Resolución de problemas de QoS de switches Catalyst 6500

Contenido

Introducción

Este documento contiene pasos básicos de Troubleshooting, limitaciones de Calidad de Servicio (QoS) y proporciona información para resolver problemas comunes de QoS en Catalyst 6500 Switches. Este documento también aborda los problemas de QoS que ocurren en la clasificación, marcado y regulación.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en los Catalyst 6500 Series Switches.

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

Convenciones

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

Antecedentes

QoS es una función de red para clasificar el tráfico y proporcionar servicios de entrega predecibles. Estos elementos explican los diversos pasos del proceso de QoS:

- **Programación de entrada**: es manejada por ASIC de puerto de hardware y es una operación QoS de Capa 2. No requiere una tarjeta de función de políticas (PFC).
- **Clasificación**: el supervisor y/o la PFC la controlan mediante el motor de lista de control de acceso (ACL). El supervisor se encarga de la operación de QoS de Capa 2. PFC gestiona el funcionamiento de QoS de Capa 2 y Capa 3.
- **Regulación de Tráfico**: PFC lo maneja a través del motor de reenvío de Capa 3. Se requiere PFC y gestiona el funcionamiento de QoS de Capa 2 y Capa 3.
- **Re-escritura de paquetes**: los ASIC del puerto de hardware se encargan de manejarlo. Es una operación de QoS de Capa 2 y Capa 3 basada en la clasificación realizada anteriormente.
- **Programación de salida**: es manejada por los ASIC de puerto de hardware. Es una operación de QoS de Capa 2 y Capa 3 basada en la clasificación realizada anteriormente.

Resolución de problemas de QoS

QoS funciona de manera diferente en los switches Catalyst 6500 que en los routers. La arquitectura de QoS es bastante compleja en los switches Catalyst 6500. Se recomienda que comprenda la tarjeta de función de switch multicapa (MSFC), PFC y la arquitectura de motor supervisor en el Catalyst 6500. La configuración de QoS en el sistema operativo híbrido necesita conocer mejor la funcionalidad CatOS de la capa 2 y la MSFC de la capa 3 con la funcionalidad Cisco IOS®. Se recomienda leer estos documentos en profundidad antes de configurar QoS:

- Configuración de QoS PFC - IOS nativo
- Configuración de QoS - CatOS

Procedimiento paso a paso para solucionar problemas

Esta sección contiene el procedimiento básico de resolución de problemas paso a paso para QoS con el fin de aislar el problema para la resolución de problemas adicional.

1. **Habilitar QoS**: el **comando show mls qos** muestra las estadísticas de regulación de tráfico y el estado de QoS, habilitado o inhabilitado.

```
Switch#show mls qos
  QoS is enabled globally
  QoS ip packet dscp rewrite enabled globally
  Input mode for GRE Tunnel is Pipe mode
  Input mode for MPLS is Pipe mode
  Vlan or Portchannel(Multi-Earl)policies supported: Yes
  Egress policies supported: Yes


 ----- Module [5] -----
  QoS global counters:
    Total packets: 244
    IP shortcut packets: 0
    Packets dropped by policing: 0
    IP packets with TOS changed by policing: 5
    IP packets with COS changed by policing: 4
    Non-IP packets with COS changed by policing: 0
    MPLS packets with EXP changed by policing: 0
```

2. **Clasificación del tráfico entrante mediante puerto de confianza**: esta clasificación clasifica el tráfico entrante en uno de los siete valores de clase de servicio (CoS). El tráfico entrante puede tener el valor CoS ya asignado por el origen. En este caso, debe configurar el puerto para que confíe en el valor CoS del tráfico entrante. Trust permite al switch mantener los valores CoS o tipo de servicio (ToS) de la trama recibida. Este comando muestra cómo verificar el estado de confianza del puerto:

```
Switch#show queueing int fa 3/40
  Port QoS is enabled
Trust state: trust CoS
  Extend trust state: not trusted [CoS = 0]
  Default CoS is 0

!--- Output suppressed.
```

