Supervisión de QoS en switches Catalyst de la serie 6500/6000

Contenido

Introducción

QoS Policing en una red determina si el tráfico de la red está dentro de un perfil especificado (contrato). Esto se puede hacer que el tráfico fuera de perfil se descarte o reduzca a otro valor DSCP (Differentiated Services Code Point) para aplicar un nivel de servicio contratado. (DSCP es una medida del nivel de QoS de la trama).

No confunda la regulación del tráfico con el modelado del tráfico. Ambos garantizan que el tráfico permanezca dentro del perfil (contrato). No almacena en búfer los paquetes fuera de perfil cuando controla el tráfico. Por lo tanto, no afecta al retardo de transmisión. Puede descartar el tráfico o marcarlo con un nivel de QoS inferior (reducción de DSCP). Por el contrario, con el modelado del tráfico, puede almacenar en búfer el tráfico fuera de perfil y suavizar las ráfagas de tráfico. Esto afecta la variación de demora y retraso. Sólo puede aplicar modelado de tráfico en una interfaz saliente. Puede aplicar políticas tanto en interfaces entrantes como salientes.

La tarjeta de función de política (PFC) Catalyst 6500/6000 y PFC2 solo admiten la regulación de entrada. El PFC3 admite la regulación de entrada y de salida. El modelado de tráfico sólo es soportado en algunos módulos WAN de la serie Catalyst 6500/7600, como por ejemplo, los Módulos de servicios ópticos (OSM) y los Módulos FlexWAN. Consulte Notas de Configuración del Módulo de Router de la Serie 7600 de Cisco para obtener más información

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.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Parámetros de QoS Policing

Para configurar la regulación, defina los reguladores y aplíquelos a los puertos (QoS basada en puerto) o a las VLAN (QoS basada en VLAN). Cada regulador define un nombre, tipo, porcentaje, ráfaga y acciones para tráfico dentro y fuera del perfil. Los reguladores de tráfico en Supervisor Engine II también admiten parámetros de velocidad excesiva. Existen dos tipos de reguladores del tráfico: microflujo y global.

- **Microflujo**: controla el tráfico para cada puerto/VLAN aplicado por separado según el flujo.
- **Agregado**: controla el tráfico en todos los puertos/VLAN aplicados.

Cada vigilante puede aplicarse a diversos puertos o redes VLAN. El flujo se define usando estos parámetros:

- Dirección IP de origen
- Dirección IP de destino
- Protocolo de capa 4 (como el protocolo de datagramas de usuario [UDP])
- número del puerto de origen
- número de puerto de destino

Puede decir que los paquetes que coinciden con un conjunto particular de parámetros definidos pertenecen al mismo flujo. (Se trata esencialmente del mismo concepto de flujo que utiliza el switching de NetFlow).

Por ejemplo, si configura un regulador de microflujo para limitar el tráfico TFTP a 1 Mbps en VLAN 1 y VLAN 3, entonces se permite 1 Mbps para cada flujo en VLAN 1 y 1 Mbps para cada flujo en VLAN 3. En otras palabras, si hay tres flujos en la VLAN 1 y cuatro flujos en la VLAN 3, el regulador de microflujo permite cada uno de estos flujos 1 Mbps. Si configura un regulador agregado, limita el tráfico TFTP para todos los flujos combinados en VLAN 1 y VLAN 3 a 1 Mbps.

