Classificação e Marcação QoS nos Switches da Série catalyst 6500/6000 que Executam o Software CatOs

Contents

Introduction

Este documento examina o que acontece com relação à marcação e classificação de um pacote em diferentes locais durante sua jornada dentro do chassi do Catalyst 6000. Apresenta casos especiais, restrições e fornece pequenos estudos de casos.

Este documento não se destina a ser uma lista exaustiva de todos os comandos do Catalyst OS (CatOS) relacionados à qualidade de serviço (QoS) ou marcação. Para obter mais informações

sobre a interface de linha de comando (CLI) do CatOS, consulte o seguinte documento:

- Configurando QoS

Observação: este documento considera apenas o tráfego IP.

Antes de Começar

Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Prerequisites

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento é válido para switches da família Catalyst 6000 que executam o CatOS Software e usam um dos seguintes Supervisor Engines:

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

Todos os exemplos de comando, porém, foram testados em um Catalyst 6506 com o SUP1A/PFC executando a versão de software 6.3.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Terminology

A seguir está uma lista da terminologia usada nesse documento:

- Ponto de código de serviços diferenciados (DSCP): Os primeiros seis bits do byte Tipo de serviço (ToS) no cabeçalho IP. O DSCP está presente somente no pacote IP.**Observação:** você também atribui um DSCP interno a cada pacote (IP ou não IP), essa atribuição interna de DSCP será detalhada posteriormente neste documento.
- Precedência 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). Consiste em qualquer um dos seguintes três bits:Os três bits dot1p na tag dot1q para o pacote IEEE dot1q.Os três bits chamados "Campo de Usuário" no cabeçalho Inter-Switch Link (ISL) para um pacote ISL encapsulado.Não há CoS presente em um pacote ISL ou não-dot1q.

- Classificação O processo usado para selecionar o tráfego a ser marcado.
- Marcação: O processo de configuração de um valor DSCP da L3 (Camada 3). Neste documento, a definição de marcação é estendida para incluir a definição de valores CoS L2.

Os Switches da família Catalyst 6000 podem fazer classificações com base nestes três parâmetros:

- DSCP
- Precedência de IP
- CoS

Os switches da família Catalyst 6000 estão fazendo classificação e marcação em locais diferentes. A seguir há um aspecto do que acontece nesses locais diferentes:

- Porta de entrada (Circuito Integrado Específico do Aplicativo (ASIC) de ingresso)
- Mecanismo de switching (Placa de Recurso de Política (PFC))
- Porta de saída (ASIC de saída)

Habilitando o QoS

Por padrão, a QoS é desabilitada nos switches Catalyst 6000. A QoS pode ser habilitada emitindo o comando CatOS **set qos enable**.

Quando a QoS é desabilitada, não há classificação ou marcação feita pelo switch e, como tal, cada pacote deixa o switch com a precedência DSCP/IP que tinha ao entrar no switch.

Manejo da porta de entrada

O principal parâmetro de configuração da porta de ingresso, em relação à classificação, é o respectivo estado de confiança. Cada porta do sistema pode ter um dos seguintes estados de confiança:

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

O restante desta seção descreve como os estados de administração de porta influenciam a classificação final do pacote. O estado de porta confiável pode ser definido ou alterado com o seguinte comando do CatOS:

set port qos *mod/port* **trust {não confiável | trust-cos | trust-ipprec | trust-dscp }**

