# Troubleshooting de QoS de los Catalyst 6500 Switch

## 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.

## prerrequisitos

### Requisitos

No hay requisitos específicos para este documento.

### Componentes Utilizados

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

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.

## Antecedentes

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

- **Scheduling de la entrada** — Es dirigido por el puerto de hardware Asics y es una operación de QoS de la capa 2. No requiere un Policy Feature Card (PFC).
- **Clasificación** — Es dirigida por el supervisor y/o el PFC vía el motor de la lista de control de acceso (ACL). El supervisor maneja la operación de QoS de la capa 2. El PFC maneja la operación de QoS de la capa 2 y de la capa 3.
- **Vigilancia** — Es dirigida por el PFC vía el Motor de reenvío de la capa 3. Se requiere el PFC y maneja la operación de QoS de la capa 2 y de la capa 3.
- **Reescritura del paquete** — Es dirigida por el puerto de hardware Asics. Es una operación de QoS de la capa 2 y de la capa 3 basada en la clasificación hecha previamente.
- **Programación de salida** — Es dirigida por el puerto de hardware Asics. Es una operación de QoS de la capa 2 y de la capa 3 basada en la clasificación hecha previamente.

## Troubleshooting QoS

Trabajos de QoS diferentemente en los Catalyst 6500 Switch que en el Routers. La arquitectura de QoS es muy compleja en los Catalyst 6500 Switch. Se recomienda que usted entiende el (MSFC) de la Multilayer Switch Feature Card, el PFC, y la arquitectura del Supervisor Engine en el Catalyst 6500. La configuración de QoS en el código abierto híbrido necesita más comprensión de las funciones y de la capa 3 MSFC de CatOS de la capa 2 con las funciones de Cisco IOS®. Se recomienda para leer estos documentos profundizados antes de que usted configure QoS:

- Configurando PFC QoS - Native IOS
- Configurando QoS - CatOS

### Procedimiento paso a paso para solucionar problemas

Esta sección contiene el procedimiento básico del Troubleshooting paso a paso para QoS para aislar el problema para el troubleshooting adicional.

1. **Permiso QoS — El comando show mls qos** muestra las estadísticas del policing y el estatus de QoS, es habilitado o discapacitado.`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 usando el puerto de la confianza** — Esta clasificación categoriza el tráfico entrante en uno de los siete valores del Clase de Servicio (CoS). El tráfico entrante puede tener el valor de CoS asignado ya por la fuente. En este caso, usted necesita configurar el puerto para confiar en el valor de CoS del tráfico entrante. La confianza permite al Switch para mantener CoS o los valores del Tipo de servicio (ToS) de la trama recibida. Este comando muestra cómo verificar al 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 es llevado solamente por el Inter-Switch Link (ISL) y las tramas del dot1q. Las tramas sin Tags no llevan los valores de CoS. Las tramas sin Tags llevan los valores TOS que se derivan de la Prioridad IP o del Differentiated Services Code Point (DSCP) del encabezado del paquete IP. Para confiar en el valor TOS, usted necesita configurar el puerto para confiar en la Prioridad IP o el DSCP. El DSCP es compatible con versiones anteriores a la Prioridad IP. Por ejemplo, si usted ha configurado un puerto del switch como puerto de la capa 3, no lleva el dot1q o las tramas ISL. En este caso, usted necesita configurar este puerto para confiar en el DSCP o la Prioridad 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 usando el ACL y los ACE** — usted puede también configurar el Switch para clasificar y para marcar el tráfico. Los pasos incluidos para configurar la Clasificación y marcado son: cree las listas de acceso, el clase-mapa, y el directiva-mapa, y publique el comando de la **entrada de política de servicio** para aplicar el directiva-mapa en la interfaz. Usted puede verificar las estadísticas del directiva-mapa 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 Note que los contadores AgForward-**por** ése corresponden a los aumentos del clase-mapa qos1. Si usted no ve las estadísticas para el clase-mapa correspondiente, verifique la lista de acceso asociada al clase-mapa.
4. **Scheduling de la entrada** — El PFC no se requiere configurar la previsión de la entrada. Usted no puede configurar los comandos del **umbral de caída de los qos del umbral** o del **conjunto de la RCV-cola** en un solo 10/100 puerto. Esto es porque la previsión de la entrada es manejada por los puertos de ASIC de la bobina que contienen doce 10/100 de los puertos. Por lo tanto, usted tiene que configurar la entrada que programa en los conjuntos de 12 puertos, tales como 1-12, 13-24, 25-36, 37-48.La arquitectura de espera se incorpora a ASIC y no puede ser configurada de nuevo. Publique el **/port del slot del FastEthernet de la interfaz para colocación en cola de la demostración | incluya el comando type** de ver la estructura de la 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 ----------

