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 del Cisco IOS Software que se relacionen con QoS o la marca. Para más información sobre el comando line interface(cli) del Cisco IOS Software, refiera a configurar PFC QoS.

prerrequisitos

Requisitos

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 Switch que ejecutan el Cisco IOS Software y el uso uno de estos motores del supervisor:Un Supervisor Engine 1A con un Policy Feature Card (PFC) y un (MSFC) de la Multilayer Switch Feature CardUn Supervisor Engine 1A con un PFC y un MSFC2Un Supervisor Engine 2 con un PFC2 y un MSFC2

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.

Terminología

La lista proporciona la terminología que este documento utiliza:

- ¿Differentiated Services Code Point (DSCP)? Los primeros seis bits del byte del 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, si IP o no IP. Las cuatro fuentes posibles para la sección del DSCP interno de este documento detallan esta asignación del DSCP interno.
- ¿Prioridad 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 consiste en ninguno de estos tres bits:Los tres bits del IEEE 802.1P (dot1p) en el IEEE 802.1Q (dot1q) marcan con etiqueta para el paquete del dot1q.**Nota:** Por abandono, los switches Cisco no marcan los paquetes del VLAN nativo con etiqueta.Los tres bits llamaron el “campo del usuario” en la encabezado del Inter-Switch Link (ISL) para un paquete encapsulado por ISL.**Nota:** CoS no está presente dentro de un non-dot1q o de un paquete ISL.
- ¿Clasificación? El proceso que se utiliza para seleccionar el tráfico para ser marcado.
- ¿Marcado? El proceso que fija un valor de la capa 3 (L3) DSCP en un paquete. Este documento amplía la definición de la marca para incluir la configuración de los valores L2 CoS.

Los Catalyst 6500/6000 Series Switch pueden hacer las clasificaciones en base de estos tres parámetros:

- DSCP
- Precedencia IP

- CoS

Los Catalyst 6500/6000 Series Switch realizan la Clasificación y marcado en las diversas etapas. Esto es qué ocurre en diversos lugares:

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

Tratamiento del puerto de entrada

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

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

Para fijar o cambiar al estado de confianza del puerto, publique este comando del Cisco IOS Software en el modo de la `interfaz`:

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

Nota: Por abandono, todos los puertos están en `estado no confiable` cuando se habilita QoS. Para habilitar QoS en el Catalyst 6500 que funcione con el Cisco IOS Software, publique el **comando mls qos** en el modo de la configuración principal.

En el nivel del puerto de entrada, usted puede también aplicar un valor por defecto CoS por el puerto. Aquí tiene un ejemplo:

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

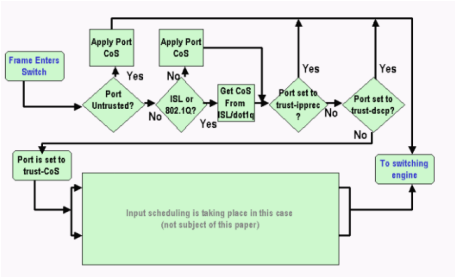
Este CoS predeterminado se aplica a todos los paquetes, tales como IP y Intercambio de paquetes entre redes (IPX). Usted puede aplicar CoS predeterminado a cualquier puerto físico.

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

- Si la trama no tiene CoS recibido (dot1q o ISL), aplique el CoS del puerto predeterminado.
- Para el dot1q y las tramas ISL, guarde CoS como es.

Entonces, pase la trama al motor de Switching.

Este ejemplo ilustra la clasificación de entrada y la marca. El ejemplo muestra cómo asignar CoS interno a cada trama:



Nota: Mientras que este ejemplo muestra, cada trama se asigna CoS interno. La asignación se basa en CoS recibido o el CoS del puerto predeterminado. CoS interno incluye las tramas sin Tags que no llevan ningún CoS real. CoS interno se escribe en un encabezado de paquete especial, que se llama encabezado de bus de datos, y se envía sobre el bus de datos al motor de Switching.

Motor de conmutación (PFC)

Cuando la encabezado alcanza el motor de Switching, el Enhanced Address Recognition Logic motor de Switching (CONDE) asigna a cada trama un DSCP interno. Este DSCP interno es una prioridad interna que es asignada a la trama por el PFC mientras que la trama transita el Switch. Éste no es el DSCP en versión IP la encabezado 4 (del IPv4). El DSCP interno se deriva de una configuración existente de CoS o TOS y se utiliza para reajustar CoS o la TOS como la trama sale el Switch. Este DSCP interno se asigna a todas las tramas que sean conmutadas o ruteadas por el PFC, incluso las tramas del no IP.

