Classificação e marcação de QoS nos Switches Catalyst 6500/6000 Series que executam o Software Cisco IOS

Contents

Introduction

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 relacionados à QoS ou marcação. Para obter mais informações sobre a interface de linha de comando (CLI) do Cisco IOS Software, consulte Configuração da QoS de PFC.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Switches Catalyst 6500/6000 Series que executam o Cisco IOS Software e usam um destes Supervisor Engines:Um Supervisor Engine 1A com uma Placa de Recurso de Política (PFC - Policy Feature Card) e uma Placa de Recurso de Switch Multicamada (MSFC - Multilayer Switch Feature Card).Um mecanismo de supervisor 1A com um PFC e um MSFC2Um Supervisor Engine 2 com PFC2 e MSFC2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Terminology

A lista fornece a terminologia que este documento usa:

- Ponto de código de serviços diferenciados (DSCP - Differentiated Services Code Point)—Os primeiros seis bits do byte de tipo de serviço (ToS - Type of Service) no cabeçalho IP. O DSCP está presente somente no pacote IP.**Observação:** o switch também atribui um DSCP interno a cada pacote, seja IP ou não IP. A seção Quatro fontes possíveis para DSCP interno deste documento detalha essa atribuição interna de DSCP.
- Precedência de IP—Os três primeiros bits 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). O CoS consiste em qualquer um destes três bits:Os três bits IEEE 802.1p (dot1p) na tag IEEE 802.1Q (dot1q) para o pacote dot1q.**Observação:** por padrão, os switches da Cisco não marcam pacotes de VLAN nativos.Os três bits chamados de "Campo do usuário" no cabeçalho do Inter-Switch Link (ISL) para um pacote encapsulado por ISL.**Observação:** CoS não está presente em um pacote não dot1q ou ISL.
- Classificação — O processo usado para selecionar o tráfego a ser marcado.
- Marcação—O processo que define um valor de DSCP de Camada 3 (L3) em um pacote. Este documento amplia a definição de marcação para incluir a configuração de valores L2 CoS.

Os switches da série Catalyst 6500/6000 podem fazer classificações com base nestes três

parâmetros:

- DSCP
- Precedência de IP
- CoS

Os switches da série Catalyst 6500/6000 executam classificação e marcação em vários estágios. Isso é o que ocorre em diferentes lugares:

- Porta de entrada (Circuito integrado específico do aplicativo de entrada [ASIC])
- Mecanismo de Switching (PFC)
- Porta de saída (ASIC de saída)

Manejo da porta de entrada

O principal parâmetro de configuração para a porta de entrada, em relação à classificação, é o estado `confiável` da porta. Cada porta do sistema pode ter um destes estados `confiáveis`:

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

Para definir ou alterar o estado de `confiança` da porta, emita este comando do Cisco IOS Software no modo `de interface`:

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

Observação: por padrão, todas as portas estão no estado `não confiável` quando a QoS está habilitada. Para habilitar a QoS no Catalyst 6500 que executa o Cisco IOS Software, execute o comando **mls qos** no modo de configuração principal.

No nível da porta de entrada, você também pode aplicar um CoS padrão por porta. Aqui está um exemplo:

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

Esse CoS padrão se aplica a todos os pacotes, como IP e Internetwork Packet Exchange (IPX). Você pode aplicar o CoS padrão a qualquer porta física.

