestra y las implicaciones se documentan en la sección de este documento.

Cómo clasificar todo el tráfico de interfaz con un único regulador

En el Catalyst 3550, el comando **match interface** no se soporta y sólo se permite un comando match por class-map. Además, Catalyst 3550 no permite que el tráfico IP sea coincidente con las ACL MAC. Por lo tanto, el tráfico IP y el tráfico no IP deben clasificarse con dos class-maps independientes. Esto dificulta la clasificación de todo el tráfico que entra en una interfaz y controla todo el tráfico con un solo regulador. La configuración de ejemplo aquí le permite lograrlo. En esta configuración, el tráfico IP y no IP se corresponden con dos class-maps diferentes. Sin embargo, cada uno utiliza un regulador común para el tráfico.

```
access-list 100 permit ip any any

class-map ip
match access-group 100
!--- This class-map classifies all IP traffic. mac access-list extended non-ip-acl
permit any any

class-map non-ip
match access-group name non-ip-acl
!--- Class-map classifies all non-IP traffic only. mls qos aggregate-policer all-traffic 8000
8000 exceed-action drop
!--- This command configures a common policer that is applied for both IP and non-IP traffic.
policy-map police-all-traffic
class non-ip
police aggregate all-traffic
class ip
police aggregate all-traffic

interface gigabitEthernet 0/7
service-policy input police-all-traffic
!--- This command applies the policy map to the physical interface.
```

Información Relacionada

- Configuración de QoS en Catalyst 3550
- Páginas de Soporte de Calidad de Servicio
- Página de Soporte de LAN Switching
- Páginas de Soporte de Productos de LAN
- Soporte Técnico y Documentación - Cisco Systems