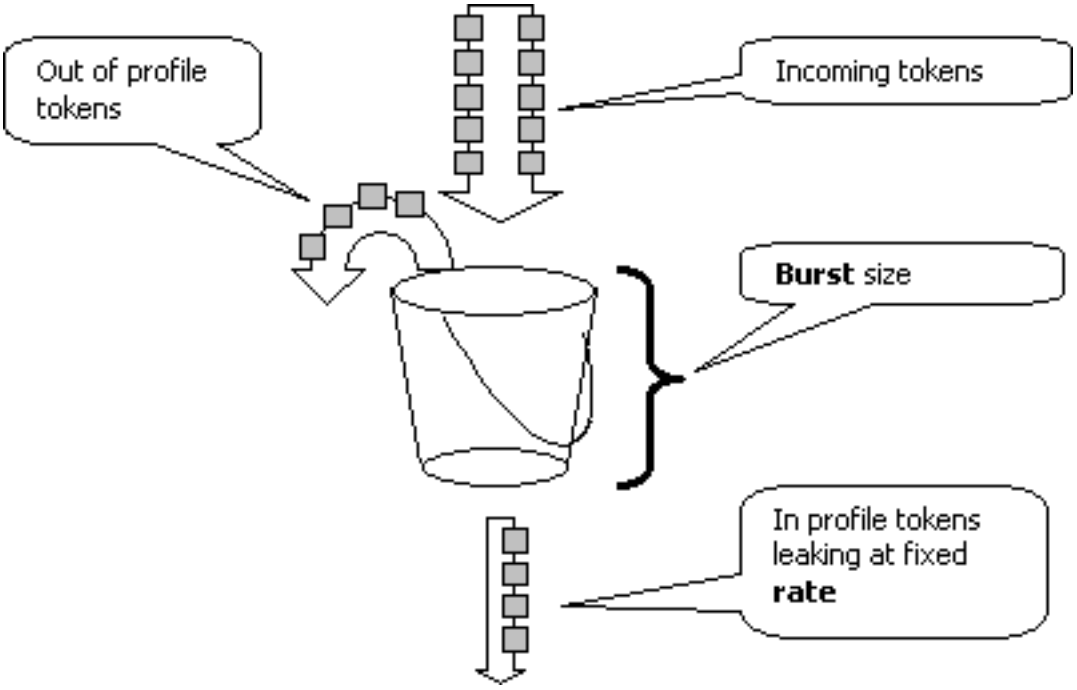
Si aplica reguladores de agregación y de microflujo, QoS siempre realiza la acción más severa especificada por los reguladores. Por ejemplo, si un regulador especifica descartar el paquete, pero otro especifica marcar el paquete, el paquete se descarta.

De forma predeterminada, los reguladores de microflujo sólo funcionan con el tráfico ruteado (Capa 3 [L3]). Para supervisar el tráfico puenteado (capa 2 [capa 2]) también, debe habilitar la regulación de microflujo puenteada. En Supervisor Engine II, debe habilitar la regulación de microflujo puenteada incluso para la regulación de microflujo L3.

La regulación de tráfico es compatible con los protocolos. Todo el tráfico se divide en tres tipos:

- IP
- Intercambio de paquetes entre redes (IPX)
- Otro

La regulación se implementa en el Catalyst 6500/6000 según el concepto de "cubeta con fuga". Los tokens correspondientes a los paquetes de tráfico entrante se colocan en una cubeta. (Cada token representa un bit, por lo que un paquete grande se representa con más tokens que un paquete pequeño.) A intervalos regulares, un número definido de fichas se elimina de la cubeta y se envían en su camino. Si no hay lugar en la cubeta para alojar los paquetes entrantes, los paquetes se consideran fuera de perfil. Se eliminan o se reducen según la acción de regulación configurada.



Nota: El tráfico no se almacena en la memoria intermedia, ya que puede aparecer en la imagen anterior. El tráfico real no pasa en absoluto por la cubeta; la cubeta sólo se utiliza para decidir si el paquete está en perfil o fuera de perfil.

Calcular parámetros

Varios parámetros controlan el funcionamiento de la cubeta con fichas, como se muestra aquí:

- **Velocidad**: 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.
- **Intervalo**: define la frecuencia con la que los tokens se quitan de la cubeta. El intervalo se fija en 0.00025 segundos para que los tokens se eliminen del compartimiento de memoria (bucket) 4,000 veces por segundo. No puede cambiarse el intervalo.
- **Ráfaga**: define el número máximo de tokens que la cubeta puede contener en cualquier momento. Para mantener la velocidad de tráfico especificada, la ráfaga no debe ser menor que la velocidad por el intervalo. Otra consideración es que el paquete de tamaño máximo debe encajar en el bloque de memoria.