   El valor de CoS sólo se transporta mediante tramas Inter-Switch Link (ISL) y dot1q. Las tramas sin etiqueta no llevan valores CoS. Las tramas sin etiqueta contienen valores ToS que se derivan de la precedencia IP o del punto de código de servicios diferenciados (DSCP) del encabezado del paquete IP. Para confiar en el valor ToS, debe configurar el puerto para confiar en la precedencia IP o DSCP. DSCP es compatible con la precedencia IP. Por ejemplo, si ha configurado un puerto de switch como puerto de Capa 3, no lleva tramas dot1q o ISL. En este caso, debe configurar este puerto para confiar en la precedencia DSCP o IP.

```
Switch#show queueing interface gigabitEthernet 1/1
Interface GigabitEthernet1/1 queueing strategy:  Weighted Round-Robin
  Port QoS is enabled
  Trust state: trust DSCP
  Extend trust state: not trusted [COS = 0]
  Default CoS is 0

!--- Output suppressed.
```

3. **Clasificación del tráfico entrante mediante ACL y ACE**: también puede configurar el switch para clasificar y marcar el tráfico. Los pasos incluidos para configurar la clasificación y el marcado son: cree listas de acceso, class-map y policy-map, y ejecute el comando **service-policy input** para aplicar el policy-map a la interfaz. Puede verificar las estadísticas del mapa de políticas como se muestra aquí:

```
Switch#show policy-map interface fa 3/13
 FastEthernet3/13

  Service-policy input: pqos2
```

```
    class-map: qos1 (match-all)
      Match: access-group 101
      set precedence 5:
      Earl in slot 5 :
        590 bytes
       5 minute offered rate 32 bps
        aggregate-forwarded 590 bytes

    Class-map: class-default (match-any)
      36 packets, 2394 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any

Switch#show mls qos ip ingress
 QoS Summary [IPv4]:      (* - shared aggregates, Mod - switch module)

      Int Mod Dir  Class-map DSCP  Agg  Trust Fl   AgForward-By   AgPoliced-By
                                   Id         Id
-------------------------------------------------------------------------------
    Fa3/13  5  In       qos1   40    1     No  10            590              0

       All  5   -    Default    0    0*    No  0          365487              0
```

Observe que los contadores **AgForward-By** que corresponden a la clase-map qos1 aumentan. Si no ve las estadísticas para el mapa de clase correspondiente, verifique la lista de acceso asociada al mapa de clase.

4. **Programación de entrada**: no se requiere PFC para configurar la programación de entrada. No puede configurar los comandos **rcv-queue threshold** o **set qos drop-threshold** en un único puerto 10/100. Esto se debe a que la programación de entrada es manejada por los puertos ASIC de bobina que contienen doce puertos 10/100. Por lo tanto, debe configurar la programación de entrada en conjuntos de 12 puertos, como 1-12, 13-24, 25-36, 37-48.La arquitectura de colocación en cola está integrada en el ASIC y no se puede reconfigurar. Ejecute el comando **show queueing interface fastethernet slot/port | incluyen el** comando **type** para ver la estructura de cola de un puerto LAN.

```
Switch#show queueing interface fastEthernet 3/40
Queueing Mode In Rx direction: mode-cos
    Receive queues [type = 1q4t]:          <--------- 1 Queue 4 Threshold
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       1         Standard            4


    queue tail-drop-thresholds
    --------------------------
    1     50[1] 60[2] 80[3] 100[4]  <------ Threshold levels 50%, 60%, 80% and 100%


  Packets dropped on Receive:
    BPDU packets:  0

    queue thresh    dropped  [cos-map]
    ---------------------------------------------------
    1     1               0  [0 1 ]
    1     2               0  [2 3 ]
    1     3               0  [4 5 ]
    1     4               0  [6 7 ]

!--- Output suppressed.
```

De forma predeterminada, los 4 umbrales son 100%. Puede ejecutar el comando **rcv-queue threshold** *<Queue Id> <Threshold 1> <Threshold 2> <Threshold 3> <Threshold 14>* para

configurar los niveles de umbral. De esta manera, los datos de valores CoS más altos no se descartan antes de los datos de valor CoS más bajos durante la congestión.

```
Switch(config)#interface range fa 3/37 - 48
Switch(config-if-range)#rcv-queue threshold 1 50 60 80 100
```