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.* Por abandono, todos los 4 umbrales son el 100%. Usted puede publicar el comando del *<Threshold 14> del <Threshold 3> del <Threshold 2> del <Threshold 1> de Id> del <Queue del* **umbral de la RCV-cola** para configurar los límites de umbral. De esta manera, los datos más altos de los valores de CoS no se caen antes de datos más bajos del valor de CoS durante la congestión.Switch(config)#**interface range fa 3/37 - 48** Switch(config-if-range)#**rcv-queue threshold 1 50 60 80 100**

5. **El asociar** — Si el puerto se configura para confiar en CoS, después utilice la tabla de asignación CoS-DSCP para asociar el valor recibido de CoS en 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 se configura para confiar en la Prioridad IP de la confianza, después utilice la tabla de asignación IP-prec-DSCP para asociar el valor de precedencia IP recibido en 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 se configura para confiar en el DSCP, después el valor recibido DSCP se utiliza como valor DSCP interno.Estas tablas deben ser lo mismo en todo el Switches en su red. Si del Switches tiene una tabla con diversas asignaciones, usted no recibe el resultado deseado. Usted puede cambiar estos valores de la 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. **Vigilancia** — Hay dos tipos de vigilancia disponibles en los Catalyst 6500 Switch:**Policing global** — Controles de policing globales el ancho de banda de un flujo en el Switch. **El comando mls qos aggregate policer de la demostración** muestra a todo el vigilante global configurado configurado en el Switch. Éstas son las estadísticas del policing: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 microflujo** — La regulación de microflujo controla el ancho de banda de un flujo por la interfaz en el Switch. Por abandono, los reguladores de microflujo afectan solamente al tráfico ruteado. Publique los **mls que los qos interligados** ordenan en la interfaz VLAN para habilitar la regulación de microflujo para el tráfico Bridged. Ésta es la verificación de las estadísticas de regulación del 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 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 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 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:** *La Mod del tipo del* **IP de los qos de los mls de la demostración***/el comando number* no muestra las estadísticas de regulación del microflujo. Muestran solamente las estadísticas globales del policing.Si usted no ve las estadísticas de vigilancia deseadas, verifique la configuración de establecimiento de política. Refiera a la Supervisión de QoS en los Catalyst 6500/6000 Series Switch para ver el ejemplo de configuración. También, vea las pautas de QoS y las limitaciones en la sección de los Catalyst 6500 Switch de este documento.

7. Marque los Release Note de su versión de OS y aseegurese allí no son ningún bug relacionado con su configuración de QoS.
8. Observe su modelo de Supervisor del Switch, el modelo PFC, el modelo MSFC y la versión de Cisco IOS/CatOS. Vea las pautas de QoS y las limitaciones en los Catalyst 6500 Switch referente a sus especificaciones. Aseegurese su configuración es aplicable.