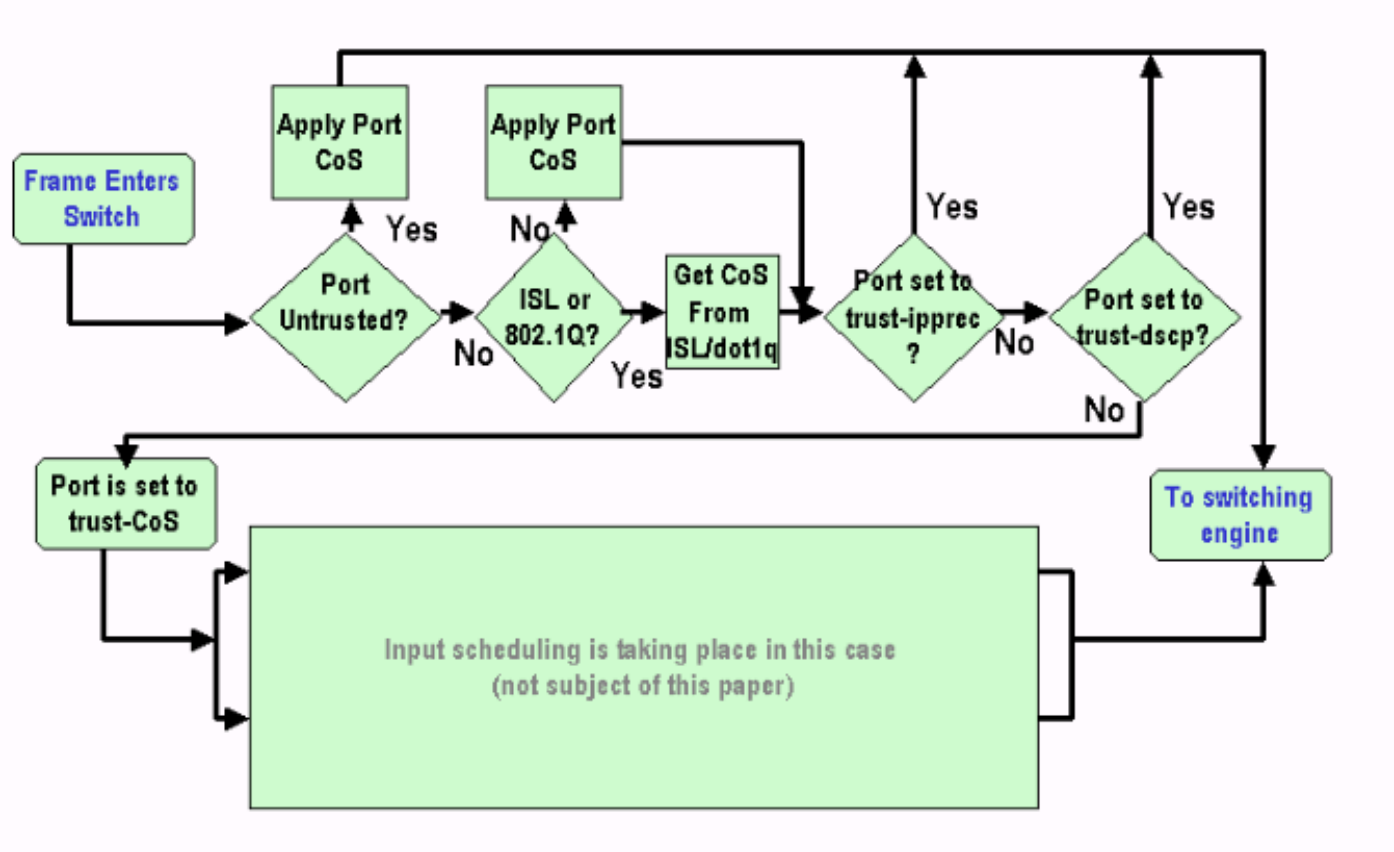
Observação: por padrão, todas as portas estão no estado não confiável quando a QoS está habilitada.

No nível de porta de entrada, você também pode aplicar um CoS padrão por porta, como no seguinte exemplo:

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

Se a porta estiver definida como um estado não confiável, marque a estrutura com o CoS padrão

da porta e passe o cabeçalho para o mecanismo de switching (PFC). Se a porta estiver definida como um dos estados confiáveis, aplique o CoS da porta padrão (se o quadro não tiver um CoS recebido (dot1q ou ISL)) ou mantenha o CoS como está (para quadros dot1q e ISL) e passe o quadro para o mecanismo de comutação. A classificação de entrada está ilustrada no seguinte fluxograma:



Observação: como mostrado no fluxograma acima, cada quadro terá um CoS interno atribuído (o CoS recebido ou o CoS de porta padrão), incluindo quadros não marcados que não transportam nenhum CoS real. Esse CoS interno e o DSCP recebido são gravados em um cabeçalho de pacote especial (chamado cabeçalho de Barramento de Dados) e enviados através do Barramento de Dados para o mecanismo de switching. Isso acontece na placa de linha de entrada e, nesse ponto, ainda não se sabe se esse CoS interno será transportado para o ASIC de saída e inserido no quadro de saída. Isso depende do que o PFC faz e é descrito mais adiante na próxima seção.