Use esta ecuación para determinar el parámetro de ráfaga:

- Ráfaga = (Velocidad [bps]) * 0.00025 [sec/interval]) *o* (tamaño máximo de paquete [bits]), el

que sea mayor.

Por ejemplo, si desea calcular el valor mínimo de ráfaga necesario para mantener una velocidad de 1 Mbps en una red Ethernet, la velocidad se define como 1 Mbps y el tamaño máximo del paquete Ethernet es de 1518 bytes. La ecuación es:

- Ráfaga = (1 000 000 bps * 00025) *o* (1518 bytes * 8 bits/byte) = 250 *o* 12144.

El resultado mayor es 12144, que equivale aproximadamente a 13 kbps.

Nota: En Cisco IOS® Software, la velocidad de regulación se define en bits por segundo (bps), en comparación con kbps en Catalyst OS (CatOS). También en Cisco IOS Software, la velocidad de ráfaga se define en bytes, en comparación con kilobits en CatOS.

Nota: Debido a la granularidad de la regulación del hardware, la velocidad exacta y la ráfaga se redondean al valor admitido más cercano. Asegúrese de que el valor de ráfaga no sea menor que el paquete de tamaño máximo. De lo contrario, se rechazan todos los paquetes más grandes que la ráfaga.

Por ejemplo, si intenta establecer la ráfaga en 1518 en Cisco IOS Software, se redondea a 1000. Esto hace que se descarten todas las tramas mayores de 1000 bytes. La solución es configurar ráfaga a 2000.

Cuando configure la velocidad de la ráfaga, tome en cuenta que algunos protocolos (como el TCP) utilizan un mecanismo de control del flujo que reacciona frente a las pérdidas de paquetes. Por ejemplo, TCP reduce la ventana a la mitad para cada paquete perdido. Por consiguiente, cuando se controla a una velocidad determinada, la utilización efectiva del link es menor que la velocidad configurada. Puede aumentar la ráfaga para alcanzar una mejor utilización. Un buen comienzo para ese tráfico es duplicar el tamaño de ráfaga. (En este ejemplo, el tamaño de ráfaga aumenta de 13 kbps a 26 kbps). Luego, controle el rendimiento y realice los ajustes necesarios.

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

Acciones de la policía

Como se menciona en la Introducción, el regulador puede hacer una de dos cosas a un paquete fuera de perfil:

- descarte el paquete (el parámetro `drop` en la configuración)
- marcar el paquete a un DSCP inferior (el parámetro `policed-dscp` en la configuración)

Para marcar el paquete, debe modificar el mapa DSCP regulado. El DSCP controlado se establece de forma predeterminada para remarcar el paquete al mismo DSCP. (No se produce ninguna marca.)

Nota: Si los paquetes "fuera de perfil" se marcan a un DSCP que se mapea en una cola de salida diferente a la DSCP original, algunos paquetes se pueden enviar fuera de orden. Por esta razón, si el orden de los paquetes es importante, se recomienda marcar los paquetes fuera de perfil a un DSCP que se mapea a la misma cola de salida que los paquetes dentro del perfil.

En el Supervisor Engine II, que admite velocidad excesiva, son posibles dos disparadores:

- Cuando el tráfico excede la velocidad normal
- Cuando el tráfico supera la velocidad excesiva

Un ejemplo de la aplicación de la velocidad excesiva es el marcado de paquetes que exceden la velocidad normal y descartan paquetes que exceden la velocidad excesiva.