5. **Mapping**: si el puerto está configurado para confiar en el CoS, utilice la tabla de mapa CoS-DSCP para mapear el valor CoS recibido en un valor DSCP interno.

```
Switch#show mls qos maps cos-dscp
   Cos-dscp map:
        cos:   0  1  2  3  4  5  6  7
     ---------------------------------
        dscp:   0  8 16 24 32 40 48 56
```

Si el puerto está configurado para confiar en la precedencia IP de confianza, utilice la tabla ip-prec-dscp map para asignar el valor de precedencia IP recibido a un valor DSCP interno.

```
Switch#show mls qos maps ip-prec-dscp
   IpPrecedence-dscp map:
      ipprec:   0  1  2  3  4  5  6  7
     ---------------------------------
        dscp:   0  8 16 24 32 40 48 56
```

Si el puerto está configurado para confiar en el DSCP, el valor DSCP recibido se utiliza como valor DSCP interno.Estas tablas deben ser las mismas en todos los switches de la red. Si alguno de los switches tiene una tabla con asignaciones diferentes, no recibirá el resultado deseado. Puede cambiar estos valores de tabla como se muestra aquí:

```
Switch(config)#mls qos map cos-dscp 0 8 16 24 40 48 48 56
Switch(config)#mls qos map ip-prec-dscp 0 8 16 24 40 48 48 56
```

6. **Regulación de Tráfico**: Hay dos tipos de regulación disponibles en Catalyst 6500 Switches:**Regulación de tráfico agregado**: la regulación de agregado controla el ancho de banda de un flujo en el switch. El comando **show mls qos aggregate-policer** muestra todo el regulador de agregado configurado en el switch. Estas son las estadísticas de regulación:

```
Switch#show mls qos ip fastEthernet 3/13
   [In] Policy map is pqos2   [Out] Default.
 QoS Summary [IPv4]:      (* - shared aggregates, Mod - switch module)

      Int Mod Dir  Class-map DSCP  Agg  Trust Fl   AgForward-By   AgPoliced-By
                                   Id         Id
-------------------------------------------------------------------------------
    Fa3/13  5  In       qos1    0    1*  dscp  0          10626         118860
    Fa3/13  5  In class-defa   40    2     No  0           3338              0

Switch#show mls qos
  QoS is enabled globally
  QoS ip packet dscp rewrite enabled globally
  Input mode for GRE Tunnel is Pipe mode
  Input mode for MPLS is Pipe mode
  Vlan or Portchannel(Multi-Earl) policies supported: Yes
  Egress policies supported: Yes


 ----- Module [5] -----
  QoS global counters:
    Total packets: 163
    IP shortcut packets: 0
    Packets dropped by policing: 120
    IP packets with TOS changed by policing: 24
    IP packets with COS changed by policing: 20
    Non-IP packets with COS changed by policing: 3
    MPLS packets with EXP changed by policing: 0
```

