Clasificación y Marcado de QoS en los Catalyst 6500/6000 Series Switches que Ejecutan Cisco IOS Software

Contenido

Introducción

Este documento examina lo qué sucede respecto al marcado y la clasificación de un paquete en las diversas etapas dentro del chasis Cisco Catalyst 6500/6000 que ejecuta el software de Cisco IOS®. Este documento describe casos y restricciones especiales y brinda breves casos prácticos.

Este documento no proporciona una lista exhaustiva de todos los comandos de Cisco IOS Software relacionados con QoS o marcado. Para obtener más información sobre la interfaz de línea de comandos (CLI) del software Cisco IOS, consulte Configuración de QoS PFC.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de hardware:

- Catalyst 6500/6000 Series Switches que ejecutan Cisco IOS Software y utilizan uno de estos Supervisor Engines:Supervisor Engine 1A con tarjeta de función de políticas (PFC) y tarjeta de función de switch multicapa (MSFC)Supervisor Engine 1A con PFC y MSFC2Supervisor Engine 2 con PFC2 y MSFC2

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.

Terminology

La lista proporciona la terminología que este documento utiliza:

- Punto de código de servicios diferenciados (DSCP): los primeros seis bits del byte de tipo de servicio (ToS) en el encabezado IP. DSCP sólo está presente en el paquete de IP.**Nota:** El switch también asigna un DSCP interno a cada paquete, ya sea IP o no. La sección Cuatro Fuentes Posibles para DSCP Interno de este documento detalla esta asignación DSCP interna.
- Precedencia IP: los primeros tres bits del byte ToS en el encabezado IP.
- Clase de servicio (CoS): el único campo que se puede utilizar para marcar un paquete en la capa 2 (L2). CoS consta de cualquiera de estos tres bits:Los tres bits IEEE 802.1p (dot1p) en la etiqueta IEEE 802.1Q (dot1q) para el paquete dot1q.**Nota:** De forma predeterminada, los switches de Cisco no etiquetan los paquetes VLAN nativos.Los tres bits denominados "Campo de usuario" en el encabezado Inter-Switch Link (ISL) para un paquete encapsulado ISL.**Nota:** El CoS no está presente dentro de un paquete sin punto1q o un paquete ISL.
- Clasificación: proceso que se utiliza para seleccionar el tráfico que se va a marcar.
- Marcado: proceso que establece un valor DSCP de capa 3 (L3) en un paquete. Este documento amplía la definición de marcado para incluir la configuración de los valores CoS L2.

Los switches Catalyst 6500/6000 Series pueden realizar clasificaciones en función de estos tres

parámetros:

- DSCP
- Precedencia IP
- CoS

Los Catalyst 6500/6000 Series Switches realizan la clasificación y el marcado en diversas etapas. Esto es lo que ocurre en diferentes lugares:

- Puerto de entrada (circuito integrado específico de la aplicación de entrada [ASIC])
- Motor de conmutación (PFC)
- Puerto de salida (ASIC de salida)

Tratamiento del puerto de entrada

El parámetro de configuración principal para el puerto de ingreso, con respecto a la clasificación, es el estado de `confianza` del puerto. Cada puerto del sistema puede tener uno de estos estados `de confianza`:

- `trust-ip-precedence`
- `trust-dscp`
- `trust-cos`
- `no confiable`

Para configurar o cambiar el estado `de confianza` del puerto, ejecute este comando de Cisco IOS Software en el `modo de interfaz`:

```
6k(config-if)#mls qos trust ?
  cos            cos keyword
  dscp           dscp keyword
  ip-precedence  ip-precedence keyword
  <cr>
```

Nota: De forma predeterminada, todos los puertos están en el estado `no confiable` cuando se habilita QoS. Para habilitar QoS en el Catalyst 6500 que ejecuta Cisco IOS Software, ejecute el **comando mls qos** en el modo de configuración principal.

En el nivel de puerto de entrada, también puede aplicar un CoS predeterminado por puerto. Aquí tiene un ejemplo:

```
6k(config-if)#mls qos cos cos-value
```

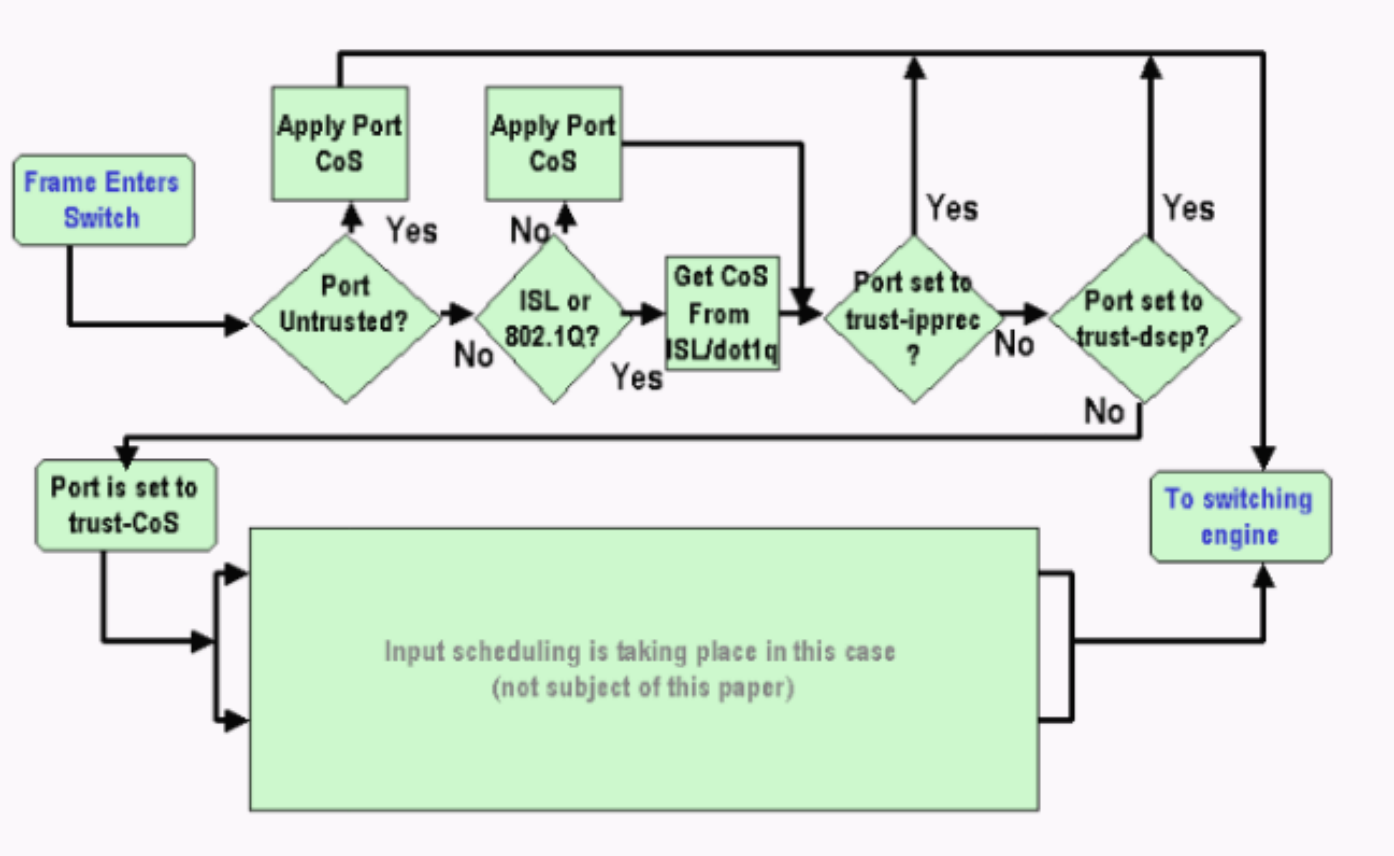
Esta clase de servicio predeterminada se aplica a todos los paquetes, como IP e Intercambio de paquetes entre redes (IPX). Puede aplicar el CoS predeterminado a cualquier puerto físico.