Funciones de regulación de tráfico admitidas por Catalyst 6500/6000

Como se indica en la Introducción, la PFC1 en el Supervisor Engine 1a y la PFC2 en el Supervisor Engine 2 sólo admiten la regulación de entrada (interfaz entrante). La PFC3 en el Supervisor Engine 720 admite la regulación de entrada y salida (interfaz saliente).

El Catalyst 6500/6000 admita hasta 63 reguladores de microflujo y hasta 1023 reguladores de agrupamiento.

El Supervisor Engine 1a admite la regulación de entrada, comenzando con la versión 5.3(1) de CatOS y la versión 12.0(7)XE del software del IOS de Cisco.

Nota: Se requiere una tarjeta secundaria PFC o PFC2 para la regulación con Supervisor Engine 1a.

El Supervisor Engine 2 admite la regulación de entrada, comenzando con la versión 6.1(1) de CatOS y la versión 12.1(5c)EX del software del IOS de Cisco. El Supervisor Engine II soporta el parámetro de regulación de velocidad excesiva.

Las configuraciones con tarjetas de reenvío distribuidas (DFC) sólo admiten la regulación basada en puertos. Además, el regulador de tráfico agregado sólo cuenta el tráfico por motor de reenvío, no por sistema. DFC y PFC son motores de reenvío; si un módulo (tarjeta de línea) no tiene un DFC, utiliza un PFC como motor de reenvío.

Actualización de las funciones de regulación del tráfico para Supervisor Engine 720

Nota: Si no está familiarizado con la regulación de QoS de Catalyst 6500/6000, asegúrese de leer las secciones Parámetros de Regulación de QoS y Funciones de Regulación Soportadas por Catalyst 6500/6000 de este documento.

El Supervisor Engine 720 introdujo estas nuevas funciones de regulación de QoS:

- **Vigilancia de salida**. El Supervisor 720 soporta el control de ingreso en un puerto o interfaz VLAN. Admite regulación de egreso en un puerto o interfaz ruteada L3 (en el caso del Cisco IOS System Software). Todos los puertos en la VLAN se controlan en la salida independientemente del modo de QoS del puerto (ya sea QoS basada en puerto o QoS basada en VLAN). La regulación de microflujo no se soporta en la salida. Las configuraciones de ejemplo se proporcionan en la sección Configurar y Monitorear Regulación de Tráfico en el Software CatOS y en la sección Configurar y Monitorear Regulación de Tráfico en Cisco IOS Software de este documento.
- **Regulación de microflujo por usuario**. El Supervisor 720 admite una mejora de la regulación

de microflujo conocida como regulación de microflujo por usuario. Esta función sólo se soporta con Cisco IOS System Software. Le permite proporcionar un cierto ancho de banda para cada usuario (por dirección IP) detrás de interfaces determinadas. Esto se logra mediante la especificación de una máscara de flujo dentro de la política de servicio. La máscara de flujo define qué información se utiliza para diferenciar entre los flujos. Por ejemplo, si especifica una máscara de flujo de sólo origen, todo el tráfico de una dirección IP se considera un flujo. Con esta técnica, puede controlar el tráfico por usuario en algunas interfaces (donde ha configurado la política de servicio correspondiente); en otras interfaces, continúa utilizando la máscara de flujo predeterminada. Es posible tener hasta dos máscaras de flujo QoS diferentes activas en el sistema en un momento dado. Sólo puede asociar una clase a una máscara de flujo. Una política puede tener hasta dos máscaras de flujo diferentes.

Otro cambio importante en la regulación del tráfico en Supervisor Engine 720 es que puede contar el tráfico por la longitud L2 de la trama. Esto difiere de Supervisor Engine 2 y Supervisor Engine 1, que cuentan las tramas IP e IPX por su longitud L3. Con algunas aplicaciones, la longitud de L2 y L3 puede no ser uniforme. Un ejemplo es un paquete L3 pequeño dentro de una trama L2 grande. En este caso, el Supervisor Engine 720 puede mostrar una velocidad de tráfico controlada ligeramente diferente en comparación con el Supervisor Engine 1 y el Supervisor Engine 2.