Regulación de tráfico de microflujo: la regulación de microflujo controla el ancho de banda de un flujo por interfaz en el switch. De forma predeterminada, los reguladores de microflujo afectan sólo al tráfico ruteado. Ejecute el comando **mls qos bridged** en la interfaz VLAN para habilitar el control de microflujo para el tráfico puenteado. Esta es la verificación de las estadísticas de regulación de microflujo:

```
Switch#show mls ip detail
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f         :AdjPtr
---------------------------------------------------------------------------
Pkts         Bytes         Age   LastSeen  Attributes
-----------------------------------------------

Mask Pi R CR Xt Prio Dsc IP_EN OP_EN Pattern Rpf FIN_RDT FIN/RST
----+--+-+--+--+----+---+-----+-----+-------+---+-------+-------
Ig/acli Ig/aclo Ig/qosi Ig/qoso Fpkt Gemini MC-hit Dirty Diags
-------+-------+-------+-------+----+------+------+-----+------

    QoS     Police Count Threshold    Leak     Drop Bucket  Use-Tbl Use-Enable
-----------+------------+---------+-----------+----+-------+-------+----------+
10.175.50.2     10.175.51.2     icmp:8      :0        --               :0x0
43           64500          84    21:37:16   L3 - Dynamic
1    1  0  0  1  0    0    1     1     0       0     0      0
0          0       0       0      0    0       0     0     0
  0x0          0                0         0       NO   1518      NO       NO
10.175.50.2     10.175.51.2     icmp:0      :0        --               :0x0
43           64500          84    21:37:16   L3 - Dynamic
1    1  0  0  1  0    0    1     1     0       0     0      0
0          0       0       0      0    0       0     0     0
  0x0          664832          0         0       NO   1491      NO       NO
0.0.0.0          0.0.0.0          0   :0      :0        --               :0x0
1980         155689         1092  21:37:16   L3 - Dynamic
0    1  0  0  1  0    0    1     1     0       0     0      0
0          0       0       0      0    0       0     0     0
  0x0          0                0         0       NO   0         NO       NO

Switch#show mls qos
  QoS is enabled globally
  QoS ip packet dscp rewrite enabled globally
  Input mode for GRE Tunnel is Pipe mode
  Input mode for MPLS is Pipe mode
  Vlan or Portchannel(Multi-Earl) policies supported: Yes
  Egress policies supported: Yes


 ----- Module [5] -----
  QoS global counters:
    Total packets: 551
    IP shortcut packets: 0
    Packets dropped by policing: 473
    IP packets with TOS changed by policing: 70
    IP packets with COS changed by policing: 44
    Non-IP packets with COS changed by policing: 11
    MPLS packets with EXP changed by policing: 0
```

Nota: El comando **show mls qos ip** *type mod/number* no muestra las estadísticas de regulación de microflujo. Solo muestra las estadísticas de regulación agregada.Si no ve las estadísticas de regulación de tráfico deseadas, verifique la configuración de regulación de tráfico. Refiérase a QoS Policing en Catalyst 6500/6000 Series Switches para ver el ejemplo de configuración. Además, consulte la sección Pautas y limitaciones de QoS en switches Catalyst 6500 de este documento.

7. Verifique las notas de versión de su versión del sistema operativo y asegúrese de que no

haya errores relacionados con su configuración de QoS.

8. Observe su modelo de supervisor de switch, modelo PFC, modelo MSFC y versión de Cisco IOS/CatOS. Consulte las Pautas y Limitaciones de QoS en los Catalyst 6500 Switches con referencia a sus especificaciones. Asegúrese de que su configuración sea aplicable.

Pautas y limitaciones de QoS en switches Catalyst 6500

Hay limitaciones de QoS que debe tener en cuenta antes de configurar QoS en switches Catalyst 6500:

- Pautas generales
- Pautas de PFC3
- Pautas de PFC2
- Restricciones del Comando Class Map
- Restricciones del Comando Policy Map
- Restricciones del Comando Policy Map Class
- Pautas y Restricciones de Mapping de Umbrales de Colas y Descartes
- Trust-cos en Limitaciones de entradas de ACL
- Limitaciones de las tarjetas de línea WS-X6248-xx, WS-X6224-xx, y WS-X6348-xx
- PFC o PFC2 no proporcionan QoS para el tráfico WAN. Con PFC o PFC2, la QoS de PFC no cambia el byte ToS en el tráfico WAN.
- El tráfico de LAN de entrada que se conmuta por Capa 3 no pasa a través de MSFC o MSFC2 y conserva el valor de CoS asignado por el motor de conmutación de Capa 3.
- La QoS no implementa la prevención de la congestión de puertos de ingreso en los puertos configurados con las palabras clave **no confiable**, **trust-ipprec** o **trust-dscp**. El tráfico va directamente al motor de conmutación.
- El switch utiliza el umbral de descarte de cola para el tráfico que transporta los valores de CoS que se asignan solamente a la cola. El switch utiliza los umbrales WRED-drop para el tráfico que transporta los valores CoS que se mapean a la cola y un umbral.
- La clasificación con un motor de conmutación de Capa 3 utiliza los valores de Capa 2, 3 y 4. La marcación con un motor de conmutación de Capa 3 utiliza los valores CoS de Capa 2 y los valores de precedencia IP o DSCP de Capa 3.
- Una ACL de trust-cos no puede restaurar la CoS recibida en el tráfico de los puertos no confiables. El tráfico de los puertos no confiables siempre tiene el valor CoS del puerto.