Si el puerto está en el estado `no confiable`, marque la trama con el CoS predeterminado del puerto y pase el encabezado al motor de conmutación (PFC). Si el puerto está configurado en uno de los estados `trust`, realice una de estas dos opciones:

- Si la trama no tiene un CoS recibido (dot1q o ISL), aplique el CoS del puerto predeterminado.
- Para las tramas dot1q e ISL, mantenga el CoS tal como está.

A continuación, pase la trama al motor de conmutación.

Este ejemplo ilustra la clasificación de entrada y el marcado. El ejemplo muestra cómo asignar una CoS interna a cada trama:



Nota: Como se muestra en este ejemplo, a cada trama se le asigna una CoS interna. La asignación se basa en el CoS recibido o en el CoS del puerto predeterminado. El CoS interno incluye tramas sin etiqueta que no llevan ninguna CoS real. El CoS interno se escribe en un encabezado de paquete especial, que se denomina encabezado de bus de datos, y se envía a través del bus de datos al motor de conmutación.

Motor de conmutación (PFC)

Cuando el encabezado alcanza el motor de conmutación, el motor de conmutación Enhanced Address Recognition Logic (EARL) asigna a cada trama un DSCP interno. Este DSCP interno es una prioridad interna que el PFC asigna a la trama a medida que la trama transita por el switch. Este no es el DSCP en el encabezado IP versión 4 (IPv4). El DSCP interno se deriva de una configuración CoS o ToS existente y se utiliza para restablecer el CoS o ToS a medida que la trama sale del switch. Este DSCP interno se asigna a todas las tramas conmutadas o ruteadas por el PFC, incluso a las tramas que no son IP.

Esta sección trata sobre cómo puede asignar una política de servicio a la interfaz para realizar una marcación. La sección también discute la configuración final del DSCP interno, que depende del estado de `confianza` de puerto y de la política de servicio que se aplica.

Configuración de la Política de Servicio para Clasificar o Marcar un Paquete en Cisco IOS Software Release 12.1(12c)E y Posteriores

Complete estos pasos para configurar la política de servicio:

1. Configure una lista de control de acceso (ACL) para definir el tráfico que desea considerar.La ACL se puede numerar o nombrar, y el Catalyst 6500/6000 soporta una ACL extendida. Ejecute el comando **access-list *xxx*** Cisco IOS Software, como muestra este ejemplo:
   ```
   (config)#access-list 101 permit ip any host 10.1.1.1
   ```

2. Configure una clase de tráfico (mapa de clase) para que coincida con el tráfico en función de la ACL que haya definido o en función del DSCP recibido.Ejecute el comando **class-map** Cisco IOS Software. La QoS de PFC no admite más de una sentencia de coincidencia por mapa de clase. Además, la QoS de PFC sólo admite estas sentencias coincidentes:**match ip access-groupmatch ip dscpmatch ip precedencematch protocolNota:** El comando **match protocol** permite el uso de Network Based Application Recognition (NBAR) para hacer coincidir el tráfico.**Nota:** De estas opciones, sólo se soportan las instrucciones **match ip dscp** y **match ip precedence** y funcionan. Sin embargo, estas declaraciones no son útiles en la marcación o clasificación de los paquetes. Puede utilizar estas sentencias, por ejemplo, para realizar la regulación de todos los paquetes que coincidan con un DSCP determinado. Sin embargo, esta acción está fuera del alcance de este documento.
   ```
   (config)#class-map class-name
   (config-cmap)#match {access-group | input-interface | ip dscp}
   ```
   Nota: Este ejemplo muestra sólo tres opciones para el comando **match**. Pero puede configurar muchas más opciones en este símbolo del sistema.**Nota:** Cualquiera de las opciones de este comando **match** se toma para los criterios de coincidencia y las otras opciones se dejan afuera, según los paquetes entrantes.Aquí tiene un ejemplo:

   ```
   class-map match-any TEST
    match access-group 101

   class-map match-all TEST2
    match ip precedence 6
   ```