## Pautas de QoS y limitaciones en los Catalyst 6500 Switch

Hay las limitaciones de QoS de las cuales usted necesita ser consciente antes de que usted configure QoS en los Catalyst 6500 Switch:

- Pautas generales
- Guías de consulta PFC3
- Guías de consulta PFC2
- Restricciones del comando class map
- Restricciones del comando de la correspondencia de políticas
- Restricciones del comando class de la correspondencia de políticas
- Guías de consulta y restricciones de la asignación de la cola y del umbral de caída
- Trust-cos en Limitaciones de entradas de ACL
- Limitaciones de las tarjetas de línea WS-X6248-xx, WS-X6224-xx, y WS-X6348-xx
- El PFC o el PFC2 no proporciona QoS para el tráfico PÁLIDO. Con el PFC o el PFC2, el PFC QoS no cambia el Byte ToS en el tráfico PÁLIDO.
- El tráfico de LAN del ingreso que es la capa 3 conmutada no pasa con el MSFC o el MSFC2 y conserva el valor de CoS que es asignado por el motor del Layer 3 Switching.
- QoS no implementa la prevención de congestión del puerto de ingreso en los puertos que se configuran con el **untrusted**, el **Trust-ipprec**, o las palabras claves del **Trust-dscp**. El tráfico va directamente al motor de Switching.
- El Switch utiliza el umbral de la eliminación de cola para el tráfico que lleva los valores de CoS que se asocian solamente a la cola. El Switch utiliza los umbrales de caída de WRED para el tráfico que lleva los valores de CoS que se asocian a la cola y a un umbral.
- La clasificación con un motor del Layer 3 Switching utiliza la capa 2,3, y 4 valores. La marca con un motor del Layer 3 Switching utiliza los valores de CoS de la capa 2 y la Prioridad IP de la capa 3 o los valores DSCP.
- Un Trust-cos ACL no puede restablecer el CoS recibido en el tráfico de los puertos untrusted. El tráfico de los puertos untrusted tiene siempre el valor del CoS del puerto.

**Nota:** El PFC QoS no detecta el uso de los comandos sin apoyo hasta que usted asocie una correspondencia de políticas a una interfaz.