Nota: La QoS de PFC no detecta el uso de comandos no admitidos hasta que se asocia un policy map a una interfaz.

Limitación de QoS_TCAM

El Ternary CAM (TCAM) es una pieza especializada de memoria diseñada para búsquedas de tabla rápidas, basadas en paquetes que pasan a través del switch, realizada por el motor ACL en PFC, PFC2 y PFC3. Las ACL se procesan en hardware en los switches Catalyst de Cisco serie 6500 que se denominan TCAM. Cuando configura ACL, mapea la ACL a la QoS y cuando aplica la política de QoS en la interfaz, el switch programa la TCAM. Si ya ha utilizado todo el espacio TCAM disponible en el switch para la QoS, encontrará este mensaje de error:

```
Switch(config)#interface vlan 52
Switch(config-if)#service-policy input test
```

```
Switch(config-if)#
3w0d: %QM-4-TCAM_ENTRY: Hardware TCAM entry capacity exceeded
```

Esta salida del comando **show tcam count** muestra que las máscaras de entrada TCAM se utilizan en un 95%. Debido a esto, cuando aplica la política de QoS en la interfaz, se encuentra con el mensaje `%QM-4-TCAM_ENTRY:` .

```
Switch#show tcam count
           Used        Free        Percent Used       Reserved
           ----        ----        ------------       --------
 Labels:(in) 43        4053            1
 Labels:(eg)  2        4094            0

ACL_TCAM
--------
  Masks:     19        4077            0                   72
Entries:     95       32673            0                  576

QOS_TCAM
--------
  Masks:   3902         194           95                   18
Entries:  23101        9667           70                  144

    LOU:      0         128            0
  ANDOR:      0          16            0
  ORAND:      0          16            0
    ADJ:      3        2045            0
```

Las entradas TCAM y las etiquetas ACL son recursos limitados. Por lo tanto, en función de la configuración de ACL, es posible que deba tener cuidado de no agotar los recursos disponibles. Además, con grandes configuraciones de ACL de QoS y lista de control de acceso de VLAN (VACL), es posible que también deba tener en cuenta el espacio de memoria de acceso aleatorio no volátil (NVRAM). Los recursos de hardware disponibles difieren en Supervisor 1a con PFC, Supervisor 2 con PFC2 y Supervisor 720 con PFC3.

Módulo Supervisor	TCAM de QoS	Etiquetas ACL
Supervisor 1a y PFC	2000 máscaras y patrones de 16 000 compartidos entre listas de control de acceso de router (RACL), VACL y ACL de QoS	512 etiquetas ACL compartidas entre RACL, VACL y ACL de QoS
Supervisor 2 y PFC2	4000 máscaras y 32 000 patrones para ACL de QoS	512 etiquetas ACL compartidas entre RACL, VACL y ACL de QoS
Supervisor 720 y PFC3	4000 máscaras y 32 000 patrones para ACL de QoS	512 etiquetas ACL compartidas entre RACL, VACL y ACL de QoS

Nota: Independientemente del límite de etiqueta de ACL 512, hay un límite de software adicional en Cisco CatOS de 250 ACL de QoS en todo el sistema cuando se utiliza el modo de

configuración predeterminado (binario). Esta restricción se elimina en el modo de configuración de texto. Ejecute el comando **set config mode text** para cambiar el modo de configuración al modo de texto. El modo de texto normalmente utiliza menos espacio de memoria NVRAM o Flash que el que utiliza el modo de configuración binaria. Debe ejecutar el comando **write memory** mientras opera en modo texto para guardar la configuración en NVRAM. Ejecute el comando **set config mode text auto-save** para guardar la configuración de texto en NVRAM automáticamente.