3. Configure un policy map para aplicar una política a una clase que haya definido previamente.El mapa de política contiene:Un nombreUn conjunto de instrucciones de clasePara cada instrucción de clase, la acción que se debe realizar para esa claseLas acciones admitidas en QoS PFC1 y PFC2 son:**trust dscptrust ip precedencetrust cosset ip dscp** en Cisco IOS Software Release 12.1(12c)E1 y posteriores**set ip precedence** en Cisco IOS Software Release 12.1(12c)E1 y posteriores**vigilanciaNota:** Esta acción está fuera del alcance de este documento.
   ```
   (config)#policy-map policy-name
   (config-pmap)#class class-name
   (config-pmap-c)#{police | set ip dscp}
   ```

   Nota: Este ejemplo muestra sólo dos opciones, pero puede configurar muchas más opciones en este símbolo del sistema `(config-pmap-c)#`.Aquí tiene un ejemplo:

   ```
   policy-map test_policy
    class TEST
      trust ip precedence
    class TEST2
      set ip dscp 16
   ```

4. Configure una entrada de política de servicio para aplicar un mapa de política definido previamente a una o más interfaces.**Nota:** Puede asociar una política de servicio a la interfaz

física o a la interfaz virtual conmutada (SVI) o a la interfaz VLAN. Si conecta una política de servicio a una interfaz VLAN, los únicos puertos que utilizan esta política de servicio son los puertos que pertenecen a esa VLAN y están configurados para QoS basada en VLAN. Si el puerto no está configurado para QoS basada en VLAN, el puerto todavía utiliza la QoS predeterminada basada en puerto y sólo observa la política de servicio que está conectada a la interfaz física.Este ejemplo aplica la política de servicio `test_policy` al puerto Gigabit Ethernet 1/1:

```
(config) interface gigabitethernet 1/1
(config-if)#service-policy input test_policy
```

Este ejemplo aplica la política de servicio `test_policy` a todos los puertos en VLAN 10 que tienen una configuración basada en VLAN desde el punto de vista de QoS:

```
(config) interface gigabitethernet 1/2
(config-if)#switchport mode access
(config-if)#switchport access vlan 10
(config-if)#mls qos vlan-based
(config-if)#exit
(config-if)#interface vlan 10
(config-if)#service-policy input test_policy
```

Nota: Puede combinar los pasos 2 y 3 de este procedimiento si omite la definición específica de la clase y asocia la ACL directamente en la definición del policy map. En este ejemplo, cuando la clase `TEST police` no se ha definido antes de la configuración del policy map, la clase se define dentro del policy map:

```
(config)#policy-map policy-name
(config-pmap)#class class_name {access-group acl_index_or_name | dscp dscp_1 [dscp_2
[dscp_N]] | precedence ipp_1 [ipp_2 [ipp_N]]}
!--- Note: This command should be on one line.

policy-map TEST
class TEST police access-group 101
```

Configuración de la Política de Servicio para Clasificar o Marcar un Paquete en Versiones de Cisco IOS Software Anteriores a la Versión 12.1(12c)E del Cisco IOS Software

En las versiones del software Cisco IOS anteriores a la versión 12.1(12c)E1 del software Cisco IOS, no puede utilizar la acción **set ip dscp** o **set ip precedence** en un policy map. Por lo tanto, la única manera de hacer un marcado del tráfico específico que define una clase es configurar un regulador con una velocidad muy alta. Esta velocidad debe ser, por ejemplo, al menos la velocidad de línea del puerto o algo lo suficientemente alto como para permitir que todo el tráfico llegue a ese regulador. Luego, utilice **set-dscp-transmit *xx*** como acción de conformidad. Siga estos pasos para configurar esta configuración:

1. Configure una ACL para definir el tráfico que desea considerar.La ACL se puede numerar o nombrar, y el Catalyst 6500/6000 soporta una ACL extendida. Ejecute el comando **access-list *xxx*** Cisco IOS Software, como muestra este ejemplo:
   ```
   (config)#access-list 101 permit ip any host 10.1.1.1
   ```

2. Configure una clase de tráfico (mapa de clase) para que coincida con el tráfico en función de la ACL que haya definido o en función del DSCP recibido.Ejecute el comando **class-map**

Cisco IOS Software. La QoS de PFC no admite más de una sentencia de coincidencia por mapa de clase. Además, la QoS de PFC sólo admite estas sentencias coincidentes:**match ip access-groupmatch ip dscpmatch ip precedencematch protocolNota:** El comando **match protocol** habilita el uso de NBAR para hacer coincidir el tráfico.**Nota:** De estas sentencias, sólo se soportan las sentencias **match ip dscp** y **match ip precedence** y funcionan. Sin embargo, estas declaraciones no son útiles para marcar o clasificar los paquetes. Puede utilizar estas sentencias, por ejemplo, para realizar la regulación de todos los paquetes que coincidan con un DSCP determinado. Sin embargo, esta acción está fuera del alcance de este documento.

```
(config)#class-map  class-name
(config-cmap)#match {access-group | input-interface | ip dscp}
```

Nota: Este ejemplo muestra sólo tres opciones para el comando **match**. Pero puede configurar muchas más opciones en este símbolo del sistema.Aquí tiene un ejemplo:

```
class-map match-any TEST
 match access-group 101

class-map match-all TEST2
 match ip precedence 6
```

3. Configure un policy map para aplicar una política a una clase que haya definido previamente.El mapa de política contiene:Un nombreUn conjunto de instrucciones de clasePara cada instrucción de clase, la acción que se debe realizar para esa claseLas acciones admitidas en QoS PFC1 o PFC2 son:**trust dscptrust ip precedencetrust cosvigilancia**Debe utilizar la instrucción **police** porque no se soportan las acciones **set ip dscp** y **set ip precedence**. Dado que en realidad no desea controlar el tráfico, sino sólo marcarlo, utilice un regulador definido para permitir todo el tráfico. Por lo tanto, configure el regulador con una velocidad y ráfaga grandes. Por ejemplo, puede configurar el regulador con la velocidad máxima permitida y la ráfaga. Aquí tiene un ejemplo:

```
policy-map test_policy
 class TEST
   trust ip precedence
 class TEST2
   police  4000000000 31250000 conform-action
   set-dscp-transmit 16 exceed-action policed-dscp-transmit
```