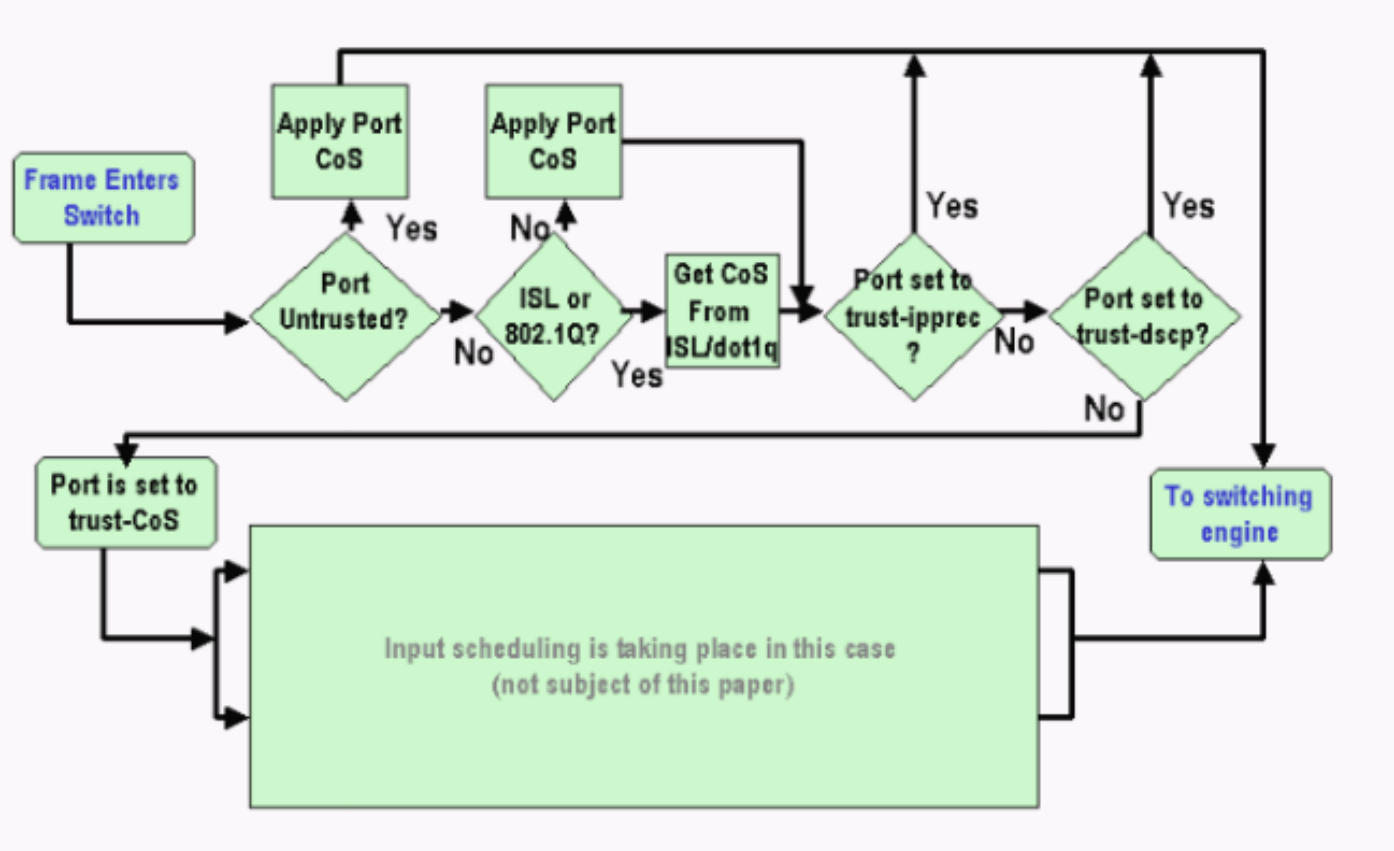
Se a porta estiver no estado `não confiável`, marque o quadro com o CoS padrão da porta e passe o cabeçalho para o mecanismo de comutação (PFC). Se a porta estiver definida como um dos estados `confiáveis`, execute uma destas duas opções:

- Se o quadro não tiver um CoS recebido (dot1q ou ISL), aplique o CoS da porta padrão.
- Para quadros dot1q e ISL, mantenha o CoS como está.

Em seguida, passe o quadro para o mecanismo de comutação.

Este exemplo ilustra a classificação e a marcação de entrada. O exemplo mostra como atribuir

um CoS interno a cada quadro:



Observação: como este exemplo mostra, a cada quadro é atribuído um CoS interno. A atribuição é baseada no CoS recebido ou no CoS da porta padrão. O CoS interno inclui quadros não marcados que não transportam nenhum CoS real. O CoS interno é gravado em um cabeçalho de pacote especial, que é chamado de cabeçalho de barramento de dados, e enviado pelo barramento de dados para o mecanismo de switching.

Mecanismo de Switching (PFC)

Quando o cabeçalho alcança o mecanismo de comutação, a EARL (Enhanced Address Recognition Logic) do mecanismo de comutação atribui a cada quadro um DSCP interno. Esse DSCP interno é uma prioridade interna atribuída ao quadro pelo PFC à medida que o quadro transita pelo switch. Este não é o DSCP no cabeçalho IP versão 4 (IPv4). O DSCP interno é derivado de uma configuração CoS ou ToS existente e é usado para redefinir o CoS ou ToS à medida que o quadro sai do switch. Esse DSCP interno é atribuído a todos os quadros que são comutados ou roteados pelo PFC, mesmo quadros não IP.

Esta seção discute como você pode atribuir uma política de serviço à interface para fazer uma marcação. A seção também discute a configuração final do DSCP interno, que depende do estado de `confiança de` porta e da política de serviço aplicada.