Esta es la solución temporal para el problema TCAM:

- Si ha implementado el comando **service-policy** en muchas interfaces de Capa 2 que pertenecen a una VLAN, puede implementar el control de tráfico basado en VLAN en lugar de basado en el puerto del switch. Aquí tiene un ejemplo:

```
Switch(config)#interface range fastethernet x/y - Z
Switch(config-if)#mls qos vlan-based
Switch(config-if)#exit
Switch(config)#interface vlan 100
Switch(config-if)#service-policy input Test_Policy
```

- Desactive las estadísticas de marcación de QoS. El comando **no mls qos mark statistics** no permite implementar el máximo de 1020 AgID. Esto se debe a que asigna el regulador predeterminado para los reguladores de tráfico dscp establecidos. La desventaja de esto es que no hay estadísticas para el regulador de tráfico específico porque todos comparten el regulador de tráfico predeterminado.

```
Switch(config)#no mls qos marking statistics
```

- Si es posible, utilice las mismas ACL en varias interfaces para reducir la contención de recursos TCAM.

Limitación de NBAR

El reconocimiento de aplicaciones basadas en red (NBAR) es un motor de clasificación que reconoce una amplia variedad de aplicaciones, que incluye protocolos basados en Web y otros de difícil clasificación que utilizan asignaciones dinámicas de puertos TCP/UDP. Cuando NBAR reconoce y clasifica una aplicación, una red puede invocar servicios para esa aplicación específica. NBAR clasifica los paquetes y luego aplica QoS al tráfico clasificado para asegurarse de que el ancho de banda de la red se utilice de manera eficiente. Hay algunas restricciones en cómo implementar QoS cuando utiliza NBAR:

- PFC3 no admite NBAR.
- Con Supervisor Engine 2, PFC2 y MSFC2:Puede configurar NBAR en interfaces de Capa 3 en lugar de QoS PFC.PFC2 proporciona soporte de hardware para las ACL de entrada en los puertos donde se configura NBAR.Cuando se habilita la QoS de PFC, el tráfico a través de los puertos donde se configura NBAR pasa a través de las colas de ingreso y egreso y los umbrales de descarte.Cuando se habilita la QoS de PFC, la MSFC2 establece la CoS de salida igual a la precedencia IP de salida en el tráfico NBAR.Después de que todo el tráfico pasa a través de una cola de ingreso, se procesa en el software en el MSFC2 en las interfaces donde se configura NBAR.

Faltan los comandos cos-map en el Supervisor 2

Bajo Native IOS Software Releases 12.1(8a)EX-12.1(8b)EX5 y 12.1(11b)E y posteriores, los CoS-

mappings de QoS predeterminados para los links ascendentes Gigabit ubicados en el Supervisor2 han cambiado. Todos los valores de CoS se han asignado a la cola 1 y al umbral 1, y no se pueden cambiar.

Estos comandos no se pueden configurar en un puerto Sup2 Gigabit Uplink en estas versiones:

```
rcv-queue cos-map
priority-queue
wrr-queue cos-map
```

Las configuraciones de QoS son limitadas y no se puede utilizar la cola de prioridad estricta. Esto afecta solamente a los puertos Gigabit ubicados físicamente en el Supervisor 2 Engine. Los puertos Gigabit en otros módulos de tarjeta de línea no se ven afectados.

Hay una actualización del firmware que resuelve este problema. Esta actualización se puede realizar a través del software. Póngase en contacto con el servicio de asistencia técnica si necesita actualizar el firmware. Tenga en cuenta que sólo se necesita una actualización del firmware si la versión de hardware del Supervisor2 es inferior a 4.0. Si la versión HW del Supervisor2 es 4.0 o posterior, QoS debe ser permitida en los puertos de link ascendente Gigabit sin la actualización del firmware. Puede ejecutar el comando **show module** para encontrar el nivel de firmware. Este problema se identifica en el Id. de bug Cisco CSCdw89764 (sólo clientes registrados) .

