Como compreender as políticas de QoS e a marcação no Catalyst 3550

Contents

Introduction

A função de vigilância determina se o nível de tráfego está dentro do perfil ou contrato especificado e permite que você descarte o tráfego fora do perfil ou o marque para um valor de Ponto de Código de Serviços Diferenciais (DSCP - Differential Services Code Point) diferente. Isto reforça um nível de serviço contratado.

O DSCP é uma medida do nível de Qualidade de Serviço (QoS) do pacote. Juntamente com o DSCP, a precedência de IP e a Classe de Serviço (CoS - Class of Service) também são usadas para transmitir o nível de QoS do pacote.

A vigilância não deve ser confundida com a modelagem de tráfego, embora ambos assegurem que o tráfego permaneça no perfil ou contrato.

A vigilância não armazena o tráfego em buffer, portanto, a vigilância não afeta o atraso da transmissão. Em vez de colocar em buffer pacotes fora do perfil, a vigilância os descarta ou os marca com níveis de QoS diferentes (marcação DSCP).

A modelagem de tráfego coloca o tráfego fora do perfil em buffer e suaviza as intermitências de tráfego, mas afeta a variação de retardo e retardo. A modelagem só pode ser aplicada na interface de saída, enquanto a vigilância pode ser aplicada na interface de entrada e de saída.

O Catalyst 3550 suporta policiamento para direções de entrada e saída. A modelagem de tráfego não é suportada.

A marcação altera o nível de QoS do pacote de acordo com uma política.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Versões de hardware e software

A vigilância e a marcação no Catalyst 3550 são suportadas com todas as versões de software. O guia de configuração mais recente está listado aqui. Consulte esta documentação para ver todos os recursos suportados.

- Configurando QoS

Vigilância de QoS e parâmetros de marcação

Para configurar o policiamento, você deve definir os mapas de política de QoS e aplicá-los às portas. Isso é conhecido como QoS baseada em porta.

Observação: a QoS baseada em VLAN não é suportada atualmente pelo Catalyst 3550.

O vigilante é definido por parâmetros de taxa e intermitência, bem como por ações para tráfego fora de perfil.

Esses dois tipos de vigilantes são suportados:

- Agregado
- Individual

O vigilante agregado age sobre o tráfego em todas as instâncias em que é aplicado. O vigilante individual age separadamente sobre o tráfego em cada instância em que é aplicado.

Observação: no Catalyst 3550, o vigilante agregado só pode ser aplicado a diferentes classes da mesma política. A vigilância agregada em várias interfaces ou políticas não é suportada.

Por exemplo, aplique o vigilante agregado para limitar o tráfego de classe cliente1 e classe

cliente2 no mesmo mapa de política para 1 Mbps. Esse vigilante permite 1 Mbps de tráfego na classe cliente1 e cliente2 juntos. Se você aplicar o vigilante individual, o vigilante limitará o tráfego para class customer1 a 1 Mbps e para class customer2 a 1 Mbps. Portanto, cada instância do vigilante é separada.

Esta tabela resume a ação de QoS sobre o pacote quando tratado pelas políticas de entrada e saída:

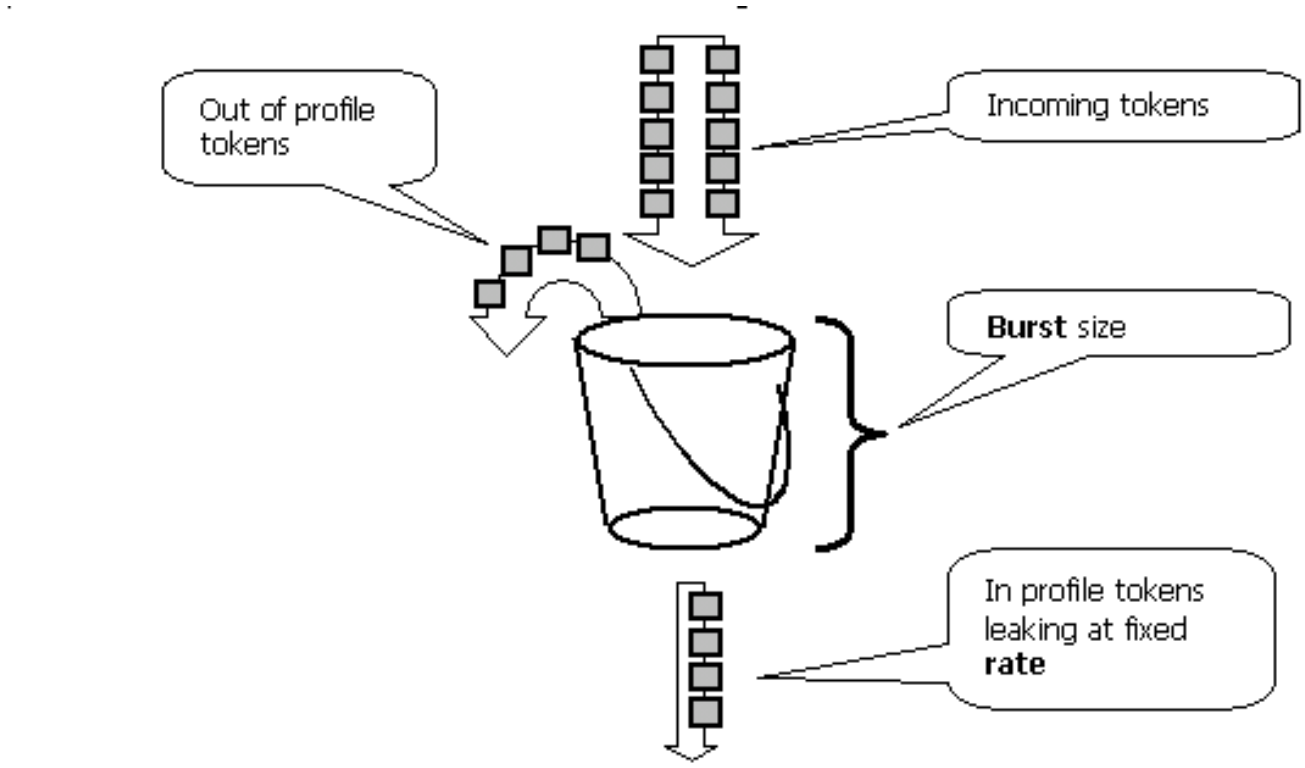
	Ingress policy			
Egress policy	Transmit	Drop	$Markdown_i$	$Mark_i$
Transmit	Transmit	Drop	$Markdown_i$	$Mark_i$
Drop	Drop	Drop	Drop	Drop
$Markdown_e$	$Markdown_e$	Drop	$Markdown_i$ then $Markdown_e$	$Mark_i$ then $Markdown_e$

Observação: é possível marcar e marcar dentro da mesma classe de tráfego da mesma política. Nesse caso, todo o tráfego para a classe específica é marcado primeiro. O policiamento e a redução ocorrem no tráfego já marcado.

O policiamento de QoS no Catalyst 3550 está em conformidade com este conceito de vazamento de bucket:

O número de tokens proporcional aos tamanhos dos pacotes de tráfego de entrada são colocados em um token bucket; o número de tokens é igual ao tamanho do pacote. Em um intervalo regular, um número definido de tokens derivados da taxa configurada é removido do bucket. Se não houver lugar no bucket para acomodar um pacote de entrada, o pacote será considerado fora de perfil e será descartado ou marcado de acordo com a ação de vigilância configurada.

Este conceito é mostrado neste exemplo:



Observação: o tráfego não é colocado em buffer no bucket como pode aparecer neste exemplo. O tráfego real não flui pelo bucket; o bucket é usado somente para decidir se o pacote está no

perfil ou fora do perfil.

Observação: a implementação de vigilância por hardware pode variar, mas funcionalmente ainda está em conformidade com este modelo.