4. Configure una entrada de política de servicio para aplicar un mapa de política definido previamente a una o más interfaces.**Nota:** La política de servicio se puede conectar a una interfaz física o a la interfaz SVI o VLAN. Si una política de servicio está conectada a una interfaz VLAN, sólo los puertos que pertenecen a esa VLAN y que están configurados para QoS basada en VLAN utilizan esta política de servicio. Si el puerto no está configurado para QoS basada en VLAN, el puerto todavía utiliza la QoS predeterminada basada en puerto y sólo observa una política de servicio que está conectada a la interfaz física.Este ejemplo aplica la política de servicio `test_policy` al puerto Gigabit Ethernet 1/1:

```
(config) interface gigabitethernet 1/1
(config-if)#service-policy input test_policy
```

Este ejemplo aplica la política de servicio `test_policy` a todos los puertos en VLAN 10 que tienen una configuración basada en VLAN desde el punto de vista de QoS:

```
(config) interface gigabitethernet 1/2
```

```
(config-if)#switchport mode access
(config-if)#switchport access vlan 10
(config-if)#mls qos vlan-based
(config-if)#exit
(config-if)#interface vlan 10
(config-if)#service-policy input test_policy
```

Cuatro causas posibles para el DSCP interno

El DSCP interno se deriva de uno de estos:

1. Un valor DSCP recibido existente, que se establece antes de que la trama entre en el switchUn ejemplo es **trust dscp**.
2. Los bits de precedencia IP recibidos que ya están configurados en el encabezado IPv4Debido a que hay 64 valores DSCP y sólo ocho valores de precedencia IP, el administrador configura una asignación que el switch utiliza para derivar el DSCP. Las asignaciones predeterminadas están en su lugar, en el caso de que el administrador no configure los mapas. Un ejemplo es **trust ip precedence**.
3. Los bits CoS recibidos que ya están configurados antes de que la trama entre en el switch y que se almacenan en el encabezado del bus de datos, o si no había CoS en la trama entrante, desde el CoS predeterminado del puerto entranteAl igual que con la precedencia IP, hay un máximo de ocho valores CoS los cuales deben ser correlacionados cada uno con uno de los valores 64 DSCP. El administrador puede configurar este mapa, o el switch puede utilizar el mapa predeterminado que ya está en su lugar.
4. La política de servicio puede establecer el DSCP interno en un valor específico.

Para los números 2 y 3 de esta lista, el mapping estático es de forma predeterminada, de esta manera:

- Para la asignación de CoS a DSCP, el DSCP derivado equivale a ocho veces el CoS.
- Para la asignación de precedencia IP a DSCP, el DSCP derivado equivale a ocho veces la precedencia IP.

Puede ejecutar estos comandos para invalidar y verificar esta asignación estática:

- **mls qos map ip-prec-dscp** *dscp_1 dscp_2 dscp_3 dscp_4 dscp_5 dscp_6 dscp_7 dscp_8*
- **mls qos map cos-dscp** *dscp_1 dscp_2 dscp_3 dscp_4 dscp_5 dscp_6 dscp_7 dscp_8*

El primer valor del DSCP que corresponde a la asignación para el CoS (o precedencia IP) es 0. El segundo valor para el CoS (o precedencia IP) es 1, y el patrón continúa de esta manera. Por ejemplo, este comando cambia la asignación de modo que el CoS 0 se mapee al DSCP de 0, y el CoS de 1 se mapee al DSCP de 8, y así sucesivamente:

```
Cat65(config)#mls qos map cos-dscp 0 8 16 26 32 46 48 54
Cat65#show mls qos maps
CoS-dscp map:
 cos:     0 1  2   3   4   5   6   7
  ---------------------------------
 dscp:    0 8 16  26  32  46  48  54
```

¿Cómo se elige el DSCP interno?

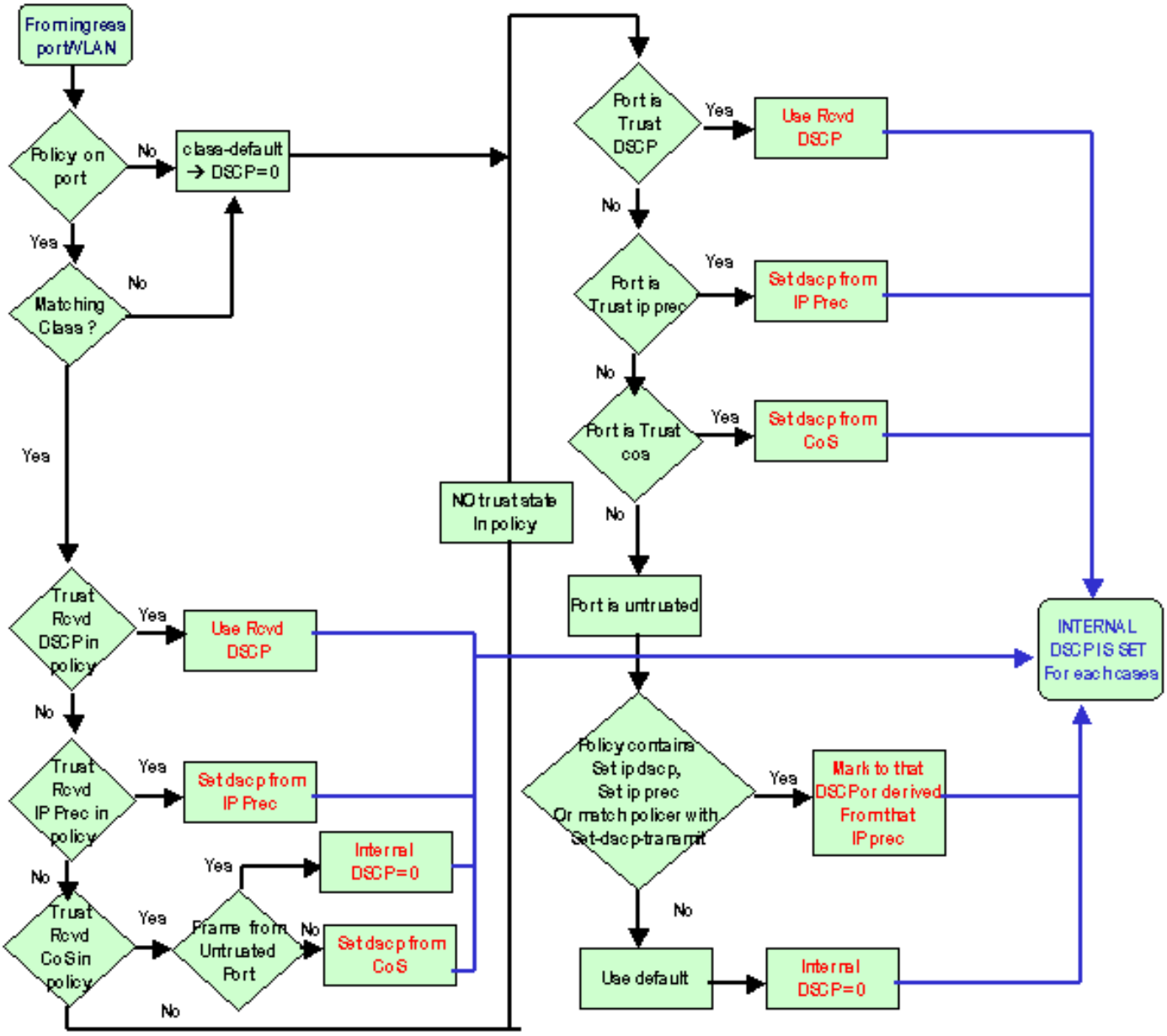
El DSCP interno se elige sobre la base de estos parámetros:

- El mapa de política de QoS que se aplica al paqueteEl mapa de política de QoS está determinado por estas reglas:Si no hay ninguna política de servicio conectada al puerto entrante o a la VLAN, utilice el valor predeterminado.**Nota:** Esta acción predeterminada es establecer el DSCP interno en 0.Si una política de servicio está conectada al puerto o VLAN entrante y si el tráfico coincide con una de las clases que define la política, utilice esta entrada.Si una política de servicio está conectada al puerto o VLAN entrante y si el tráfico no coincide con una de las clases que define la política, utilice el valor predeterminado.
- El estado de seguridad del puerto y la acción de correspondencia de políticasCuando el puerto tiene un estado de `confianza` específico y una política con un marcado determinado (acción de confianza al mismo tiempo), estas reglas se aplican:El comando **set ip dscp** o el DSCP que se define por regulador en un policy map sólo se aplica si el puerto se deja en el estado `no confiable`.Si el puerto tiene un estado `trust`, este `estado trust` se utiliza para derivar el DSCP interno. El estado de confianza del puerto siempre tiene prioridad sobre el comando set ip dscp.El comando **trust *xx en un policy map tiene precedencia sobre el estado*** `trust` **del puerto**.Si el puerto y la política contienen un estado de `confianza` diferente, se considera el `estado de confianza` que proviene del policy map.

Por lo tanto, el DSCP interno depende de estos factores:

- El estado `de confianza` del puerto
- La política de servicio (con uso de ACL) conectada al puerto
- El mapa de política predeterminado**Nota:** El valor predeterminado restablece el DSCP a 0.
- Ya sea basado en VLAN o basado en puerto con respecto a la ACL

Este diagrama resume cómo se elige el DSCP interno en base a la configuración:



PFC también puede elaborar políticas. Esto puede eventualmente dar lugar a un descenso del DSCP interno. Para obtener más información sobre regulación, consulte QoS Policing en Catalyst 6500/6000 Series Switches.

Tratamiento del puerto de salida

No puede hacer nada en el nivel del puerto de salida para cambiar la clasificación. Sin embargo, marque el paquete sobre la base de estas reglas:

- Si el paquete es un paquete IPv4, copie el DSCP interno que el motor de conmutación asigna al byte ToS del encabezado IPv4.
- Si el puerto de salida está configurado para una encapsulación ISL o dot1q, utilice un CoS derivado del DSCP interno. Copie el CoS en la trama ISL o dot1q.

Nota: El CoS se deriva del DSCP interno según una estática. Ejecute este comando para configurar el static:

```
Router(config)#mls qos map dscp-cos dscp1 [dscp2 [dscp3 [dscp4 [dscp5 [dscp6 [dscp7
```

```
[dscp8]]]]]]] to cos_value
!--- Note: This command should be on one line.
```

Aquí aparecen las configuraciones predeterminadas. De forma predeterminada, el CoS es la parte entera del DSCP, dividido por ocho. Ejecute este comando para ver y verificar la asignación:

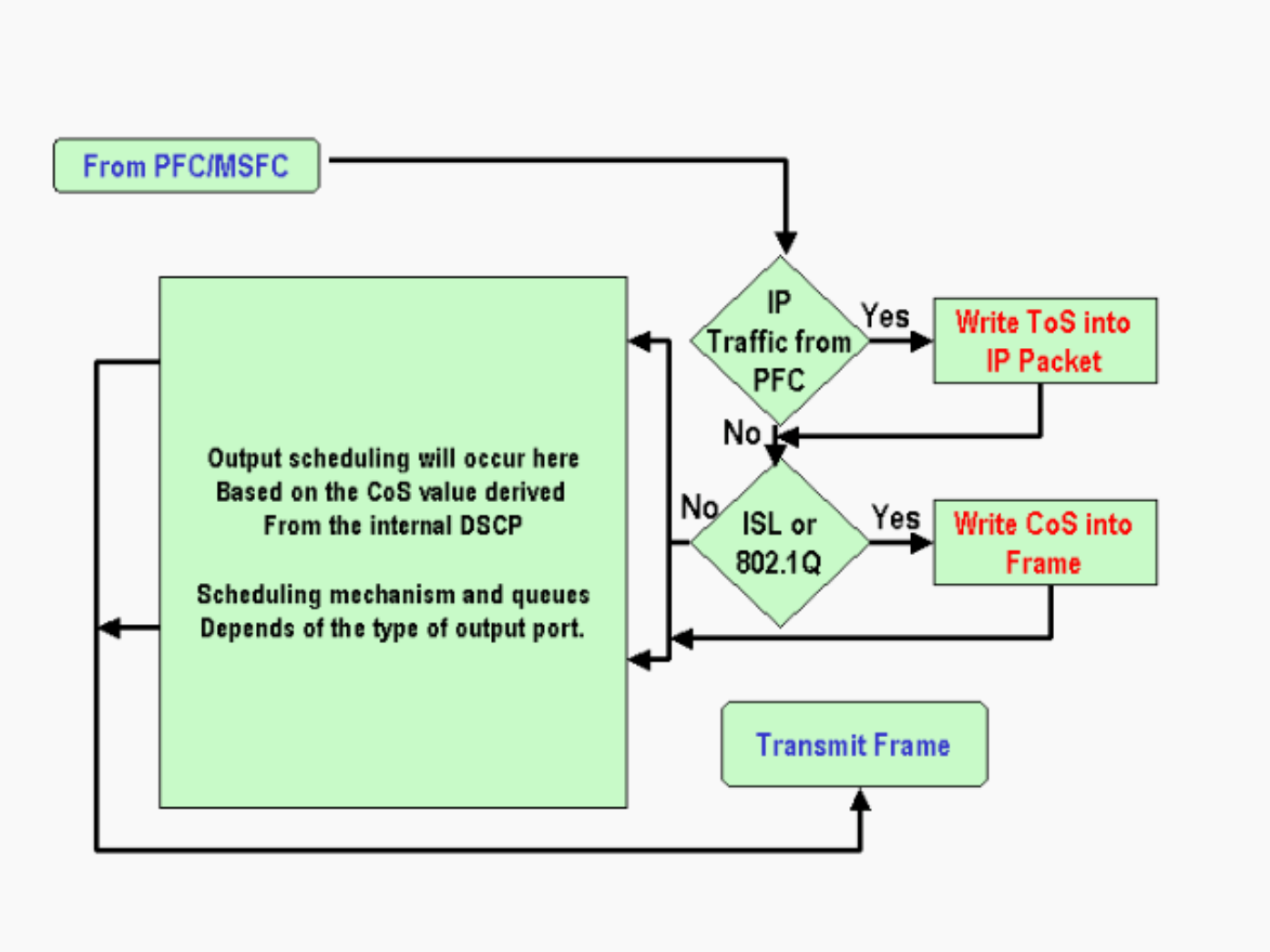
```
cat6k#show mls qos maps
...
  Dscp-cos map:                                     (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 02 02 02 02
      2 :    02 02 02 02 03 03 03 03 03 03
      3 :    03 03 04 04 04 04 04 04 04 04
      4 :    05 05 05 05 05 05 05 05 06 06
      5 :    06 06 06 06 06 06 07 07 07 07
      6 :    07 07 07 07
```

Para cambiar este mapping, ejecute este comando de configuración en el modo de configuración normal:

```
mls qos map dscp-cos 0 1 2 3 4 5 6 7 to 0
mls qos map dscp-cos 8 9 10 11 12 13 14 15 to 1
mls qos map dscp-cos 16 17 18 19 20 21 22 23 to 2
...
```

Después de que el DSCP se escribe en el encabezado IP y el CoS se deriva del DSCP, el paquete se envía a una de las colas de salida para la programación de salida sobre la base del CoS. Esto ocurre incluso si el paquete no es un dot1q o un ISL. Para obtener más información sobre la programación de cola de salida, refiérase a Programación de Salida QoS en Catalyst 6500/6000 Series Switches que Ejecutan Cisco IOS System Software.

Este diagrama resume el procesamiento del paquete con respecto al marcado en el puerto de salida:



Notas y limitaciones

La ACL (Lista de control de acceso) predeterminada

La ACL predeterminada utiliza "dscp 0" como la palabra clave de clasificación. Todo el tráfico que ingresa al switch a través de un puerto no confiable y no llega a una entrada de política de servicio se marca con un DSCP de 0 si se habilita QoS. Actualmente, no puede cambiar la ACL predeterminada en Cisco IOS Software.

Nota: En el software Catalyst OS (CatOS), puede configurar y cambiar este comportamiento predeterminado. Para obtener más información, consulte la sección *ACL Predeterminada de Clasificación y Marcado de QoS en Switches Catalyst 6500/6000 Series que Ejecutan el Software CatOS*.

Limitaciones de las tarjetas de línea WS-X61xx, WS-X6248-xx, WS-X6224-xx y WS-X6348-xx

Esta sección solo se refiere a estas tarjetas de línea:

- WS-X6224-100FX-MT: Catalyst 6000 FX Multimodo de 24 puertos 100
- WS-X6248-RJ-45 : MÓDULO RJ-45 DE 48 PUERTOS 10/100 DE CATALYST 6000
- WS-X6248-TEL MÓDULO TELCO DE 48 PUERTOS 10/100 DE CATALYST 6000

- WS-X6248A-RJ-45 : CATALYST 6000 48-PORT 10/100, ENHANCED QOS
- WS-X6248A-TEL : CATALYST 6000 48-PORT 10/100, ENHANCED QOS
- WS-X6324-100FX-MM : Catalyst 6000 FX de 24 puertos 100, QoS mejorada, MT
- WS-X6324-100FX-SM : Catalyst 6000 FX de 24 puertos 100, QoS mejorada, MT
- WS-X6348-RJ-45: CATALYST 6000 48-PORT 10/100, ENHANCED QOS
- WS-X6348-RJ21V: CATALYST 6000 de 48 puertos 10/100 con alimentación en línea
- WS-X6348-RJ45V: Catalyst 6000 48-Port 10/100, QoS mejorada, alimentación en línea
- WS-X6148-RJ21V: Alimentación en línea 10/100 de 48 puertos de Catalyst 6500
- WS-X6148-RJ45V: Alimentación en línea 10/100 de 48 puertos de Catalyst 6500

Estas tarjetas de línea tienen una limitación. En el nivel de puerto, no puede configurar el estado `trust` con el uso de cualquiera de estas palabras clave:

- `trust-dscp`
- `trust-ipprec`
- `trust-cos`

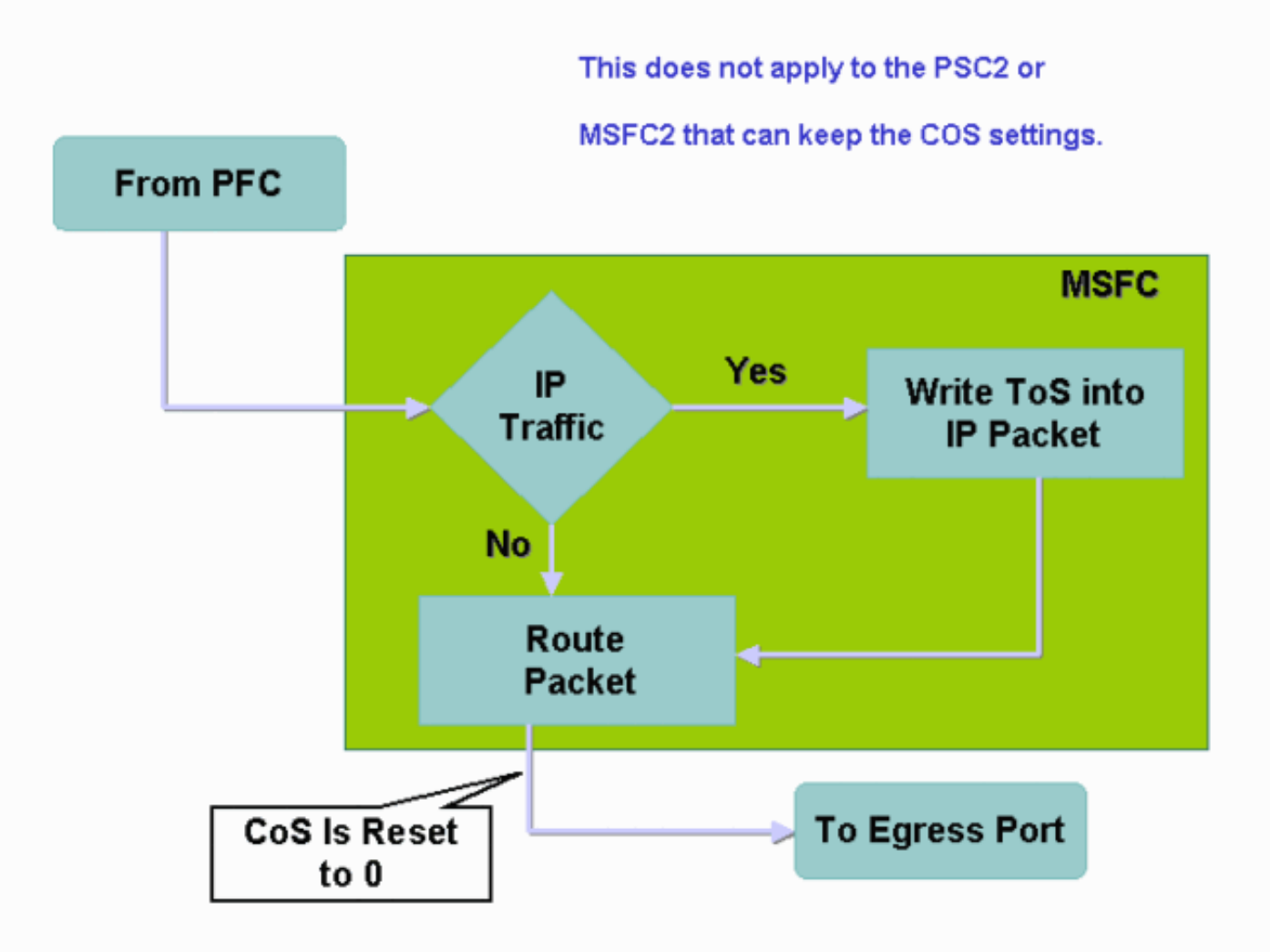
Sólo puede utilizar el estado `no confiable`. Cualquier intento de configurar un estado de `confianza` en uno de estos puertos muestra uno de estos mensajes de advertencia:

```
Tank(config-if)#mls qos trust ?
  extend  extend keyword
Tank(config-if)#mls qos trust
% Incomplete command.
Tank(config-if)#mls qos trust cos
                              ^
% Invalid input detected at '^' marker.
Tank(config-if)#mls qos trust ip-pre
                              ^
% Invalid input detected at '^' marker.
```

Debe adjuntar una política de servicio al puerto o a la VLAN si desea que una trama de confianza entre en dicha tarjeta de línea. Utilice el método del caso 1: Marcado en la sección Borde de este documento.

Paquetes que vienen de MSFC1 o MSFC2 en Supervisor Engine 1A/PFC

Todos los paquetes que vienen de MSFC1 o MSFC2 tienen un CoS de 0. El paquete puede ser un paquete ruteado por software o un paquete que emita la MSFC. Esta es una limitación de la PFC porque restablece la CoS de todos los paquetes que vienen de la MSFC. La precedencia DSCP e IP se mantiene. El PFC2 no tiene esta limitación. El CoS saliente del PFC2 es igual a la precedencia IP del paquete.



Resumen de la clasificación

En las tablas de esta sección se muestra el DSCP que resulta a partir de estas clasificaciones:

- El estado de confianza del puerto entrante
- La palabra clave de clasificación dentro de la ACL aplicada

Esta tabla proporciona un resumen genérico para todos los puertos excepto WS-X62xx y WS-X63xx:

Palabra clave de correspondencia de políticas / Estado de Seguridad de Puertos	set-ip-dscp xx ó set-dscp-transmit xx	trust-dscp	trust-ipprec	trust-cos
no confiable	xx1	DSCP Rx[2]	derivado de ipprec de Rx	0
trust-dscp	Rx dscp	Rx dscp	derivado de	Derivado de Rx CoS o

			ipprec de Rx	del puerto CoS
trust-ipprec	derivado de ipprec de Rx	Rx dscp	derivado de ipprec de Rx	Derivado de Rx CoS o del puerto CoS
trust-cos	Derivado de Rx CoS o del puerto CoS	Rx dscp	derivado de ipprec de Rx	Derivado de Rx CoS o del puerto CoS

1 Esta es la única manera de hacer una nueva marcación en una trama.

[2] Rx = recibir

Esta tabla proporciona un resumen de los puertos WS-X61xx, WS-X62xx y WS-X63xx:

Palabra clave de correspondencia de políticas **Estado de Seguridad de Puertos**	**set-ip-dscp xx ó set-dscp-transmit xx**	**trust-dscp**	**trust-ipprec**	**trust-cos**
no confiable	xx	Rx dscp	derivado de ipprec de Rx	0
trust-dscp	No soportados	No soportados	No soportados	No soportados
trust-ipprec	No soportados	No soportados	No soportados	No soportados
trust-cos	No soportados	No soportados	No soportados	No soportados

Supervisión y verificación de una configuración

Verifique la configuración del puerto

Ejecute el comando **show queuing interface** *interface-id* para verificar la configuración y configuración del puerto.