## Limitación de QoS_TCAM

El Ternary CAM (TCAM) es un pedazo especializado de memoria diseñado para las búsquedas en la tabla rápidas, sobre la base de los paquetes que pasan a través del Switch, realizado por el motor ACL en el PFC, el PFC2, y el PFC3. Los ACL se procesan en hardware en los Cisco Catalyst 6500 Series Switch que se llaman TCAM. Cuando usted configura el ACL, asocie el ACL al QoS y cuando usted aplica política de calidad de servicio (QoS) encendido la interfaz, el Switch programa el TCAM. Si usted ha utilizado ya todo el espacio disponible TCAM en el Switch para el QoS, usted encuentra 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
```

Este ouput del **comando count del tcam de la demostración** muestra que las máscaras de la entrada TCAM son los 95% usados. Debido a esto, cuando usted aplica política de calidad de servicio (QoS) encendido la interfaz usted encuentra el `%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 escrituras de la etiqueta ACL son recursos limitados. Por lo tanto, dependiendo de su configuración ACL, usted puede ser que necesite tener cuidado de no agotar a los recursos disponibles. Además, con las configuraciones grandes de QoS ACL y del VLAN Access Control List (VACL), usted también puede ser que necesite considerar el espacio permanente de memoria de acceso aleatorio (NVRAM). Los Recursos de hardware disponibles diferencian en el supervisor 1a con el PFC, el supervisor 2 con el PFC2, y el supervisor 720 con el PFC3.

| Módulo de Supervisor | QoS TCAM | Escrituras de la etiqueta ACL |
|---|---|---|
| Supervisor 1a y PFC | máscaras 2K y modelos 16K compartidos entre los Router Access Control List (RACL), VACL y QoS ACL | 512 escrituras de la etiqueta ACL compartidas entre los RACL, los VACL, y QoS ACL |
| Supervisor 2 y PFC2 | máscaras 4K y 32k modelos para QoS ACL | 512 escrituras de la etiqueta ACL compartidas entre los RACL, los VACL, y QoS ACL |
| Supervisor 720 y PFC3 | máscaras 4K y 32k modelos para QoS ACL | 512 escrituras de la etiqueta ACL compartidas entre los RACL, los VACL, y QoS ACL |

**Nota:** Independiente del límite de la escritura de la etiqueta de 512 ACL, hay un límite de software adicional en Cisco CatOS de 250 QoS ACL sistema-ancho cuando usted utiliza al modo de configuración (binario) predeterminado. Esta restricción se quita en el modo de la configuración de texto. Publique el **comando set config mode text** para cambiar al modo de configuración al

Modo de texto. El Modo de texto utiliza típicamente menos NVRAM o espacio de memoria Flash que lo que el modo de la configuración binaria utiliza. Usted debe publicar el **comando write memory** mientras que usted actúa en el Modo de texto para salvar la configuración en el NVRAM. Publique el **comando set config mode text auto-save** para salvar la configuración de texto en el NVRAM automáticamente.

Ésta es la solución alternativa para el problema TCAM:

- Si usted ha implementado el **comando service-policy** en muchos interfaz de capa 2 que pertenecen a un VLA N, usted puede implementar el policing basado VLA N en vez del puerto del switch basado. 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`
- Estadísticas de la marca de QoS de la neutralización. **Los ningunos qos de los mls que marcan el comando statistics** no permiten que el máximo de 1020 AgIDs sea implementado. Esto es porque afecta un aparato el policer predeterminado para el policers del dscp del conjunto. La desventaja de esto es allí no es ninguna estadística para el policer específico porque todos comparten el policer predeterminado.`Switch(config)#no mls qos marking statistics`
- Si es posible, utilice los mismos ACL a través de las interfaces múltiples para reducir la contención del Recurso TCAM.

## Limitación NBAR

El Network-Based Application Recognition (NBAR) es un motor de clasificación que reconoce una amplia variedad de aplicaciones, que incluye basado en web y otro difícil-a-clasifica los protocolos que utilizan las asignaciones de puertos dinámicas TCP/UDP. Cuando una aplicación es reconocida y clasificada por el NBAR, una red puede invocar los servicios para esa aplicación específica. El NBAR clasifica los paquetes y después aplica QoS al tráfico clasificado para asegurarse de que el ancho de banda de la red está utilizado eficientemente. Hay algunas restricciones en cómo implementar QoS cuando usted utiliza el NBAR:

- El PFC3 no soporta el NBAR.
- Con un Supervisor Engine 2, un PFC2, y un MSFC2:Usted puede configurar el NBAR en las interfaces de la capa 3 en vez de PFC QoS.El PFC2 proporciona el soporte del hardware para las entradas ACL en los puertos en donde usted configura el NBAR.Cuando se habilita el PFC QoS, el tráfico a través de los puertos en donde usted configura los pasos NBAR a través del ingreso y las colas de administración del tráfico y los umbrales de caída de la salida.Cuando se habilita el PFC QoS, el MSFC2 fija la salida CoS igual a la Prioridad IP de la salida en el tráfico NBAR.Después de todo el tráfico pasa a través de una cola del ingreso, él se procesa en el software en el MSFC2 en las interfaces donde usted configura el NBAR.

## El mapa de CoS ordena a los desaparecidos en el supervisor 2

Bajo versiones de software 12.1(8a)EX-12.1(8b)EX5 y 12.1(11b)E del Native IOS y posterior, las CoS-asignaciones predeterminadas de QoS para los links ascendentes Gigabit situados en el Supervisor2 han cambiado. Todos los valores de CoS se han asignado para hacer cola 1 y el umbral 1, y no pueden ser cambiados.

Estos comandos no se pueden configurar en un puerto de link ascendente Gigabit del Sup2 en

estas versiones:

**rcv-queue cos-map priority-queue wrr-queue cos-map**
Las configuraciones de QoS son limitadas, y la cola de prioridad estricta no puede ser utilizada. Esto afecta solamente a los puertos Gigabit establecidos físicamente en el motor del supervisor 2. Los puertos Gigabit en otros módulos del linecard no son afectados.

