Clasificación y marcación de QoS en los switches de la serie Catalyst 6500/6000 con software CatOS

Contenido

Introducción

Este documento examina qué sucede con el marcado y la clasificación de un paquete en diferentes lugares durante su recorrido dentro del chasis del Catalyst 6000. Describe casos especiales, restricciones y ofrece casos prácticos breves.

Este documento no pretende ser una lista exhaustiva de todos los comandos de Catalyst OS (CatOS) relacionados con la calidad de servicio (QoS) o la marcación. Para obtener más

información sobre la interfaz de línea de comandos (CLI) de CatOS, consulte el siguiente documento:

- Configuración de QoS

Nota: Este documento sólo tiene en cuenta el tráfico IP.

Antes de comenzar

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Prerequisites

No hay requisitos previos específicos para este documento.

Componentes Utilizados

Este documento es válido para los switches de la familia Catalyst 6000 que ejecutan el software CatOS y que utilizan uno de los siguientes motores de supervisor:

- SUP1A + PFC
- SUP1A + PFC + MSFC
- SUP1A + PFC + MSFC2
- SUP2 + PFC2
- SUP2 + PFC2 + MSFC2

No obstante, todos los comandos de muestra se han probado en un Catalyst 6506 mientras se ejecutaba un software SUP1A/PFC versión 6.3.

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Terminology

En la lista a continuación se cita la terminología utilizada en este documento:

- Punto de código de servicios diferenciados (DSCP): Los primeros seis bits del byte Tipo de servicio (ToS) en el encabezado IP. DSCP sólo está presente en el paquete de IP.**Nota:** También asigna un DSCP interno a cada paquete (IP o no IP), esta asignación DSCP interna se detallará más adelante en este documento.
- Precedencia de 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). Está formado por cualquiera de los siguientes tres bits:Los tres bits dot1p en el indicador dot1q para el paquete IEEE dot1q.Los tres bits denominados "Campo del usuario" en el encabezado del link entre switches (ISL) para un paquete encapsulado por ISL.No hay

un CoS dentro de un paquete ISL o no dot1q.
- Clasificación: El proceso utilizado para seleccionar el tráfico que se marcará.
- Marcación: El proceso por el que se establece un valor de DSCP de Capa 3 (L3) en un paquete. En este documento, la definición de marcación se ha extendido para incluir la configuración de valores CoS L2.

Los switches de la familia Catalyst 6000 pueden realizar clasificaciones basadas en los siguientes tres parámetros:

- DSCP
- Precedencia IP
- CoS

Los switches de la familia Catalyst 6000 están realizando clasificaciones y marcaciones en diferentes lugares. A continuación se brinda un panorama sobre lo que ocurre en estos diferentes sitios:

- Puerto de entrada (circuito integrado específico de la aplicación (ASIC) de ingreso)
- Switching Engine (Tarjeta de función de política [PFC])
- Puerto de salida (ASIC de salida)

Activación de QoS

De forma predeterminada, QoS se inhabilita en los switches Catalyst 6000. QoS se puede habilitar ejecutando el comando CatOS **set qos enable**.

Cuando se inhabilita QoS, el switch no realiza ninguna clasificación ni marcación y, como tal, cada paquete deja el switch con la precedencia DSCP/IP que tenía al ingresar al switch.

Tratamiento del puerto de entrada

El parámetro de configuración principal para el puerto de ingreso, en lo que se refiere a la clasificación, es el estado trust del puerto. Cada puerto del sistema puede tener uno de los siguientes estados de confianza:

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

El resto de esta sección describe el modo en que el estado de confianza del puerto afecta la clasificación final del paquete. El estado de seguridad de puertos puede configurarse o cambiarse utilizando el siguiente comando CatOS:

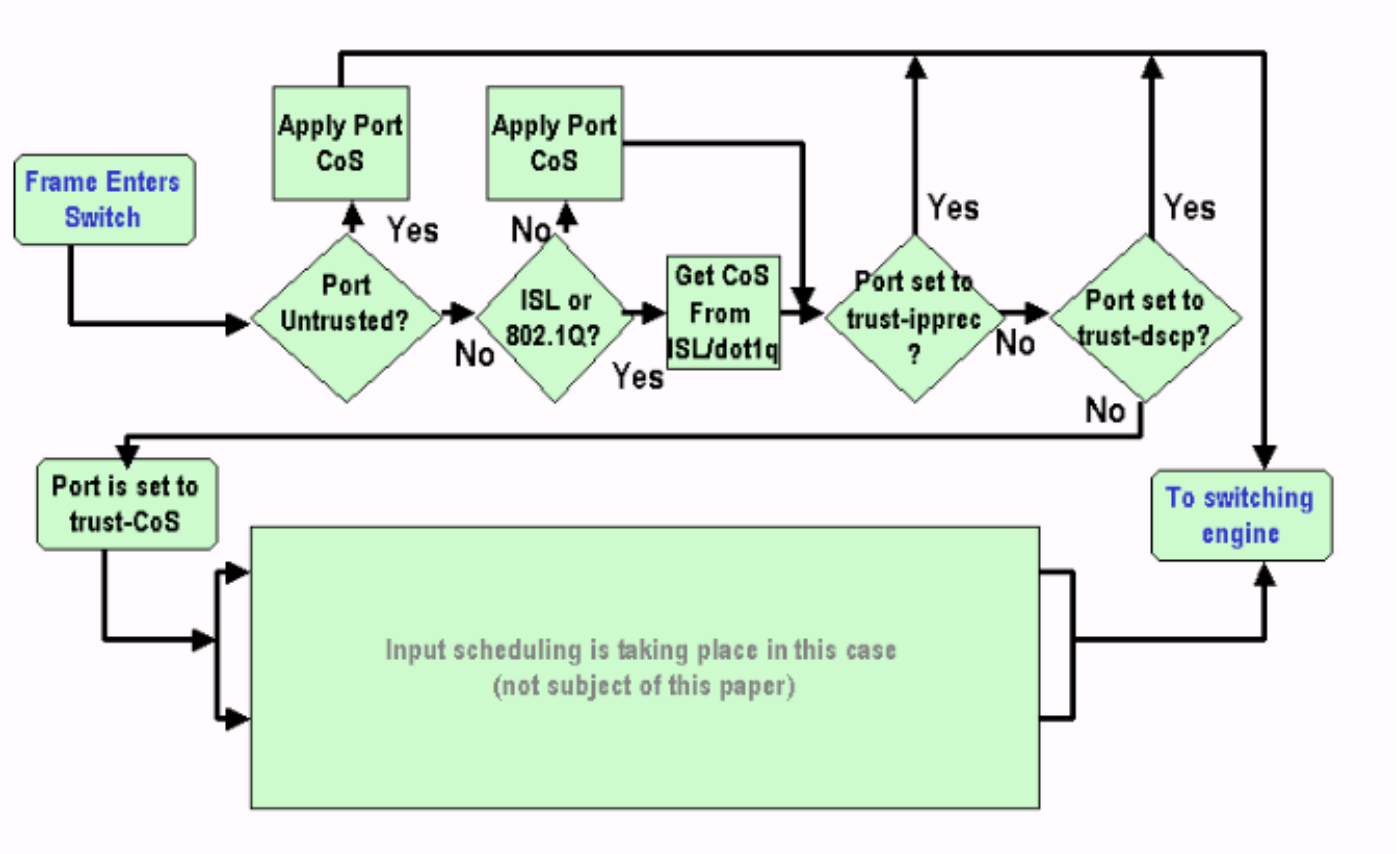
set port qos *mod/port* **trust {no confiable | trust-cos | trust-ipprec | trust-dscp }**

Nota: De forma predeterminada, todos los puertos se encuentran en estado no confiable cuando se habilita QoS.

También puede aplicar un CoS predeterminado por cada puerto a nivel del puerto de entrada como en los siguientes ejemplos:

set port qos *mod/port* **cos** *cos-value*

Si el puerto está configurado en estado inseguro, sólo debe marcar el entramado con el CoS predeterminado del puerto y pasar el encabezado al motor de conmutación (PFC). Si el puerto está configurado en uno de los estados de confianza, aplique el CoS de puerto predeterminado (si la trama no tiene un CoS recibido (dot1q o ISL)), o mantenga el CoS tal como está (para tramas dot1q e ISL) y pase la trama al motor de conmutación. En el siguiente organigrama se ilustra la clasificación de entrada:



Nota: Como se muestra en el diagrama de flujo anterior, cada trama tendrá una CoS interna asignada (ya sea la CoS recibida o la CoS del puerto predeterminado), incluidas las tramas no etiquetadas que no llevan ninguna CoS real. Esta CoS interna y el DSCP recibido se escriben en un encabezado de paquete especial (denominado encabezado Data Bus) y se envía a través del Data Bus al motor de conmutación. Esto sucede en la tarjeta de línea de ingreso y en este punto aún no se sabe si esta CoS interna se transportará al ASIC de salida e insertada en la trama saliente. Todo ello depende de lo que haga la PFC y se describe con más detalle en la siguiente sección.

Motor de conmutación (PFC)

Una vez que el encabezado haya alcanzado el motor de switching, el motor de switching Encoded Address Recognition Logic (EARL) asignará a cada trama un DSCP interno. Este DSCP interno es una prioridad interna asignada a la trama por el PFC a medida que transita a través del switch. Éste no es el DSCP en el encabezado IPv4. Se deriva de un parámetro CoS o ToS existente y se utiliza para restablecer el CoS o ToS mientras la trama sale del switch. Este DSCP interno es asignado a todas las tramas conmutadas (o enrutadas) por el PFC, inclusive las tramas que no son IP.

Cuatro causas posibles para el DSCP interno

El DSCP interno estará derivado de una de las siguientes opciones:

1. Un valor DSCP existente, configurado antes que la trama ingrese al switch.
2. Los bits de precedencia IP recibidos ya configurados en el encabezado IPV4. Dado que existen 64 valores de DSCP y sólo ocho valores de precedencia de IP, el administrador configurará una asignación que es utilizada por el switch para derivar DSCP. Los mapas predeterminados están listos para ser usados, en caso de que el administrador no configure otros.
3. Los bits de CoS recibidos ya están configurados antes del ingreso de la trama al switch, o desde la CoS predeterminada del puerto de entrada, si no había una CoS en la trama entrante. Al 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. Se puede configurar este mapa, o el switch puede usar el mapa que tenga predeterminado.
4. El DSCP puede ser configurado para la trama con el valor predeterminado DSCP asignado generalmente a través de una entrada de una Lista de control de acceso (ACL).

Para los números 2 y 3 de la lista anterior, el mapping estático utilizado es de forma predeterminada, como se indica a continuación:

- DSCP derivado equivale a CoS ocho veces, para CoS a la correlación DSCP.
- El DSCP derivado es igual a ocho veces la precedencia IP, en la precedencia IP para la asignación DSCP.

El usuario puede invalidar esta asignación estática mediante la ejecución de los siguientes comandos:

set qos ipprec-dscp-map <dscp1> <dscp2>...<dscp8>

set qos cos-dscp-map <dscp1> <dscp2>...<dscp8>

El primer valor del DSCP correspondiente al mapeo para la CoS (o precedencia IP) es "0", el segundo para la CoS (o precedencia IP) es "1" y así sucesivamente.

¿Cuál de los cuatro orígenes posibles para el DSCP interno se utilizará?

Esta sección describe las reglas que determinan cuál de las cuatro fuentes posibles descritas más arriba se utilizará para cada paquete. Eso depende de los siguientes parámetros:

1. ¿Qué ACL QoS se aplicará al paquete? Esto está determinado por las siguientes reglas:**Nota:** Cada paquete pasa por una entrada ACL.Si no hay ninguna ACL conectada al puerto entrante o VLAN, aplique la ACL predeterminada.Si existe una ACL conectada al puerto o VLAN de entrada y si el tráfico coincide con una de las entradas de la ACL, use esta entrada.Si existe una ACL conectada al puerto o VLAN de entrada, y si el tráfico no coincide con una de las entradas de la ACL, use la ACL predeterminada.
2. Cada entrada contiene una palabra clave de clasificación. A continuación se muestra una lista de posibles palabras clave y sus descripciones:trust-ipprec: El DSCP interno se derivará de la precedencia de IP recibida de acuerdo con la asignación estática independientemente de cuál sea el estado de confianza del puerto.trust-dscp: El DSCP interno se derivará del DSCP recibido independientemente de cuál sea el estado de confianza del puerto.trust-cos: La DSCP interna se derivará de la CoS recibida de acuerdo con el mapeo estático, si el estado de confianza del puerto es confiable (trust-cos, trust-dscp, trust-ipprec). Si el estado

de confianza del puerto es confianza-xx, el DCP se derivará a partir del puerto CoS predeterminado según la misma correspondencia estática.dscp xx: El DSCP interno dependerá de los siguientes estados de confianza del puerto entrante:Si el puerto no es confiable, el DSCP interno se establecerá en *xx*.Si el puerto es trust-dscp, la DSCP interna será la DCSP recibida en el paquete entrante.Si el puerto es trust-CoS, el DSCP interno se derivará del CoS del paquete recibido.Si el puerto es trust-ipprec, la DSCP interna derivará de la precedencia IP del paquete recibido.

3. Cada ACL de QoS se puede aplicar a un puerto o a una VLAN, pero hay un parámetro de configuración adicional que se debe tener en cuenta; el tipo de puerto ACL. Se puede configurar un puerto para que esté basado en la VLAN o en el puerto. La siguiente es una descripción de los dos tipos de configuraciones.Un puerto configurado para estar basado en VLAN sólo buscará la ACL aplicada a la VLAN a la que pertenece el puerto. Si hay una ACL conectada al puerto, la ACL será ignorada para el paquete que ingresa en ese puerto.Si un puerto perteneciente a una VLAN está configurado como basado en un puerto, incluso si hay una ACL conectada a esa VLAN, no será considerado para el tráfico que ingrese de ese puerto.

La sintaxis siguiente permite crear una ACL de QoS para marcar tráfico IP:

set qos acl ip *acl_name* [dscp xx | trust-cos | trust-dscp *regla* | trust-ipprec] *de entrada de acl*

La siguiente ACL, marcará todo el tráfico IP dirigido al host 1.1.1.1 con un DSCP de "40" y confiará-dscp para el resto del tráfico IP:

set qos acl TEST_ACL dscp 40 ip any host 1.1.1.1

set qos acl TEST_ACL trust-dscp ip any any

Una vez que la ACL ha sido creada, debe conectarla a un puerto o una VLAN; esto puede hacerse utilizando el siguiente comando:

set qos acl map *acl_name* [module/port | VLAN]

De forma predeterminada, cada puerto se basa en el puerto para la ACL, por lo que si desea conectar una ACL a una VLAN, debe configurar los puertos de esta VLAN como basados en vlan. Esto puede hacerse enviando el siguiente comando:

set port qos *module/port* vlan-based

También puede volver al modo basado en puerto ejecutando el siguiente comando:

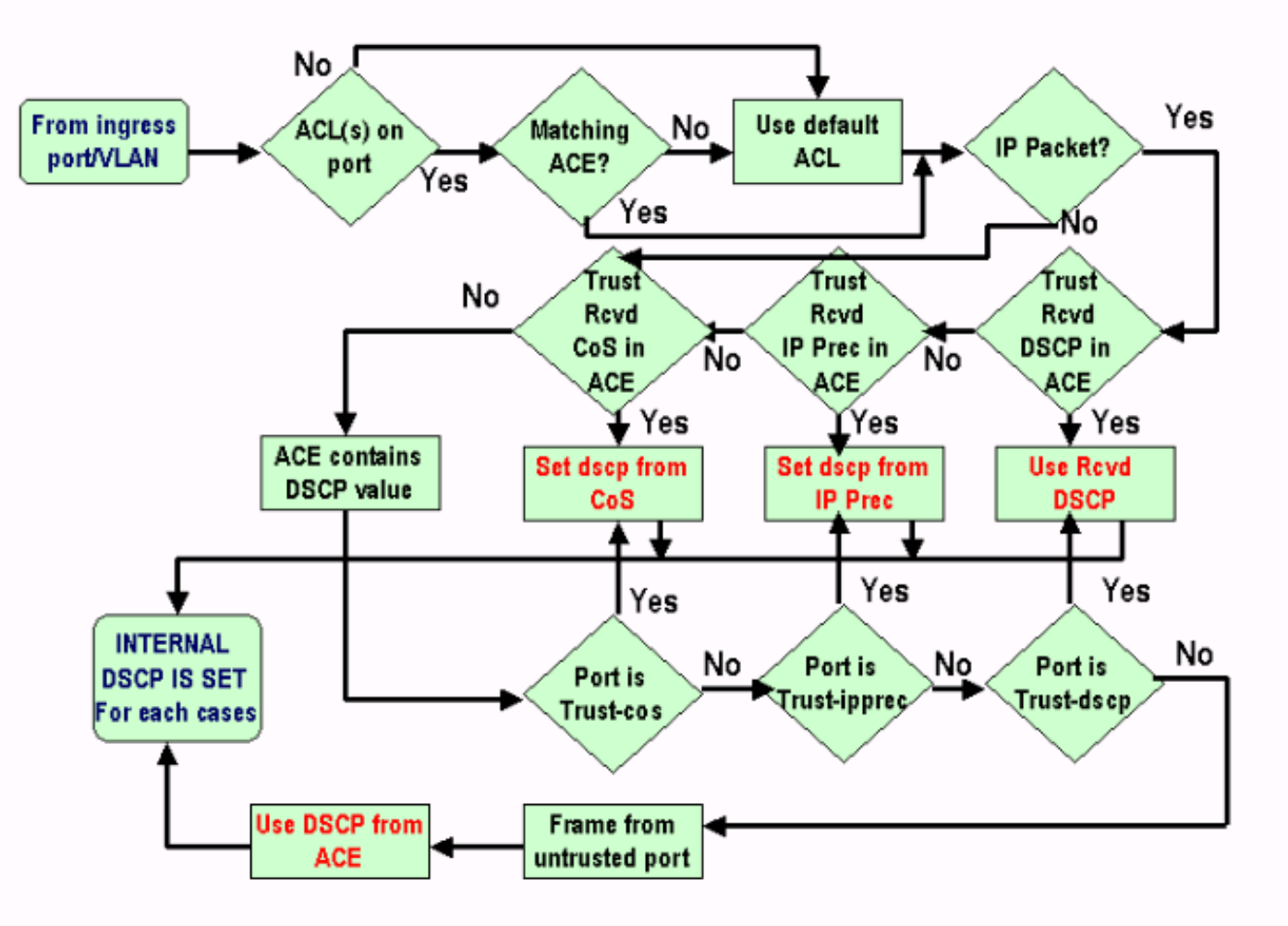
set port qos *module/port*-based

Resumen ¿Cómo se elige el DSCP interno?

Por lo tanto, el DSCP interno depende de los siguientes factores:

- estado de seguridad de puertos
- ACL conectado al puerto
- ACL predeterminada
- Basado en VLAN o basado en puerto en relación con la ACL

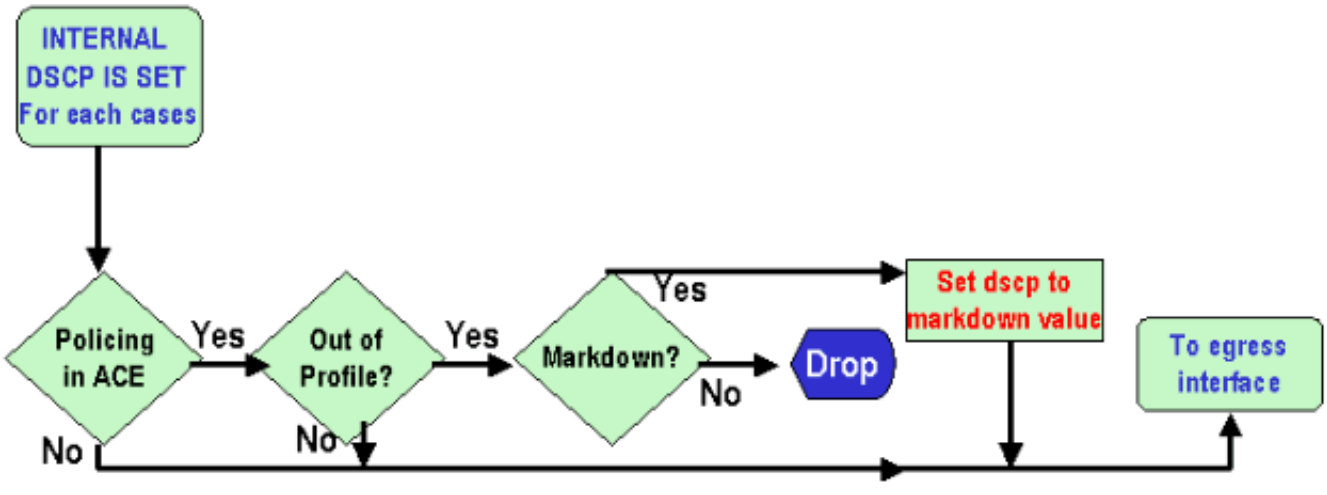
El siguiente organigrama resume cómo se elige el DSCP interno, según la configuración:



PFC también puede elaborar políticas. Esto podría resultar eventualmente en el marcado del DSCP interno para eliminación. Si desea obtener más información sobre regulación, consulte el siguiente documento:

- QoS Policing en el Catalyst 6000

El siguiente diagrama de flujo muestra cómo se aplica el regulador de tráfico:



Tratamiento del puerto de salida

No hay nada que se pueda hacer al nivel del puerto de salida para modificar la clasificación; sin embargo, en esta sección, usted marcará el paquete de acuerdo con las siguientes reglas:

- Si el paquete es un paquete IPv4, copie el DSCP interno asignado por el motor de switching en el byte ToS del encabezado IPv4.
- Si el puerto de salida está configurado para una encapsulación ISL o dot1q, utilice una CoS derivada del DSCP interno y cópiela en la trama ISL o dot1q.

Nota: El CoS se deriva del DSCP interno de acuerdo con una estática configurada por el usuario que ejecuta el siguiente comando:

Nota: **set qos dscp-cos-map** ***dscp_list:cos_value***

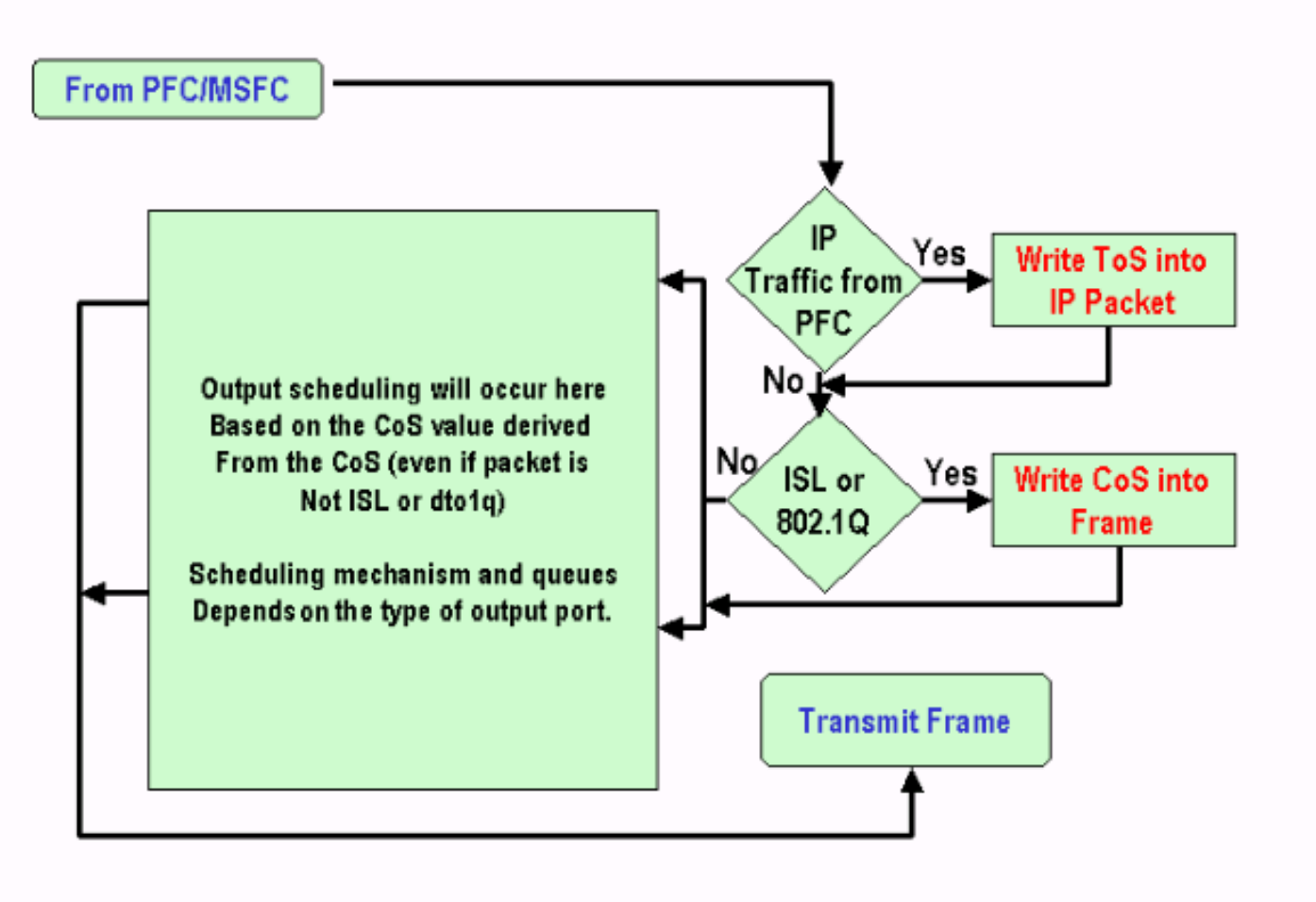
Nota: Las siguientes son las configuraciones predeterminadas. El CoS será por defecto la parte entera del DSCP dividido en ocho:

```
set qos dscp-cos-map 0-7:0
set qos dscp-cos-map 8-15:1
set qos dscp-cos-map 16-23:2
set qos dscp-cos-map 24-31:3
set qos dscp-cos-map 32-39:4
set qos dscp-cos-map 40-47:5
set qos dscp-cos-map 48-55:6
set qos dscp-cos-map 56-63:7
```

Una vez que el DSCP esté escrito en el encabezado IP, y el CoS haya sido derivado desde el DSCP, el paquete se enviará a una de las colas de salida para una programación de salida basada en su CoS (incluso si el paquete no es un dot1q ni un ISL). Si desea más información sobre programación de cola de salida, consulte los siguientes documentos:

- QoS en switches Catalyst serie 6000: Programación de salida en Catalyst 6000 con PFC o PFC 2 usando el software CatOS

El siguiente organigrama resume el procesamiento del paquete con respecto a la marcación en el puerto de salida:



Notas y limitaciones

La ACL (Lista de control de acceso) predeterminada

Por defecto, la ACL predeterminada usa "dscp 0" como palabra clave de clasificación. Esto significa que todo el tráfico que ingresa al switch a través de un puerto no confiable se marcará con un DSCP de "0" si se habilita QoS. Puede verificar la ACL predeterminada para la IP ejecutando el siguiente comando:

```
Boris-1> (enable) show qos acl  info default-action  ip
set qos acl default-action
-------------------------
ip dscp 0
```

La ACL predeterminada también se puede cambiar ejecutando el siguiente comando:

set qos acl default-action ip [dscp xx | trust-CoS | trust-dscp | trust-ipprec]

Trust-cos en Limitaciones de entradas de ACL

Existe una limitación adicional que aparece cuando se usa la palabra clave trust-CoS dentro de una entrada. Sólo puede confiarse en la Clase de servicio (CoS) de una entrada si el estado de confianza de recepción es confiable. Al intentar configurar una entrada con trust-CoS, aparecerá la siguiente advertencia:

```
Telix  (enable) set qos acl ip test_2 trust-CoS ip any any
Warning: ACL trust-CoS should only be used with ports that are also configured with port
trust=trust-CoS
test_2 editbuffer modified. Use 'commit' command to apply changes.
```

Esta limitación es el resultado de lo que se observó antes en la sección Manejo de puertos de entrada. Tal como se ve en el diagrama de flujo de esa sección, si el puerto no es confiable, a la trama se le asigna, inmediatamente, el puerto predeterminado CoS. Por lo tanto, el CoS entrante no se conserva o no se envía al motor del switch, lo que resulta en la incapacidad de confiar el CoS aún con un ACL específico.

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

Esta sección sólo concierne a las siguientes tarjetas de línea:

- WS-X6224-100FX-MT: MODO MÚLTIPLE DE 24 PUERTOS 100 FX DE CATALYST 6000
- 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 24-PORT 100FX, ENH QOS, MT
- WS-X6324-100FX-SM : CATALYST 6000 24-PORT 100FX, ENH QOS, MT
- WS-X6348-RJ-45: CATALYST 6000 DE 48 PUERTOS 10/100, QO MEJORADA
- 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, ENERGÍA EN LÍNEA

Sin embargo, estas tarjetas de línea tienen algunas limitaciones adicionales:

- En el puerto, no puede ejecutar trust-dscp o trust-ipprec.
- En el nivel de puerto, si el estado de confianza del puerto es trust-CoS, se aplican las siguientes sentencias:El umbral de recepción para la programación de entrada está habilitado. Además, el CoS en el paquete de recepción se utiliza para priorizar los paquetes para acceder al bus.El CoS no será de confianza y no se utilizará para derivar el DSCP interno, a menos que también haya configurado la ACL para ese tráfico en trust-cos. Además, no es suficiente para las tarjetas de línea configurar trust-cos en el puerto, también necesita contar con un ACL con trust-cos para ese tráfico.
- Si el estado de confianza del puerto no es confiable, se producirá un marcado normal (como en el caso estándar). Esto depende de la ACL aplicada al tráfico.

Frente a cualquier intento de configurar un estado de confianza en uno de estos puertos aparecerá uno de los siguientes mensajes de advertencia:

```
telix (enable) set port qos 3/24 trust trust-ipprec
Trust type trust-ipprec not supported on this port.

telix (enable) set port qos 8/4 trust trust-dscp
Trust type trust-dscp not supported on this port.

telix (enable) set port qos 3/24 trust trust-cos
Trust type trust-cos not supported on this port.
Receive thresholds are enabled on port 3/24.
Port  3/24 qos set to untrusted.
```

Resumen de la clasificación

Las tablas siguientes muestran el DSCP resultante clasificado de la siguiente manera:

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

Resumen de tabla genérica para todos los puertos excepto WS-X62xx y WS-X63xx

Palabra clave de ACL / Estado de Seguridad de Puertos	dscp xx	trust-dscp	trust-ipprec	trust-CoS
No confiable	xx (1)	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) Ésta es la única manera de realizar una nueva marca de una trama.

Resumen de tabla para WS-X62 *xx* o WS-X63 *xx*

Palabra clave de ACL / Estado de Seguridad de Puertos	dscp 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	xx	Rx dscp	derivado de ipprec de Rx	derivado de CoS Rx o CoS de puerto (2)

(2) Éste es el único modo de preservar la CoS entrante para tráfico proveniente de una tarjeta de línea de 62xx o 63xx.

Control y verificación de una configuración

Verificación de la configuración del puerto

Los parámetros y las configuraciones del puerto se pueden verificar mediante la emisión del siguiente comando:

show port qos ***module/port***

Al emitir este comando, puede verificar, entre otros parámetros, los siguientes parámetros de clasificación:

- basado en puerto o basado en VLAN
- trust port type
- ACL conectado al puerto

A continuación se proporciona un ejemplo de la salida de este comando con los campos importantes relativos a la clasificación resaltados:

```
tamer (enable) show port qos 1/1
QoS is enabled for the switch.
QoS policy source for the switch set to local.


Port  Interface Type Interface Type Policy Source Policy Source
      config         runtime        config        runtime
----- -------------- -------------- ------------- -------------
 1/1    port-based     port-based      COPS           local

Port  TxPort Type  RxPort Type  Trust Type   Trust Type    Def CoS Def CoS
                                config       runtime       config  runtime
----- ------------ ------------ ------------ ------------- ------- -------
 1/1     1p2q2t       1p1q4t     untrusted     untrusted      0       0

(*)Runtime trust type set to untrusted.

Config:
Port  ACL name                         Type
----- -------------------------------- ----
 1/1  test_2                           IP

Runtime:
Port  ACL name                         Type
----- -------------------------------- ----
 1/1  test_2                            IP
```

Nota: Para cada campo, hay el parámetro configurado y el parámetro de tiempo de ejecución. El parámetro que se aplica al paquete es el del tiempo de ejecución.

Verificando el ACL

Puede verificar la ACL que ha sido aplicada y visualizada en los comandos anteriores mediante el siguiente comando:

show qos acl info runtime *acl_name*

```
tamer (enable) show qos acl info run test_2
set qos acl IP test_2
---------------------------------------------
1. dscp 32 ip any host 1.1.1.1
2. trust-dscp any
```

Estudios de casos de ejemplo

Los siguientes ejemplos son configuraciones de muestra de casos comunes que podrían aparecer en una red.

Caso 1: Marcado en el borde

Suponga que está configurando un Catalyst 6000 como switch de acceso con muchos usuarios conectados en la ranura 2, en la cual se encuentra instalada una tarjeta de línea WS-X6348 (10/100M). Los usuarios pueden enviar:

- Tráfico de datos normal: Esto siempre está en la VLAN 100 y necesita obtener un DSCP de "0".
- Tráfico de voz desde un teléfono IP: Esto siempre está en la VLAN 101 auxiliar de voz y necesita obtener un DSCP de "40".
- Tráfico de aplicación esencial para la misión: También viene en VLAN 100 y es dirigido al servidor 10.10.10.20. Este tráfico necesita obtener un DSCP de "32".

Ningún tráfico está marcado por la aplicación. Por lo tanto, dejará el puerto como no confiable y configurará una ACL específica para clasificar el tráfico. Se aplicará una ACL a la VLAN 100 y una ACL a la VLAN 101. También debe configurar todos los puertos como basados en VLAN. El siguiente es un ejemplo de la configuración resultante:

```
set qos enable
set port qos 2/1-48 vlan-based
!--- Not needed, as it is the default. set port qos 2/1-48 trust untrusted set qos acl ip
Data_vlan dscp 32 ip any host 10.10.10.20 !--- Not needed, because if it is not present you
would !--- use the default ACL which has the same effect. Set qos acl ip Data_vlan dscp 0 ip any
any set qos acl ip Voice_vlan dscp 40 ip any any commit qos acl all set qos acl map Data_vlan
100 set qos acl map Voice_vlan 101
```

Caso 2: Confianza en el núcleo sólo con una interfaz Gigabit

Suponga que está configurando un Catalyst 6000 central con sólo una interfaz Gigabit en la ranura 1 y la ranura 2 (sin tarjeta de línea 62xx o 63xx en el chasis). El tráfico ha sido correctamente marcado con anterioridad por los switches de acceso, entonces, no es necesario

que haga ninguna remarcación, pero es necesario que se asegure la confianza del DSCP entrante. Este es el caso más fácil ya que todos los puertos se marcarán como trust-dscp y eso será suficiente:

```
set qos enable
set port qos 1/1-2 trust trust-dscp
set port qos 2/1-16 trust trust-dscp
...
```

Caso 3: Confianza en el núcleo con un puerto 62xx or 63xx en el chasis

Suponga que está configurando un dispositivo de núcleo/distribución con un link Gigabit en una tarjeta de línea También, necesita confiar en todo el tráfico entrante ya que se marcó anteriormente al nivel del switch de acceso. Debido a que no puede confiar en dscp en la tarjeta de línea 6348, el método más fácil en este caso sería dejar todos los puertos como no confiables y cambiar la ACL predeterminada a trust-dscp, como en el siguiente ejemplo:

```
set qos enable
set port qos 2/1-16 trust untrusted
set port qos 3/1-48 trust untrusted
set qos acl default-action ip trust-dscp
```

Información Relacionada

- Soporte de Producto de LAN
- Soporte de Tecnología de LAN Switching
- Soporte Técnico - Cisco Systems