Mecanismo de Switching (PFC)

Assim que o cabeçalho tiver atingido o mecanismo de switching, o mecanismo de switching EARL (lógica de reconhecimento de endereço codificado) atribuirá a cada quadro um DSCP interno. Este DSCP interno é uma prioridade interna atribuída ao quadro pelo PFC enquanto faz a transição do Switch. Não é o DSCP no cabeçalho de IPv4. Deriva-se de uma configuração já existente de CoS ou ToS e é usado para redefinir o CoS ou o ToS quando o quadro existir no Switch. Esse DSCP interno é atribuído a todos os quadros comutados (ou roteados) pelo PFC, inclusive quadros que não são IP.

Quatro fontes possíveis para DSCP interno

O DSCP interno será derivado de um dos seguintes itens:

1. Um valor DSCP existente, definido antes de quadro entrar no Switch.
2. Bits de precedência do IP já definidos no cabeçalho IPV4. Como há 64 valores DSCP e apenas oito valores de precedência IP, o administrador configurará um mapeamento que seja usado pelo Switch para derivar o DSCP. Os mapeamentos padrão estão prontos, caso o administrador não configure os mapas.
3. Os bits CoS recebidos já definidos antes da entrada do quadro no Switch ou a partir do CoS padrão da porta de recebimento caso não exista CoS no quadro recebido. Assim 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. Esse mapa pode ser configurado ou o Switch pode usar o mapa padrão já estabelecido.
4. O DSCP pode ser configurado para o quadro usando um valor padrão de DSCP normalmente atribuído através de uma entrada de ACL (Lista de controle de acesso).

Para n.os 2 e 3 na lista acima, o mapeamento estático usado é, por padrão, o seguinte:

- O DSCP derivado é igual a oito vezes o CoS, para mapeamento do CoS para o DSCP.
- O DSCP derivado é igual a 8 vezes a precedência de IP, para a precedência de IP para o mapeamento DSCP.

Esse mapeamento estático pode ser substituído pelo usuário emitindo os seguintes comandos:

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

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

O primeiro valor do DSCP correspondente ao mapeamento para o CoS (ou precedência IP) é "0", o segundo para o CoS (ou precedência de IP) é "1" e esse padrão continua.

Qual das quatro possíveis origens para DSCP interna será utilizada?

Esta seção descreve as regras que determinam qual das quatro possíveis origens descritas acima será usada para cada pacote. Isso depende dos seguintes parâmetros:

1. Qual ACL de QoS será aplicada ao pacote? Isso é determinado pelas seguintes regras:**Observação:** cada pacote passa por uma entrada de ACL.Se não tiver uma ACL conectada à porta de recebimento ou à VLAN, aplique a ACL padrão.Se houver uma ACL conectada à porta de recebimento ou à VLAN e se o tráfego corresponde a uma das entradas na ACL, use esta entrada.Se houver uma ACL conectada à porta de entrada ou à VLAN e se o tráfego não tiver correspondente em uma das entradas da ACL, use o padrão ACL.
2. Cada entrada contém uma palavra-chabe de classificação. A seguir está uma lista de possíveis palavras-chave e suas descrições:trust-ipprec: O DSCP interno será derivado da precedência IP recebida, de acordo com o mapeamento estático, independentemente de qual possa ser o estado de confiança da porta.trust-dscp: O DSCP interno será derivado do DSCP recebido, independentemente de qual possa ser o estado de confiança da porta.trust-cos: O DSCP interno será derivado do CoS recebido de acordo com o mapeamento estático, caso o estado de confiança da porta seja confiável (trust-cos, trust-dscp, trust-ipprec). Se o estado de confiança da porta for trust-xx, o DSCP será derivado da porta padrão CoS de acordo com o mesmo mapeamento estático.dscp xx: O DSCP interno dependerá dos seguintes estados de confiança de porta recebida:Se a porta não for confiável, o DSCP

interno será definido como *xx*.Se a porta for trust-dscp, o DSCP interno será o DSCP recebido no pacote de entrada.Se a porta for trust-CoS, o DSCP interno será derivado do CoS do pacote recebido.Se a porta for a trust-ipprec, o DSCP interno será derivado do IP que precede o pacote recebido.

