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 Vigilancia de tráfico con el modelado de tráfico. Ambos se aseguran de que el tráfico permanezca dentro del perfil (contrato). Usted no mitiga los paquetes fuera de perfil cuando usted limpia el tráfico. Por lo tanto, usted no afecta al retraso de la transmisión. Usted cae el tráfico o lo marca con un nivel más bajo de QoS (DSCP reducido). En cambio, con el modelado de tráfico, usted mitiga el tráfico fuera de perfil y alisa las ráfagas de tráfico. Esto afecta al retardo y a la variación de retraso. Usted puede aplicar solamente el modelado de tráfico en una interfaz de salida. Usted puede aplicar el policing en entrante y las interfaces de salida.

El Policy Feature Card del Catalyst 6500/6000 (PFC) y solamente policing del ingreso del soporte PFC2. El PFC3 soporta el ingreso y el policing de la 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. Refiera a las notas de la configuración de módulos del Cisco 7600 Series Router para más información

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.

Convenciones

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

Parámetros de QoS Policing

Para configurar el policing, usted define el policers y los aplica a los puertos (acceso basado QoS) o a los VLA N (QoS VLAN basado). 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.

- **Microflow** — la policía trafica para cada port/VLAN aplicado por separado sobre una base del por-flujo.
- **Agregado** — limpie el tráfico a través de todos los puertos/VLA N aplicados.

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

- dirección IP de origen
- IP Address de destino
- Protocolo de la capa 4 (tal como protocolo UDP [UDP])
- número del puerto de origen
- número de puerto de destino

Usted puede decir que los paquetes que hacen juego un conjunto determinado de los parámetros definidos pertenecen al mismo flujo. (Éste es esencialmente el mismo concepto de flujo que el que el Switching de Netflow utilice.)

Como un ejemplo, si usted configura un regulador de microflujo para limitar el tráfico TFTP al 1 Mbps en el VLAN1 y el VLAN3, después el 1 Mbps se permite para cada flujo en el VLAN1 y el 1 Mbps para cada flujo en el VLA N 3. es decir si hay tres flujos en el VLAN1 y cuatro flujos en el VLAN3, el regulador de microflujo permite cada uno de este 1 Mbps de los flujos. Si usted configura a un vigilante global, limita el tráfico TFTP para todos los flujos combinados en el VLAN1 y el VLAN3 al 1 Mbps.

Si usted aplica el agregado y los reguladores de microflujo, QoS toma siempre la mayoría de la acción severa especificada por el policers. Por ejemplo, si un policer especifica para caer el paquete, solamente otro especifica para marcar abajo del paquete, el paquete se cae.

Por abandono, los reguladores de microflujo funcionan solamente con (la capa 3 [L3]) el tráfico ruteado. Para limpiar interligó (la capa 2 [L2]) el tráfico también, usted necesitan habilitar el bridged microflow policing. En el Supervisor Engine II, usted necesita habilitar el bridged microflow policing incluso para la regulación de microflujo L3.

El policing está protocolo-enterado. Todo el tráfico se divide en tres tipos:

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

El policing se implementa en el Catalyst 6500/6000 según un concepto del “contador dinámico”. Los tokens correspondiente a los paquetes del tráfico entrante se colocan en un compartimiento. (Cada token representa un bit, así que un paquete grande es representado por más tokens que un pequeño paquete.) A intervalos regulares, un número definido de tokens se quita del compartimiento y se envía encendido su manera. Si no hay lugar en el compartimiento para acomodar los paquetes de entrada, los paquetes se consideran fuera de perfil. Se caen o se marcan abajo según la acción de regulación configurada.

Nota: El tráfico no está mitigado en el compartimiento, pues puede aparecer en la imagen arriba. El tráfico real no pasa a través del compartimiento en absoluto; el compartimiento se utiliza solamente para decidir a si el paquete es en perfil o fuera de perfil.

Calcule los parámetros

Varios parámetros controlan la operación del token bucket, como se muestra aquí:

- **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.
- **Intervalo** — define cuantas veces los tokens se quitan del compartimiento. 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.
- **Explosión** — define el número máximo de tokens que el compartimiento pueda sostener a cualquier momento. Para sostener la velocidad de tráfico especificada, la explosión debe ser ninguna menos que las velocidades multiplicadas por timpo 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:

- Explosión = (tarifa [bps]) * 0.00025 [sec/interval]) *o* (tamaño máximo de paquete [bits]), cualquiera es mayor.

Por ejemplo, si usted quiere calcular el valor mínimo de ráfaga necesario para sostener un índice de 1 Mbps en una red Ethernet, la tarifa se define como 1 Mbps y el tamaño de paquete Ethernet máximo es 1518 bytes. La ecuación es:

- Explosión = (1,000,000 BPS * 0.00025) *o* (1518 bytes * 8 bits/byte) = 250 *o* 12144.

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

Nota: En el software de Cisco IOS®, la velocidad de tráfico ordenado se define en los bits por segundo (BPS), en comparación con el kbps en el Catalyst OS (CatOS). También en Cisco IOS Software, la velocidad de ráfaga se define en los bytes, en comparación con los kilobites en CatOS.

Nota: Debido a la granularidad de control de hardware, a la velocidad exacta y a la explosión se redondea al valor admitido más cercano. Esté seguro que el valor de ráfaga es no menos que el paquete de tamaño máximo. De lo contrario, se rechazan todos los paquetes más grandes que la

ráfaga.

Por ejemplo, si usted intenta fijar la explosión a 1518 en Cisco IOS Software, se redondea a 1000. Esto hace a todas las tramas de 1000 bytes más grandes ser caída. La solución es configurar la explosión 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, el TCP reduce la visualización en una ventana por la mitad para cada paquete perdido. Por lo tanto, cuando está limpiada a una cierta velocidad, la utilización de link eficaz es más baja que la velocidad configurada. Puede aumentar la ráfaga para alcanzar una mejor utilización. Un buen comienzo para tal tráfico es doblar el tamaño de ráfaga. (En este ejemplo, el tamaño de ráfaga se aumenta a partir de 13 kbps a 26 kbps). Luego, controle el rendimiento y realice los ajustes necesarios.

Por la misma razón, no se recomienda para evaluar la operación de regulador de tráfico usando el tráfico orientado a la conexión. Esto muestra generalmente el menor rendimiento que los permisos del policer.

Acciones policiales

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

- caiga el paquete (el parámetro del `descenso` en la configuración)
- marque el paquete a un DSCP más bajo (el parámetro limpiar-`DSCP` en la configuración)

Para marcar abajo del paquete, usted debe modificar el mapa DSCP limpiado. El DSCP limpiado se fija por abandono para comentar el paquete al mismo DSCP. (Ninguna marca abajo ocurre.)

Nota: Si los paquetes del “fuera de perfil” se marcan abajo a un DSCP que se asocie en una diversa cola de salida que el DSCP original, algunos paquetes se pueden enviar fuera de servicio. Por este motivo, si la pedido de los paquetes es importante, se recomienda para marcar abajo de los paquetes fuera de perfil a un DSCP que se asocie a la misma cola de salida que los paquetes del en perfil.

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

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

Un ejemplo de la aplicación de la velocidad excesiva es marcar abajo de los paquetes que exceden los paquetes normales de la tarifa y del descenso que exceden la velocidad excesiva.

Características de regulación de tráfico soportadas por el Catalyst 6500/6000

Como se afirma en la introducción, el PFC1 en el Supervisor Engine 1A y el PFC2 en el Supervisor Engine 2 soportan solamente el policing del ingreso (interfaz de entrada). El PFC3 en el Supervisor Engine 720 soporta el ingreso y el policing de la salida (interfaz de salida).

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

agrupamiento.

El Supervisor Engine 1A soporta el policing del ingreso, empezando por la versión CatOS 5.3(1) y el Cisco IOS Software Release 12.0(7)XE.

Nota: Una placa hija PFC o PFC2 se requiere para limpiar con el Supervisor Engine 1A.

El Supervisor Engine 2 soporta el policing del ingreso, empezando por la versión CatOS 6.1(1) y el Cisco IOS Software Release 12.1(5c)EX. El Supervisor Engine II soporta el parámetro de regulación de tráfico de la velocidad excesiva.

Las configuraciones con los indicadores luminosos LED amarillo de la placa muestra gravedad menor de envío distribuidos (DFC) soportan solamente el policing del acceso basado. También, el vigilante global cuenta solamente el tráfico sobre una base del per-forwarding-engine, no por sistema. El DFC y el PFC son ambos motores de reenvío; si un módulo (linecard) no tiene un DFC, utiliza un PFC como motor de reenvío.

Las características de regulación de tráfico se ponen al día para el Supervisor Engine 720

Nota: Si usted es desconocido con la Supervisión de QoS del Catalyst 6500/6000, esté seguro de leer los parámetros y las características de regulación de tráfico de la Supervisión de QoS soportados por las secciones del Catalyst 6500/6000 de esto documento.

El Supervisor Engine 720 introdujo estas nuevas características de la Supervisión de QoS:

- **Policing de la salida**. El policing del ingreso de los soportes del supervisor 720 en un puerto o una interfaz VLAN. Soporta el policing de la salida en un puerto o una interfaz ruteada L3 (en el caso del software del sistema del Cisco IOS). Todos los puertos en el VLA N se limpian en la salida sin importar el modo de QoS del puerto (si acceso basado QoS o QoS VLAN basado). La regulación de microflujo no se soporta en la salida. Las configuraciones de muestra se proporcionan en la configuración y monitorean el policing en la sección del software CatOS y configuran y monitorean el policing en la sección del Cisco IOS Software de este documento.
- **Por usuario regulación de microflujo**. El supervisor 720 soporta una mejora a la regulación de microflujo conocida como por usuario regulación de microflujo. Esta característica se soporta solamente con el software del sistema del Cisco IOS. Permite que usted proporcione cierto ancho de banda para cada usuario (por la dirección IP) detrás de las interfaces dadas. Esto es alcanzada especificando una máscara del flujo dentro de la política de servicio. La máscara del flujo define qué información se utiliza para distinguir entre los flujos. Por ejemplo, si usted especifica una máscara del flujo de la fuente-solamente, todo el tráfico a partir de una dirección IP se considera un flujo. Usando esta técnica, usted puede limpiar el tráfico por el usuario en algunas interfaces (donde usted ha configurado la política de servicio correspondiente); en otras interfaces, usted continúa utilizando la máscara predeterminada del flujo. Es posible tener hasta dos diversas máscaras del flujo de QoS activas en el sistema en un momento dado. Usted puede asociar solamente una clase a una máscara del flujo. Una directiva puede tener hasta dos diversas máscaras del flujo.

Otro cambio importante en el policing en el Supervisor Engine 720 es que puede contar el tráfico por la longitud L2 del bastidor. Esto diferencia del Supervisor Engine 2 y del Supervisor Engine 1,

que cuentan las tramas IP y IPX por su longitud L3. Con ciertas aplicaciones, longitud L2 y L3 no puede ser constante. Un ejemplo es un paquete L3 pequeño dentro de una trama L2 grande. En este caso, el Supervisor Engine 720 puede visualizar las relaciones del tráfico limpiadas levemente diversas con respecto al Supervisor Engine 1 y al Supervisor Engine 2.

Configuración y policing del monitor en software CatOS

La configuración de establecimiento de política para CatOS consiste en tres pasos principales:

1. Defina un policer — las relaciones del tráfico, la velocidad excesiva (si procede), la explosión, y la acción de regulación de tráfico normales.
2. Cree un QoS ACL para seleccionar el tráfico para limpiar, y asocie un policer a este ACL.
3. Aplique el QoS ACL a los puertos necesarios o a los VLA N.

Este ejemplo muestra cómo limpiar todo el tráfico al puerto 111 UDP 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 próximo ejemplo es lo mismo; sin embargo, en este ejemplo, usted asocia el policer a un VLA N. El puerto 2/8 pertenece al VLAN20.

Nota: Usted necesita cambiar el puerto QoS al modo VLAN-`basado`. Haga esto con el **comando set port qos**.

Este policer evalúa el tráfico de todos los puertos en ese VLA N configurado para QoS VLAN basado:

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.
```

Después, en vez de los paquetes fuera de perfil de caída con el DSCP 32, marqúelos abajo 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 el policing de la configuración para egreso para el Supervisor Engine 720 solamente. Muestra cómo limpiar todo el tráfico IP saliente en el VLAN3 al agregado del 10 Mbps.

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.
```

Utilice el **policed-dscp-map del tiempo de ejecución de las correspondencias de los qos de la demostración** para ver el mapa DSCP limpiado corriente.

Utilice los **qos de la demostración policer runtime {***policer_name* **| todos}** para verificar los parámetros del policer. Usted puede también ver el QoS ACL al cual se asocia el policer.

Nota: Con el Supervisor Engine 1 y 1a, no es posible tener los vigilantes globales de las estadísticas para el individuo del policing. Para ver las estadísticas por sistema del policing, 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 marcar las estadísticas de regulación del 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 el Supervisor Engine II, usted puede ver las estadísticas globales del policing sobre una base del por-policer con el **comando show qos statistics aggregate-policer**.

Por este ejemplo, un generador de tráfico se asocia al puerto 2/8. Envía el 17 Mbps del tráfico UDP con el puerto destino 111. Usted espera que el policer caiga 16/17 del tráfico, así que el 1 Mbps debe ir a través:

```
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: Note que los paquetes permitidos han aumentado en 65 y los paquetes en exceso han aumentado en 1090. Esto significa que el policer ha caído 1090 paquetes y 65 permitidos para pasar a través. Usted puede calcular que 65/(1090 + 65) = 0.056, o áspero 1/17. Por lo tanto, el policer trabaja correctamente.

Configuración y policing del monitor en Cisco IOS Software

La configuración para limpiar en Cisco IOS Software implica estos pasos:

1. Defina un policer.
2. Cree un ACL para seleccionar el tráfico para limpiar.
3. Defina una correspondencia de la clase para seleccionar el tráfico con la precedencia ACL y/o DSCP/IP.
4. Defina una política de servicio que utilice la clase, y aplique el policer a una clase especificada.
5. Aplique la política de servicio a un puerto o a un VLA N.

Considere el mismo ejemplo que ése proporcionado en la configuración de la sección y monitoree el policing en software CatOS, pero ahora con el Cisco IOS Software. Por este ejemplo, usted tiene un generador de tráfico asociado al puerto 2/8. Envía el 17 Mbps del tráfico UDP con el

puerto 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 vigilantes globales en Cisco IOS Software: con nombre y por interfaz. El Supervisor de tráfico total designado limpia el tráfico combinado de todas las interfaces a las cuales sea aplicado. Éste es el tipo usado en el ejemplo antedicho. El per-interface policer limpia el tráfico por separado en cada interfaz de entrada a la cual sea aplicado. Se define un vigilante por interfaz dentro de la configuración de correspondencia de políticas. Considere este ejemplo, que tiene un regulador de tráfico total por interfaz:

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.
```

Los reguladores de microflujo se definen dentro de la configuración de correspondencia de políticas, al igual que reguladores de tráfico total por interfaz. En el ejemplo abajo, cada flujo del host 192.168.2.2 que entra en el VLAN2 se limpia a 100 kbps. Todo el tráfico de 192.168.2.2 se limpia al agregado del kbps 500. El VLAN2 incluye las interfaces fa4/11 y fa4/12:

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.
```

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

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.
```

El ejemplo abajo muestra una configuración para por usuario limpiar para el Supervisor Engine 720. Trafique que viene adentro de los usuarios detrás del puerto 1/1 hacia Internet se limpia al 1 Mbps por el usuario. Trafique que viene de Internet hacia los usuarios se limpia al 5 Mbps por el 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 monitorear el policing, usted 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 en exceso han aumentado en 5068. Esto significa que el policer ha caído 5068 paquetes y 304 permitidos para pasar a través. Dado la velocidad de entrada de 17 Mbps, el policer debe pasar 1/17 del tráfico. Si usted compara los paquetes caídos y remitidos, usted ve que éste ha sido el caso: 304/(304 + 5068) = 0.057, o áspero 1/17. Una cierta variación de poca importancia es posible debido a la granularidad de control de hardware.

Para las estadísticas de regulación del 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 de conteo de la policía` muestra el número de paquetes limpiados por el 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