Limitaciones de la política de servicio

Para aplicar policy-map a la interfaz, ejecute el comando **service-policy**. Si tiene un comando no admitido en policy-map, después de aplicarlo con el comando **service-policy**, el switch solicita los mensajes de error en la consola. Estos puntos deben tenerse en cuenta al resolver los problemas **relacionados con la política de servicio**.

- No adjunte una política de servicio a un puerto que sea miembro de un EtherChannel.
- Con las tarjetas de reenvío distribuido (DFC) instaladas, PFC2 no admite QoS basada en VLAN. No puede ejecutar el comando **mls qos vlan-based** ni adjuntar políticas de servicio a las interfaces VLAN.
- PFC QoS soporta la palabra clave output solamente con PFC3 y solamente en interfaces de Capa 3 (ya sea puertos LAN configurados como interfaces de Capa 3 o interfaces VLAN). Con PFC3, puede asociar un mapa de política de entrada y de salida a una interfaz de Capa 3.
- La QoS de PFC basada en VLAN o basada en puerto en los puertos de Capa 2 no es relevante para las políticas conectadas a las interfaces de Capa 3 con la palabra clave output.
- Las políticas adjuntas a la palabra clave output no admiten la regulación de microflujo.
- No puede asociar un policy map que configure un estado de confianza con el resultado del comando **service-policy**.
- La QoS de PFC no admite el descenso de entrada con caída de salida o caída de entrada con reducción de salida.

Las sentencias de salida de política de servicio no aparecen en el resultado del comando running-config

Cuando configura QoS en el link múltiple en el Módulo FlexWan, no puede ver el resultado del comando **service-policy** en el resultado del comando **show running-config**. Esto ocurre cuando el switch ejecuta las versiones de Cisco IOS anteriores a 12.2SX. FlexWAN para la serie 7600 de Cisco admite dLLQ en interfaces que no sean de paquete. No soporta dLLQ en interfaces de agrupamiento MLPPP. Este soporte está disponible con la versión 12.2S del software del IOS de Cisco.

La solución temporal para eludir esta limitación es adjuntar la política de servicio a interfaces desagrupadas o actualizar la versión de Cisco IOS a 12.2SX o posterior, donde se soporta la función.

Limitación de regulación

La regulación se realiza en hardware en PFC sin el impacto del rendimiento del switch. La regulación del tráfico no puede ocurrir en la plataforma 6500 sin PFC. En el sistema operativo híbrido, la regulación debe configurarse en el CatOS. Estos puntos deben tenerse en cuenta al resolver problemas de regulación:

- Cuando se aplica la regulación de entrada y la regulación de salida al mismo tráfico, tanto la política de entrada como la de salida deben marcar el tráfico o descartarlo. La QoS de PFC no admite el descenso de entrada con caída de salida o caída de entrada con reducción de salida.
- Cuando se crea un regulador que no utiliza la palabra clave pir y el parámetro maximum_burst_bytes es igual al parámetro normal_burst_bytes (que es el caso si no se ingresa el parámetro maximum_burst_bytes), las palabras clave de exceso-acción policed-dscp-transmit hacen que la QoS de PFC marque el tráfico como se define en el mapa de reducción policed-dscp max-burst.
- Cuando se descarta la acción de exceso, la QoS de PFC ignora cualquier acción de violación configurada.
- Cuando configura drop como la acción de conformidad, PFC QoS configura drop como la acción de exceso y la acción de violación.
- Los requisitos de máscara de flujo de la regulación de microflujo, NetFlow y NetFlow Data Export (NDE) podrían entrar en conflicto.