3. Cada ACL de QoS pode ser aplicada a uma porta ou a uma VLAN, mas há um parâmetro de configuração adicional a ser considerado; o tipo de porta ACL. Uma porta pode ser configurada para se basear em VLAN ou em uma porta. Veja a seguir uma descrição dos dois tipos de configurações:Uma porta configurada para ser baseada em VLAN procurará somente a ACL aplicada à VLAN à qual a porta pertence. Se houver uma ACL conectada à porta, a ACL será ignorada para o pacote que entra nessa porta.Se uma porta que pertence a uma VLAN for configurada como baseada em porta, mesmo se houver um ACL anexado àquela VLAN, ela não será levada em consideração para o tráfego que vier daquela porta.

Veja a seguir a seqüência para criar uma ACL de QoS para marcar o tráfego IP:

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

A ACL a seguir marcará todo o tráfego IP direcionado ao host 1.1.1.1 com um DSCP de "40" e confiará em dscp para todo o tráfego IP restante:

set qos acl TEST_ACL dscp 40 ip any host 1.1.1.1

set qos acl TEST_ACL trust-dscp ip any any

Após a criação da ACL, será necessário mapeá-la para uma porta ou uma VLAN, o que pode ser feito com a emissão do seguinte comando:

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

Por padrão, cada porta é baseada em porta para a ACL, portanto, se você quiser anexar uma ACL a uma VLAN, será necessário configurar as portas dessa VLAN como baseada em vlan. Isso pode ser feito emitindo o seguinte comando:

set port qos ***module/port*** **vlan-based**

Também pode ser revertido para o modo com base em porta emitindo o seguinte comando:

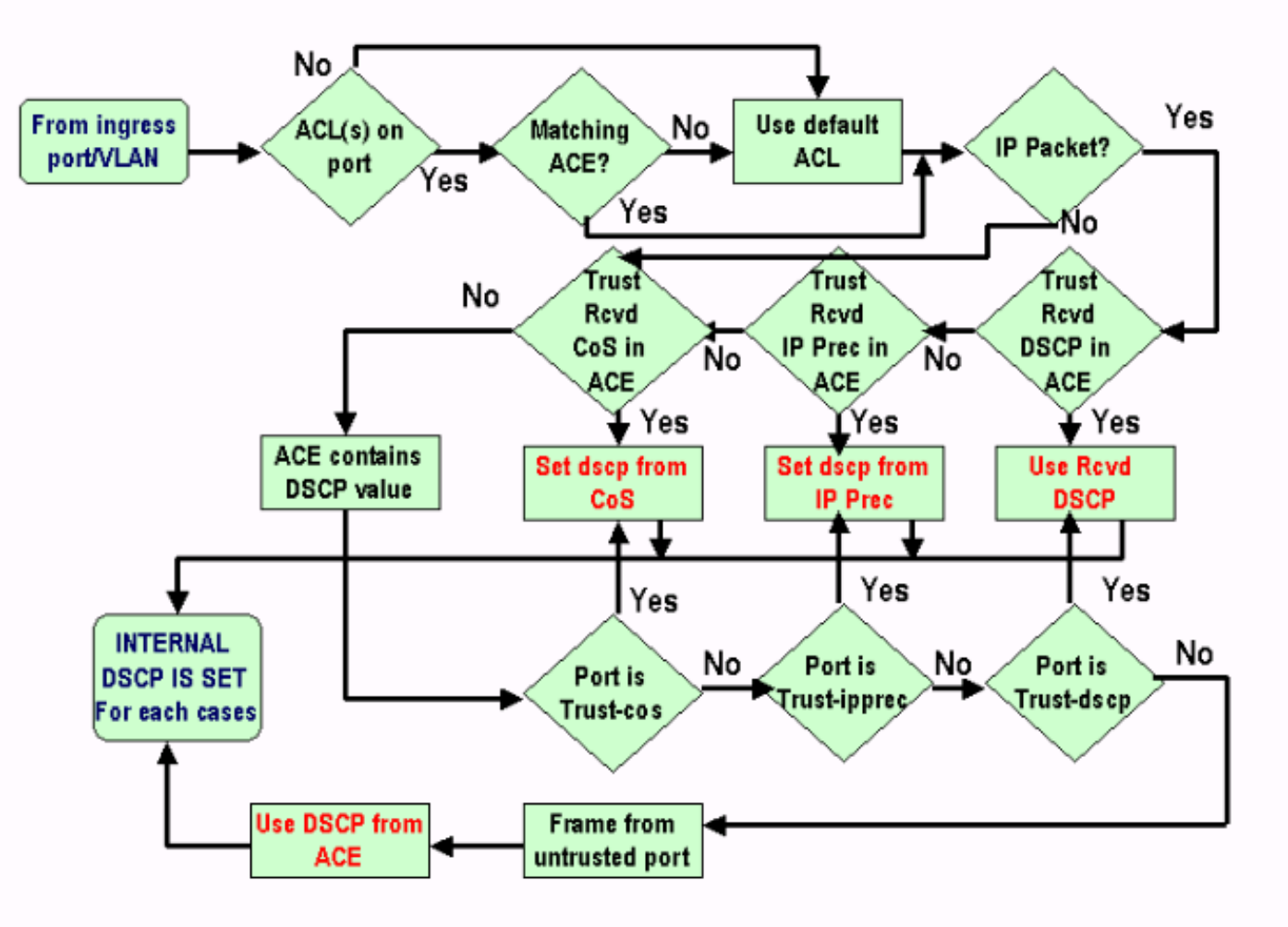
set port qos ***module/port*****-based**

Resumo: Como o DSCP interno é escolhido?

O DSCP interno depende dos seguintes fatores:

- Estado de confiança da porta
- ACL conectado à porta
- ACL padrão
- Com base em VLAN ou com base em porta com relação ao ACL

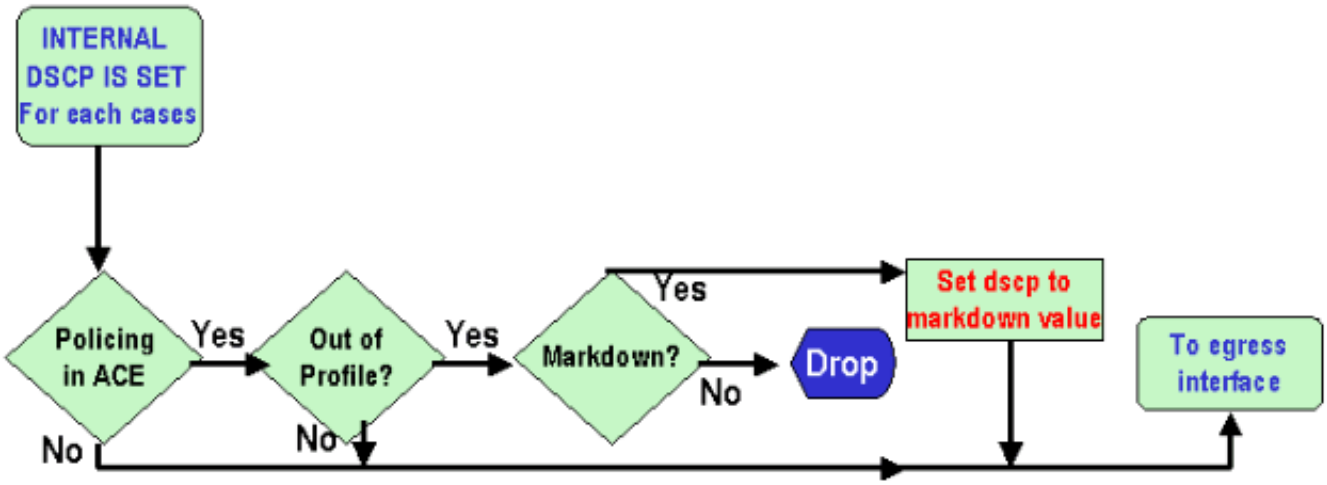
O seguinte fluxograma resume como o DSCP interno é escolhido dependendo da configuração:



O PFC também é capaz de realizar vigilância. Eventualmente, isso pode resultar em uma redução do DSCP interno. Para obter mais informações, consulte o seguinte documento:

- Vigilância de QoS no Catalyst 6000

O seguinte fluxograma mostra como o vigilante é aplicado:



Manejo da porta emissora

Nada pode ser feito no nível da porta de saída para alterar a classificação mas, nesta seção, você marcará o pacote de acordo com as seguintes regras:

- Se o pacote for um pacote IPv4, copie o DSCP interno atribuído pelo mecanismo de switching no byte ToS do cabeçalho de IPv4.
- Se a porta de saída estiver configurada para um encapsulamento de ISL ou dot1q, utilize um CoS derivado de DSCP interno e copie-o no ISL ou no quadro dot1q.

Observação: o CoS é derivado do DSCP interno de acordo com uma estática configurada pelo usuário que emite o seguinte comando:

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

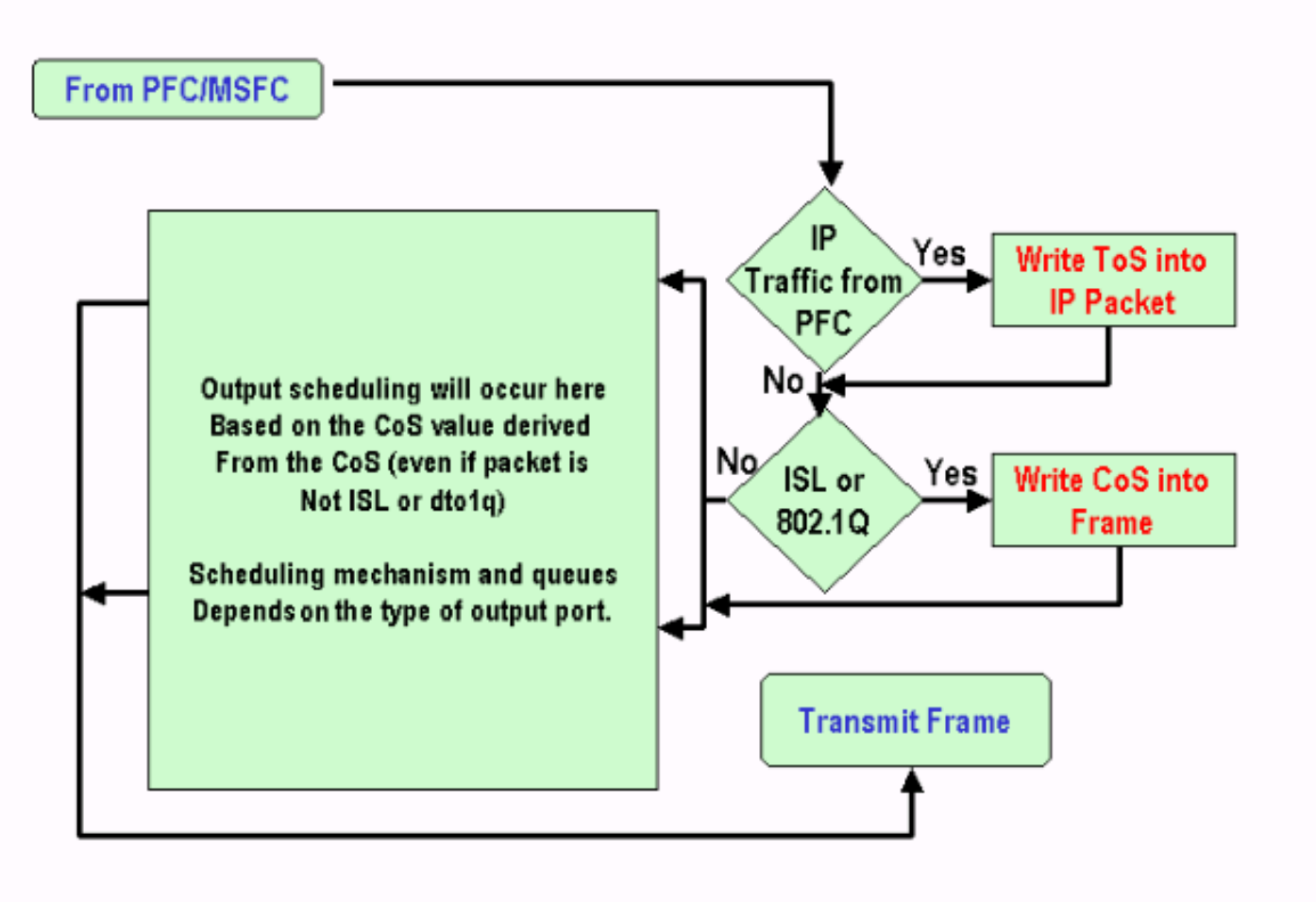
Observação: as configurações padrão são as seguintes. Por padrão, o CoS será a parte inteira do DSCP dividido por oito:

```
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
```