Configuración y supervisión de políticas en el software CatOS

La configuración de regulación para CatOS consta de tres pasos principales:

1. Defina un regulador: la velocidad de tráfico normal, la velocidad excesiva (si corresponde), la ráfaga y la acción de regulación.
2. Cree una ACL de QoS para seleccionar el tráfico que se va a vigilar y adjunte un regulador a esta ACL.
3. Aplique la ACL de QoS a los puertos o VLAN necesarios.

Este ejemplo muestra cómo controlar todo el tráfico al puerto UDP 111 en el puerto 2/8.

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 drop !--- This defines a
policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip
udp_qos_port dscp 0 aggregate udp_1mbps udp any any eq
111 !--- This creates QoS ACL to select traffic and
attaches !--- the policer to the QoS ACL. commit qos acl
all !--- This compiles the QoS ACL. set qos acl map
udp_qos_port 2/8 !--- This maps the QoS ACL to the
switch port.
```

El siguiente ejemplo es el mismo; sin embargo, en este ejemplo, usted asocia el regulador de tráfico a una VLAN. El puerto 2/8 pertenece a la VLAN 20.

Nota: Debe cambiar la QoS del puerto al modo `basado en vlan`. Haga esto con el comando **set port qos**.

Este regulador evalúa el tráfico de todos los puertos en esa VLAN configurada para QoS basada

en VLAN:

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 drop !--- This defines a
policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip
udp_qos_vlan dscp 0 aggregate udp_1mbps udp any any eq
111 !--- This creates the QoS ACL to select traffic and
attaches !--- the policer to QoS ACL. commit qos acl all
!--- This compiles the QoS ACL. set port qos 2/8 vlan-
based !--- This configures the port for VLAN-based QoS.
set qos acl map udp_qos_vlan 20 !--- This maps QoS ACL
to VLAN 20.
```

Luego, en lugar de descartar paquetes fuera de perfil con DSCP 32, márquelos a un DSCP de 0 (mejor esfuerzo).

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 policed-dscp !--- This
defines a policer. For the calculation of rate and
burst, !--- refer to Calculate Parameters. set qos acl
ip udp_qos_md trust-ipprec aggregate udp_1mbps udp any
any eq 111 dscp-field 32 !--- Note: The above command
should be on one line. !--- This creates the QoS ACL to
select traffic and attaches !--- the policer to the QoS
ACL.

commit qos acl all
!--- This compiles the QoS ACL. set qos policed-dscp-map
32:0 !--- This modifies the policed DSCP map to mark
down DSCP 32 to DSCP 0. set port qos 2/8 vlan-based !---
This configures the port for VLAN-based QoS. set qos acl
map udp_qos_md 20 !--- This maps the QoS ACL to VLAN 20.
```

Este ejemplo muestra la configuración para el control de egreso sólo para Supervisor Engine 720. Muestra cómo controlar todo el tráfico IP saliente en VLAN 3 a 10 Mbps agregado.

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
egress_10mbps rate 10000 burst 20 drop !--- This defines
a policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip egress_pol
trust-ipprec aggregate egress_10mbps ip any any !---
This creates the QoS ACL to select traffic and attaches
!--- the policer to the QoS ACL. commit qos acl all !---
This compiles the QoS ACL. set qos acl map egress_pol 3
output !--- This maps the QoS ACL to VLAN 3 in the
output direction.
```

Utilice **show qos maps runtime policed-dscp-map** para ver el mapa DSCP regulado actual.

Utilizar **show qos policer runtime {*policer_name* | todo para** verificar los parámetros del regulador de tráfico. También puede ver la ACL de QoS a la que está conectado el regulador.