Esta sección discute cómo usted puede asignar una política de servicio a la interfaz para hacer una marca. La sección también discute la configuración final del DSCP interno, que depende del estado de confianza del puerto y de la política de servicio que es aplicada.

Configure la política de servicio para clasificar o para marcar un paquete en el Cisco IOS Software Release 12.1(12c)E y Posterior

Complete estos pasos para configurar la política de servicio:

1. Configure un Access Control List (ACL) para definir el tráfico que usted quiere considerar.El ACL puede ser numerado o ser nombrado, y el Catalyst 6500/6000 soporta un ACL ampliado. Publique el comando del Cisco IOS Software del *xxx de la* **lista de acceso**, como este ejemplo muestra:`(config)#`**`access-list 101 permit ip any host 10.1.1.1`**
2. Configure una clase de tráfico (correspondencia de la clase) para hacer juego el tráfico en base del ACL que usted ha definido o en base del DSCP recibido.Publique el comando del Cisco IOS Software del clase-**mapa**. El PFC QoS no soporta más de una declaración de coincidencia por la correspondencia de la clase. También, el PFC QoS soporta solamente estas declaraciones de coincidencia:**match ip access-groupmatch ip dscpmatch ip precedenceprotocolo de la coincidenciaNota: El comando match protocol** habilita el uso del Reconocimiento de aplicaciones basadas en la red (NBAR) de hacer juego el tráfico.**Nota:** De estas opciones, las declaraciones de la **Prioridad IP** solamente de la **coincidencia del IP del dscp** y de la **coincidencia** se soportan y trabajan. Estas declaraciones, sin embargo, no son útiles en la marca o la clasificación de los paquetes. Usted puede utilizar estas declaraciones, por ejemplo, para hacer el policing en todos los paquetes que hagan juego cierto DSCP. 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 solamente tres opciones para el **comando match**. Pero usted puede configurar muchas más opciones en este comando prompt.**Nota:** De las opciones en este **comando match** se toma para los criterios de concordancia y las otras opciones se dejan hacia fuera, 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 una correspondencia de políticas para aplicar una directiva a una clase que usted

definió previamente.La correspondencia de políticas contiene:Un nombreUn conjunto de las instrucciones classPara cada instrucción class, medidas que necesitan ser tomadas para esa claseLas acciones soportadas en PFC1 y PFC2 QoS son:**trust dscptrust ip precedencetrust cosfije el dscp del IP** en el Cisco IOS Software Release 12.1(12c)E1 y Posterior**fije la Prioridad IP** en el Cisco IOS Software Release 12.1(12c)E1 y Posterior**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 solamente dos opciones, pero usted puede configurar muchas más opciones en esto `(config-pmap-c) #` comando prompt.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 una correspondencia de políticas que usted previamente definió a uno o más la interfaz.**Nota:** Usted puede asociar una política de servicio a la interfaz física o al Switched Virtual Interface (SVI) o a la interfaz VLAN. Si usted asocia una política de servicio a una interfaz VLAN, los únicos puertos que utilizan esta política de servicio son los puertos que pertenecen a ese VLA N y se configuran para QoS VLAN basado. Si el puerto no se fija para QoS VLAN basado, el puerto todavía utiliza el acceso basado predeterminado QoS y mira solamente la política de servicio que se asocia a la interfaz física.Este ejemplo aplica el `test_policy de la` política de servicio a los Ethernetes de Gigabit de un puerto 1/1:`(config)` **`interface gigabitethernet 1/1`** `(config-if)#`**`service-policy input test_policy`**Este ejemplo aplica el `test_policy de la` política de servicio a todos los puertos en el VLAN10 que tengan una configuración VLAN basada 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:** Usted puede combinar el paso 2 y el paso 3 de este procedimiento si usted salta la definición específica de la clase y asocia el ACL directamente en la definición de la correspondencia de políticas. En este ejemplo, donde no han definido a la `policía del` PRUEBA de clase antes de la configuración de la correspondencia de políticas, la clase se define dentro de la correspondencia de políticas:`(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`**

Configure la política de servicio para clasificar o para marcar un paquete en las versiones de Cisco IOS Software anterior que el Cisco IOS Software Release 12.1(12c)E

En las versiones de Cisco IOS Software anterior que el Cisco IOS Software Release 12.1(12c)E1, usted no puede utilizar la acción de la **Prioridad IP del dscp** o del **conjunto del IP del conjunto** en una correspondencia de políticas. Por lo tanto, la única forma de hacer una marca del tráfico específico que una clase defina es configurar un policer con mismo una alta velocidad. Esta tarifa debe ser, por ejemplo, por lo menos la línea tarifa del puerto o algo arriba bastante de permitir que todo el tráfico golpee ese policer. Entonces, **set-dscp-transmit** *xx del* uso como la acción de conformidad. Siga los siguientes pasos para configurar esta configuración:

1. Configure un ACL para definir el tráfico que usted quiere considerar.El ACL puede ser numerado o ser nombrado, y el Catalyst 6500/6000 soporta un ACL ampliado. Publique el comando del Cisco IOS Software del *xxx de la* **lista de acceso**, como este ejemplo muestra:`(config)#`**`access-list 101 permit ip any host 10.1.1.1`**

2. Configure una clase de tráfico (correspondencia de la clase) para hacer juego el tráfico en base de cualquier el ACL que usted ha definido o en base del DSCP recibido.Publique el comando del Cisco IOS Software del clase-**mapa**. El PFC QoS no soporta más de una declaración de coincidencia por la correspondencia de la clase. También, el PFC QoS soporta solamente estas declaraciones de coincidencia:**match ip access-groupmatch ip dscpmatch ip precedenceprotocolo de la coincidenciaNota: El comando match protocol** habilita el uso del NBAR de hacer juego el tráfico.**Nota:** De estas declaraciones, las declaraciones de la **Prioridad IP** solamente de la **coincidencia del IP del dscp** y de la **coincidencia** se soportan y trabajan. Estas declaraciones, sin embargo, no son útiles en la marca o la clasificación de los paquetes. Usted puede utilizar estas declaraciones, por ejemplo, para hacer el policing en todos los paquetes que hagan juego cierto DSCP. 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 solamente tres opciones para el **comando match**. Pero usted puede configurar muchas más opciones en este comando prompt.Aquí tiene un ejemplo:**`class-map match-any TEST  match access-group 101 class-map match-all TEST2  match ip precedence 6`**
3. Configure una correspondencia de políticas para aplicar una directiva a una clase que usted definió previamente.La correspondencia de políticas contiene:Un nombreUn conjunto de las instrucciones classPara cada instrucción class, medidas que necesitan ser tomadas para esa claseLas acciones soportadas en PFC1 o PFC2 QoS son:**trust dscptrust ip precedencetrust cosvigilancia**Usted debe utilizar la **declaración de política** porque las acciones de la **Prioridad IP del dscp** y del **conjunto del IP del conjunto** no se soportan. Puesto que usted no quiere realmente limpiar el tráfico, pero apenas marcarlo, utilice un policer que se defina para permitir todo el tráfico. Por lo tanto, configure el policer con una tarifa grande y reparta. Por ejemplo, usted puede configurar el policer con la tarifa permitida máximo y repartir. 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 una correspondencia de políticas que usted definió previamente a una o más interfaces.**Nota:** La política de servicio se puede asociar a una interfaz física o al SVI o a la interfaz VLAN. Si una política de servicio se asocia a una interfaz VLAN, sólo los puertos que pertenecen a ese VLA N y que se configuran para el uso VLAN basado de QoS esta política de servicio. Si el puerto no se fija para QoS VLAN basado, el puerto todavía utiliza el acceso basado predeterminado QoS y mira solamente una política de servicio que se asocie a la interfaz física.Este ejemplo aplica el `test_policy de la` política de servicio a los Ethernetes de Gigabit de un puerto 1/1:`(config)` **`interface gigabitethernet 1/1`** `(config-if)#`**`service-policy input test_policy`**Este ejemplo aplica el `test_policy de la` política de servicio a todos los puertos en el VLAN10 que tengan una configuración VLAN basada 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 a partir del uno de éstos:

1. Una existencia recibió el valor DSCP, se fija que antes de que la trama ingrese el SwitchUn ejemplo es **dscp de la confianza**.

2. Los bits de precedencia IP recibidos que se fijan ya en la encabezado del IPv4Porque hay 64 valores DSCP y solamente ocho valores de precedencia IP, el administrador configura una asignación que el Switch utilice para derivar el DSCP. Los mapeos predeterminados existen, en caso de que el administrador no configure las correspondencias. Un ejemplo es **Prioridad IP de la confianza**.
3. Los bits recibidos del CoS que se fijan ya antes de que la trama ingrese el Switch y que se salvan en encabezado de bus de datos, o si no había CoS en la trama entrante, del CoS predeterminado del puerto entranteAl igual que con la precedencia IP, hay un máximo de ocho valores CoS, cada uno de los cuales deben asignarse a uno de los 64 valores DSCP. El administrador puede configurar esta correspondencia, o el Switch puede utilizar la correspondencia predeterminada que es ya en el lugar.
4. La política de servicio puede fijar el DSCP interno a un valor específico.

Para los números 2 y 3 en esta lista, la correlación estática está por abandono, de este modo:

- Para mapeo de COS a DSCP, el DSCP que es iguales derivados ocho veces CoS.
- Para el IP asignación de precedencia a DSCP, el DSCP que es iguales derivados ocho veces la Prioridad IP.

Usted puede publicar estos comandos para reemplazar y verificar esta correlación estática:

- **los qos de los mls asocian IP-prec-DSCP** *dscp_1 dscp_2 dscp_3 dscp_4 dscp_5 dscp_6 dscp_7 dscp_8*
- **los qos de los mls asocian 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 CoS (o la Prioridad IP) es 0. El segundo valor para CoS (o la Prioridad IP) es 1, y el modelo continúa de esta manera. Por ejemplo, este comando cambia la asignación para asociar CoS 0 al DSCP de 0, y CoS de 1 se asocia 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 en base de estos parámetros:

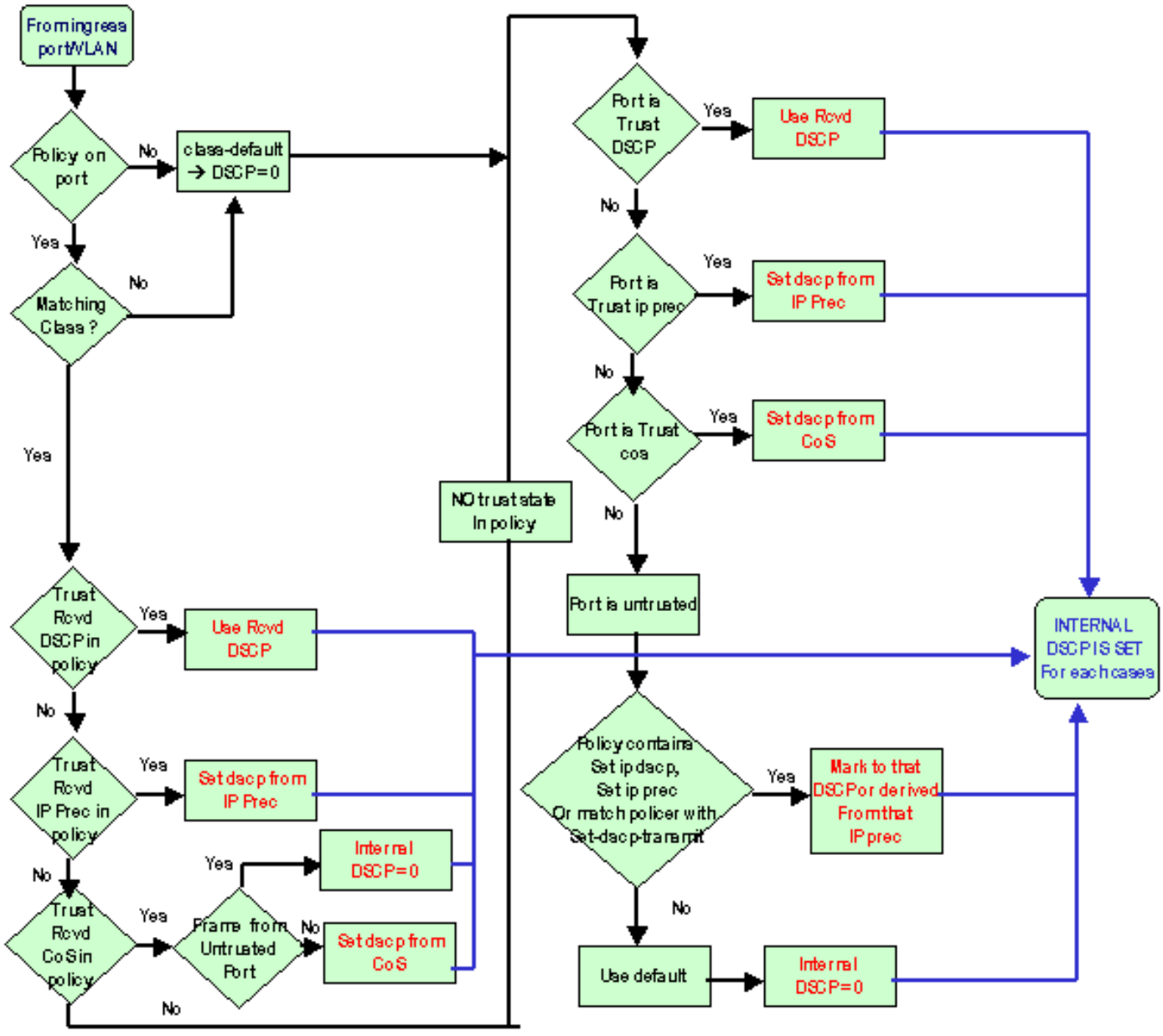
- Política de calidad de servicio (QoS) la correspondencia que se aplica al paquetePolítica de calidad de servicio (QoS) la correspondencia es determinada por estas reglas:Si no se asocia ninguna política de servicio al puerto entrante o al VLA N, utilice el valor por defecto.**Nota:** Esta acción predeterminada es fijar el DSCP interno a 0.Si una política de servicio se asocia al puerto entrante o al VLA N, y si el tráfico hace juego una de las clases que la directiva define, utilice esta entrada.Si una política de servicio se asocia al puerto entrante o al VLA N, y si el tráfico no hace juego una de las clases que la directiva define, utilice el valor por defecto.
- `El estado confiable del` puerto y la acción de la correspondencia de políticasCuando el puerto tiene un `estado confiable` específico y una directiva con cierta marca (que confía en la acción al mismo tiempo), estas reglas se aplican:**El comando set ip dscp** o el DSCP que se define por el policer en una correspondencia de políticas es solamente aplicado si el puerto se sale en `estado no confiable`.Si el puerto tiene un `estado confiable`, utilizan a este `estado confiable` 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 una correspondencia de políticas toma la precedencia sobre el estado de confianza del puerto.Si el puerto y la directiva contienen a un diverso `estado confiable`, consideran al `estado confiable` que viene de la correspondencia de políticas.

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

- El estado de confianza del puerto
- La política de servicio (con el uso del ACL) que se asocia al puerto
- La correspondencia de la política predeterminada**Nota:** El valor por defecto reajusta el DSCP a 0.
- Si es VLAN basado o acceso basado con respecto al ACL

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



PFC también puede elaborar políticas. Esto puede dar lugar eventual a una disminución del DSCP interno. Para más información sobre el policing, refiera a la Supervisión de QoS en los Catalyst 6500/6000 Series Switch.

Tratamiento del puerto de salida

Usted no puede hacer cualquier cosa en el nivel del puerto de egreso para cambiar la

clasificación. Sin embargo, marque el paquete en base de estas reglas:

- Si el paquete es paquete IPV4, copie el DSCP interno que el motor de Switching asigna en el Byte ToS de la encabezado del IPv4.
- Si el puerto de egreso se configura para una encapsulación ISL o del dot1q, utilice CoS que se derive del DSCP interno. Copie CoS en la trama ISL o del dot1q.

Nota: CoS se deriva del DSCP interno según los parásitos atmosféricos. Publique este comando para configurar los parásitos atmosféricos:

```
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.
```

Las configuraciones predeterminadas aparecen aquí. Por abandono, CoS es la parte entera del DSCP, dividida por ocho. Publique este comando para ver y verificar la asignación:

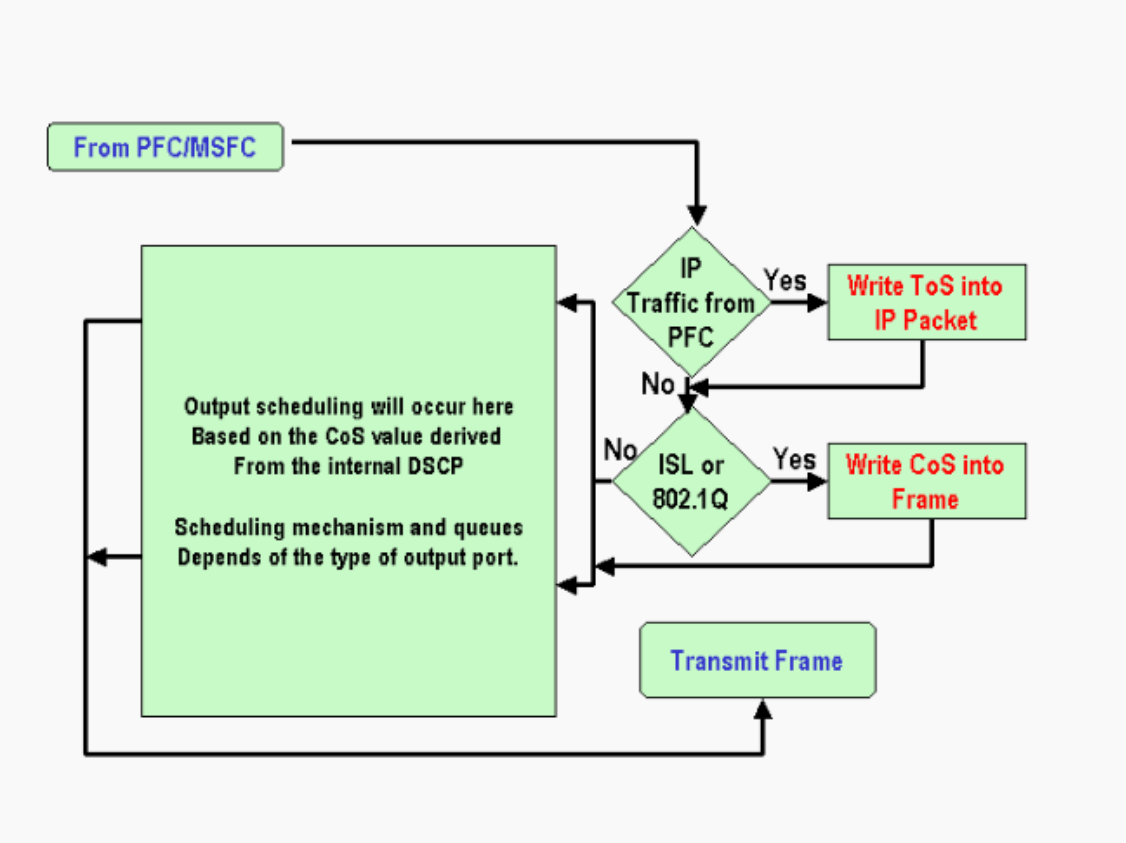
```
cat6k#show mls qos maps...  Dscp-cos map:                                    (dscp= d1d2)     d1 :
d2 0  1  2  3  4  5  6  7  8  9      ---------------------------------------      0 :    00 00 00
00 00 00 00 00 01 01        1 :    01 01 01 01 01 01 02 02 02 02        2 :    02 02 02 02 03 03
03 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 esta asignación, publique este comando configuration en el modo de la configuración normal:

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

Después de que el DSCP se escriba en el encabezado IP y CoS se deriva del DSCP, el paquete se envía a una de las colas de salida para la programación de salida en base de CoS. Esto ocurre incluso si el paquete no es un dot1q o un ISL. Para más información sobre la cola de salida que programa, refiera a la programación de salida de QoS en los Catalyst 6500/6000 Series Switch que funcionan con el software del sistema del Cisco IOS.

Este diagrama resume el proceso del paquete con respecto a la marca en el puerto de egreso:



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 el Switch con puerto no confiable y no golpea una entrada de la política de servicio se marca con un DSCP de 0 si se habilita QoS. Actualmente, usted no puede cambiar el ACL predeterminado en Cisco IOS Software.

Nota: En el software del Catalyst OS (CatOS), usted puede configurar y cambiar este comportamiento predeterminado. Para más información, refiera *el* sección del *ACL predeterminado de la* clasificación de QoS y de la marca en los Catalyst 6500/6000 Series Switch que funcionan con el software CatOS.

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

Esta sección se refiere solamente a este linecards:

- WS-X6224-100FX-MT: Catalyst 6000 24-Port 100 FX con varios modos de funcionamiento
- WS-X6248-RJ-45 : Módulo 48-Port 10/100 RJ-45 del Catalyst 6000
- WS-X6248-TEL MÓDULO TELCO 48-Port 10/100 del Catalyst 6000
- WS-X6248A-RJ-45 : Catalyst 6000 48-Port 10/100, QoS aumentado
- WS-X6248A-TEL : Catalyst 6000 48-Port 10/100, QoS aumentado
- WS-X6324-100FX-MM : Catalyst 6000 24-Port 100 FX, QoS aumentado, MT
- WS-X6324-100FX-SM : Catalyst 6000 24-Port 100 FX, QoS aumentado, MT
- WS-X6348-RJ-45: Catalyst 6000 48-Port 10/100, QoS aumentado
- WS-X6348-RJ21V: Catalyst 6000 48-Port 10/100, alimentación en línea
- WS-X6348-RJ45V: Catalyst 6000 48-Port 10/100, QoS aumentado, alimentación en línea
- WS-X6148-RJ21V: Alimentación en línea del Catalyst 6500 48-Port 10/100
- WS-X6148-RJ45V: Alimentación en línea del Catalyst 6500 48-Port 10/100

Este linecards tiene una limitación. En el nivel del puerto, usted no puede configurar al `estado confiable` con el uso de ninguno de estos palabras claves:

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

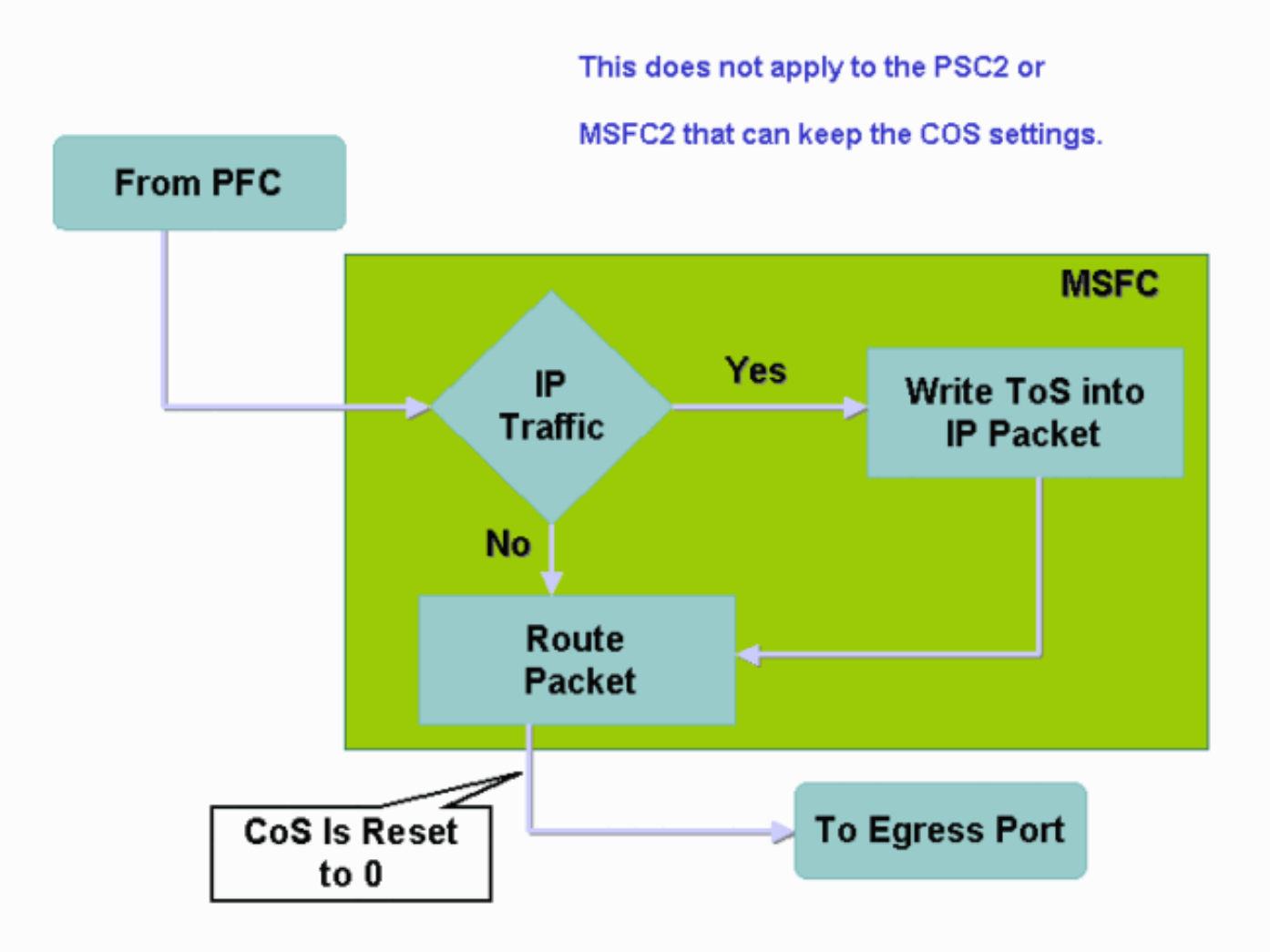
Usted puede utilizar solamente `estado no confiable`. Cualquier tentativa de configurar a un `estado confiable` en uno de estos puertos visualiza uno de estos mensajes de advertencia:

```
Tank(config-if)#mls qos trust ?        extend  extend keywordTank(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.
```

Usted debe asociar una política de servicio al puerto o al VLA N si usted quisiera que una trama que confía en viniera adentro en tal linecard. Utilice el método en el caso 1: Marca en la sección del borde de este documento.

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

Todos los paquetes que vienen del MSFC1 o del MSFC2 tienen CoS de 0. El paquete puede ser un Software-Routed Packet o un paquete ese los problemas MSFC. Ésta es una limitación del PFC porque reajusta CoS de todos los paquetes que vengan del MSFC. El DSCP y la Prioridad IP todavía se mantienen. El PFC2 no tiene esta limitación. CoS de salida del PFC2 es igual a la Prioridad IP del paquete.



Resumen de la clasificación

Las tablas en esta sección muestran a DSCP ese los resultados en base de estas clasificaciones:

- `El estado confiable del` puerto entrante
- La palabra clave de clasificación dentro del ACL aplicado

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

Palabra clave de correspondencia de políticas	set-ip-dscp xx ó set-dscp-transmit xx	trust-dscp	trust-ipprec	Trust-cos
Estado de Seguridad de Puertos				

no confiable	xx1	Rx DSCP	derivado de ipprec de Rx	0
trust-dscp	Rx dscp	Rx dscp	derivado de ipprec de Rx	Derivado de Rx CoS o 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 = reciben

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

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

Monitoree y verifique una configuración

Marque la configuración del puerto

Publique el **comando show queuing interface interface-id** para verificar las configuraciones de puerto y las configuraciones.

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

- Si acceso basado o VLAN basado
- El tipo de puerto de la `confianza`
- El ACL que se asocia al puerto

Aquí está una muestra de esta salida de comando. Los campos importantes con respecto a la clasificación aparecen en la negrilla:

```
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]:
```

La salida muestra que la configuración de este puerto específico está con la `confianza lechuga romana` en el nivel del puerto. También, el CoS del puerto predeterminado es 0.

Clases definidas del control

Publique el **comando show class-map** para marcar 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)
```

Marque la correspondencia de políticas que se aplica a una interfaz

Publique estos comandos para marcar la correspondencia de políticas que es aplicada y considerada en los comandos anteriores:

- **muestre la** *id del interfaz de la* **interfaz del IP de los qos de los mls**
- *id del interfaz del* **show policy-map interface**

Aquí están las muestras de la salida de la aplicación 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: Usted puede mirar estos campos que se relacionen con la clasificación:

- ¿`Clase-mapa`? Le dice qué clase se asocia a la política de servicio que se asocia a esta interfaz.
- ¿`Confianza`? Le dice si la acción policial en esa clase contiene un **comando trust** y qué se

confía en la clase.
- ¿DSCP? Le dice el DSCP que se transmite para los paquetes que golpean 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 las configuraciones de muestra de los casos comunes que pueden aparecer en una red.

Caso 1: Marcado en el borde

Asuma que usted configura un Catalyst 6000 que se utilice como switch de acceso. Muchos usuarios conectan con el slot 2 del Switch, que es un linecard WS-X6348 (10/100 Mbps). Los usuarios pueden enviar:

- ¿Tráfico de datos normales? Este tráfico está siempre en el VLAN 100 y necesita conseguir un DSCP de 0.
- ¿Tráfico de voz de un teléfono del IP? Este tráfico está siempre en el VLAN auxiliar 101 de la Voz y necesita conseguir un DSCP de 46.
- ¿Tráfico de la aplicación esencial para la misión? Este tráfico también viene en el 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, salga del puerto como `untrusted` y configure un ACL específico para clasificar el tráfico. Un ACL se aplica al VLAN 100, y un ACL se aplica al VLAN 101. Usted también necesita configurar todos los puertos como VLAN basados. Aquí está un ejemplo de la configuración que resulta:

```
Boris(config)#mls qosBoris(config)#interface range fastethernet 2/1-48Boris(config-if)#mls qos
vlan-basedBoris(config-if)#exitBoris(config)#ip access-list extended
Mission_criticalBoris(config-ext-nacl)#permit ip any host 10.10.10.20Boris(config)#ip access-
list extended Voice_trafficBoris(config-ext-nacl)#permit ip any anyBoris(config)#class-map voice
Boris(config-cmap)#match access-group Voice_trafficBoris(config)#class-map CriticalBoris(config-
cmap)#match access-group Mission_criticalBoris(config)#policy-map Voice_vlanBoris(config-
pmap)#class voiceBoris(config-pmap-c)#set ip dscp 46Boris(config)#policy-map
Data_vlanBoris(config-pmap)#class CriticalBoris(config-pmap-c)#set ip dscp
32Boris(config)#interface vlan 100Boris(config-if)#service-policy input
Data_vlanBoris(config)#interface vlan 101Boris(config-if)#service-policy input Voice_vlan
```

Caso 2: El confiar en la base con solamente las interfaces de Ethernet Gigabite

Asuma que usted configura un núcleo de Catalyst 6000 con solamente una interfaz de Ethernet Gigabite en el slot1 y el slot 2. El tráfico previamente marcado de los switches de acceso correctamente. Por lo tanto, usted no necesita hacer la observación. Sin embargo, usted necesita asegurarse de que el switch del núcleo confíe en el DSCP entrante. Este caso es el caso más fácil porque todos los puertos se marcan como `Trust-dscp`, que deben ser suficiente:

```
6k(config)#mls qos6k(config)#interface range gigabitethernet 1/1-2 , gigabitethernet 2/1-
26k(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