Hay una actualización del firmware que resuelve este problema. Esta actualización se puede hacer vía el software. Soporte técnico del contacto si se requiere una actualización del firmware. Observe que una actualización del firmware está necesitada solamente si la versión HW del Supervisor2 es menos de 4.0. Si la versión HW del Supervisor2 es 4.0 o más adelante, QoS debe ser permisible en los puertos de link ascendente Gigabit sin la actualización del firmware. Usted puede publicar el **comando show module** para encontrar el nivel de firmware. Este problema se identifica en el Id. de bug Cisco CSCdw89764 (clientes registrados solamente).

## Limitaciones de la Servicio-directiva

Para aplicar el directiva-mapa a la interfaz, publique el **comando service-policy**. Si usted tiene un comando sin apoyo en el directiva-mapa, después de que usted lo aplique con el **comando service-policy**, el Switch indica los mensajes de error en la consola. Estas puntas necesitan ser consideradas mientras que usted resuelve problemas los asuntos relacionados de la servicio-**directiva**.

- No asocie una política de servicio a un puerto que sea un miembro de un EtherChannel.
- Con los indicadores luminosos LED amarillo de la placa muestra gravedad menor de envío distribuidos (DFC) instalados, el PFC2 no soporta QoS VLAN basado. Usted no puede publicar el **comando mls qos vlan-based** o asociar las políticas de servicio a las interfaces VLAN.
- El PFC QoS soporta la palabra clave de la salida solamente con el PFC3 y solamente en las interfaces de la capa 3 (los puertos LAN configurados como interfaces de la capa 3 o las interfaces VLAN). Con el PFC3, usted puede asociar una entrada y una correspondencia de la política de resultado a una interfaz de la capa 3.
- VLAN basado o el acceso basado PFC QoS en los puertos de la capa 2 no sea relevante a las directivas asociados para acodar 3 interfaces con la palabra clave de la salida.
- Las directivas asociadas con la palabra clave de la salida no soportan la regulación de microflujo.
- Usted no puede asociar una correspondencia de políticas que configure a un estado confiable con la salida del **comando service-policy**.
- El PFC QoS no soporta la disminución del ingreso con el descenso de la salida o el descenso del ingreso con la disminución de la salida.

## Las declaraciones de la salida de la Servicio-directiva no aparecen en la salida del comando running-config

Cuando usted configura QoS en el multilink en el módulo FlexWan, usted no puede ver el **comando service-policy** hacer salir en la salida del **comando show running-config**. Esto ocurre cuando el Switch funciona con las versiones deL Cisco IOS anterior que 12.2SX. El FlexWan para las Cisco 7600 Series soporta el dLLQ en las interfaces del NON-conjunto. No soporta dLLQ en interfaces de agrupamiento MLPPP. Tal soporte está disponible con el Cisco IOS Software

Release 12.2S.

La solución alternativa para desviar esta limitación es asociar la servicio-directiva a las interfaces desmontonadas o actualizar la versión deL Cisco IOS a 12.2SX o a más adelante, donde se soporta la característica.

## Vigilancia de la limitación

El policing se realiza en hardware en el PFC sin el impacto del funcionamiento del Switch. El policing no puede ocurrir en la plataforma 6500 sin el PFC. En el código abierto híbrido, la vigilancia se debe configurar en el CatOS. Estas puntas necesitan ser consideradas mientras que usted resuelve problemas los problemas de políticas:

- Cuando usted aplica el policing y la salida del ingreso que limpian al mismo tráfico, la política de entrada y la política de resultado deben marcar abajo del tráfico o del tráfico del descenso. El PFC QoS no soporta la disminución del ingreso con el descenso de la salida o el descenso del ingreso con la disminución de la salida.
- Cuando usted crea un policer que no utiliza la palabra clave del pir y el parámetro de los maximum_burst_bytes es igual al parámetro de los normal_burst_bytes (que es el caso si usted no ingresa el parámetro de los maximum_burst_bytes), la acción de excedente limpiar-DSCP-transmite la causa PFC QoS de las palabras claves para marcar el tráfico abajo según lo definido por el mapa reducido de la explosión del máximo limpiar-DSCP.
- Cuando la acción de excedente es descenso, el PFC QoS ignora cualquier acción de violación configurada.
- Cuando usted configura el descenso como la acción de conformidad, el PFC QoS configura el descenso como la acción de excedente y la acción de violación.
- Los requisitos del flowmask de la regulación de microflujo, del Netflow, y de la Exportación de datos de NetFlow (NDE) pudieron estar en conflicto.

## Tarifa-límite o problemas de políticas con el MSFC en el código abierto híbrido

En los Catalyst 6500 Switch que funcionan con el código abierto híbrido, la configuración del tarifa-límite no da la salida deseada. Por ejemplo, si usted configura el **comando rate-limit** bajo **comando interface vlan** en el MSFC, no hace realmente tarifa-límite el 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:

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

La razón detrás de esto es que el MSFC toma el cuidado solamente de las funciones de control, pero el reenvío de tráfico real ocurre en PFC Asics en el supervisor. El MSFC compila el FIB y las tablas de adyacencia, así como la otra información de control, y lo descarga al PFC para implementar en hardware. Con la configuración usted ha creado, usted tarifa-límite solamente el tráfico conmutado por software, que debe ser mínimo (o ninguno).

La solución alternativa es utilizar el comando line interface(cli) de CatOS para configurar el tarifa-límite en el supervisor. Refiera a CatOS QoS para la explicación detallada de cómo configurar la Supervisión de QoS en CatOS. Usted puede también referir a la Supervisión de QoS en los

Catalyst 6500/6000 Series Switch para ver el ejemplo de configuración.

## Media del comando shape no soportada en las interfaces VLAN del Cisco 7600

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