Nota: Con Supervisor Engine 1 y 1a, no es posible tener estadísticas de regulación de tráfico para cada regulador de tráfico agregado. Para ver las estadísticas de regulación por sistema, utilice este comando:

```
Cat6k> (enable) show qos statistics l3stats
Packets dropped due to policing: 1222086
IP packets with ToS changed: 27424
IP packets with CoS changed: 3220
Non-IP packets with CoS changed: 0
```

Para verificar las estadísticas de regulación de microflujo, utilice este comando:

```
Cat6k> (enable) show mls entry qos short
Destination-IP  Source-IP Port  DstPrt SrcPrt Uptime  Age
--------------- --------------- ----- ------ ------ -------- --------

IP bridged entries:
239.77.77.77 192.168.10.200UDP   63 6300:22:02 00:00:00
Stat-Pkts : 165360
Stat-Bytes : 7606560
Excd-Pkts : 492240
Stat-Bkts : 1660
239.3.3.3192.168.11.200UDP  888 77700:05:38 00:00:00
Stat-Pkts : 42372
Stat-Bytes : 1949112
Excd-Pkts : 126128
Stat-Bkts : 1628

Only out of the profile MLS entries are displayed
Cat6k> (enable)
```

Con Supervisor Engine II, puede ver estadísticas de regulación agregada por regulador con el comando **show qos statistics aggregate-policer**.

Para este ejemplo, un generador de tráfico se conecta al puerto 2/8. Envía 17 Mbps de tráfico UDP con el puerto de destino 111. Se espera que el regulador descarte 16/17 del tráfico, por lo que 1 Mbps debe pasar por:

```
Cat6k> (enable) show qos statistics aggregate-policer udp_1mbps
QoS aggregate-policer statistics:
Aggregate policerAllowed packet Packets exceed Packets exceed
                count        normal rate       excess rate
------------------------------ -------------- -------------- --------------
udp_1mbps58243997321089732108

Cat6k> (enable) show qos statistics aggregate-policer udp_1mbps
QoS aggregate-policer statistics:
Aggregate policerAllowed packet Packets exceed Packets exceed
                count        normal rate       excess rate
------------------------------ -------------- -------------- --------------
udp_1mbps58250497331989733198
```

Nota: Observe que los paquetes permitidos han aumentado en 65 y que el exceso de paquetes ha aumentado en 1090. Esto significa que el regulador de tráfico ha descartado 1090 paquetes y ha permitido que 65 pasen. Puede calcular que 65 / (1090 + 65) = 0,056, o aproximadamente 1/17. Por lo tanto, el regulador funciona correctamente.

Configuración y Supervisión de Regulación de Tráfico en Cisco IOS Software

La configuración para la regulación del tráfico en Cisco IOS Software implica estos pasos:

1. Defina un regulador.
2. Cree una ACL para seleccionar el tráfico que se va a supervisar.
3. Defina un mapa de clase para seleccionar el tráfico con precedencia de ACL o DSCP/IP.
4. Defina una política de servicio que utilice la clase y aplique el regulador de tráfico a una clase especificada.
5. Aplique la política de servicio a un puerto o VLAN.

Considere el mismo ejemplo que el proporcionado en la sección Configuración y Monitoreo de Regulación de Tráfico en el Software CatOS, pero ahora con el Cisco IOS Software. Para este ejemplo, tiene un generador de tráfico conectado al puerto 2/8. Envía 17 Mbps de tráfico UDP con el puerto de destino 111:

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. mls qos aggregate-policer
udp_1mbps 1000000 2000 conform-action transmit exceed-
action drop !--- Note: The above command should be on
one line. !--- This defines a policer. For the
calculation of rate and burst, !--- refer to Calculate
Parameters. !--- Note: The burst is 2000 instead of
1518, due to hardware granularity.