Configure a política de serviço para classificar ou marcar um pacote no Cisco IOS Software Release 12.1(12c)E ou Posterior

Conclua estes passos para configurar a política de serviço:

1. Configure uma lista de controle de acesso (ACL) para definir o tráfego que você deseja

considerar.A ACL pode ser numerada ou nomeada, e o Catalyst 6500/6000 suporta uma ACL estendida. Emita o comando **access-list *xxx*** do Cisco IOS Software, como mostrado neste exemplo:

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

2. Configure uma classe de tráfego (mapa de classe) para corresponder o tráfego com base na ACL que você definiu ou com base no DSCP recebido.Emita o comando **class-map** Cisco IOS Software. A QoS de PFC não suporta mais de uma instrução de correspondência por mapa de classe. Além disso, o PFC QoS suporta apenas estas instruções de correspondência:**match ip access-groupmatch ip dscpprecedência compatível de ipmatch protocolObservação:** o comando **match protocol** permite o uso do NBAR (Network Based Application Recognition, reconhecimento de aplicativos baseados em rede) para corresponder o tráfego.**Observação:** dessas opções, somente as instruções **match ip dscp** e **match ip precedence** são suportadas e funcionam. Essas instruções, no entanto, não são úteis na marcação ou classificação dos pacotes. Você pode usar essas instruções, por exemplo, para fazer policiamento em todos os pacotes que correspondem a um determinado DSCP. No entanto, esta ação está além do escopo deste documento.

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

Observação: este exemplo mostra apenas três opções para o comando **match**. Mas você pode configurar muitas outras opções neste prompt de comando.**Observação:** qualquer uma das opções neste comando **match** é tomada para critérios de correspondência e as outras opções são deixadas de fora, de acordo com os pacotes de entrada.Aqui está um exemplo:

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

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

3. Configure um mapa de política para aplicar uma política a uma classe que você definiu anteriormente.O mapa de políticas contém:Um nomeUm conjunto de instruções de classePara cada instrução de classe, a ação que precisa ser executada para essa classeAs ações suportadas na QoS PFC1 e PFC2 são:**trust dscpprecedência de IP confiáveltrust cosset ip dscp** no software Cisco IOS versão 12.1(12c)E1 e posterior**defina a precedência de ip** no Cisco IOS Software Release 12.1(12c)E1 e posterior**políciaObservação:** esta ação está além do escopo deste documento.

```
(config)#policy-map policy-name
(config-pmap)#class class-name
(config-pmap-c)#{police | set ip dscp}
```

Observação: este exemplo mostra apenas duas opções, mas você pode configurar muitas mais opções neste prompt de comando `(config-pmap-c)#`.Aqui está um exemplo:

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

4. Configure uma entrada de política de serviço para aplicar um mapa de política definido anteriormente para uma ou mais interfaces.**Observação:** você pode anexar uma política de

serviço à interface física ou à interface virtual comutada (SVI) ou à interface VLAN. Se você anexar uma política de serviço a uma interface VLAN, as únicas portas que usam essa política de serviço são as portas que pertencem a essa VLAN e são configuradas para QoS baseada em VLAN. Se a porta não estiver definida para QoS baseada em VLAN, a porta ainda usará a QoS baseada em porta padrão e somente observará a política de serviço que está conectada à interface física.Este exemplo aplica a política de serviço `test_policy` à porta Gigabit Ethernet 1/1:

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

Este exemplo aplica a política de serviço `test_policy` a todas as portas na VLAN 10 que têm uma configuração baseada 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
```

Observação: você pode combinar as etapas 2 e 3 deste procedimento se ignorar a definição específica da classe e anexar a ACL diretamente na definição do mapa de política. Neste exemplo, onde a classe `TEST police` não foi definida antes da configuração do mapa de políticas, a classe é definida no mapa 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 a política de serviço para classificar ou marcar um pacote em versões do Cisco IOS Software anteriores ao Cisco IOS Software Release 12.1(12c)E

Nas versões do Cisco IOS Software anteriores à versão 12.1(12c)E1 do Cisco IOS Software, você não pode usar a ação **set ip dscp** ou **set ip precedence** em um mapa de política. Portanto, a única maneira de fazer uma marcação de tráfego específico que uma classe define é configurar um vigilante com uma taxa muito alta. Essa taxa deve ser, por exemplo, pelo menos a taxa de linha da porta ou algo alto o suficiente para permitir que todo o tráfego atinja esse vigilante. Em seguida, use **set-dscp-transmit *xx*** como a ação de conformidade. Siga estas etapas para configurar esta configuração:

1. Configure uma ACL para definir o tráfego que você deseja considerar.A ACL pode ser numerada ou nomeada, e o Catalyst 6500/6000 suporta uma ACL estendida. Emita o comando **access-list *xxx*** do Cisco IOS Software, como mostrado neste exemplo:
   ```
   (config)#access-list 101 permit ip any host 10.1.1.1
   ```

2. Configure uma classe de tráfego (mapa de classe) para corresponder o tráfego com base na ACL que você definiu ou com base no DSCP recebido.Emita o comando **class-map** Cisco IOS Software. A QoS de PFC não suporta mais de uma instrução de correspondência por

mapa de classe. Além disso, o PFC QoS suporta apenas estas instruções de correspondência:**match ip access-groupmatch ip dscpprecedência compatível de ipmatch protocolObservação:** o comando **match protocol** permite o uso do NBAR para corresponder o tráfego.**Observação:** dessas instruções, somente as instruções **match ip dscp** e **match ip precedence** são suportadas e funcionam. Essas instruções, no entanto, não são úteis na marcação ou na classificação dos pacotes. Você pode usar essas instruções, por exemplo, para fazer policiamento em todos os pacotes que correspondem a um determinado DSCP. No entanto, esta ação está além do escopo deste documento.

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

Observação: este exemplo mostra apenas três opções para o comando **match**. Mas você pode configurar muitas outras opções neste prompt de comando.Aqui está um exemplo:

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

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