Estes parâmetros controlam a operação de vigilância:

- **Rate** — define quantos tokens são removidos em cada intervalo. Isso define efetivamente a taxa de vigilância. Todo o tráfego abaixo da taxa é considerado no perfil. As taxas suportadas variam de 8 Kbps a 2 Gbps e aumentam em 8 Kbps.
- **Intervalo** — define a frequência com que os tokens são removidos do bucket. O intervalo é fixado em 0,125 milissegundos (ou 8000 vezes por segundo). Não é possível alterar este intervalo.
- **Intermitência** — define a quantidade máxima de tokens que o bucket pode conter a qualquer momento. As intermitências suportadas variam de 8000 bytes a 2000000 bytes e aumentam em 64 bytes.

Observação: embora as strings de ajuda de linha de comando mostrem um grande intervalo de valores, a opção rate-bps não pode exceder a velocidade de porta configurada e a opção burst-byte não pode exceder 2000000 bytes. Se você inserir um valor maior, o switch rejeitará o mapa de política quando você o anexar a uma interface.

Para sustentar a taxa de tráfego especificada, a intermitência não deve ser inferior à soma desta equação:

```
Burstmin (bits) = Rate (bps) / 8000 (1/sec)
```

Por exemplo, calcule o valor mínimo de intermitência para sustentar uma taxa de 1 Mbps. A taxa é definida como 1000 Kbps, de modo que a intermitência mínima necessária é a soma desta equação:

```
1000 (Kbps) / 8000 (1/sec) =125 (bits)
```

O tamanho mínimo de intermitência suportada é 8000 bytes, que é mais do que a intermitência mínima calculada.

Observação: devido à granularidade da vigilância de hardware, a taxa exata e a intermitência são arredondadas para o valor suportado mais próximo.

Ao configurar a taxa de burst, você deve levar em conta que alguns protocolos implementam mecanismos que reagem à perda de pacotes. Por exemplo, o Transmission Control Protocol (TCP) reduz a janela pela metade para cada pacote perdido. Isso causa um efeito "dente de serra" no tráfego TCP quando o TCP tenta acelerar para a taxa de linha e é limitado pelo vigilante. Se a taxa média do tráfego dos dentes de serra for calculada, essa taxa será muito mais baixa do que a taxa vigiada. No entanto, você pode aumentar a intermitência para obter melhor utilização. Um bom começo é definir a intermitência igual ao dobro do tráfego enviado com a taxa desejada durante o tempo de ida e volta (TCP RTT). Se o RTT não for conhecido, você poderá dobrar o valor do parâmetro de intermitência.

Pelo mesmo motivo, não é recomendado fazer o benchmark da operação do vigilante por tráfego orientado a conexão. Esse cenário geralmente mostra um desempenho mais baixo do que o permitido pelo vigilante.

O tráfego sem conexão também pode reagir a políticas de forma diferente. Por exemplo, o Network File System (NFS) usa blocos, que podem consistir em mais de um pacote UDP (User Datagram Protocol). Um pacote descartado pode disparar muitos pacotes, mesmo o bloco inteiro, para serem retransmitidos.

Este exemplo calcula a intermitência de uma sessão TCP com uma taxa de vigilância de 64 Kbps e, como o TCP RTT é 0,05 segundos:

```
<burst> = 2*  *  = 2 * 0.05 [sec] * 64000/8 [bytes/sec] = 800    [bytes]
```

Neste exemplo, `<burst>` é para uma sessão TCP. Dimensione esse número para calcular a média do número esperado de sessões que passam pelo vigilante.

Observação: este é apenas um exemplo, em cada caso você precisa avaliar os requisitos de tráfego e aplicativos e o comportamento em relação aos recursos disponíveis para escolher parâmetros de vigilância.

A ação de vigilância pode ser descartar o pacote ou alterar o DSCP do pacote (markdown). Para marcar o pacote, um mapa de DSCP policiado deve ser modificado. Um mapa DSCP policiado padrão comenta o pacote no mesmo DSCP. Portanto, não ocorre redução de valor.

Os pacotes podem ser enviados fora de ordem quando um pacote fora de perfil é marcado para um DSCP mapeado em uma fila de saída diferente do DSCP original. Se a ordem dos pacotes for importante, direcione pacotes fora de perfil para o DSCP mapeado para a mesma fila de saída dos pacotes no perfil.

Vigiando e marcando recursos suportados pelo Catalyst 3550

Esta tabela fornece um resumo dos recursos relacionados à política e marcação suportados pelo Catalyst 3550, divididos por direção:

	Direction	
Feature	Ingress	Egress
Individual policers	Yes, totally 128 for GE and 8 for FE including ingress aggregate policers	Yes, totally 8 including egress aggregate policers
Aggregate policers	Yes, totally 128 for GE and 8 for FE including ingress individual policers	Yes, totally 8 including egress individual policers
Marking	Yes	No
Policer Markdown	Yes	Yes
Match with ACL	Yes	**No**
Match DSCP	Yes	**Yes**
Match IP precedence	Yes	No
Match COS	Yes, for non-IP traffic	No
Trust DSCP	Yes	No
Trust COS	Yes	No
Trust IP precedence	Yes	No

Uma instrução match é suportada por class-map. Estas são instruções de correspondência válidas para a política de entrada:

- match access-group
- match ip dscp
- precedência compatível de ip

Observação: no Catalyst 3550, o comando **match interface** não é suportado e somente um comando match é permitido em um mapa de classe. Portanto, é difícil classificar todo o tráfego que entra por meio de uma interface e policiar todo o tráfego com um único vigilante. Consulte Como classificar todo o tráfego de interface com um único policer neste documento.

Esta é a instrução de correspondência válida para a política de saída:

- match ip dscp

Estas são ações de política válidas para a política de ingresso:

- polícia
- set ip dscp (marcação)
- set ip precedence (marcação)
- trust dscp
- trust ip-precedence
- trust cos

Esta tabela mostra a matriz de políticas de QoS de entrada suportadas:

Trust I/F	Match DSCP[1]	Match ACL	Trust Class[2]	Set DSCP[3]	Police	Result
						Traffic is assigned default QOS level of the port (0 by default)
√						QOS level of incoming traffic is preserved, according to what is trusted
	√		√		√	IP Traffic is matched by DSCP and then trusted then policed, excess traffic dropped or marked down
	√		√			IP Traffic is matched by DSCP/IP precedence and its QOS level is preserved
	√			√		IP Traffic is matched by DSCP/IP precedence then marked
	√			√	√	IP Traffic is matched by DSCP/IP precedence then marked then policed
		√	√		√	Traffic is matched by access list, QOS level of the matched traffic is preserved, then traffic is policed
		√	√			Traffic is matched by access list and its QOS level is preserved according to what is trusted
		√		√	√	Traffic is matched by access list then marked and then policed
		√		√		Traffic is matched by ACL then marked with specified DSCP/IP precedence
		MAC ACL w/COS	√			Match non-IP traffic by MAC EtherType and COS and preserve QOS level
		MAC ACL w/COS	√		√	Match non-IP IP traffic by MAC EtherType and COS and preserve QOS level then police
		MAC ACL w/COS		√		Match non-IP IP traffic by MAC EtherType and COS then mark matched traffic
		MAC ACL W/COS		√	√	Match non-IP IP traffic by MAC EtherType and COS then mark and then police

1. Essa opção também cobre a precedência de IP correspondente.
2. Esta opção cobre a confiança em CoS, precedência de IP e DSCP.
3. Essa opção também abrange a definição da precedência de IP.

Esta é a ação de política válida para a política de saída:

- polícia

Esta tabela mostra a matriz de políticas de QoS de saída suportadas:

Match DSCP	Police	Result
		Traffic is sent out with COS and IP precedence according to QOS maps and internal DSCP after ingress QOS processing
√	√	Traffic is matched by DSCP and policed

A marcação permite que o nível de QoS do pacote seja alterado com base na classificação ou na vigilância. A classificação divide o tráfego em diferentes classes para o processamento de QoS com base nos critérios definidos.

O processamento de QoS é baseado no DSCP interno; a medida do nível de QoS do pacote. O DSCP interno é derivado de acordo com a configuração de confiança. O sistema oferece suporte a interfaces confiáveis de CoS, DSCP, precedência de IP e não confiáveis. A confiança especifica o campo do qual o DSCP interno é derivado para cada pacote, da seguinte forma:

- Ao confiar em CoS, o nível de QoS é derivado do cabeçalho da Camada 2 (L2) do Inter-Switch Link Protocol (ISL) ou do pacote encapsulado 802.1Q.
- Ao confiar no DSCP ou na precedência de IP, o sistema deriva o nível de QoS do campo de precedência de DSCP ou IP do pacote de acordo.

Confiar em CoS é significativo apenas em interfaces de entroncamento, e confiar em DSCP (ou precedência de IP) faz sentido apenas para pacotes IP.

Quando uma interface não é confiável, o DSCP interno é derivado do CoS padrão configurável para a interface correspondente. Esse é o estado padrão quando a QoS está habilitada. Se nenhum CoS padrão estiver configurado, o valor padrão será zero.

Uma vez determinado o DSCP interno, ele pode ser alterado por marcação e vigilância ou mantido.

Depois que o pacote passa pelo processamento de QoS, seus campos de nível de QoS (dentro do campo IP/DSCP para IP e dentro do cabeçalho ISL/802.1Q, se houver) são atualizados do DSCP interno. Há estes mapas especiais de QoS relevantes para a política:

- **DSCP para DSCP policiado** — usado para derivar o DSCP policiado quando você marca o pacote.
- **DSCP-to-CoS** —usado para derivar o nível de CoS do DSCP interno para atualizar o cabeçalho ISL/802.1Q do pacote de saída.
- **CoS para DSCP** —usado para derivar o DSCP interno do CoS de entrada (cabeçalho ISL/802.1Q) quando a interface está no modo de Confiança CoS.

Estas são considerações importantes e específicas da implementação:

- A política de serviço de ingresso não pode ser conectada à interface quando ela está configurada para confiar em qualquer uma das métricas de QoS, como CoS/DSCP ou precedência de IP. Para corresponder na precedência de DSCP/IP e na polícia na entrada, você deve configurar a confiança para a classe específica na política, não na interface. Para marcar com base na precedência de DSCP/IP, nenhuma confiança deve ser configurada.
- Somente o tráfego IPv4 sem opções de IP e o encapsulamento Ethernet II Advanced Research Projects Agency (ARPA) é considerado tráfego IP do ponto de vista de hardware e

QoS. Todo o tráfego restante é considerado não IP, incluindo IP com opções, como o IP encapsulado do SubNetwork Access Protocol (SNAP) e IPv6.
- Para pacotes não IP, "match access group" é o único método de classificação porque você não pode corresponder DSCP para tráfego não IP. Uma ACL (Media Access Control) é usada para esse fim; os pacotes podem ser correspondentes com base no endereço MAC origem, no endereço MAC destino e no EtherType. Não é possível combinar o tráfego IP com a ACL MAC, já que o switch faz uma distinção entre o tráfego IP e o tráfego não IP.

Configurar e monitorar políticas

Estas etapas são necessárias para configurar a vigilância no Cisco IOS:

1. Definir um vigilante (para vigilantes agregados)
2. Definir critérios para selecionar o tráfego para vigilância
3. Definir um mapa de classe para selecionar o tráfego usando critérios definidos
4. Definir uma política de serviço usando a classe e aplicando um vigilante à classe especificada
5. Aplicar uma política de serviço a uma porta

Esses dois tipos de vigilantes são suportados:

- Agregado nomeado
- Individual

O vigilante agregado nomeado policia o tráfego combinado de todas as classes na mesma política para onde ele é aplicado. A vigilância agregada em diferentes interfaces não é suportada.

Observação: o vigilante agregado não pode ser aplicado a mais de uma política. Se estiver, esta mensagem de erro será exibida:

```
QoS: Cannot allocate policer for policy map <policy name>
```

Considere este exemplo:

Há um gerador de tráfego conectado à porta GigabitEthernet0/3 que envia aproximadamente 17 Mbps de tráfego UDP com a porta destino 111. Também há tráfego TCP da porta 20. Você deseja que esses dois fluxos de tráfego sejam policiados até 1 Mbps e o tráfego excessivo deve ser descartado. Este exemplo mostra como isso é feito:

```
!--- Globally enables QoS. mls qos !--- Defines the QoS policer, sets the burst !--- to 16000
for better TCP performance. mls qos aggregate-policer pol_1mbps 1000000 16000 exceed-action drop
!--- Defines the ACLs to select traffic. access-list 123 permit udp any any eq 111
access-list 145 permit tcp any eq 20 any
!--- Defines the traffic classes to be policed. class-map match-all cl_udp111 match access-group
123
class-map match-all cl_tcp20
  match access-group 145
!--- Defines the QoS policy, and attaches !--- the policer to the traffic classes. policy-map
po_test
  class cl_udp111
    police aggregate pol_1mbps
  class cl_tcp20
```

```
    police aggregate pol_1mbps
!--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport switchport
access vlan 2 service-policy input po_test
!
```

O primeiro exemplo usou o vigilante agregado nomeado. O vigilante individual, ao contrário do vigilante nomeado, policia o tráfego separadamente em cada classe em que é aplicado. O vigilante individual é definido na configuração do mapa de política. Neste exemplo, duas classes de tráfego são vigiadas por dois vigilantes individuais; cl_udp111 é policiado para 1 Mbps por rajada de 8K e cl_tcp20 é policiado para 512 Kbps por rajada de 32K:

```
!--- Globally enables QoS. mls qos !--- Defines the ACLs to select traffic. access-list 123
permit udp any any eq 111
access-list 145 permit tcp any eq 20 any
!--- Defines the traffic classes to be policed. class-map match-all cl_udp111
  match access-group 123
class-map match-all cl_tcp20
  match access-group 145
!--- Defines QoS policy, and creates and attaches !--- the policers to the traffic classes.
policy-map po_test2
  class cl_udp111
    police 1000000 8000 exceed-action drop
  class cl_tcp20
    police 512000 32000 exceed-action drop
!--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport switchport
access vlan 2 service-policy input po_test2
```

Este comando é usado para monitorar a operação de vigilância:

```
cat3550#show mls qos interface g0/3 statistics
GigabitEthernet0/3
Ingress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
Others: 267718     0          267717     0          0
Egress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
Others: 590877        n/a        n/a      266303     0

WRED drop counts:
  qid  thresh1    thresh2   FreeQ
   1 : 0          0         1024
   2 : 0          0         1024
   3 : 0          0         8
   4 : 0          0         1024
```

Observação: por padrão, não há estatísticas por DSCP. O Catalyst 3550 suporta uma coleção de estatísticas por interface e por direção para até oito valores de DSCP diferentes. Isso é configurado quando você emite o comando **mls qos monitor**. Para monitorar estatísticas para DSCPs 8, 16, 24 e 32, você deve emitir este comando **por interface**:

```
cat3550(config-if)#mls qos monitor dscp 8 16 24 32
```

Observação: o **comando mls qos monitor dscp 8 16 24 32** altera a saída do comando **show mls qos int g0/3 statistics** para:

```
cat3550#show mls qos interface g0/3 statistics
GigabitEthernet0/3
Ingress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
    8 : 0          0          675053785  0          0
    16: 1811748    0          0          0          0         ? per DSCP statistics
    24: 1227820404 15241073   0          0          0
    32: 0          0          539337294  0          0
Others: 1658208    0          1658208    0          0
Egress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
    8 : 675425886     n/a        n/a      0          0
    16: 0             n/a        n/a      0          0         ? per DSCP statistics
    24: 15239542      n/a        n/a      0          0
    32: 539289117     n/a        n/a      536486430  0
Others: 1983055       n/a        n/a      1649446    0

WRED drop counts:
  qid  thresh1    thresh2   FreeQ
   1 : 0          0         1024
   2 : 0          0         1024
   3 : 0          0         6
   4 : 0          0         1024
```

Esta é uma descrição dos campos no exemplo:

- **Entrada**—mostra quantos pacotes chegam de cada direção
- **NO_change** — mostra quantos pacotes eram confiáveis (como o nível de QoS não alterado)
- **Classificado** — mostra quantos pacotes foram atribuídos a este DSCP interno após a classificação
- **Policiado** — mostra quantos pacotes foram marcados como inativos pela vigilância; DSCP mostrado antes da marcação.
- **Descartado** — mostra quantos pacotes foram descartados por vigilância

Esteja ciente destas considerações específicas de implementação:

- Se oito valores de DSCP forem configurados quando você emitir o comando **mls qos monitor**, os outros contadores vistos quando você emite o comando **show mls qos int statistics** poderão exibir informações inadequadas.
- Não há nenhum comando específico para verificar a taxa de tráfego por vigilante oferecida ou de saída.
- Como os contadores são recuperados do hardware sequencialmente, é possível que os contadores não sejam adicionados corretamente. Por exemplo, a quantidade de pacotes policiados, classificados ou descartados pode ser um pouco diferente do número de pacotes de entrada.

Configurar e monitorar a marcação

Estas etapas são necessárias para configurar a marcação:

1. Definir os critérios para classificar o tráfego
2. Definir classes de tráfego a serem classificadas com os critérios definidos anteriormente
3. Criar um mapa de políticas que vincula ações de marcação e ações de vigilância às classes definidas
4. Configurar a(s) interface(s) correspondente(s) para o modo de confiança

5. Aplique o mapa de política a uma interface

Neste exemplo, você deseja que o tráfego IP de entrada para o host 192.168.192.168 seja marcado com precedência de IP 6 e policiado para 1 Mbps; o excesso de tráfego deve ser marcado para a precedência 2 do IP:

```
!--- Globally enables QoS. mls qos !--- Defines the ACLs to select traffic. access-list 167
permit ip any host 192.168.192.168
!--- Defines the traffic class. class-map match-all cl_2host
  match access-group 167
!--- Defines QoS policy, and creates and attaches !--- the policers to the traffic classes.
policy-map po_test3
  class cl_2host
!--- Marks all the class traffic with the IP precedence 6. set ip precedence 6
!--- Polices down to 1 Mbps and marks down according to the QoS map. police 1000000 8000 exceed-
action policed-dscp-transmit
!--- Modifies the policed DSCP QoS map, so the !--- traffic is marked down from IP precedence 6
to 2. !--- In terms of DSCP, this is from 48 to 16 (DSCP=IPprec x8). mls qos map policed-dscp 48
to 16 !--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport
switchport access vlan 2 service-policy input po_test3
```

O mesmo comando **show mls qos interface statistics** é emitido para monitorar a marcação. Exemplos de resultados e implicações estão documentados na seção deste documento.

Como classificar todo o tráfego de interface com um único vigilante

No Catalyst 3550, o comando **match interface** não é suportado e somente um comando match é permitido por class-map. Além disso, o Catalyst 3550 não permite que o tráfego IP seja correspondido pelas ACLs MAC. Portanto, o tráfego IP e não IP deve ser classificado com dois mapas de classe separados. Isso torna difícil classificar todo o tráfego que entra em uma interface e policiar todo o tráfego com um único vigilante. O exemplo de configuração aqui permite que você faça isso. Nesta configuração, o tráfego IP e não IP são correspondidos com dois mapas de classe diferentes. No entanto, cada um usa um vigilante comum para ambos os tráfegos.

```
access-list 100 permit ip any any

class-map ip
match access-group 100
!--- This class-map classifies all IP traffic. mac access-list extended non-ip-acl
permit any any

class-map non-ip
match access-group name non-ip-acl
!--- Class-map classifies all non-IP traffic only. mls qos aggregate-policer all-traffic 8000
8000 exceed-action drop
!--- This command configures a common policer that is applied for both IP and non-IP traffic.
policy-map police-all-traffic
class non-ip
police aggregate all-traffic
class ip
police aggregate all-traffic

interface gigabitEthernet 0/7
service-policy input police-all-traffic
!--- This command applies the policy map to the physical interface.
```

Informações Relacionadas

- Configurando a QoS no Catalyst 3550
- Páginas de suporte de qualidade de serviço
- Página de suporte da switching de LAN
- Páginas de Suporte de Produtos de LAN
- Suporte Técnico e Documentação - Cisco Systems