Introducción a QoS Policing y Marcación en el Catalyst 3550

Contenido

Introducción

La función de regulación le determina si el nivel de tráficog está dentro del perfil específicado o del contrato, y permite al tráfico fuera de perfil del descenso o lo marca abajo a un diverso valor del Differential Services Code Point (DSCP). Esto aplica un nivel de servicio contratado.

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

El policing no debe ser confundido con el modelado de tráfico, aunque ambos se aseeguren las estancias del tráfico dentro del perfil o del contrato.

El policing no mitiga el tráfico, así que el policing no afecta al retraso de la transmisión. En vez de mitigar los paquetes fuera de perfil, la vigilancia los cae o los marca con diversos niveles de QoS (DSCP reducido).

El modelado de tráfico mitiga el tráfico fuera de perfil y alisa las ráfagas de tráfico, pero afecta al retardo y a la variación de retraso. El shaping se puede aplicar solamente en la interfaz saliente, mientras que la vigilancia se puede aplicar en ambos las interfaces entrante y saliente.

El Catalyst 3550 soporta el policing para entrante y las direcciones de salida. El modelado de tráfico no se soporta.

El marcado cambia el paquete QoS llano según una directiva.

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.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

Versiones de hardware y de software

Las Políticas y marcado en el Catalyst 3550 se soportan con todas las versiones de software. La última guía de configuración se enumera aquí. Refiera a esta documentación para todas las características admitidas.

- Configuración de QoS

QoS Policing y Parámetros de Marcación

Para configurar el policing, usted debe definir política de calidad de servicio (QoS) las correspondencias y aplicarlas a los puertos. Esto se conoce de otra manera como acceso basado QoS.

Nota: QoS VLAN basado no es soportado actualmente por el Catalyst 3550.

El policer es definido por la tarifa y los parámetros de ráfaga así como acción para el tráfico fuera de perfil.

Soportan a estos dos tipos de policers:

- Agregado
- Individual

El vigilante global actúa sobre el tráfico a través de todos los casos donde está aplicado. Los actos del regulador individual por separado sobre el tráfico a través de cada caso donde está aplicado.

Nota: En el Catalyst 3550, el vigilante global puede ser aplicado solamente a diversas clases de la misma directiva. El policing global a través de las interfaces múltiples o de las directivas no se soporta.

Por ejemplo, aplique al vigilante global para limitar el tráfico del customer1 y de la clase customer2 de la clase en el mismo directiva-mapa al 1 Mbps. Tal policer permite el 1 Mbps del tráfico en el customer1 de la clase y customer2 junto. Si usted aplica el regulador individual, el policer limita el tráfico para el customer1 de la clase al 1 Mbps y para la clase customer2 al 1 Mbps. Por lo tanto, cada caso del policer es separado.

Esta tabla resume la acción de QoS sobre el paquete cuando es tratado por ambas políticas de ingreso y egreso:

Nota: Es posible marcar y disminución dentro de la misma clase de tráfico de la misma directiva. En tal caso, todo el tráfico para la clase determinada se marca primero. El policing y la disminución ocurre en el tráfico ya marcado.

La Supervisión de QoS en el Catalyst 3550 cumple con este concepto de contador dinámico:

El número de tokens proporcionales a los tamaños de paquete de tráfico entrante se pone en un token bucket; el número de tokens iguala el tamaño del paquete. En un intervalo regular, un número definido de tokens derivados de la velocidad configurada se quita del compartimiento. Si no hay lugar en el compartimiento para acomodar un paquete entrante, el paquete se considera fuera de perfil y se cae o se marca abajo según la acción de regulación configurada.

Este concepto se muestra en este ejemplo:

Nota: El tráfico no está mitigado en el compartimiento mientras que puede aparecer en este ejemplo. El tráfico real no atraviesa el compartimiento en absoluto; el compartimiento se utiliza solamente para decidir a si el paquete está en el perfil o el fuera de perfil.

Nota: La implementación de hardware del policing puede variar, pero todavía cumple funcionalmente a este modelo.

Estos parámetros controlan la operación del policing:

- **Tarifa** — define cuántos tokens se quitan en cada intervalo. Esto fija de manera eficaz la velocidad de tráfico ordenado. Todo el tráfico debajo de la tarifa se considera en el perfil. Las velocidades soportadas se extienden a partir de 8 kbps al 2 Gbps, y incrementan por 8 kbps.
- **Intervalo** — define cuantas veces los tokens se quitan del compartimiento. El intervalo se repara en 0.125 milisegundos (o 8000 veces por segundo). Este intervalo no puede ser cambiado.
- **Explosión** — define la cantidad máxima de tokens que el compartimiento puede sostenerse en cualquier momento. Rango de explosiones soportado a partir de 8000 bytes a 2000000 bytes, y al incremento por 64 bytes.