3. Configure um mapa de política para aplicar uma política a uma classe que você definiu anteriormente.O mapa de políticas contém:Um nomeUm conjunto de instruções de classePara cada instrução de classe, a ação que precisa ser executada para essa classeAs ações suportadas na QoS PFC1 ou PFC2 são:**trust dscpprecedência de IP confiáveltrust cospolícia**Você deve usar a instrução **police** porque as ações **set ip dscp** e **set ip precedence** não são suportadas. Como você não quer realmente policiar o tráfego, mas apenas marcá-lo, use um vigilante definido para permitir todo o tráfego. Portanto, configure o vigilante com uma taxa grande e intermitência. Por exemplo, você pode configurar o vigilante com a taxa máxima permitida e a intermitência. 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. Configure uma entrada de política de serviço para aplicar um mapa de política definido anteriormente para uma ou mais interfaces.**Observação:** a política de serviço pode ser conectada a uma interface física ou à interface SVI ou VLAN. Se uma política de serviço estiver conectada a uma interface VLAN, somente as portas que pertencem a essa VLAN e que estão configuradas para QoS baseada em VLAN usarão essa política de serviço. Se a porta não estiver definida para QoS baseada em VLAN, a porta ainda usará a QoS baseada em porta padrão e somente observará uma política de serviço que está conectada à interface física.Este exemplo aplica a política de serviço `test_policy` à porta Gigabit Ethernet 1/1:

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

Este exemplo aplica a política de serviço `test_policy` a todas as portas na VLAN 10 que têm uma configuração baseada 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 de DSCP recebido existente, que é definido antes do quadro entrar no switchUm exemplo é **trust dscp**.
2. Os bits de precedência de IP recebidos que já estão definidos no cabeçalho IPv4Como há 64 valores de DSCP e apenas oito valores de precedência de IP, o administrador configura um mapeamento que o switch usa para derivar o DSCP. Os mapeamentos padrão estão em vigor, caso o administrador não configure os mapas. Um exemplo é **trust ip precedence**.
3. Os bits de CoS recebidos que já estão definidos antes do quadro entrar no switch e que são armazenados no cabeçalho do barramento de dados ou se não havia CoS no quadro de entrada, do CoS padrão da porta de entradaAssim 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 esse mapa ou o switch pode usar o mapa padrão que já está no lugar.
4. A política de serviço pode definir o DSCP interno para um valor específico.

Para os números 2 e 3 nesta lista, o mapeamento estático é por padrão, desta maneira:

- Para o mapeamento CoS para DSCP, o DSCP derivado é igual a oito vezes o CoS.
- Para o mapeamento de precedência de IP para DSCP, o DSCP derivado é igual a oito vezes a precedência de IP.

Você pode emitir estes comandos para substituir e verificar este mapeamento estático:

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

