Regulación y Marcado de QoS con Supervisor Engines basados en IOS 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.

La regulación no debe confundirse con el modelado del tráfico, aunque ambos garantizan 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 del tráfico almacena en búfer el tráfico fuera del perfil y suaviza las ráfagas de tráfico, pero afecta a la variación de demora y retraso. El modelado sólo se puede aplicar en una interfaz saliente, mientras que la regulación se puede aplicar tanto en las interfaces entrantes como en las salientes.

Catalyst 4000/4500 con Supervisor Engine 3, 4 y 2+ (SE3, SE4, SE2+ a partir de ahora en este documento) admite la regulación de tráfico en direcciones entrantes y salientes. También se admite el modelado de tráfico; sin embargo, este documento solo se ocupará de la regulación y la marcación. El marcado es un proceso de cambio del nivel del paquete QoS 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.

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 el regulador de agregado para limitar el tráfico del protocolo de transferencia de archivos trivial (TFTP) a 1 Mbps en las VLAN 1 y 3. Este regulador permitirá 1 Mbps de tráfico TFTP en las VLAN 1 y 3 juntas. 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 egreso a un paquete, se tomará la decisión más severa. Es decir, si el regulador de tráfico de ingreso especifica descartar el paquete y el regulador de egreso especifica marcar el paquete hacia abajo, el paquete se descartará. 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

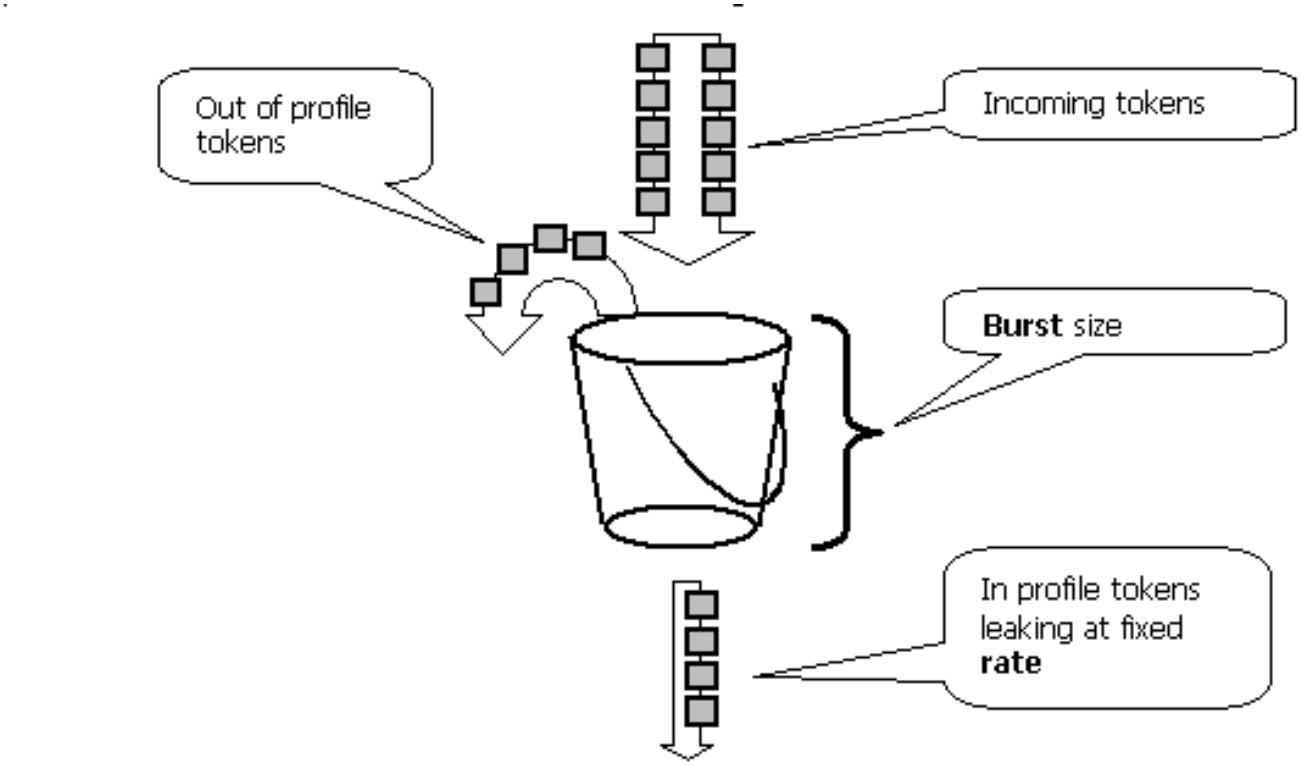
El hardware de QoS de Catalyst 4000 SE3, SE4, SE2+ se implementa de tal manera que el marcado real del paquete ocurre después del regulador de egreso. Esto significa que si bien la política de ingreso remarca el paquete (mediante la marcación del supervisor o la marcación regular), la política de egreso 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 lo 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 reguladores agregados son por dirección. Es decir, si se aplica un regulador agregado tanto a la entrada como a la salida, habrá dos reguladores de tráfico agregados, uno en la entrada y otro en la salida.
- Cuando se aplica un regulador agregado dentro de la política a las VLAN y a la interfaz física, habrá efectivamente dos reguladores de tráfico agregados: 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.