Nota: Aunque las cadenas de la ayuda de la línea de comandos muestren una amplia gama de valores, la opción tarifa-BPS no puede exceder la velocidad del puerto configurado, y la opción del byte de ráfaga no puede exceder 2000000 bytes. Si usted ingresa un valor más grande, el Switch rechaza la correspondencia de políticas cuando usted lo asocia a una interfaz.

Para sostener la velocidad de tráfico especificada, la explosión debe ser ninguna menos que la suma de esta ecuación:

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

Por ejemplo, calcule el valor mínimo de ráfaga para sostener un índice de 1 Mbps. La tarifa se define como 1000 kbps, así que la ráfaga mínima necesaria es la suma de esta ecuación:

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

El tamaño de ráfaga soportado mínimo es 8000 bytes, que es más que la ráfaga mínima calculada.

Nota: Debido a la granularidad de control de hardware, a la velocidad exacta y a la explosión se redondea al valor admitido más cercano.

Cuando usted configura la velocidad de ráfaga, usted debe tener en cuenta que algunos mecanismos de implementación del protocolo que reaccionen a la pérdida del paquete. Por ejemplo, el Transmission Control Protocol (TCP) reduce la ventana por la mitad para cada paquete perdido. Esto causa “un efecto del diente de la sierra” en tráfico TCP cuando el TCP intenta acelerar a la línea tarifa y es estrangulado por el policer. Si la tasa promedio del tráfico del diente de la sierra se calcula, esta tarifa es mucho más baja que la tarifa limpiada. Sin embargo, usted puede aumentar la explosión para alcanzar una mejor utilización. Un buen comienzo es fijar la explosión igual dos veces a la cantidad del tráfico enviado con la velocidad deseada durante el Round-Trip Time (TCP RTT). Si el RTT no se sabe, usted puede doblar el valor del parámetro de ráfaga.

Por la misma razón, no es recomendado para evaluar la operación de regulador de tráfico por el tráfico orientado a la conexión. Este escenario muestra generalmente el menor rendimiento que permitido por el policer.

El Tráfico sin conexión puede también reaccionar a la vigilancia diferentemente. Por ejemplo, el Network File System (NFS) utiliza los bloques, que podrían consistir en más de un paquete del User Datagram Protocol (UDP). Un paquete caído puede accionar muchos paquetes, incluso el bloque entero, para ser retransmitido.

Este ejemplo calcula la explosión para una sesión TCP con una velocidad de tráfico ordenado de 64 kbps y dado el TCP RTT son, 0.05 segundos:

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

En este ejemplo, el `<burst>` está para una sesión TCP. Escale esta figura para hacer un promedio del número esperado de sesiones que viajan con el policer.

Nota: Esto es un ejemplo solamente, en cada caso usted necesita evaluar el tráfico y los requerimientos de la aplicación y comportamiento contra los recursos disponibles para elegir los parámetros de regulación de tráfico.

La acción de regulación de tráfico puede ser caer el paquete o cambiar el DSCP del paquete (disminución). Para la disminución el paquete, un mapa DSCP limpiado debe ser modificada. Un mapa DSCP limpiado valor por defecto comenta el paquete al mismo DSCP. Por lo tanto, ninguna disminución ocurre.

Los paquetes pueden ser enviados fuera de servicio cuando un paquete fuera de perfil se marca abajo a un DSCP asociado en una diversa cola de salida que el DSCP original. Si la pedido de los paquetes es importante, los paquetes fuera de perfil de la disminución al DSCP asociaron a la misma cola de salida que los paquetes del en perfil.

Políticas y características de marcación soportados por Catalyst 3550

Esta tabla proporciona un resumen de las características relacionadas Políticas y marcadas soportadas por el Catalyst 3550, analizado por la dirección:

Una declaración de coincidencia se soporta por el clase-mapa. Éstas son declaraciones de coincidencia válida para la política de ingreso:

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

Nota: En el Catalyst 3550, no soportan al **comando match interface** y se permite a solamente un comando match en un clase-mapa. Por lo tanto, es difícil clasificar todo el tráfico que viene adentro a través de una interfaz y limpia todo el tráfico con un solo policer. Vea cómo clasificar todo el tráfico de la interfaz con una sola sección del policer de este documento.

Ésta es la declaración de coincidencia válida para la política de egress:

- match ip dscp

Éstas son acciones de política válida para la política de ingreso:

- vigilancia
- fije el dscp del IP (la marca)
- fije la Prioridad IP (la marca)
- trust dscp
- trust ip-precedence
- trust cos

Esta tabla muestra la matriz soportada de las directivas de QoS del ingreso:

1. Esta opción también cubre la Prioridad IP de la coincidencia.
2. Esta opción cubre confiar en CoS, la Prioridad IP, y el DSCP.
3. Esta opción también cubre la determinación de la Prioridad IP.

Ésta es la acción de política válida para la política de egress:

- vigilancia

Esta tabla muestra la matriz soportada de las directivas de QoS de la salida:

La marca permite que el QoS llano del paquete cambie basado sobre la clasificación o el policing. La clasificación parte el tráfico en diversas clases para el proceso de QoS basado en los criterios definidos.

El proceso de QoS se basa en el DSCP interno; la medida del QoS llano del paquete. El DSCP interno se deriva según la configuración de la confianza. Los soportes de sistema que confían en el CoS, el DSCP, la Prioridad IP, y las interfaces no confiables. La confianza especifica el campo del cual el DSCP interno se deriva para cada paquete, como sigue:

- Al confiar en CoS, el nivel de QoS se deriva de la encabezado de la capa 2 (L2) del protocolo inter-switch link (ISL) o del paquete encapsulado del 802.1Q.

- Al confiar en el DSCP o la Prioridad IP, el sistema deriva el QoS llano del DSCP o del campo de precedencia IP del paquete por consiguiente.

Confiar en CoS es solamente significativo en las interfaces troncales, y confiar en el DSCP (o la Prioridad IP) tiene sentido para los paquetes del IP solamente.

Cuando una interfaz no se confía en, el DSCP interno se deriva de CoS predeterminado configurable para la interfaz correspondiente. Éste es el estado predeterminado cuando se habilita QoS. Si no se configura ningún valor por defecto CoS, el valor predeterminado es cero.

Una vez que se determina el DSCP interno, puede ser cambiado marcando y limpiando, o ser conservado.

Después de que el paquete experimente el QoS que procesa, sus campos del nivel de QoS (dentro del campo IP/DSCP para el IP, y dentro de la encabezado ISL/802.1Q, si ninguno) son actualizados del DSCP interno. Hay estas correspondencias especiales de QoS relevantes a la vigilancia:

- **DSCP DSCP-a-limpiado** — usado para derivar el DSCP limpiado cuando usted disminución traga el paquete.
- **DSCP-a-CoS** — usado para derivar el nivel de CoS del DSCP interno para poner al día la encabezado del paquete de salida ISL/802.1Q.
- **CoS-to-DSCP** — usado para derivar el DSCP interno de CoS entrante (encabezado ISL/802.1Q) cuando la interfaz está en el modo de CoS de la confianza.

Éstas son consideraciones específicas de implementación importantes:

- La política de servicio del ingreso no se puede asociar a la interfaz cuando la interfaz se configura para confiar en las métricas QoS unas de los, tales como CoS/DSCP o Prioridad IP. Para hacer juego en la precedencia y la policía DSCP/IP en el ingreso, usted debe configurar la confianza para la clase determinada dentro de la directiva, no en la interfaz. Para marcar basó en la precedencia DSCP/IP, ninguna confianza debe ser configurado.
- Solamente el tráfico del IPv4 sin las opciones IP y la encapsulación del Advanced Research Projects Agency del Ethernet II (ARPA) se considera tráfico IP del hardware y del punto de vista de QoS. El resto del tráfico se considera no IP incluyendo, IP con las opciones, tales como IP encapsulado del Subnetwork Access Protocol (BROCHE) y IPv6.
- Para los paquetes del no IP, el “grupo de acceso de la coincidencia” es el único método de clasificación porque usted no puede hacer juego el DSCP para el tráfico no IP. Una lista de acceso (ACL) del Media Access Control (MAC) se utiliza para ese propósito; los paquetes se pueden corresponder con sobre la base del MAC Address de origen, de la dirección MAC del destino, y del Ethertype. No es posible hacer juego el tráfico IP con el MAC ACL, puesto que el Switch hace una distinción entre el IP y el tráfico no IP.

Configuración y policing del monitor

Estos pasos son necesarios para configurar el policing en el Cisco IOS:

1. Defina un policer (para los vigilantes globales)
2. Defina los criterios para seleccionar el tráfico para limpiar
3. Defina un clase-mapa para seleccionar el tráfico usando los criterios definidos
4. Defina una servicio-directiva usando la clase y la aplicación de un policer a la clase

especificada

5. Aplique una servicio-directiva a un puerto

Soportan a estos dos tipos de policers:

- Total mencionado
- Individual

El Supervisor de tráfico total designado limpia el tráfico combinado de todas las clases dentro de la misma directiva a donde está aplicada. El policing global a través de diversas interfaces no se soporta.

Nota: El vigilante global no puede ser aplicado a más de una directiva. Si es, se visualiza este mensaje de error:

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

Tenga en cuenta este ejemplo:

Hay un generador de tráfico asociado para virar GigabitEthernet0/3 hacia el lado de babor que envíe aproximadamente el 17 Mbps del tráfico UDP con el puerto destino 111. Hay también tráfico TCP del puerto 20. Usted quisiera que estos dos flujos de tráfico fueran limpiados abajo al 1 Mbps, y el tráfico excesivo debe ser caído. 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
!
```

El primer ejemplo utilizó al Supervisor de tráfico total designado. El regulador individual, a diferencia del regulador de tráfico designado, limpia el tráfico por separado en cada clase donde está aplicado. El regulador individual se define dentro de la configuración de correspondencia de políticas. En este ejemplo, dos clases de tráfico son limpiadas por dos reguladores individuales; cl_udp111 se limpia al 1 Mbps por la explosión 8K, y cl_tcp20 se limpia a 512 kbps por 32k la explosión:

```
!--- 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 el funcionamiento de establecimiento de políticas:

```
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: Por abandono, no hay estadísticas por-DSCP. El Catalyst 3550 soporta un por interface, recolección de estadísticas de la por-dirección para hasta ocho diversos valores DSCP. Se configura esto cuando usted publica el **comando mls qos monitor**. Para monitorear las estadísticas para DSCP 8, 16, 24, y 32, usted debe publicar 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
```

Ésta es una descripción de los campos en el ejemplo:

- **Entrante** — muestra cuántos paquetes llegan de cada dirección
- **NO_change** — muestra cuántos paquetes eran confiados en (por ejemplo el nivel de QoS no cambiado)

- **Clasificado** — muestra cuántos se han asignado los paquetes a este DSCP interno después de la clasificación
- **Limpiado** — muestra cuántos paquetes fueron marcados abajo limpiando; DSCP mostrado antes de la disminución.
- **Caído** — muestra cuántos paquetes fueron caídos limpiando

Sea consciente de estas consideraciones específicas de implementación:

- Si se configuran ocho valores DSCP cuando usted publica el **comando mls qos monitor**, los otros al revés vistos cuando usted publica el **comando show mls qos int statistics** podrían visualizar la información inadecuada.
- No hay comando específico para verificar velocidad de tráfico ofrecido o saliente por regulador.
- Puesto que los contadores se extraen del hardware secuencialmente, es posible que los contadores no agregan para arriba correctamente. Por ejemplo, la cantidad de limpiado, clasificada, o los paquetes perdidos puede ser levemente diferentes que el número de paquetes entrantes.

Configuración y marca del monitor

Estos pasos son necesarios para configurar la marca:

1. Defina los criterios para clasificar el tráfico
2. Defina las clases de tráfico que se clasificarán con los criterios definidos previamente
3. Cree una correspondencia de políticas que asocie las acciones y las acciones de regulación de tráfico de la marca a las clases definidas
4. Configure la interfaz correspondiente para confiar en el modo
5. Aplique la correspondencia de políticas a una interfaz

En este ejemplo, usted quisiera que el tráfico IP entrante recibiera 192.168.192.168 marcado con la Prioridad IP 6 y limpiado abajo al 1 Mbps; el tráfico en exceso se debe marcar abajo a la Prioridad 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
```

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

Cómo clasificar todos interconecte el tráfico con un solo policer

En el Catalyst 3550, no soportan al **comando match interface**, y se permite a solamente un

comando match por el clase-mapa. Por otra parte, el Catalyst 3550 no permite que el tráfico IP sea correspondido con por el MAC ACL. Tan el IP y el tráfico no IP se deben clasificar con dos class-maps separados. Esto lo hace difícil para clasificar todo el tráfico que entra en una interfaz y limpia todo el tráfico con un solo policer. La configuración de muestra aquí le deja lograr esto. En esta configuración, el IP y el tráfico no IP se corresponden con con dos diversos class-maps. Sin embargo, cada uno utiliza un regulador en común para ambos 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

- Configurar QoS en el Catalyst 3550
- Páginas del soporte de control de calidad de servicio
- Página de Soporte de LAN Switching
- Páginas de Soporte de Productos de LAN
- Soporte Técnico y Documentación - Cisco Systems