O primeiro valor do DSCP que corresponde ao mapeamento para CoS (ou precedência de IP) é 0. O segundo valor para o CoS (ou precedência de IP) é 1, e o padrão continua dessa maneira. Por exemplo, este comando altera o mapeamento de forma que o CoS 0 seja mapeado para o DSCP de 0, e o CoS de 1 seja mapeado para o 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 de política de QoS que é aplicado ao pacoteO mapa da política de QoS é

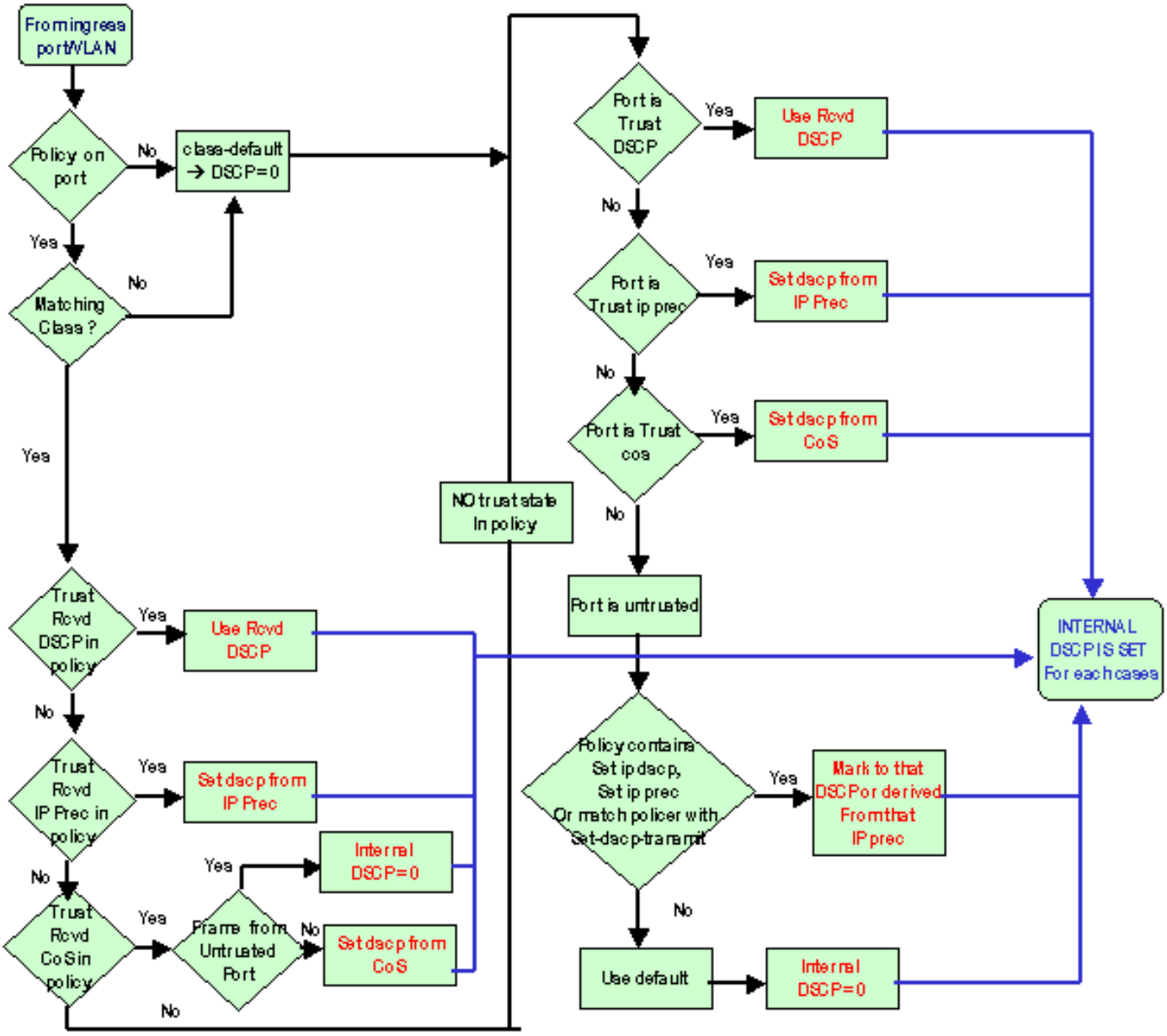
determinado pelas seguintes regras:Se nenhuma política de serviço estiver conectada à porta de entrada ou à VLAN, use o padrão.**Observação:** esta ação padrão é definir o DSCP interno como 0.Se uma política de serviço estiver conectada à porta de entrada ou VLAN e se o tráfego corresponder a uma das classes definidas pela política, use essa entrada.Se uma política de serviço estiver conectada à porta de entrada ou à VLAN e se o tráfego não corresponder a uma das classes definidas pela política, use o padrão.

- O estado de confiança da porta e a ação do mapa de políticasQuando a porta tem um estado de `confiança` específico e uma política com uma determinada marcação (ação de confiança ao mesmo tempo), estas regras se aplicam:O comando **set ip dscp** ou DSCP definido por vigilante em um mapa de política só será aplicado se a porta for deixada no estado `não confiável`.Se a porta tiver um estado `confiável`, esse `estado confiável` será 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 tem precedência sobre o estado `confiável` da porta.Se a porta e a política contiverem um estado de `confiança` diferente, o estado de `confiança` que vem do mapa de políticas será considerado.

Portanto, o DSCP interno depende destes fatores:

- O estado `de confiança` da porta
- A política de serviço (com o uso da ACL) conectada à porta
- O mapa de política padrão**Observação:** o padrão redefine o DSCP como 0.
- Se baseado em VLAN ou baseado em porta em relação à ACL

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



O PFC também é capaz de realizar vigilância. Isso pode resultar em uma redução do DSCP interno. Para obter mais informações sobre policiamento, consulte Política de QoS em Switches Catalyst 6500/6000 Series.

Manejo da porta emissora

Não é possível fazer nada no nível da porta de saída para alterar a classificação. No entanto, marque o pacote com base nessas regras:

- Se o pacote for um pacote IPv4, copie o DSCP interno que o mecanismo de comutação atribui ao byte ToS do cabeçalho IPv4.
- Se a porta de saída estiver configurada para um encapsulamento ISL ou dot1q, use um CoS derivado do DSCP interno. Copie o CoS no quadro ISL ou dot1q.

Observação: o CoS é derivado do DSCP interno de acordo com uma estática. Execute este comando para 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 são exibidas aqui. Por padrão, o CoS é a parte inteira do DSCP, dividida por oito. Execute este comando para ver e verificar o mapeamento:

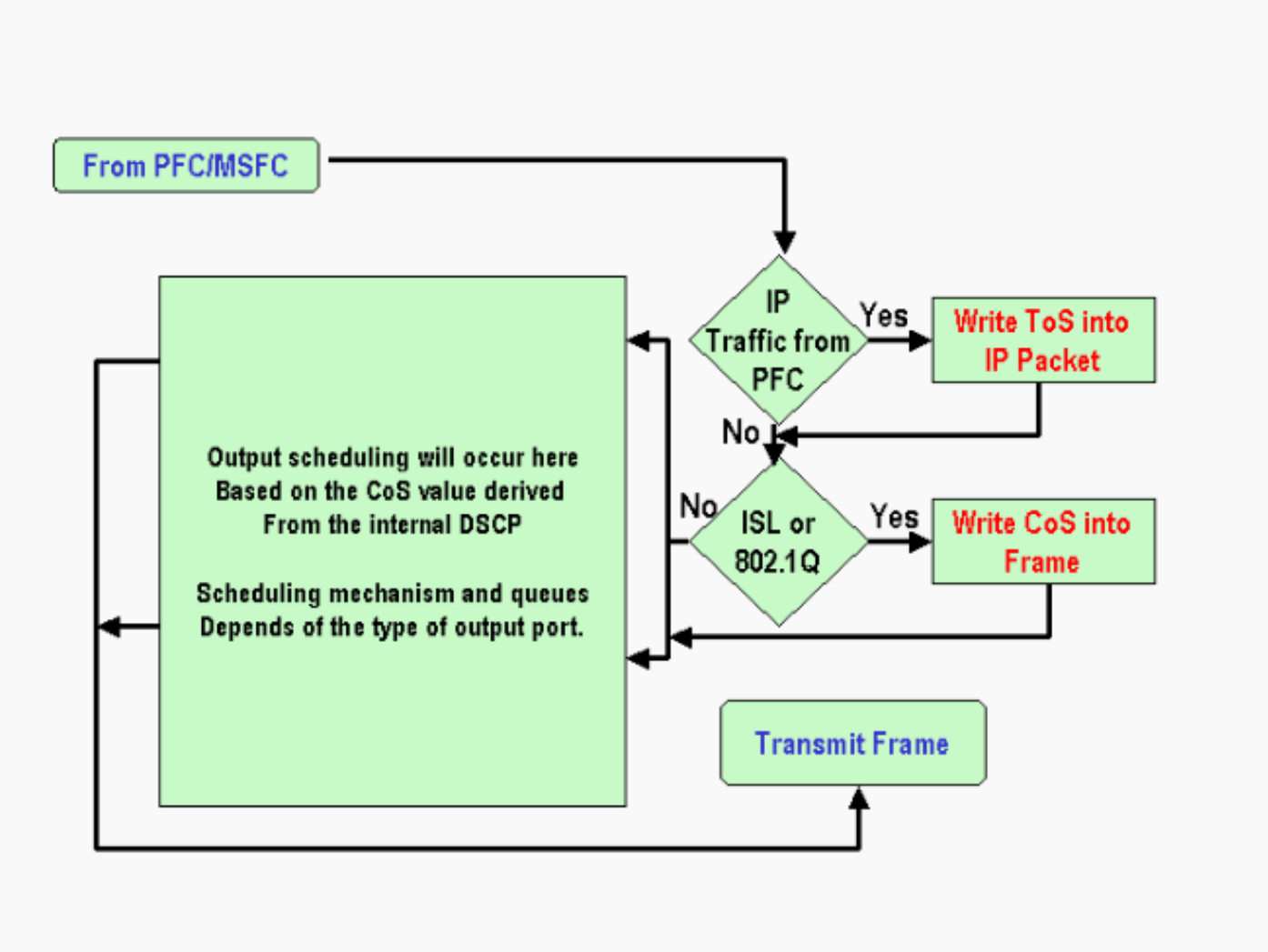
```
cat6k#show mls qos maps
...
  Dscp-cos map:                                     (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ------------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 02 02 02 02
      2 :    02 02 02 02 03 03 03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