Cuando ejecuta este comando, puede verificar estos parámetros de clasificación, entre otros parámetros:

- Ya sea basado en puerto o en VLAN
- El tipo de puerto `trust`
- La ACL conectada al puerto

Aquí hay un ejemplo de este resultado de comando. Los campos importantes con respecto a la clasificación aparecen en negrita:

```
6500#show queuing interface gigabitethernet 3/2
Interface GigabitEthernet3/2 queuing strategy:  Weighted Round-Robin
  Port QoS is enabled
  Trust state: trust COS
  Default COS is 0
  Transmit queues [type = 1p2q2t]:
```

El resultado muestra que la configuración de este puerto específico es con `trust cos` en el nivel del puerto. Además, el CoS del puerto predeterminado es 0.

Comprobar clases definidas

Ejecute el comando **show class-map** para verificar las clases definidas. Aquí tiene un ejemplo:

```
Boris#show class-map
 Class Map match-all test (id 3)
   Match access-group  112

 Class Map match-any class-default (id 0)
   Match any
 Class Map match-all voice (id 4)
```

Verifique el Policy Map que se Aplica a una Interfaz

Ejecute estos comandos para verificar el policy map que se aplica y se ve en los comandos anteriores:

- **show mls qos ip interface** ***interface-id***
- **show policy-map interface** ***interface-id***

A continuación se muestran ejemplos de la salida de la ejecución de estos comandos:

```
Boris#show mls qos ip gigabitethernet 1/1
   [In] Default.   [Out] Default.
 QoS Summary [IP]:      (* - shared aggregates, Mod - switch module)

 Int  Mod Dir  Class-map  DSCP AgId Trust FlId AgForward-Pk AgPoliced-k
 ---------------------------------------------------------------------
 Gi1/1 1  In   TEST       0    0*   No    0    1242120099             0
```

Nota: Puede ver estos campos relacionados con la clasificación:

- `Class-map`: le indica qué clase está conectada a la política de servicio que se adjunta a esta interfaz.
- `Confianza`: indica si la acción de la policía en esa clase contiene un comando **trust** y qué es de confianza en la clase.
- `DSCP`: le dice el DSCP que se transmite para los paquetes que llegan a esa clase.

```
Tank#show policy-map interface fastethernet 4/4

 FastEthernet4/4

  service-policy input: TEST_aggre2

    class-map: Test_marking (match-all)
      27315332 packets
      5 minute offered rate 25726 pps
      match: access-group 101
      police :
        10000000 bps 10000 limit 10000 extended limit
        aggregate-forwarded 20155529 packets action: transmit
        exceeded 7159803 packets action: drop
        aggregate-forward 19498 pps exceed 6926 pps
```

Estudios de casos de ejemplo

Esta sección proporciona configuraciones de ejemplo de casos comunes que pueden aparecer en una red.

Caso 1: Marcado en el borde

Suponga que configura un Catalyst 6000 que se utiliza como switch de acceso. Muchos usuarios se conectan al switch slot 2, que es una tarjeta de línea WS-X6348 (10/100 Mbps). Los usuarios pueden enviar:

- Tráfico de datos normal: este tráfico siempre está en la VLAN 100 y necesita un DSCP de 0.
- Tráfico de voz desde un teléfono IP: este tráfico siempre está en la VLAN 101 auxiliar de voz y necesita un DSCP de 46.
- Tráfico de aplicaciones críticas: este tráfico también se produce en la VLAN 100 y se dirige al servidor 10.10.10.20. Este tráfico necesita obtener un DSCP de 32.

La aplicación no marca ninguno de este tráfico. Por lo tanto, deje el puerto como `no confiable` y configure una ACL específica para clasificar el tráfico. Una ACL se aplica a la VLAN 100 y una ACL a la VLAN 101. También debe configurar todos los puertos como basados en VLAN. Este es un ejemplo de la configuración que resulta:

```
Boris(config)#mls qos
Boris(config)#interface range fastethernet 2/1-48
Boris(config-if)#mls qos vlan-based
Boris(config-if)#exit
Boris(config)#ip access-list extended Mission_critical
Boris(config-ext-nacl)#permit ip any host 10.10.10.20
Boris(config)#ip access-list extended Voice_traffic
Boris(config-ext-nacl)#permit ip any any
Boris(config)#class-map voice

Boris(config-cmap)#match access-group Voice_traffic
Boris(config)#class-map Critical

Boris(config-cmap)#match access-group Mission_critical
Boris(config)#policy-map Voice_vlan
Boris(config-pmap)#class voice
Boris(config-pmap-c)#set ip dscp 46
Boris(config)#policy-map Data_vlan
Boris(config-pmap)#class Critical
```

```
Boris(config-pmap-c)#set ip dscp 32
Boris(config)#interface vlan 100
Boris(config-if)#service-policy input Data_vlan
Boris(config)#interface vlan 101
Boris(config-if)#service-policy input Voice_vlan
```

Caso 2: Confianza en el núcleo con interfaces Gigabit Ethernet solamente

Suponga que configura un Catalyst 6000 de núcleo con sólo una interfaz Gigabit Ethernet en el slot 1 y el slot 2. Los switches de acceso marcaron previamente el tráfico correctamente. Por lo tanto, no es necesario que realice ninguna observación. Sin embargo, debe asegurarse de que el switch de núcleo confíe en el DSCP entrante. Este caso es el más fácil porque todos los puertos están marcados como `trust-dscp`, lo que debería ser suficiente:

```
6k(config)#mls qos
6k(config)#interface range gigabitethernet 1/1-2 , gigabitethernet 2/1-2
6k(config-if)#mls qos trust dscp
```

Información Relacionada

- La calidad del servicio en la familia de switches Catalyst 6000
- Clasificación y marcación de QoS en los switches de la serie Catalyst 6500/6000 con software CatOS
- Soporte de Producto de LAN
- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems