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

Índice

Introdução

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

Este documento não é pretendido ser uma lista exaustiva de todos os comandos do OS do catalizador (Cactos) em relação ao Qualidade de Serviço (QoS) ou à marcação. Para obter mais

informações sobre do comando line interface(cli) de Cactos, refira o seguinte documento:

- Configurando QoS

Nota: Este documento considera apenas tráfego de IP.

Antes de Começar

Convenções

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

Pré-requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento é válido para os Catalyst 6000 Family Switch que executam o Cactos Software, e usando um dos seguintes motores do supervisor:

- 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. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Terminologia

A seguir está uma lista da terminologia usada nesse documento:

- 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:** Atribua também um DSCP interno a cada pacote (IP ou não-IP); essa atribuição de DSCP interno será detalhada posteriormente neste documento.
- 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). 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 para 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 Catalyst 6000 Family Switch podem fazer as classificações baseadas nos seguintes três parâmetros:

- DSCP
- Precedência de IP
- CoS

Os Catalyst 6000 Family Switch estão fazendo a classificação e marcação em lugares 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

Àrevelia, QoS é desabilitado em Catalyst 6000 Switch. QoS pode ser permitido emitindo o **set qos enable do** comando cactos.

Quando QoS é desabilitado não há nenhuma classificação ou marcação feita pelo interruptor, e como tal, cada pacote deixa o interruptor com a precedência que DSCP/IP teve ao incorporar o interruptor.

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:

confiança da */porta modificação dos* **qos do set port {não-confiável | trust-cos | trust-ipprec | Trust-dscp}**

Nota: Por padrão, todas as portas ficam no estado não confiável quando a QoS estiver 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 reais, aplique o CoS de porta padrão (se o quadro não tiver um CoS recebido ((dot1q ou ISL)), ou mantenha o CoS como é (para o dot1q e os quadros ISL) e passe o quadro ao mecanismo de switching. A classificação de entrada está ilustrada no seguinte fluxograma:

Nota: Como mostra o fluxograma acima, cada frame terá um CoS interno atribuído (o CoS recebido ou o CoS de porta padrão), incluindo frames não rotulados que não carregam 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. Isto acontece na placa de linha do ingresso e neste momento não se sabe ainda se este CoS interno estará levado aos egresss ASIC e introduzido no frame enviado. Este tudo depende do que o PFC faz e é descrito mais 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 como ele transita pelo interruptor. Não é o DSCP no cabeçalho de IPv4. 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. 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 existente DSCP, grupo antes do quadro que incorpora o interruptor.
2. Os bit de precedência IP recebidos já ajustados no encabeçamento do IPv4. Desde que há 64 valores DSCP e somente oito valores de precedência IP, o administrador configurará um mapeamento que seja usado pelo interruptor para derivar o DSCP. Os mapeamentos padrão estão prontos, caso o administrador não configure os mapas.
3. Os bit recebidos de CoS já ajustaram-se antes do quadro que incorpora o interruptor, ou do padrão CoS da porta de recebimento se não havia nenhum CoS no frame de entrada. 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. Este mapa pode ser configurado, ou o interruptor pode usar o mapa padrão já no lugar.
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 no. 2 e 3 na lista acima, o mapeamento estático usado é à revelia, como segue:

- 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.

Este mapeamento estático pode ser cancelado pelo usuário emitindo os comandos seguintes:

ajuste o Ipprec-dscp-map <dscp1> <dscp2>...<dscp8> dos **qos**

ajuste o Cos-dscp-map <dscp1> <dscp2>...<dscp8> dos **qos**

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:**Nota:** Cada pacote dirige uma entrada 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. O seguinte é uma lista de palavras-chaves possíveis e de 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 é não confiável, o DSCP interno estará ajustado a *xx*.Se a porta for trust-dscp, o DSCP interno será o DSCP recebido no pacote de entrada.Se a porta é Trust-cos, o DSCP interno estará 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 QoS ACL pode ser aplicado a uma porta ou a um VLAN, mas há um parâmetro de configuração adicional a levar em consideração; 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 com base em VLAN olhará somente ao ACL aplicado ao VLAN a que a porta pertence. Se há um ACL anexado à porta, o ACL estará ignorado para o pacote que vem dentro 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:

ajuste o *acl_name* **acl IP dos qos [dscp xx | trust-cos | trust-dscp |** *regra da entrada acl do* **Trust-ipprec]**

O seguinte ACL, marcará todo o tráfego IP dirigido hospedar 1.1.1.1 com um DSCP de "40" e Trust-dscp para todo 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:

ajuste o *acl_name do* **mapa acl dos qos [/porta do módulo | VLAN]**

Àrevelia, cada porta é com base na porta para o ACL, assim que se você quer anexar um ACL a um VLAN, você precisa de configurar as portas deste VLAN como VLAN-baseadas. Isso pode ser feito emitindo o seguinte comando:

/porta do módulo dos **qos do set port VLAN-baseada**

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

/porta do módulo dos **qos do set port com base na porta**

Resumo: Como o DSCP interno é escolhido?

O DSCP interno depende dos seguintes fatores:

- port trust state
- 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.

Nota: O CoS é derivado do DSCP interno de acordo com a estática configurada pelo usuário, emitindo o seguinte comando:

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

Nota: A seguir há configurações padrão. 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 em Catalyst 6000 Series Switch: Programação de emissor no catalizador 6000 com PFC ou PFC2 usando o Cactos Software

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 incorpora o interruptor através de uma porta não-confiável estará identificado por meio de um DSCP de "0" se QoS é permitido. Você pode verificar o ACL padrão para o IP emitindo o comando seguinte:

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

O ACL padrão pode igualmente ser mudado emitindo o comando seguinte:

ajuste a ação padrão IP acl dos qos [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 CATALIZADOR 6000 48-PORT 10/100, QO AUMENTADO
- 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.
- A nível da porta, se o port trust state é Trust-cos, as seguintes indicações aplicam-se:O ponto inicial da recepção para a programação da entrada é permitido. Além, o CoS no pacote da recepção é usado para dar a prioridade a pacotes para alcançar o barramento.O CoS não será confiado e não será usado para derivar o DSCP interno, a menos que você igualmente configurar o ACL para esse tráfego ao 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 port trust state é não-confiável, a marcação normal acontecerá (como com o 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.
- As palavras-chave de classificação dentro do ACL aplicado.

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	xx (1)	Rx	derivado	0

confiável		dscp	de Rx ipprec	
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 de tabela para WS-X62XX ou WS-X63XX

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	Não suportado	Não suportado	Não suportado	Não suportado
trust-ipprec	Não suportado	Não suportado	Não suportado	Não suportado
trust-cos	xx	Rx dscp	derivado de Rx ipprec	derivado de RX CoS ou porta CoS (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:

/porta do módulo do **show port qos**

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
```

Nota: Para cada campo, há um parâmetro configurado e um 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:

mostre o *acl_name do* tempo de execução de informações acl dos qos

```
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

Supõe que você está configurando um catalizador 6000 usado como um switch de acesso com muitos usuários conectados para entalhar 2, que seja uma placa de linha WS-X6348 (10/100M). Os usuários podem enviar:

- Tráfego de dados normal: Isto está sempre no VLAN 100, e precisa de 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. Este tráfego precisa de obter 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. Um ACL será aplicado ao VLAN 100 e um ACL será aplicado ao VLAN 101. Você igualmente precisa de configurar todas as portas como com base 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 tem sido marcado corretamente previamente pelos switch de acesso, consequentemente você não precisa de fazer a observação, mas você precisa de assegurar-se de que você confie o DSCP entrante. 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 igualmente precisa de confiar todo o tráfego de entrada porque tem sido marcado mais cedo a nível do switch de acesso. Porque você não pode Trust-dscp na placa de linha 6348, o método o mais fácil neste caso seria deixar todas as portas como o não-confiável e mudar o ACL padrão ao Trust-dscp, como no exemplo seguinte:

```
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