```
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 **medio de la dimensión de una variable** no se soporta para las interfaces VLAN en el Cisco 7600. En lugar usted necesita utilizar el policing.

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

Refiera a configurar el policing de la clase de la correspondencia de políticas para más información sobre cómo implementar el tráfico del tarifa-límite del policing.

Mientras que usted asocia esta servicio-directiva a una interfaz VLAN (SVI), usted necesita habilitar QoS VLAN basado en todo el ésos los puertos de la capa 2 que pertenecen a este VLA N en el cual usted quisiera que este directiva-mapa fuera aplicado.

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

Refiera a habilitar PFC VLAN basado QoS en los puertos LAN de la capa 2 para más información.

## QOS-ERROR: La adición/la modificación hizo al policymap [chars] y se rechaza la clase [chars] es inválida, comando

```
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 Switch. Hay algunas restricciones durante la configuración de las acciones de clase de correspondencia de políticas.

- Usted no puede hacer los tres de éstos en una clase de la correspondencia de políticas:Marque el tráfico con los **comandos set**Configure al estado confiableConfigure el policingUsted puede solamente cualquier tráfico de la marca con los **comandos set**.OConfigure al estado confiable y/o configure el policing.
- Para el tráfico conmutado por hardware, el PFC QoS no soporta el **ancho de banda**, **prioridad**, cola-**límite**, o al azar-**detecte los** comandos class de la correspondencia de políticas. Usted puede configurar estos comandos porque pueden ser utilizados para el tráfico conmutado por software.
- El PFC QoS no apoya los comandos class de la correspondencia de políticas del qos-**grupo del conjunto**.

Refiera a configurar las acciones de clase de correspondencia de políticas para más información sobre tales restricciones.

# Información Relacionada

- Clasificación de QoS y marca en los Catalyst 6500/6000 Series Switch que funcionan con el Cisco IOS Software

- Programación de salida de QoS en los Catalyst 6500/6000 Series Switch que funcionan con el software del sistema del Cisco IOS
- 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