Para alterar esse mapeamento, emita este comando de configuração no modo de 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 é gravado no cabeçalho IP e o CoS é derivado do DSCP, o pacote é enviado para uma das filas de saída para programação de saída com base no CoS. Isso ocorre mesmo se o pacote não for um dot1q ou um ISL. Para obter mais informações sobre o agendamento da fila de saída, consulte Agendamento de Saída de QoS em Catalyst 6500/6000 Series Switches com Cisco IOS System Software.

Este diagrama resume o processamento do pacote em relação à marcação na porta de saída:



Notas e limitações

ACL padrão

O ACL padrão usa "dscp 0" como a palavra-chave de classificação. Todo o tráfego que entra no switch através de uma porta não confiável e não atinge uma entrada de política de serviço é marcado com um DSCP de 0 se a QoS estiver habilitada. Atualmente, não é possível alterar a ACL padrão no software Cisco IOS.

Observação: no software Catalyst OS (CatOS), você pode configurar e alterar esse comportamento padrão. Para obter mais informações, consulte a seção *ACL padrão da* Classificação e Marcação de QoS nos Catalyst 6500/6000 Series Switches com CatOS Software.

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

Esta seção abrange apenas estas placas de linha:

- WS-X6224-100FX-MT : Multimodo Catalyst 6000 de 24 portas 100 FX
- WS-X6248-RJ-45: MÓDULO RJ-45 10/100 CATALYST 6000 de 48 portas
- WS-X6248-TEL: MÓDULO CATALYST 6000 48 PORTAS 10/100 TELCO
- 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 portas 100 FX, QoS avançada, MT
- WS-X6324-100FX-SM: Catalyst 6000 24 portas 100 FX, QoS avançada, MT
- WS-X6348-RJ-45 CATALYST 6000 48-PORT 10/100, ENHANCED QOS
- WS-X6348-RJ21V: CATALYST 6000 48 PORTAS 10/100, POTÊNCIA EM LINHA
- WS-X6348-RJ45V: Catalyst 6000 48 portas 10/100, QoS avançada, alimentação em linha
- WS-X6148-RJ21V: Alimentação em linha Catalyst 6500 de 48 portas 10/100
- WS-X6148-RJ45V: Alimentação em linha Catalyst 6500 de 48 portas 10/100

Essas placas de linha têm uma limitação. No nível da porta, você não pode configurar o estado `confiável` com o uso de qualquer uma destas palavras-chave:

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

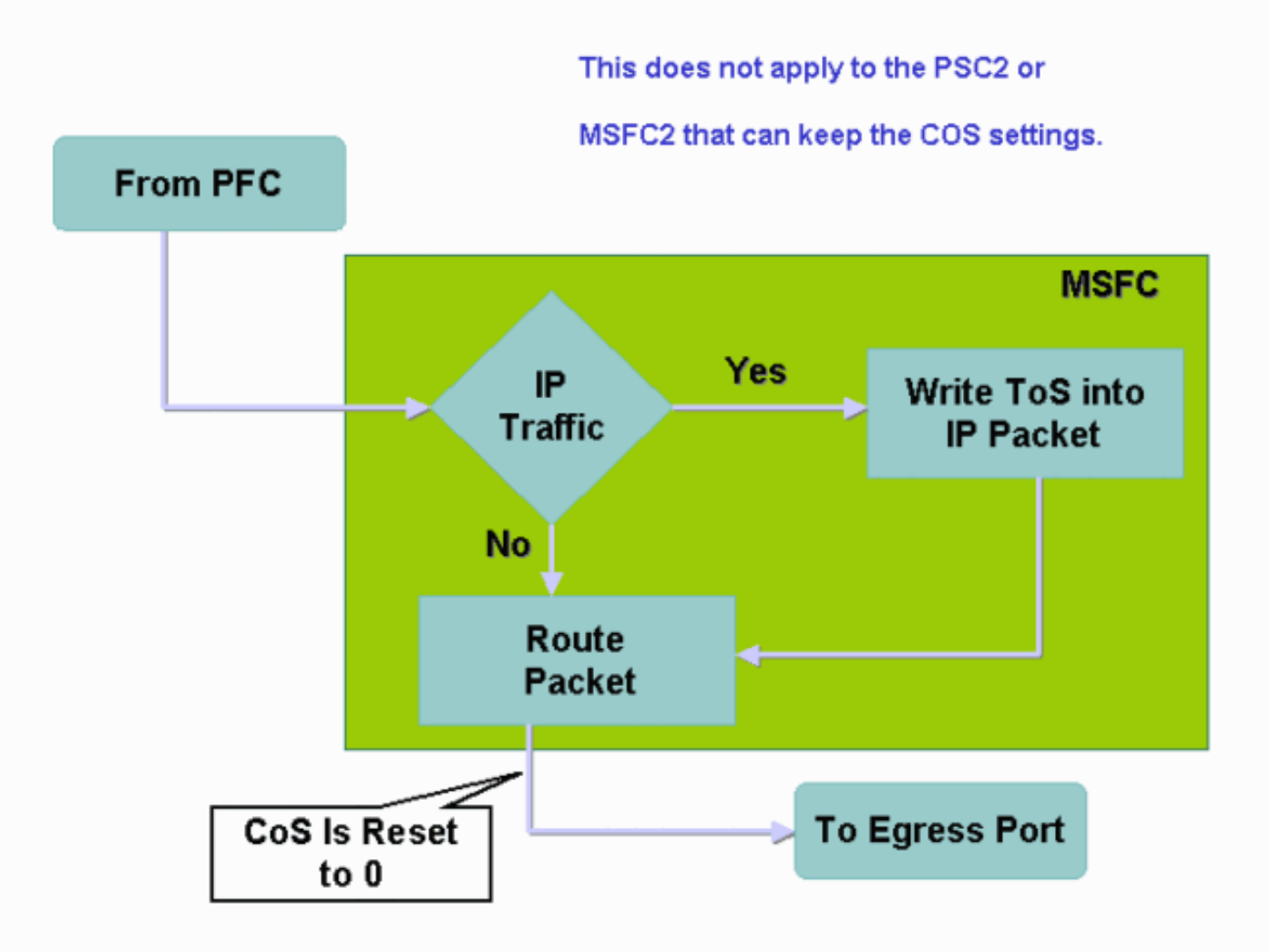
Você só pode usar o estado `não confiável`. Qualquer tentativa de configurar um estado `confiável` em uma dessas portas exibe uma destas mensagens de aviso:

```
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 serviço à porta ou à VLAN se quiser que um quadro confiável entre nessa placa de linha. Use o método no Caso 1: Marcação na seção Borda deste documento.

Pacotes que vêm do MSFC1 ou 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 roteado por software ou um pacote que o MSFC emita. Essa é uma limitação do PFC porque ele redefine o CoS de todos os pacotes que vêm do MSFC. O DSCP e a precedência de IP ainda são mantidos. O PFC2 não tem essa limitação. O CoS existente do PFC2 é igual à precedência IP do pacote.



Resumo de classificação

As tabelas nesta seção mostram o DSCP que resulta com base nestas classificações:

- Estado de confiança da porta de entrada
- A palavra-chave de classificação na ACL aplicada

Esta tabela fornece 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] x = recepção

Esta tabela fornece um resumo 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	Not Supported	Not Supported	Not Supported	Not Supported
trust-ipprec	Not Supported	Not Supported	Not Supported	Not Supported
trust-cos	Not Supported	Not Supported	Not Supported	Not Supported

Monitorar e verificar uma configuração

Verifique a configuração da porta

Execute o comando **show queuing interface** ***interface-id*** para verificar as configurações e as configurações da porta.

Ao emitir esse comando, você pode verificar esses parâmetros de classificação, entre outros:

- Baseado em portas ou em VLAN
- O tipo de porta `confiável`
- A ACL conectada à porta

Aqui está um exemplo dessa saída de comando. Os campos importantes relativos à classificação aparecem em 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 está com `trust cos` no nível da porta. Além disso, a porta padrão CoS é 0.

Verificar classes definidas

Emita o comando **show class-map** para 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 aplicado a uma interface

Execute estes comandos para verificar o mapa de política aplicado e visto em comandos anteriores:

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

Aqui estão exemplos da saída da emissão 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 ver estes campos relacionados à classificação:

- `Class-map`—Informa qual classe está anexada à política de serviço que está anexada a esta interface.
- `Trust`—Informa se a ação policial nessa classe contém um comando **trust** e o que é confiável na classe.
- `DSCP` —Informa o DSCP que é transmitido para os pacotes que atingem 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 exemplos de configurações de casos comuns que podem aparecer em uma rede.

Caso 1: Marcação na ponta

Suponha que você configure um Catalyst 6000 usado como um switch de acesso. Muitos usuários se conectam ao slot 2 do switch, que é uma placa de linha WS-X6348 (10/100 Mbps). Os usuários podem enviar:

- Tráfego de dados normal — esse tráfego está sempre na VLAN 100 e precisa obter um DSCP de 0.
- Tráfego de voz de um telefone IP—Esse tráfego está sempre na VLAN 101 auxiliar de voz e precisa ter um DSCP de 46.
- Tráfego de aplicativos de missão crítica—Esse tráfego também vem na VLAN 100 e é direcionado ao servidor 10.10.10.20. Esse tráfego necessita obter um DSCP de 32.

O aplicativo não marca nenhum desse tráfego. Portanto, deixe a porta como `não confiável` e configure uma ACL específica para classificar o tráfego. Uma ACL é aplicada à VLAN 100 e uma ACL é aplicada à VLAN 101. Você também precisa configurar todas as portas como baseadas em VLAN. Aqui está um exemplo da configuração que resulta em:

```
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 apenas interfaces Gigabit Ethernet

Suponha que você configure um Catalyst 6000 central com apenas uma interface Gigabit

Ethernet nos slots 1 e 2. Os switches de acesso marcavam anteriormente o tráfego corretamente. Portanto, você não precisa fazer nenhuma remarcação. No entanto, você precisa garantir que o switch central confie no DSCP de entrada. Este caso é o caso mais fácil porque todas as portas estão marcadas como `trust-dscp`, o que deve ser suficiente:

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

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