Límite de velocidad o problemas de regulación de tráfico con MSFC en sistema operativo híbrido

En los switches Catalyst 6500 que ejecutan el sistema operativo híbrido, la configuración de rate-limit no proporciona el resultado deseado. Por ejemplo, si configura el comando **rate-limit** bajo el comando **interface vlan** en la MSFC, en realidad no limita la velocidad del tráfico.

```
interface Vlan10
 rate-limit input 256000 2000 2000 conform-action transmit exceed-action drop
 rate-limit output 256000 2000 2000 conform-action transmit exceed-action drop
```

O bien:

```
interface Vlan10
service-policy input Test_Policy
```

La razón detrás de esto es que la MSFC se ocupa solamente de las funciones de control, pero el

reenvío de tráfico real ocurre en los ASIC PFC en el supervisor. La MSFC compila la FIB y las tablas de adyacencia, así como otra información de control, y la descarga a la PFC para implementarla en hardware. Con la configuración que ha creado, limita la velocidad sólo el tráfico conmutado por software, que debe ser mínimo (o ninguno).

La solución alternativa es utilizar la interfaz de línea de comandos (CLI) de CatOS para configurar el límite de velocidad en el supervisor. Refiérase a QoS de CatOS para obtener la explicación detallada de cómo configurar la regulación de QoS en CatOS. También puede consultar QoS Policing en Catalyst 6500/6000 Series Switches para ver el ejemplo de configuración.

Promedio de forma de comando no admitido en interfaces VLAN de Cisco 7600

Cuando aplica una entrada de política de servicio a una interfaz en Cisco 7600, aparece este mensaje de error:

```
7600_1(config)#int Gi 1/40
7600_1(config-if)#service-policy input POLICY_1
shape average command is not supported for this interface
```

El comando **shape promedio** no se soporta para las interfaces VLAN en Cisco 7600. En su lugar, debe utilizar la regulación.

```
7600_1(config)#policy-map POLICY_1
7600_1(config-pmap)#class TRAFFIC_1
7600_1(config-pmap-c)#police conform-action transmit exceed-action drop
```

Refiérase a Configuración de Policy Map Class Policing para obtener más información sobre cómo implementar la regulación del tráfico para limitar la velocidad.

Al asociar esta política de servicio a una interfaz VLAN (SVI), debe habilitar la QoS basada en VLAN en todos los puertos de capa 2 que pertenecen a esta VLAN en los que desea que se aplique este mapa de políticas.

```
7600_1(config)#interface Gi 1/40
7600_1(config-if)#mls qos vlan-based
```

Consulte Habilitación de QoS de PFC Basada en VLAN en los Puertos LAN de Capa 2 para obtener más información.

ERROR DE QoS: La adición/modificación realizada a policy map [chars] y class [chars] no es válida, el comando se rechaza

```
QoS-ERROR: Addition/Modification made to policymap vtc-map and class voice-video is
not valid, command is rejected
```

Este mensaje de error indica que las acciones definidas en la clase mencionada no están permitidas en los Cisco Catalyst 6500 Series Switches. Hay algunas restricciones durante la configuración de las acciones de clase de policy map.

- No puede hacer los tres siguientes en una clase de policy map:Marcar el tráfico con los comandos **set**Configuración del estado de confianzaConfiguración del control de tráficoSólo puede marcar el tráfico con los comandos **set**.OConfigure el estado de confianza y/o

configure la regulación.
- Para el tráfico conmutado por hardware, la QoS de PFC no soporta los comandos de clase de policy map **bandwidth**, **priority**, **queue-limit** o **random-detect**. Puede configurar estos comandos porque se pueden utilizar para el tráfico conmutado por software.
- La QoS de PFC no soporta los comandos **set qos-group** policy map class.

Refiérase a Configuración de Acciones de Clase de Policy Map para obtener más información sobre tales restricciones.

Información Relacionada

- Clasificación y Marcado de QoS en los Catalyst 6500/6000 Series Switches que Ejecutan Cisco IOS Software
- Programación de salida de QoS en switches Catalyst 6500/6000 Series que ejecutan Cisco IOS System Software
- Supervisión de QoS en switches Catalyst de la serie 6500/6000
- Clasificación y marcación de QoS en los switches de la serie Catalyst 6500/6000 con software CatOS
- Programa de salida de QoS en los switches de la serie Catalyst 6500/6000 con software del sistema CatOS
- Páginas de Soporte de Productos de LAN
- Página de Soporte de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems