Classificação de QoS e marcação no Catalyst 6500/6000 series switch que executa o Cisco IOS Software

Índice

Introdução

Este documento examina os aspectos relacionados à marcação e à classificação de um pacote em várias fases dentro do chassi do Cisco Catalyst 6500/6000 que executa o Cisco IOS® Software. Este documento descreve casos especiais, restrições e fornece estudos de caso sucintos.

Este documento não fornece uma lista exaustiva de todos os comandos do Cisco IOS Software que se relacionam a QoS ou a marcação. Para obter mais informações sobre do comando line interface(cli) do Cisco IOS Software, refira configurar PFC QoS.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de hardware:

- Catalyst 6500/6000 series switch que executa o Cisco IOS Software e o uso um destes motores do supervisor:Um Supervisor Engine 1A com um Policy Feature Card (PFC) e um Multilayer Switch Feature Card (MSFC)Um Supervisor Engine 1A com um PFC e um MSFC2Um Supervisor Engine 2 com um PFC2 e um MSFC2

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Terminologia

A lista fornece a terminologia que este documento usa:

- Differentiated Services Code Point (DSCP) — Os primeiros seis bit do byte do Tipo de serviço (ToS) no cabeçalho IP. O DSCP está presente somente no pacote IP.**Nota:** O interruptor igualmente atribui um DSCP interno a cada pacote, se IP ou não-IP. Os quatro origens possíveis para a seção do DSCP interno deste documento detalham esta atribuição do DSCP interno.
- Precedência IP — Os primeiros três bit do byte ToS no cabeçalho IP.
- Classe de serviço (CoS) — O único campo que pode ser usado para marcar um pacote na camada 2 (L2). CoS consiste em qualquens um três bit:Os três bit do IEEE 802.1P (dot1p) no IEEE 802.1Q (dot1q) etiquetam para o pacote do dot1q.**Nota:** À revelia, os switch Cisco não etiquetam pacotes do VLAN nativo.Os três bit chamados do “campo usuário” no encabeçamento do Inter-Switch Link (ISL) para um pacote ISL-encapsulado.**Nota:** CoS não está atual dentro de um non-dot1q ou de um pacote de ISL.
- Classificação — O processo que é usado para selecionar o tráfego para ser marcado.
- Marcar — O processo que ajusta um valor da camada 3 (L3) DSCP em um pacote. Este documento estende a definição da marcação para incluir o ajuste de valores L2 CoS.

O Catalyst 6500/6000 series switch pode fazer classificações com base nestes três parâmetros:

- DSCP
- Precedência de IP
- CoS

O Catalyst 6500/6000 series switch executa a classificação e marcação em várias fases. Este é o que ocorre em lugares diferentes:

- Porta de entrada ([ASIC] dos circuitos integrados do aplicativo específicos do ingresso)
- Mecanismo de Switching (PFC)
- Porta de saída (ASIC de saída)

Manejo da porta de entrada

O parâmetro da configuração principal para a porta de ingresso, no que diz respeito à classificação, é o `estado de confiança da` porta. Cada porta do sistema pode ter um destes `estados de confiança`:

- `trust-ip-precedence`
- `trust-dscp`
- `trust-cos`
- `não confiável`

A fim ajustar ou mudar o port trust state, emita este comando do Cisco IOS Software no modo da `relação`:

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

Nota: À revelia, todas as portas estão no `estado não-confiável` quando QoS é permitido. A fim permitir QoS no Catalyst 6500 que executa o Cisco IOS Software, emita o **comando mls qos no** modo da configuração principal.

A nível da porta de entrada, você pode igualmente aplicar um padrão CoS pela porta. Aqui está um exemplo:

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

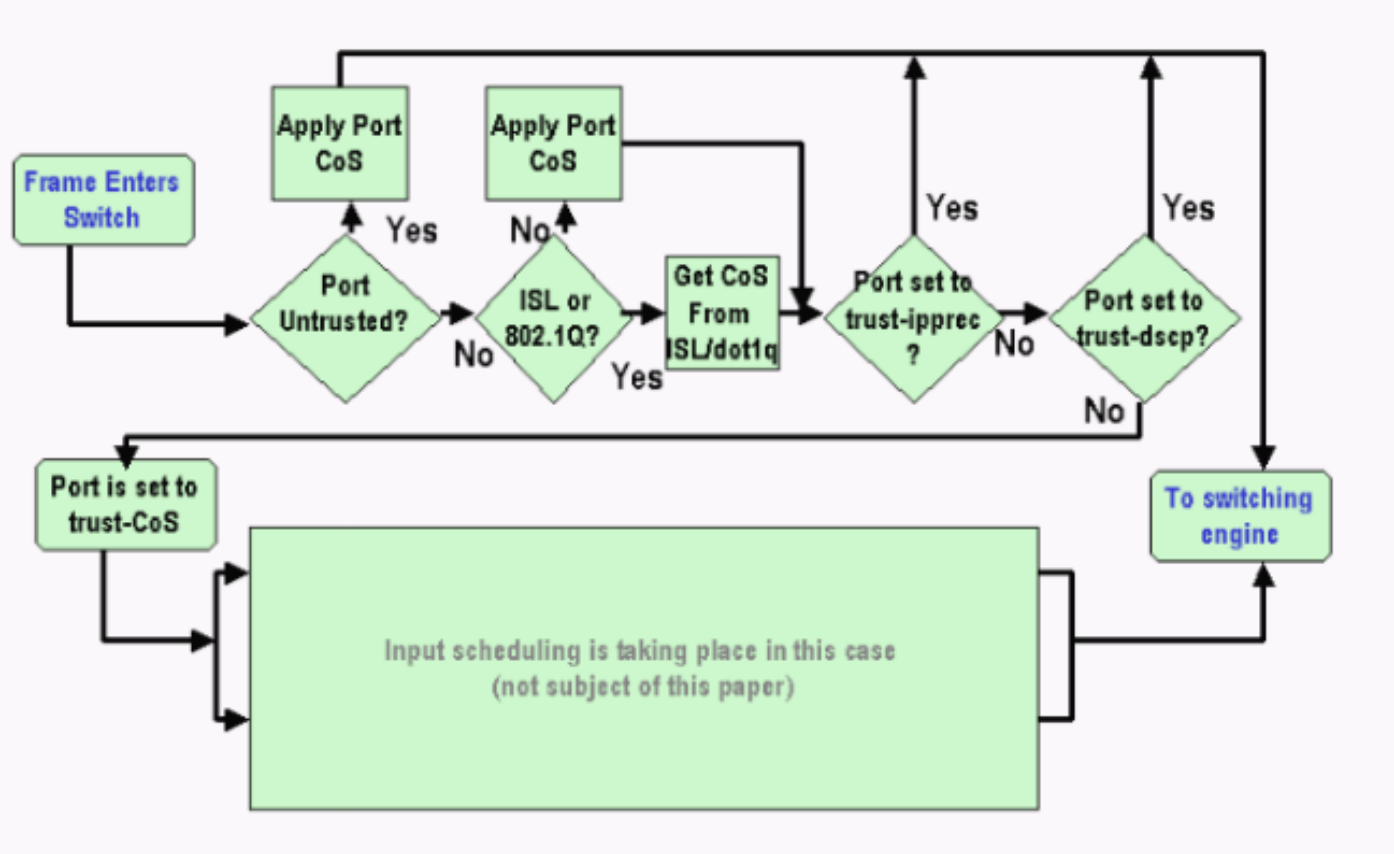
Este padrão CoS aplica-se a todos os pacotes, tais como o IP e as Trocas de Pacote Entre Redes IPX (IPX). Você pode aplicar o padrão CoS a toda a porta física.

Se a porta está no `estado não-confiável`, marque o quadro com o padrão de porta CoS e passe o encabeçamento ao mecanismo de switching (PFC). Se a porta é ajustada a um dos `estados de confiança`, execute uma destas duas opções:

- Se o quadro não tem um CoS recebido (dot1q ou ISL), aplique a porta CoS padrão.
- Para o dot1q e os quadros ISL, mantenha o CoS como é.

Então, passe o quadro ao mecanismo de switching.

Este exemplo ilustra a classificação de entrada e a marcação. O exemplo mostra como atribuir um CoS interno a cada quadro:



Nota: Enquanto este exemplo mostra, cada quadro está atribuído um CoS interno. A atribuição é baseada no CoS recebido ou na porta CoS padrão. O CoS interno inclui os frames sem etiqueta que não levam nenhum CoS real. O CoS interno é escrito em um cabeçalho de pacote especial, que seja chamado um cabeçalho de barramento de dados, e enviado sobre o barramento de dados ao mecanismo de switching.

Mecanismo de Switching (PFC)

Quando o encabeçamento alcança o mecanismo de switching, o Enhanced Address Recognition Logic do mecanismo de switching (EARL) atribui a cada quadro um DSCP interno. Este DSCP interno é uma prioridade interna que esteja atribuída ao quadro pelo PFC enquanto o quadro transita pelo interruptor. Este não é o DSCP no encabeçamento da versão IP 4 (IPv4). O DSCP interno está derivado de um ajuste existente de CoS ou ToS e usado para restaurar o CoS ou o ToS enquanto o quadro retira o interruptor. Este DSCP interno é atribuído a todos os quadros que são comutados ou distribuídos pelo PFC, mesmo quadros não-IP.

Esta seção discute como você pode atribuir uma política de serviços à relação a fim fazer uma marcação. A seção igualmente discute a configuração final do DSCP interno, que depende do port trust state e da política de serviços que é aplicada.

Configurar a política de serviços para classificar ou marcar um pacote no Cisco IOS Software Release 12.1(12c)E e Mais Recente

Termine estas etapas a fim configurar a política de serviços:

1. Configurar um Access Control List (ACL) para definir o tráfego que você quer considerar.O ACL pode ser numerado ou nomeado, e o Catalyst 6500/6000 apoia um ACL extendido. Emita o comando do Cisco IOS Software da **lista de acesso** *xxx*, como este exemplo

mostra:`(config)#`**`access-list 101 permit ip any host 10.1.1.1`**

2. Configurar uma classe de tráfego (mapa da classe) para combinar o tráfego com base no ACL que você definiu ou com base no DSCP recebido.Emita o comando do Cisco IOS Software do **mapa de classe**. O PFC QoS não apoia mais de uma instrução compatível pelo mapa da classe. Também, o PFC QoS apoia somente estas instruções compatível:**match ip access-groupmatch ip dscpprecedência compatível de ipprotocolo do fósforoNota: O comando match protocol** permite o uso do Network Based Application Recognition (NBAR) combinar o tráfego.**Nota:** Destas opções, somente o **dscp do fósforo IP** e as indicações da **Precedência IP do fósforo** são apoiados e trabalham. Estas indicações, contudo, não são úteis na marcação ou na classificação dos pacotes. Você pode usar estas indicações, por exemplo, para fazer o policiamento em todos os pacotes que combinam um determinado DSCP. Contudo, esta ação é além do alcance deste documento.`(config)#`**`class-map`** *`class-name`*
`(config-cmap)#`**`match {access-group | input-interface | ip dscp}`** **Nota:** Este exemplo mostra somente três opções para o **comando match**. Mas você pode configurar muito mais opções neste comando prompt.**Nota:** Qualquer das opções neste **comando match** é tomado para critérios de verificação de repetição de dados e as outras opções são deixadas para fora, de acordo com os pacotes recebidos.Aqui está um exemplo:
```
class-map match-any TEST
 match access-group 101

class-map match-all TEST2
 match ip precedence 6
```
3. Configurar um mapa de política para aplicar uma política a uma classe que você defina previamente.O mapa de política contém:Um nomeUm grupo de indicações da classePara cada indicação da classe, a ação que precisa de ser tomada para essa classeAs ações apoiadas em PFC1 e em PFC2 QoS são:**trust dscptrust ip precedencetrust cosajuste o dscp IP no** Cisco IOS Software Release 12.1(12c)E1 e Mais Recente**ajuste a Precedência IP no** Cisco IOS Software Release 12.1(12c)E1 e Mais Recente**políciaNota:** Esta ação é além do alcance deste documento.`(config)#`**`policy-map`** *`policy-name`*
`(config-pmap)#`**`class`** *`class-name`*
`(config-pmap-c)#`**`{police | set ip dscp}`**
Nota: Este exemplo mostra somente duas opções, mas você pode configurar muito mais opções nesta `(configuração-pmap-C) #` comando prompt.Aqui está um exemplo:
```
policy-map test_policy
 class TEST
   trust ip precedence
 class TEST2
   set ip dscp 16
```
4. Configurar uma entrada de política de serviço para aplicar um mapa de política que você defina previamente a uns ou vários a relação.**Nota:** Você pode anexar uma política de serviços à interface física ou ao Switched Virtual Interface (SVI) ou à interface de VLAN. Se você anexa uma política de serviços a uma interface de VLAN, as únicas portas que usam esta política de serviços são as portas que pertencem a esse VLAN e estão configuradas para QoS com base em VLAN. Se a porta não é ajustada para QoS com base em VLAN, a porta ainda usa o padrão QoS com base na porta e olha somente a política de serviços que é anexada à interface física.Este exemplo aplica o `test_policy da` política de serviços às portas de Ethernet em gigabit 1/1:`(config)` **`interface gigabitethernet 1/1`**
`(config-if)#`**`service-policy input test_policy`**
Este exemplo aplica o `test_policy da` política de serviços a todas as portas no VLAN10 que têm uma configuração com base em VLAN do ponto 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: Você pode combinar etapa 2 e etapa 3 deste procedimento se você salta a definição específica da classe e anexa o ACL diretamente na definição do mapa de política. Neste exemplo, onde a `polícia do` teste de classe não foi definida antes da configuração do mapa de política, a classe é definida dentro do mapa de política:`(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
```

Configurar a política de serviços para classificar mais cedo ou marcar um pacote nos Cisco IOS Software Release do que o Cisco IOS Software Release 12.1(12c)E

Nos Cisco IOS Software Release mais cedo do que o Cisco IOS Software Release 12.1(12c)E1, você não pode usar o **dscp do grupo IP** ou a ação da **Precedência IP do grupo em um** mapa de política. Consequentemente, a única maneira de fazer uma marcação do tráfego específico que uma classe defina é configurar muito um vigilante com uma taxa alta. Esta taxa deve ser, por exemplo, pelo menos a linha taxa da porta ou de algo altamente bastante permitir que todo o tráfego bata esse vigilante. Então, **set-dscp-transmit** *xx do* uso como a conform action. Siga estas etapas a fim estabelecer esta configuração:

1. Configurar um ACL para definir o tráfego que você quer considerar.O ACL pode ser numerado ou nomeado, e o Catalyst 6500/6000 apoia um ACL extendido. Emita o comando do Cisco IOS Software da **lista de acesso** *xxx*, como este exemplo mostra:`(config)#`**`access-list 101 permit ip any host 10.1.1.1`**
2. Configurar uma classe de tráfego (mapa da classe) para combinar o tráfego com base no um ou outro o ACL que você definiu ou com base no DSCP recebido.Emita o comando do Cisco IOS Software do **mapa de classe**. O PFC QoS não apoia mais de uma instrução compatível pelo mapa da classe. Também, o PFC QoS apoia somente estas instruções compatível:**match ip access-groupmatch ip dscpprecedência compatível de ipprotocolo do fósforoNota: O comando match protocol** permite o uso do NBAR combinar o tráfego.**Nota:** Destas indicações, somente o **dscp do fósforo IP** e as indicações da **Precedência IP do fósforo** são apoiados e trabalham. Estas indicações, contudo, não são úteis na marcação ou na classificação dos pacotes. Você pode usar estas indicações, por exemplo, para fazer o policiamento em todos os pacotes que combinam um determinado DSCP. Contudo, esta ação é além do alcance deste documento.`(config)#`**`class-map`** *`class-name`*
`(config-cmap)#`**`match {access-group | input-interface | ip dscp}`**
Nota: Este exemplo mostra somente três opções para o **comando match**. Mas você pode configurar muito mais opções neste comando prompt.Aqui está um exemplo:
```
class-map match-any TEST
 match access-group 101

class-map match-all TEST2
 match ip precedence 6
```
3. Configurar um mapa de política para aplicar uma política a uma classe que você defina

previamente.O mapa de política contém:Um nomeUm grupo de indicações da classePara cada indicação da classe, a ação que precisa de ser tomada para essa classeAs ações apoiadas em PFC1 ou em PFC2 QoS são:**trust dscptrust ip precedencetrust cospolícia**Você deve usar a **declaração de vigia** porque o **dscp do grupo IP** e as ações da **Precedência IP do grupo** não são apoiados. Desde que você não quer realmente policiar o tráfego, mas o marcar apenas, use um vigilante que seja definido para permitir todo o tráfego. , Configurar consequentemente o vigilante com uma grande taxa e estoure. Por exemplo, você pode configurar o vigilante com a taxa permitida máximo e estourar. Aqui está um exemplo:

```
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. Configurar uma entrada de política de serviço para aplicar um mapa de política que você defina previamente a umas ou várias relações.**Nota:** A política de serviços pode ser anexada a uma interface física ou ao SVI ou à interface de VLAN. Se uma política de serviços é anexada a uma interface de VLAN, simplesmente as portas que pertencem a esse VLAN e que são configuradas para o uso com base em VLAN de QoS esta política de serviços. Se a porta não é ajustada para QoS com base em VLAN, a porta ainda usa o padrão QoS com base na porta e olha somente uma política de serviços que seja anexada à interface física.Este exemplo aplica o `test_policy da` política de serviços às portas de Ethernet em gigabit 1/1:`(config)` **`interface gigabitethernet 1/1`**
`(config-if)#`**`service-policy input test_policy`**
Este exemplo aplica o `test_policy da` política de serviços a todas as portas no VLAN10 que têm uma configuração com base em VLAN do ponto 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
```

Quatro fontes possíveis para DSCP interno

O DSCP interno é derivado de um destes:

1. Um valor recebido existente DSCP, que seja ajustado antes que o quadro incorporar o interruptorUm exemplo é **dscp da confiança**.
2. Os bit de precedência IP recebidos que são ajustados já no encabeçamento do IPv4Porque há 64 valores DSCP e somente oito valores de precedência IP, o administrador configura um mapeamento que o interruptor se use para derivar o DSCP. Os mapeamentos padrão são no lugar, no caso em que o administrador não configurar os mapas. Um exemplo é **Precedência IP da confiança**.
3. Os bit recebidos de CoS que são ajustados já antes que o quadro incorporar o interruptor e que estejam armazenados no cabeçalho de barramento de dados, ou se não havia nenhum CoS no frame de entrada, do padrão CoS da porta de recebimentoAssim como ocorre com a precedência IP, existe um máximo de oito valores CoS, sendo que cada um deve ser mapeado para um dos valores 64 DSCP. O administrador pode configurar este mapa, ou o interruptor pode usar o mapa padrão que é já no lugar.

4. A política de serviços pode ajustar o DSCP interno a um valor específico.

Para os números 2 e 3 nesta lista, o mapeamento estático é à revelia, desse modo:

- Para o mapeamento de CoS-to-DSCP, o DSCP que é iguais derivados oito vezes o CoS.
- Para o mapeamento de precedência a DSCP IP, o DSCP que é iguais derivados oito vezes a Precedência IP.

Você pode emitir estes comandos a fim cancelar e verificar este mapeamento estático:

- **os qos dos mls traçam IP-prec-DSCP** *dscp_1 dscp_2 dscp_3 dscp_4 dscp_5 dscp_6 dscp_7 dscp_8*
- **os qos dos mls traçam cos-DSCP** *dscp_1 dscp_2 dscp_3 dscp_4 dscp_5 dscp_6 dscp_7 dscp_8*

O primeiro valor do DSCP que corresponde ao mapeamento para o CoS (ou a Precedência IP) é 0. O segundo valor para o CoS (ou a Precedência IP) é 1, e o teste padrão continua desta maneira. Por exemplo, este comando muda o mapeamento de modo que o CoS 0 seja traçado ao DSCP de 0, e o CoS de 1 é traçado ao DSCP de 8, e assim por diante:

```
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
```

Como o DSCP interno é escolhido?

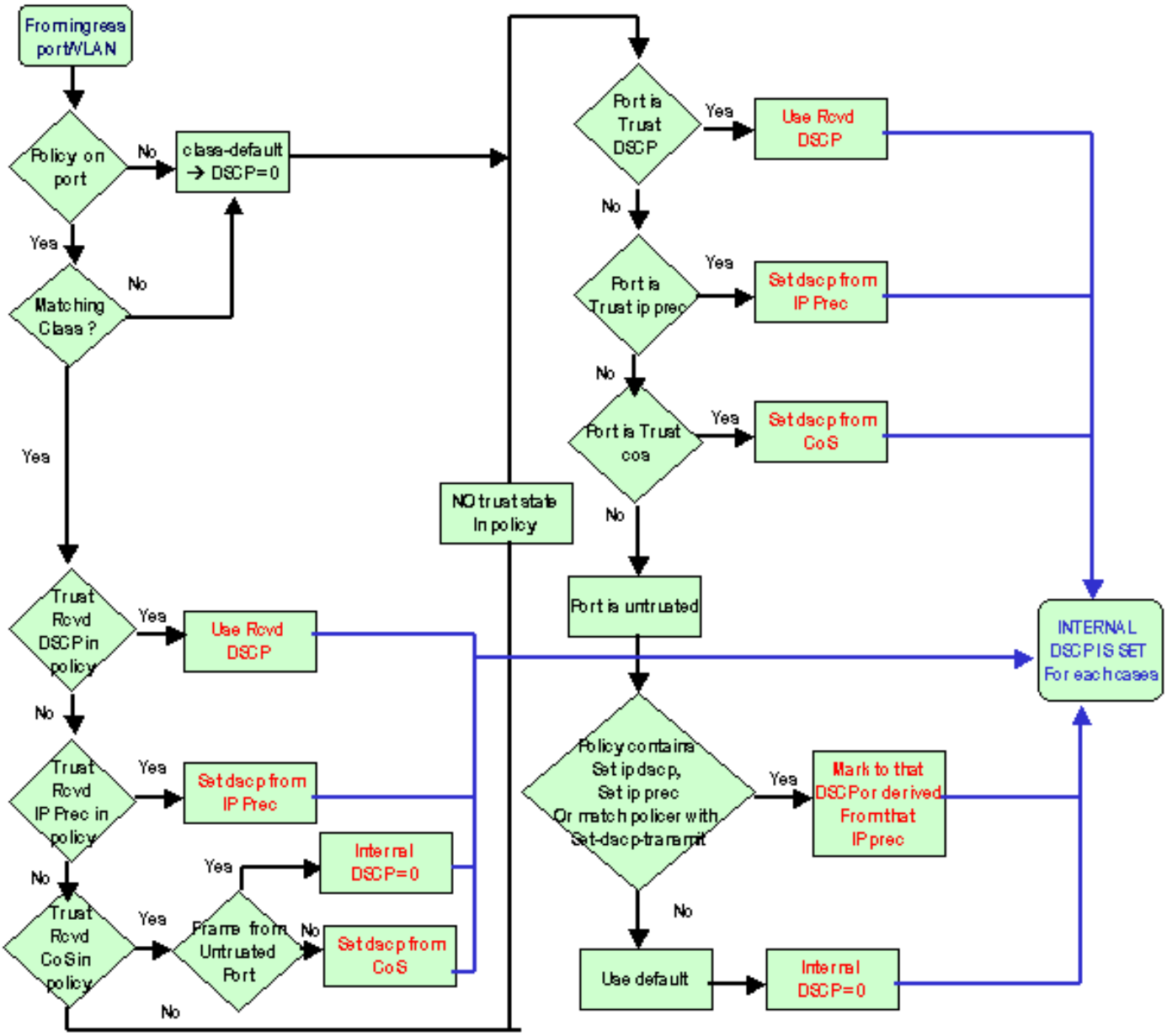
O DSCP interno é escolhido com base nestes parâmetros:

- O mapa da política de QoS que é aplicado ao pacoteO mapa da política de QoS é determinado por estas regras:Se nenhuma política de serviços é anexada à porta de recebimento ou ao VLAN, use o padrão.**Nota:** Esta ação padrão é ajustar o DSCP interno a 0.Se uma política de serviços é anexada à porta de recebimento ou ao VLAN, e se o tráfego combina uma das classes que a política define, use esta entrada.Se uma política de serviços é anexada à porta de recebimento ou ao VLAN, e se o tráfego não combina uma das classes que a política define, use o padrão.
- `O estado de confiança da` porta e a ação do mapa de políticaQuando a porta tiver um `estado de confiança` específico e uma política com uma determinada marcação (que confia a ação ao mesmo tempo), estas regras aplicam-se:**O comando set ip dscp** ou o DSCP que é definido pelo vigilante em um mapa de política são somente aplicado se a porta é deixada no `estado não-confiável`.Se a porta tem um `estado de confiança`, este `estado de confiança` está usado para derivar o DSCP interno. O estado confiável de porta sempre tem precedência sobre o comando set ip dscp.**O comando trust xx em um** mapa de política toma a precedência sobre o port trust state.Se a porta e a política contêm um `estado de confiança` diferente, o `estado de confiança` que vem do mapa de política está considerado.

Consequentemente, o DSCP interno depende destes fatores:

- O port trust state
- A política de serviços (com uso do ACL) que é anexada à porta
- O mapa da política padrão**Nota:** O padrão restaura o DSCP a 0.
- Se com base em VLAN ou com base na porta no que diz respeito ao ACL

Este diagrama resume como o DSCP interno é escolhido com base na configuração:



O PFC também é capaz de realizar vigilância. Isto pode eventualmente conduzir a um markdown do DSCP interno. Para obter mais informações sobre do policiamento, refira o Regulamentação QoS no Catalyst 6500/6000 series switch.

Manejo da porta emissora

Você não pode fazer qualquer coisa a nível da porta de saída a fim mudar a classificação. Contudo, marque o pacote com base nestas regras:

- Se o pacote é um pacote IPv4, copie o DSCP interno que o mecanismo de switching atribui no byte ToS do encabeçamento do IPv4.
- Se a porta emissora é configurada para um encapsulamento ISL ou de dot1q, use um CoS que seja derivado do DSCP interno. Copie o CoS no quadro ISL ou de dot1q.

Nota: O CoS é derivado do DSCP interno de acordo com uma estática. Emita este comando a fim configurar a estática:

```
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.
```

As configurações padrão aparecem aqui. À revelia, o CoS é a peça de número inteiro do DSCP, dividida por oito. Emita este comando a fim ver e verificar o mapeamento:

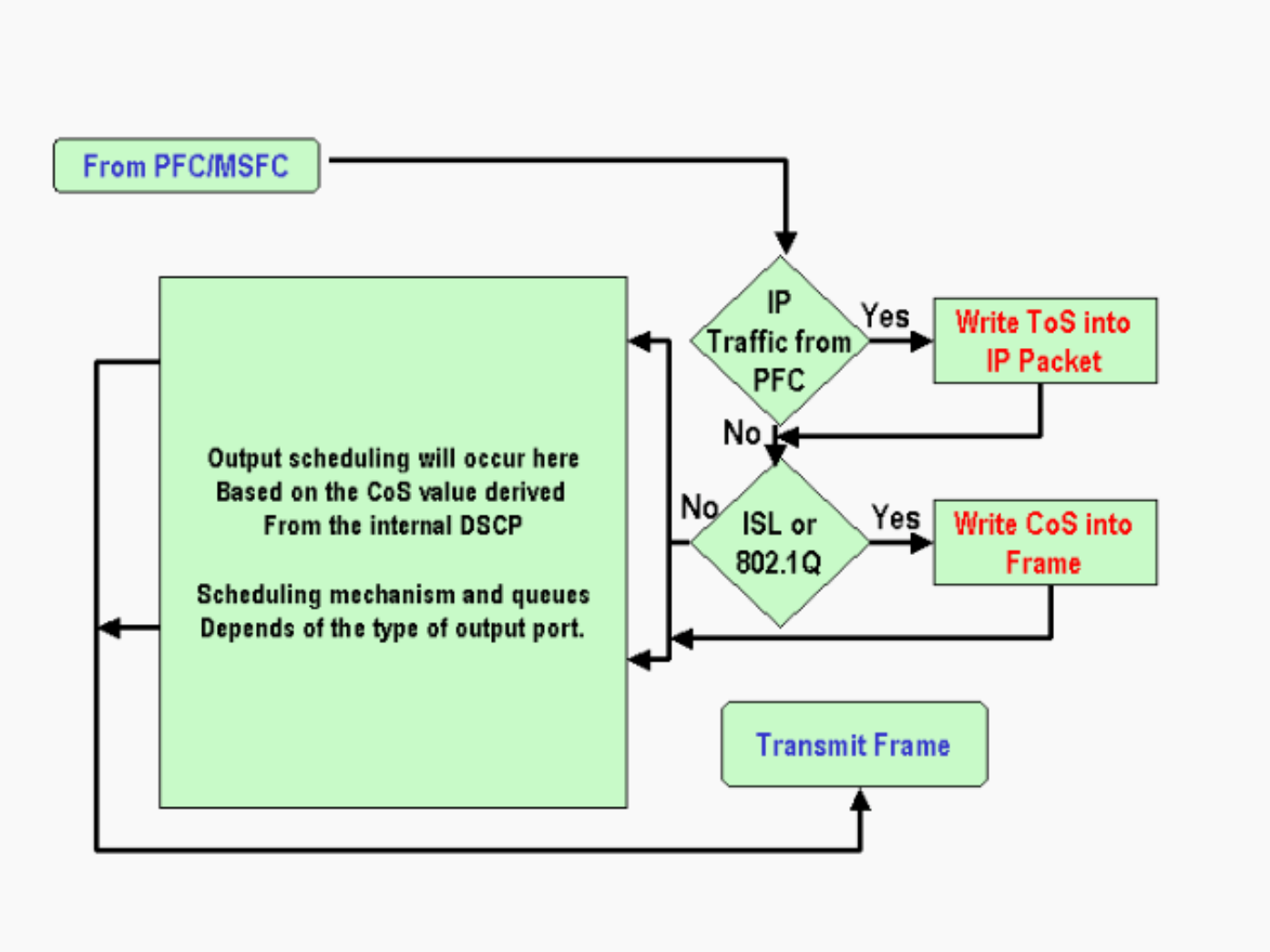
```
cat6k#show mls qos maps
...
  Dscp-cos map:                                     (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 02 02 02 02
      2 :    02 02 02 02 03 03 03 03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

A fim mudar este mapeamento, emita este comando configuration no modo da configuração 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
...
```

Depois que o DSCP está escrito no cabeçalho IP e o CoS está derivado do DSCP, o pacote está enviado a uma das filas de saída para a programação de emissor com base no CoS. Isto ocorre mesmo se o pacote não é um dot1q ou um ISL. Para obter mais informações sobre da programação da fila de saída, refira a programação de emissor de QoS no Catalyst 6500/6000 series switch que executa o software do sistema do Cisco IOS.

Este diagrama resume o processamento do pacote no que diz respeito à marcação na porta emissora:



Notas e limitações

ACL padrão

O ACL padrão usa "dscp 0" como a palavra-chave de classificação. Todo o tráfego que incorpora o interruptor através de uma porta não-confiável e não bate uma entrada da política de serviços está identificado por meio de um DSCP de 0 se QoS é permitido. Atualmente, você não pode mudar o ACL padrão no Cisco IOS Software.

Nota: No software do OS do catalizador (Cactos), você pode configurar e mudar este comportamento padrão. Para mais informação, refira *o a* seção do *ACL padrão da* classificação de QoS e da marcação no Catalyst 6500/6000 series switch que executa o Cactos Software.

Limitações das placas de linha WS-X61xx, WS-X6248-xx, WS-X6224-xx e WS-X6348-xx

Esta seção refere-se somente a estas placas de linha:

- WS-X6224-100FX-MT : Catalizador 6000 24-Port 100 FX multimodo
- WS-X6248-RJ-45: Módulo 48-Port 10/100 RJ-45 do catalizador 6000
- WS-X6248-TEL: Módulo telco 48-Port 10/100 do catalizador 6000
- WS-X6248A-RJ-45 : Catalizador 6000 48-Port 10/100, QoS aumentado

- WS-X6248A-TEL : Catalizador 6000 48-Port 10/100, QoS aumentado
- WS-X6324-100FX-MM: Catalizador 6000 24-Port 100 FX, QoS aumentado, MT
- WS-X6324-100FX-SM: Catalizador 6000 24-Port 100 FX, QoS aumentado, MT
- WS-X6348-RJ-45 Catalizador 6000 48-Port 10/100, QoS aumentado
- WS-X6348-RJ21V: Catalizador 6000 48-Port 10/100, potência em linha
- WS-X6348-RJ45V: Catalizador 6000 48-Port 10/100, QoS aumentado, potência em linha
- WS-X6148-RJ21V: Potência em linha do Catalyst 6500 48-Port 10/100
- WS-X6148-RJ45V: Potência em linha do Catalyst 6500 48-Port 10/100

Estas placas de linha têm uma limitação. A nível da porta, você não pode configurar o `estado de confiança` com o uso de qualqueras um palavras-chaves:

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

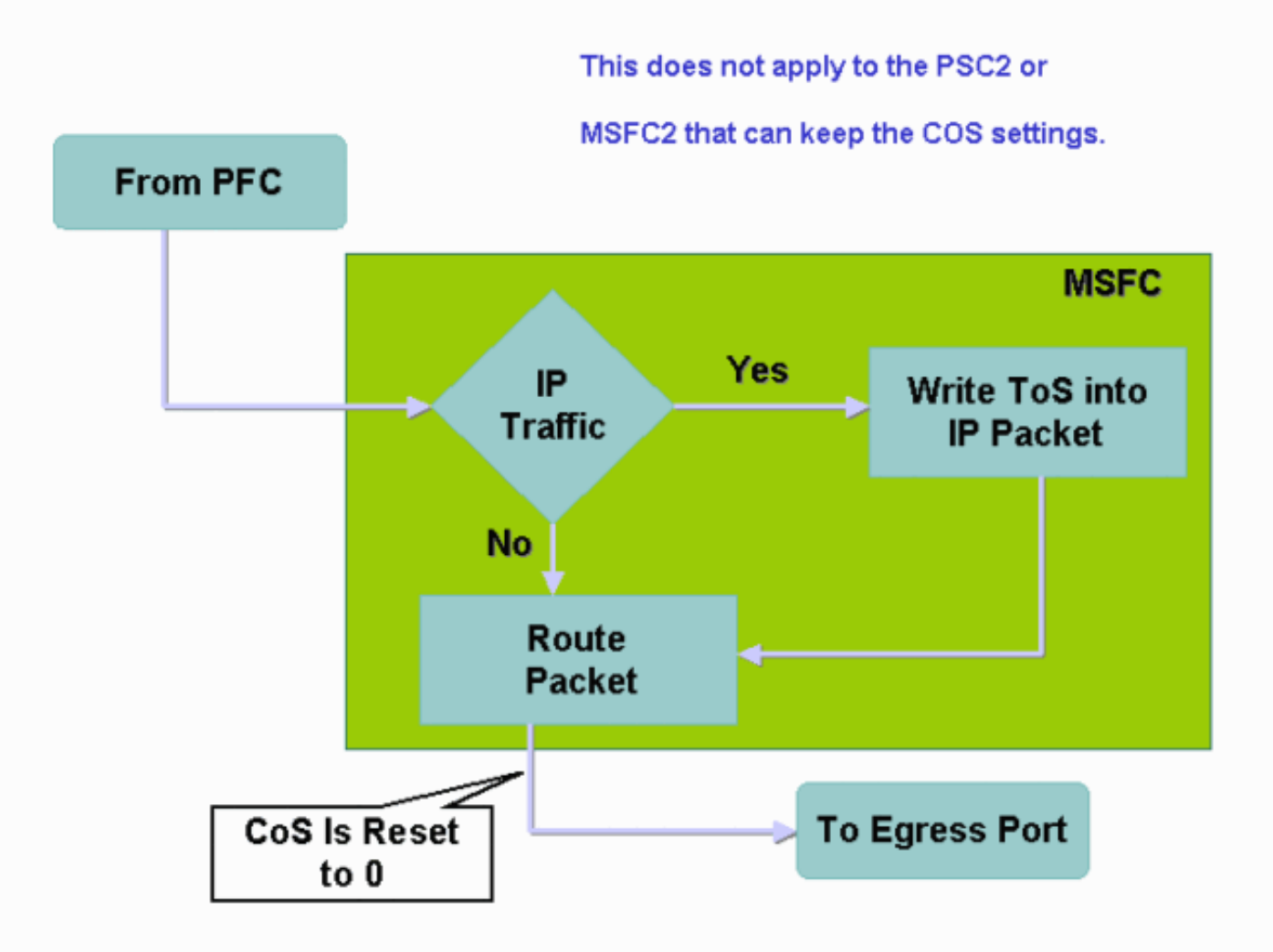
Você pode somente usar o `estado não-confiável`. Toda a tentativa de configurar um `estado de confiança em` uma destas portas indica um destes mensagens de advertência:

```
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.
```

Você deve anexar uma política de serviços à porta ou ao VLAN se você quer um quadro de confiança vir dentro em tal placa de linha. Use o método no caso 1: Marcação na seção da borda deste documento.

Pacotes que vêm do MSFC1 ou do MSFC2 no Supervisor Engine 1A/PFC

Todos os pacotes que vêm do MSFC1 ou do MSFC2 têm um CoS de 0. O pacote pode ser um pacote do roteado por software ou um pacote esse as edições MSFC. Esta é uma limitação do PFC porque restaura o CoS de todos os pacotes que vêm do MSFC. O DSCP e a Precedência IP são mantidos ainda. O PFC2 não tem esta limitação. O CoS de retirada do PFC2 é igual à Precedência IP do pacote.



Resumo de classificação

As tabelas nesta seção mostram ao DSCP esse resultados com base nestas classificações:

- `O estado de confiança da` porta de recebimento
- As palavras-chave de classificação dentro do ACL aplicado

Esta tabela fornece é um resumo genérico para todas as portas exceto WS-X62xx e WS-X63xx:

Palavra-chave de mapa de política Estado de confiança da porta	set-ip-dscp xx ou set-dscp-transmit xx	trust-dscp	trust-ipprec	trust-cos
não confiável	xx1	RX[2] DSCP	derivado de Rx ipprec	0
trust-dscp	Rx dscp	Rx dscp	derivado de Rx ipprec	derivado de Rx Cos ou porta CoS
trust-ipprec	derivado de Rx	Rx dscp	derivado de Rx	derivado de Rx Cos ou

	ipprec		ipprec	porta CoS
trust-cos	derivado de Rx Cos ou porta CoS	Rx dscp	derivado de Rx ipprec	derivado de Rx Cos ou porta CoS

Esta é a única maneira de criar uma nova marcação de quadro.

$^{2\,o}$ RX = recebe

Esta tabela fornece um sumário para as portas WS-X61xx, WS-X62xx, e WS-X63xx:

Palavra-chave de mapa de política **Estado de confiança da porta**	**set-ip-dscp xx ou set-dscp-transmit xx**	**trust-dscp**	**trust-ipprec**	**trust-cos**
não confiável	xx	Rx dscp	derivado de Rx ipprec	0
trust-dscp	Não suportado	Não suportado	Não suportado	Não suportado
trust-ipprec	Não suportado	Não suportado	Não suportado	Não suportado
trust-cos	Não suportado	Não suportado	Não suportado	Não suportado

Monitore e verifique uma configuração

Verifique a configuração de porta

Emita o **comando show queuing interface interface-id** a fim verificar as configurações de porta e as configurações.

Quando você emite este comando, você pode verificar estes parâmetros de classificação, entre outros parâmetros:

- Se com base na porta ou com base em VLAN
- O tipo de porta da `confiança`
- O ACL que é anexado à porta

Está aqui uma amostra desta saída do comando. Os campos importantes no que diz respeito à classificação aparecem no negrito:

```
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]:
```

A saída mostra que a configuração desta porta específica é com `confiança cos no` nível da porta. Também, a porta CoS padrão é 0.

Verifique classes definidas

Emita o **comando show class-map** a fim verificar as classes definidas. Aqui está um exemplo:

```
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 o mapa de política que é aplicado a uma relação

Emita estes comandos a fim verificar o mapa de política que é aplicado e visto em comandos precedentes:

- **mostre o** *ID de interface da* **relação dos qos IP dos mls**
- **mostre o** *ID de interface da* **relação do mapa de política**

Estão aqui as amostras da saída da introdução destes 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: Você pode olhar estes campos que se relacionam à classificação:

- `Mapa de classe` — Diz-lhe que classe é anexada à política de serviços que é anexada a esta relação.
- `Confiança` — Diz lhe se a ação policial nessa classe contém um **comando trust** e o que é confiado na classe.
- `DSCP` — Diz-lhe o DSCP que é transmitido para os pacotes que batem essa classe.

```
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
```

Exemplo de estudos de caso

Esta seção fornece configurações de amostra dos casos comuns que podem aparecer em uma rede.

Caso 1: Marcação na ponta

Supõe que você configura um catalizador 6000 que seja usado como um switch de acesso. Muitos usuários conectam ao entalhe 2 do interruptor, que é uma placa de linha WS-X6348 (10/100 Mbps). Os usuários podem enviar:

- Tráfego de dados normal — Este tráfego está sempre no VLAN 100 e precisa de obter um DSCP de 0.
- Tráfego de voz de um telefone IP — Este tráfego está sempre no VLAN auxiliar 101 da Voz e precisa de obter um DSCP de 46.
- Tráfego do aplicativo de missão crítica — Este tráfego vem no VLAN 100 e é dirigido igualmente ao server 10.10.10.20. Esse tráfego necessita obter um DSCP de 32.

O aplicativo não marca algum deste tráfego. , Deixe consequentemente a porta como o `não-confiável` e configurar um ACL específico para classificar o tráfego. Um ACL é aplicado ao VLAN 100, e um ACL é aplicado ao VLAN 101. Você igualmente precisa de configurar todas as portas como com base em VLAN. Está aqui um exemplo da configuração 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: Confiança no núcleo com somente interfaces Gigabit Ethernet

Supõe que você configura um core catalyst 6000 com somente uma interface Gigabit Ethernet no slot1 e no entalhe 2. O tráfego previamente marcado dos switch de acesso corretamente. Consequentemente, você não precisa de fazer a observação. Contudo, você precisa de assegurar-se de que o switch central confie o DSCP entrante. Este caso é o caso mais fácil

porque todas as portas são marcadas como o `Trust-dscp`, que devem ser suficientes:

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

Informações Relacionadas

- Entendendo a qualidade do serviço nos Switches da família Catalyst 6000
- Classificação e Marcação QoS nos Switches da Série catalyst 6500/6000 que Executam o Software CatOs
- Suporte a Produtos de LAN
- Suporte de tecnologia de switching de LAN
- Suporte Técnico e Documentação - Cisco Systems