Depois que o DSCP for gravado no cabeçalho IP, e o CoS for derivado do DSCP, o pacote será enviado a uma das filas de saída para a programação de saídas em seu CoS (mesmo que o pacote não seja um dot1q ou um ISL). Para obter informações adicionais sobre a programação da fila de saída, consulte o seguinte documento:

- QoS nos switches Catalyst 6000 Series: Programação de saída no Catalyst 6000 com PFC ou PFC 2 usando software CatOS

O seguinte fluxograma resume o processamento do pacote com relação à marcação na porta de saída:



Notas e limitações

ACL padrão

Como padrão, a ACL padrão utiliza dscp 0" como a palavra-chave de classificação. Isso significa que todo o tráfego que entra no switch por meio de uma porta não confiável será marcado com um DSCP de "0" se a QoS estiver habilitada. Você pode verificar a ACL padrão para o IP emitindo o seguinte comando:

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

A ACL padrão também pode ser alterada emitindo o seguinte comando:

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

trust-cos nas limitações de entrada do ACL

Há uma outra limitação que aparece ao usar a palavra-chave trust-CoS em uma entrada. O CoS só pode ser confiável em uma entrada se o estado confiável de recebimento não for não confiável. A tentativa de configurar uma entrada com trust-CoS exibirá o seguinte aviso:

```
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.
```

Essa limitação é uma conseqüência do que foi visto anteriormente na seção Manipulação da Porta de Entrada. Como mostra o fluxograma nessa seção, se a porta não for confiável, o quadro será imediatamente atribuído à parta padrão CoS. Portanto, o CoS de entrada não está preservado e não foi enviado para o mecanismo de switching, resultando em uma incapacidade de confiar no CoS, mesmo com um ACL específico.

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

Esta seção abrange apenas as seguintes placas de linha:

- WS-X6224-100FX-MT : CATALYST 6000 24 PORTAS 100 FX MULTIMODE
- 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: MT CATALYST 6000 24 PORTAS 100FX, QOS AVANÇADO
- WS-X6324-100FX-SM: MT CATALYST 6000 24 PORTAS 100FX, QOS AVANÇADO
- WS-X6348-RJ-45 CATALYST 6000 48 PORTAS 10/100, QO APRIMORADO
- WS-X6348-RJ21V: CATALYST 6000 48 PORTAS 10/100, POTÊNCIA EM LINHA
- WS-X6348-RJ45V: CATALYST 6000 48-PORT 10/100, ENH QOS, INLI NE POWER

Entretanto, essas placas de linha têm algumas limitações adicionais:

- No nível da porta, não é possível obter trust-dscp nem trust-ipprec.
- No nível da porta, se o estado de confiança da porta for trust-CoS, as seguintes instruções se aplicam:O limite de recepção para agendamento de entrada está ativado. Além disso, o CoS no pacote de recepção é usado para priorizar pacotes para acessar o barramento.O CoS não será confiável e não será usado para derivar o DSCP interno, a menos que você também tenha configurado a ACL para esse tráfego como trust-cos. Além disso, não é suficiente para as placas de ingresso fazer trust-cos na porta, você precisa ter também um ACL com trust-cos para esse tráfego.
- Se o estado de confiança da porta não for confiável, a marcação normal ocorrerá (como no caso padrão). Isto depende do ACL aplicado ao tráfego.

Qualquer tentativa de configurar um estado confiável em uma dessas portas exibirá uma das seguintes mensagens de advertência:

```
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.
```

Resumo de classificação

As tabelas abaixo mostram o DSCP resultante classificado pelo seguinte:

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

Sumário de Tabela Genérica para Todas as Portas, com Exceção de WS-X62xx e WS-X63xx

Palavra-chave do ACL / Estado de confiança da porta	dscp xx	trust-dscp	trust-ipprec	trust-cos
Não confiável	xx (1)	Rx 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 ipprec	Rx dscp	derivado de Rx ipprec	derivado de Rx Cos ou porta CoS
trust-cos	derivado de Rx Cos ou porta CoS	Rx dscp	derivado de Rx ipprec	derivado de Rx Cos ou porta CoS

(1) Esta é a única maneira de fazer uma nova marcação de uma estrutura.

Resumo da tabela para WS-X62*xx* ou WS-X63*xx*

Palavra-chave do ACL / Estado de confiança da porta	dscp 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	xx	Rx dscp	derivado de Rx ipprec	derivado de CoS Rx ou CoS de

				porta (2)

(2) Esta é a única maneira de preservar o CoS recebido do tráfego vindo de uma placa de ingresso 62cc ou 63xx.

Monitorando e verificando uma configuração

Verificando a configuração de porta

As definições e configurações da porta podem ser verificadas emitindo o seguinte comando:

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

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

- com base em porta ou com base em VLAN
- confiar no tipo de porta
- ACL conectado à porta

A seguir encontra-se uma amostra dessa saída de comando com os campos importantes relacionados à classificação em destaque:

```
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
```

Observação: para cada campo, há o parâmetro configurado e o parâmetro de tempo de execução. Aquele que será aplicado ao pacote é o parâmetro de tempo de execução.

Verificando o ACL

Você pode verificar o ACL aplicado e visto em comandos anteriores emitindo o seguindo 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
```

Exemplo de estudos de caso

Os seguintes exemplos são amostras de configurações de casos comuns que poderiam aparecer em uma rede.

Caso 1: Marcação na ponta

Suponhamos que você esteja configurando um Catalyst 6000 utilizado como Switch de acesso com vários usuários conectados ao slot 2, que é uma placa de linha WS-X6348 (10/100M). Os usuários podem enviar:

- Tráfego normal de dados: Isso está sempre na VLAN 100 e precisa obter um DSCP de "0".
- Tráfego de voz a partir de um telefone IP: Está sempre no VLAN 101 auxiliar de voz e precisa obter um DSCP de "40".
- Tráfego de aplicativos vital: Esse tráfego também entra no VLAN 100 e é direcionado para o servidor 10.10.10.20. Esse tráfego precisa ter um DSCP de "32".

Esse tráfego não é marcado pelo aplicativo, portanto, a porta será mantida não confiável e configurará um ACL específico para classificar o tráfego. Uma ACL será aplicada à VLAN 100 e uma ACL será aplicada à VLAN 101. Você também precisa configurar todas as portas como baseadas em VLAN. A seguir, está um exemplo da configuração 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: Confiando no núcleo com apenas uma interface de gigabit

Considere que você está configurando um núcleo Catalyst 6000 com uma interface de apenas um Gigabit nos slots 1 e 2 (nenhuma placa de linha 62xx ou 63xx no chassis). O tráfego foi corretamente marcado anteriormente pelos Switches de acesso; assim, não é necessário fazer nenhuma remarcação, mas garanta que o DSCP de recebimento é confiável. Esse é o caso mais fácil, uma vez que todas as portas estarão marcadas como trust-dscp e isso deve ser suficiente:

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

Caso 3: Confiando no núcleo com uma porta 62xx ou 63xx no chassi

Vamos supor que você está configurando um dispositivo principal/de distribuição com um link de Gigabit em uma placa de linha WS-X6416-GBIC (no slot 2) e um link 10/100 em uma placa de linha WS-X6348 (no slot 3). Você também precisa confiar em todo o tráfego de entrada, como foi marcado anteriormente no nível do Switch de acesso. Como você não pode confiar em dscp na placa de linha 6348, o método mais fácil nesse caso seria deixar todas as portas como não confiáveis e alterar a ACL padrão para trust-dscp, como no exemplo a seguir:

```
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
```

Informações Relacionadas

- Suporte a Produtos de LAN
- Suporte de tecnologia de switching de LAN
- Suporte Técnico - Cisco Systems