La regulación del tráfico en Catalyst 4000 SE3, SE4, SE2+ cumple con el concepto de cubeta con fugas, como ilustra el siguiente modelo. 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. La cubeta sólo se utiliza para decidir si el paquete está en perfil o fuera de perfil.

Tenga en cuenta que la implementación exacta del hardware de la regulación podría ser diferente, funcionalmente cumple con el modelo anterior.

Los siguientes parámetros controlan la operación de regulación de tráfico:

- La 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.
- 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.

Refiérase a la sección Comparación de Regulación de Tráfico y Marcado en Catalyst 6000 y Catalyst 4000/4500 IOS Based Supervisor Engines al final de este documento para ver las diferencias en ráfaga entre Catalyst 6000 y 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 hardware de QoS de Catalyst 4000 SE3, SE4, SE2+ tiene cierta granularidad para la regulación. De acuerdo con la velocidad configurada, la desviación máxima de la velocidad es 1.5% de ella.

Al configurar la velocidad de ráfaga, debe tener en cuenta que algunos protocolos (como TCP) implementan mecanismos de control de flujo que reaccionan ante la pérdida de paquetes. Por ejemplo, TCP reduce la ventana a la mitad para cada paquete perdido. Cuando se controla a una velocidad determinada, la utilización efectiva del link será menor que la velocidad configurada. Uno puede aumentar la ráfaga para lograr una mejor utilización. Un buen comienzo para este tráfico sería establecer la ráfaga en el doble de la cantidad de tráfico enviada con la velocidad deseada durante el tiempo de ida y vuelta (RTT). Por la misma razón, no se recomienda comparar la operación del regulador por tráfico orientado a la conexión, ya que generalmente mostrará un rendimiento inferior al permitido por el regulador.

Nota: El tráfico sin conexión también podría reaccionar a la regulación de forma diferente. 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 descartado podría activar la retransmisión de muchos paquetes (bloque completo).

Por ejemplo, el siguiente es un cálculo de la ráfaga para una sesión TCP, con una velocidad de regulación de 64 Kbps y un RTT TCP de 0,05 segundos:

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

Nota: <burst> es para una sesión TCP, por lo que debe ampliarse para que promedie el número esperado de sesiones que pasan a través del regulador de tráfico. 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 controlado por defecto señala el paquete al mismo DSCP, es decir, no se produce una reducción.

Nota: Los paquetes se pueden enviar fuera de servicio cuando un paquete fuera de perfil se marca en un DSCP a una cola de salida diferente a la DSCP original. Por esta razón, si el pedido de paquetes es importante, se recomienda marcar los paquetes fuera de perfil a DSCP mapeados a la misma cola de salida que los paquetes dentro del perfil.

Funciones de Regulación y Marcado Soportadas por los Motores Supervisor Basados en IOS de Catalyst 4000/4500

Tanto la regulación de entrada (interfaz entrante) como la de salida (interfaz saliente) son compatibles con Catalyst 4000 SE3, SE4, SE2+. El switch admite 1024 reguladores de tráfico de ingreso y 1024 de egreso. El sistema utiliza dos reguladores de entrada y dos de salida para el comportamiento predeterminado de no regulación.

Tenga en cuenta que cuando el regulador agregado se aplica dentro de la política a una VLAN y a una interfaz física, se utiliza una entrada de regulador de hardware adicional. 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 soporte para regulación. El Catalyst 4000 admite hasta 8 sentencias de coincidencia válidas por clase y se admiten hasta 8 clases por policy-map. Las instrucciones de coincidencia válidas son las siguientes:

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

Nota: Para los paquetes V4 que no son de IP, la instrucción **match ip dscp** es la única forma de clasificación, siempre que los paquetes entren en los puertos troncales confiando en el 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 válidas son las siguientes:

- 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 divide el tráfico en diferentes clases para el procesamiento de QoS basado en criterios definidos. Para que coincida con la precedencia IP o el DSCP, la interfaz entrante correspondiente se debe establecer en el modo de confianza. El switch admite CoS de confianza, DSCP de confianza e 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 DSCP, el switch derivará el nivel de QoS 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. Estos mapas son los siguientes:

- DSCP a DSCP regulado; 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 para la implementación de QoS en Catalyst 4000 SE3, SE4, SE2+.

Configuración y control de tráfico

La configuración de la regulación en IOS implica los siguientes pasos:

1. Definición de la regulación de tráfico.
2. Definición de criterios de selección de tráfico para el establecimiento de políticas.
3. Definir política de servicio mediante la clase y aplicar un regulador 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 conectado al puerto 5/14 que envía ~17 Mbps de 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
```

El siguiente comando se utiliza para monitorear la operación de regulación:

```
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.

Tenga en cuenta las siguientes consideraciones específicas sobre la implementación:

- 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.
- Los reguladores no mantienen los contadores de paquetes, sólo se soportan 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 actualizan periódicamente. 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 van a clasificar utilizando criterios previamente definidos.
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 queremos que el tráfico entrante con precedencia IP 3 se asigne al puerto UDP 192.168.196.3 77 del host a la precedencia 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.

```
! enable QoS globally
qos
! define ACL to select UDP traffic to 192.168.196.3 port 777
ip access-list extended acl_test4
permit udp any host 192.168.196.3 eq 777
! define class of traffic using ACL and ip precedence matching
class-map match-all cl_test10
match ip precedence 3
match access-group name acl_test4
! all the remaining ip precedence 3 traffic will match this class
class-map match-all cl_test11
match ip precedence 3
! define policy with above classes
policy-map po_test10
class cl_test10
```

```
! mark traffic belonging to class with ip precedence 6
set ip precedence 6
class cl_test11
! police and mark down all other ip precedence 3 traffic
police 1 mbps 1000 exceed-action policed-dscp-transmit
!
! adjust DSCP to policed DSCP map so to map DSCP 24 to DSCP 16
qos map dscp policed 24 to dscp 16
!
interface FastEthernet5/14
! set interface to trust IP DSCP
qos trust dscp
! apply policy to interface
service-policy input po_test10
!
```

El comando **sh policy interface** se utiliza para monitorear el marcado. La salida de ejemplo y las consecuencias están documentadas en la configuración de la regulación del tráfico antes mencionada.

Comparación de Regulación de Tráfico y Marcado en Motores Supervisor Basados en Catalyst 6000 y Catalyst 4000/4500 IOS

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