access-list 111 permit udp any any eq 111
!--- This defines the ACL to select traffic. class-map
match-all udp_qos match access-group 111 !--- This
defines the traffic class to police. policy-map
udp_policy class udp_qos police aggregate udp_1mbps !---
This defines the QoS policy that attaches the policer to
the traffic class. interface GigabitEthernet2/8
switchport service-policy input udp_policy !--- This
applies the QoS policy to an interface.
```

Hay dos tipos de reguladores agregados en el Cisco IOS Software: **con nombre y por interfaz.** El regulador agregado designado controla el tráfico combinado de todas las interfaces a las que se aplica. Este es el tipo utilizado en el ejemplo anterior. El regulador por interfaz controla el tráfico por separado en cada interfaz entrante a la que se aplica. Se define un vigilante por interfaz dentro de la configuración de correspondencia de políticas. Considere este ejemplo, que tiene un regulador de tráfico agregado por interfaz:

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 111 permit udp any
any eq 111 !--- This defines the ACL to select traffic.
class-map match-all udp_qos match access-group 111 !---
This defines the traffic class to police. policy-map
udp_policy class udp_qos !--- This defines the QoS
policy that attaches the policer to the traffic class.
police 1000000 2000 2000 conform-action transmit exceed-
```

```
action drop !--- This creates a per-interface aggregate
!--- policer and applies it to the traffic class.
interface GigabitEthernet2/8 switchport service-policy
input udp_policy !--- This applies the QoS policy to an
interface.
```

Los reguladores de tráfico de microflujo se definen dentro de la configuración del mapa de políticas, al igual que los reguladores de tráfico agregados por interfaz. En el siguiente ejemplo, cada flujo desde el host 192.168.2.2 que llega a la VLAN 2 se controla a 100 kbps. Todo el tráfico de 192.168.2.2 se controla a un agregado de 500 kbps. VLAN 2 incluye interfaces fa4/11 y fa4/12:

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 1 permit 192.168.2.2
!--- This defines the access list to select traffic from
host 192.168.2.2. class-map match-all host_2_2 match
access-group 1 !--- This defines the traffic class to
police. policy-map host class host_2_2 !--- This defines
the QoS policy. police flow 100000 2000 conform-action
transmit exceed-action drop !--- This defines a
microflow policer. For the calculation of rate and !---
burst, refer to Calculate Parameters. police 500000 2000
2000 conform-action transmit exceed-action drop !---
This defines the aggregate policer to limit !--- traffic
from the host to 500 kbps aggregate. interface fa4/11
mls qos vlan-based interface fa4/12 mls qos vlan-based
!--- This configures interfaces in VLAN 2 for VLAN-based
QoS. interface vlan 2 service-policy input host !---
This applies the QoS policy to VLAN 2.
```

El siguiente ejemplo muestra una configuración para la regulación de egreso para el Supervisor Engine 720. Establece la regulación de todo el tráfico saliente en la interfaz Gigabit Ethernet de 8/6 a 100 kbps:

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 111 permit ip any any
!--- This defines the ACL to select traffic. All IP
traffic is subject to policing. class-map match-all
cl_out match access-group 111 !--- This defines the
traffic class to police. policy-map pol_out class cl_out
police 100000 3000 3000 conform-action transmit exceed-
action drop !--- This creates a policer and attaches it
to the traffic class. interface GigabitEthernet8/6 ip
address 3.3.3.3 255.255.255.0 service-policy output
pol_out !--- This attaches the policy to an interface.
```

El siguiente ejemplo muestra una configuración para la regulación por usuario para Supervisor Engine 720. El tráfico que llega de los usuarios detrás del puerto 1/1 hacia Internet se controla a 1 Mbps por usuario. El tráfico que viene de Internet hacia los usuarios se controla a 5 Mbps por usuario:

Catalyst 6500/6000

```
mls qos
```

```
!--- This enables QoS. access-list 111 permit ip any any
!--- This defines the ACL to select user traffic. class-
map match-all cl_out match access-group 111 !--- This
defines the traffic class for policing. policy-map
pol_out class cl_out police flow mask src-only 1000000
32000 conform-act transmit exceed-act drop
!--- Only the source IP address is considered for flow
creation !--- on interfaces with this policy attached.
interface gigabit 1/1 !--- 1/1 is the uplink toward the
users. service-policy input pol_out !--- Traffic comes
in from users, so the policy is attached !--- in the
input direction. class-map match-all cl_in match access-
group 111 policy-map pol_in class cl_in police flow mask
dest-only 5000000 32000 conform-act transmit exceed-act
drop
!--- Only the destination IP address is considered for
flow creation !--- on interfaces with this policy
attached. interface gigabit 1/2 !--- 1/2 is the uplink
to the Internet. service-policy input pol_in
```

Para supervisar la regulación, puede utilizar estos comandos:

```
bratan# show mls qos
QoS is enabled globally
Microflow policing is enabled globally
QoS global counters:
Total packets: 10779
IP shortcut packets: 0
Packets dropped by policing: 2110223
IP packets with TOS changed by policing: 0
IP packets with COS changed by policing: 0
Non-IP packets with COS changed by policing: 0

bratan# show mls qos ip gigabitethernet 2/8
[In] Policy map is udp_policy [Out] Default.
QoS Summary [IP]: (* - shared aggregates, Mod - switch module)

Int   Mod Dir Class-map DSCP AgId Trust FlId AgForward-Pk AgPoliced-Pk
--------------------------------------------------------------------------------
Gi2/8 1   In  udp_qos   0    1*   No0 127451  2129602


bratan# show mls qos ip gigabitethernet 2/8
[In] Policy map is udp_policy [Out] Default.
QoS Summary [IP]: (* - shared aggregates, Mod - switch module)

Int   Mod Dir Class-map DSCP AgId Trust FlId AgForward-Pk AgPoliced-Pk
--------------------------------------------------------------------------------
Gi2/8 1   In  udp_qos   0    1*   No0 127755  2134670
```

Nota: Los paquetes permitidos han aumentado en 304 y los paquetes excedentes han aumentado en 5068. Esto significa que el regulador de tráfico ha descartado 5068 paquetes y ha permitido que 304 pasen. Dada la velocidad de entrada de 17 Mbps, el regulador de tráfico debe pasar 1/17 del tráfico. Si compara los paquetes perdidos y reenviados, verá que este ha sido el caso: 304 / (304 + 5068) = 0,057, o aproximadamente 1/17. Es posible realizar alguna variación menor debido a la granularidad de la regulación del hardware.

Para las estadísticas de regulación de microflujo, utilice el comando **show mls ip detail**:

```
Orion# show mls ip detail
```

```
IP Destination IP Source        Protocol L4 Ports     Vlan Xtag L3-protocol
--------------+---------------+--------+------------+----+----+-----------+
192.168.3.33192.168.2.2udp555 / 5550   1ip
192.168.3.3192.168.2.2udp63 / 630   1ip

[IN/OUT] Ports Encapsulation RW-Vlan RW-MACSourceRW-MACDestinationBytes
--------------+-------------+-------+--------------+-----------------+------------+
Fa4/11 - ----ARPA3    0030.7137.1000  0000.3333.3333314548
Fa4/11 - ----ARPA3    0030.7137.1000  0000.2222.2222314824

Packets     Age   Last SeenQoS      Police Count ThresholdLeak
------------+-----+---------+-----------+------------+---------+-----------+
6838     36   18:50:090x80  34619762*2^5 3*2^0
6844     36   18:50:090x80  34669562*2^5 3*2^0

Drop Bucket  Use-Tbl Use-Enable
----+-------+-------+----------+
YES   1968     NONO
YES   1937     NONO
```

Nota: El campo `Recuento de policías` muestra el número de paquetes controlados por flujo.

Información Relacionada

- Configuración de QoS
- La calidad del servicio en la familia de switches Catalyst 6000
- Soporte de Producto de LAN
- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems