Compreendendo a Vigilância de QoS e a Marcação no Catalyst 3550

Índice

Introdução

A função de vigilância determina se o nível de tráfego está dentro do perfil especificado ou do contrato, e permite-o ao tráfego fora de perfil da gota ou marca-o para baixo a um valor diferente do Differential Services Code Point (DSCP). Isto reforça um nível de serviço contratado.

DSCP é uma medida do nível de QoS (Qualidade de Serviço) do pacote. Junto com o DSCP, a Precedência IP e o Classe de serviço (CoS) são usados igualmente a fim transportar o QoS em nível do pacote.

Policiar não deve ser confundida com o modelagem de tráfego, embora ambos se certifiquem das estadas do tráfego dentro do perfil ou do contrato.

Policiar não protege o tráfego, assim que policiar não afeta o retardo de transmissão. Em vez dos pacotes de fora de perfil da proteção, policiar deixa-os cair ou identifica-os por meio de níveis diferentes de QoS (mapa de DSCP).

O modelagem de tráfego protege o tráfego fora de perfil e alisa as intermitências de tráfego, mas afeta o atraso e a variação de retardo. Dar forma pode somente ser aplicado na interface enviada, quando policiar puder ser aplicado em ambos a interface recebida e enviada.

O Catalyst 3550 apoia o policiamento para entrante e direções de saída. O modelagem de tráfego não é apoiado.

Marcar muda o pacote QoS em nível de acordo com uma política.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

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

Convenções

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

Versões de hardware e software

A vigilância e marcação no Catalyst 3550 é apoiada com todas as versões de software. O manual de configuração o mais atrasado é alistado aqui. Refira esta documentação para todas as características suportadas.

- Configurando QoS

Vigilância de QoS e parâmetros de marcação

A fim estabelecer o policiamento, você deve definir os mapas da política de QoS e aplicá-los às portas. Isto é sabido de outra maneira como QoS com base na porta.

Note: QoS com base em VLAN não é apoiado atualmente pelo Catalyst 3550.

O vigilante é definido pela taxa e os parâmetros de intermitência assim como a ação para o tráfego fora de perfil.

Estes dois tipos de vigilantes são apoiados:

- Agregado
- Individual

O policer agregado atua em cima do tráfego através de todos os exemplos onde é aplicado. O vigilante individual atua separadamente em cima do tráfego através de cada exemplo onde é aplicado.

Note: No Catalyst 3550, o policer agregado pode somente ser aplicado às classes diferentes da mesma política. O policiamento agregado através das interfaces múltiplas ou das políticas não é

apoiado.

Por exemplo, aplique o policer agregado a fim limitar o tráfego do cliente1 da classe e da classe customer2 no mesmo mapa de política ao 1 Mbps. Tal vigilante permite o 1 Mbps do tráfego no cliente1 da classe e no customer2 junto. Se você aplica o vigilante individual, o vigilante limita o tráfego para o cliente1 da classe ao 1 Mbps e para a classe customer2 ao 1 Mbps. Consequentemente, cada exemplo do vigilante é separado.

Esta tabela resume a ação QoS em cima do pacote quando tratado por ambas as políticas de ingresso e saída:

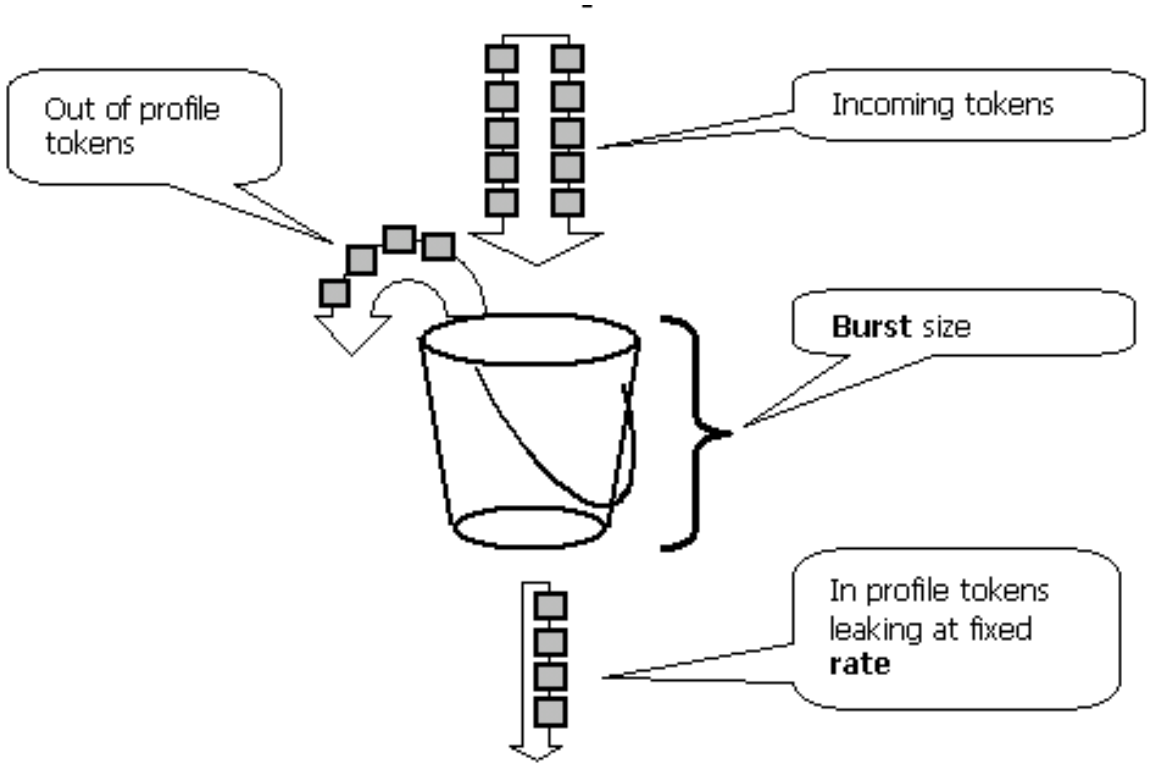
	Ingress policy			
Egress policy	Transmit	Drop	$Markdown_i$	$Mark_i$
Transmit	Transmit	Drop	$Markdown_i$	$Mark_i$
Drop	Drop	Drop	Drop	Drop
$Markdown_e$	$Markdown_e$	Drop	$Markdown_i$ then $Markdown_e$	$Mark_i$ then $Markdown_e$

Note: É possível marcar e markdown dentro da mesma classe de tráfego da mesma política. Em tal caixa, todo o tráfego para a classe particular é marcado primeiramente. O policiamento e o markdown ocorrem em tráfego já marcado.

O Regulamentação QoS no Catalyst 3550 segue com este conceito de leaky bucket:

O número de tokens proporcionais aos tamanhos de pacote de tráfego recebido é colocado em um Token Bucket; o número de tokens iguala o tamanho do pacote. Em um intervalo regular, um número definido de tokens derivados da taxa configurada é removido da cubeta. Se não há nenhum lugar na cubeta para acomodar um pacote recebido, o pacote está considerado fora de perfil e deixado cair ou marcado para baixo de acordo com a ação de vigilância configurada.

Este conceito é mostrado neste exemplo:



Note: O tráfego não está protegido na cubeta enquanto pode aparecer neste exemplo. O tráfego real não corre através da cubeta de todo; a cubeta é usada somente a fim decidir se o pacote está no perfil ou fora de perfil.

Note: A implementação de hardware do policiamento pode variar, mas funcionalmente ainda segue a este modelo.

Estes parâmetros controlam a operação do policiamento:

- **Taxa** — 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 ao 2 Gbps, e de incremento por 8 kbps.
- **Intervalo** — define como os tokens são removidos frequentemente da cubeta. O intervalo é fixo em 0.125 milissegundos (ou em 8000 vezes por segundo). Este intervalo não pode ser mudado.
- **Explosão** — define a quantidade máxima de tokens que a cubeta pode guardar a qualquer hora. Escala de explosões apoiada de 8000 bytes a 2000000 bytes, e a incremento por 64 bytes.

Note: Embora as cordas da ajuda dos dados da linha de comando mostrem uma grande escala dos valores, a opção taxa-bps não pode exceder a velocidade da porta configurada, e a opção do byte de intermitência não pode exceder 2000000 bytes. Se você incorpora um valor maior, o interruptor rejeita o mapa de política quando você o anexa a uma relação.

A fim sustentar a taxa especificada de tráfego, a explosão deve ser nenhuma menos do que a soma desta equação:

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

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

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

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

Note: Devido à granularidade de vigilância de hardware, à taxa exata e à explosão é arredondado ao valor suportado o mais próximo.

Quando você configura a taxa de intermitência, você deve levar em consideração que alguns protocolos implementam mecanismo que reagem à perda de pacotes. Por exemplo, o Transmission Control Protocol (TCP) reduz o indicador pela metade para cada pacote perdido. Isto causa da “um efeito do dente serra” no tráfego TCP quando o TCP tenta acelerar à linha taxa e é estrangulado pelo vigilante. Se a taxa média do tráfego do dente da serra é calculada, esta taxa é muito mais baixa do que a taxa policiada. Contudo, você pode aumentar a explosão a fim conseguir a melhor utilização. Um bom começo é ajustar duas vezes a explosão igual à quantidade do tráfego enviado com a taxa desejada durante o Round-Trip Time (TCP RTT). Se o RTT não é sabido, você pode dobrar o valor do parâmetro de intermitência.

Pela mesma razão, não é recomendado avaliar a operação de vigilância pelo tráfego orientado de conexão. Esta encenação mostra geralmente o desempenho mais baixo do que permitido pelo

vigilante.

O tráfico sem conexão pode igualmente reagir ao policiamento diferentemente. Por exemplo, o Network File System (NFS) usa os blocos, que poderiam consistir em mais de um pacote do User Datagram Protocol (UDP). Um pacote deixado cair pode provocar muitos pacotes, mesmo o bloco inteiro, para ser retransmitido.

Este exemplo calcula a explosão para uma sessão de TCP com uma taxa de vigilância de 64 kbps e dado o TCP RTT são, 0.05 segundos:

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

Neste exemplo, o `<burst>` é para uma sessão de TCP. Escale esta figura para calcular a média do número esperado de sessões que viajam com o vigilante.

Note: Este é um exemplo somente, em cada caso você precisa de avaliar o tráfego e os requisitos do aplicativo e o comportamento contra recursos disponíveis a fim escolher parâmetros de vigilância.

A ação de vigilância pode ser deixar cair o pacote ou mudar o DSCP do pacote (markdown). O markdown o pacote, um mapa dscp policiado deve ser alterado. Um mapa dscp policiado padrão observa o pacote ao mesmo DSCP. Consequentemente, nenhum markdown ocorre.

Os pacotes podem ser enviados a fora de serviço quando um pacote de fora de perfil é marcado para baixo a um DSCP traçado em uma fila de saída diferente do que o DSCP original. Se a ordem dos pacotes é importante, os pacotes de fora de perfil do markdown ao DSCP traçaram à mesma fila de saída que pacotes em perfil.

Vigiando e marcando recursos suportados pelo Catalyst 3550

Esta tabela fornece um sumário das características relativas vigilância e marcação apoiadas pelo Catalyst 3550, dividido pelo sentido:

	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 compatível é apoiada pelo mapa de classe. Estas são declarações de compatibilidade válida para a política de ingresso:

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

Note: No Catalyst 3550, o **comando match interface** não é apoiado e a somente é permitido um comando match em um mapa de classe. Consequentemente, é complicada classificar todo o tráfego que entra através de uma relação e policia todo o tráfego com um único vigilante. Veja como classificar todo o tráfego da relação com uma única seção do vigilante deste documento.

Esta é a declaração de compatibilidade válida para a política de saída:

- match ip dscp

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

- polícia
- ajuste o dscp IP (a marcação)
- ajuste a Precedência IP (a marcação)
- trust dscp
- trust ip-precedence
- trust cos

Esta tabela mostra a matriz apoiada das políticas de QoS do ingresso:

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. Esta opção igualmente cobre a Precedência IP do fósforo.
2. Esta opção cobre a confiança de CoS, de Precedência IP, e de DSCP.
3. Esta opção igualmente cobre o ajuste da Precedência IP.

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

- polícia

Esta tabela mostra a matriz apoiada das políticas de QoS da saída:

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 QoS em nível do pacote mude baseado na classificação ou no policiamento. A classificação racha o tráfego em classes diferentes para o processamento de QoS baseado nos critérios definidos.

O processamento de QoS é baseado no DSCP interno; a medida do QoS em nível do pacote. O DSCP interno é derivado de acordo com a configuração da confiança. Os suportes de sistema que confiam CoS, DSCP, Precedência IP, e interfaces não confiável. A confiança especifica o campo de que o DSCP interno é derivado para cada pacote, como segue:

- Ao confiar CoS, o nível de QoS é derivado do encabeçamento da camada 2 (L2) do protocolo inter-switch link (ISL) ou do pacote encapsulado do 802.1Q.
- Ao confiar o DSCP ou a Precedência IP, o sistema deriva o QoS em nível do DSCP ou do campo de precedência IP do pacote em conformidade.

Confiar CoS é somente significativa em interfaces de entroncamento, e confiar o DSCP (ou a Precedência IP) faz o sentido para pacotes IP somente.

Quando uma relação não é confiada, o DSCP interno está derivado do padrão configurável CoS para a interface correspondente. Este é o estado padrão quando QoS é permitido. Se nenhum padrão CoS é configurado, o valor padrão é zero.

Uma vez que o DSCP interno é determinado, pode ser mudado marcando e policiando, ou ser retido.

Depois que o pacote se submete ao QoS que processa, seus campos do nível de QoS (dentro do campo IP/DSCP para o IP, e dentro do encabeçamento ISL/802.1Q, se algum) estão atualizados do DSCP interno. Há estes mapas especiais de QoS relevantes ao policiamento:

- **DSCP DSCP-à-policiado** — usado a fim derivar o DSCP policiado quando você markdown tragar o pacote.
- **DSCP-à-CoS** — usado a fim derivar o nível de CoS do DSCP interno para atualizar o encabeçamento do pacote de saída ISL/802.1Q.
- **CoS-to-DSCP** — usado a fim derivar o DSCP interno do CoS entrante (encabeçamento ISL/802.1Q) quando a relação reagir do modo de CoS da confiança.

Estas são considerações específicas de implementação importantes:

- A política de serviços do ingresso não pode ser anexada à relação quando a relação é configurada para confiar algum do métrico QoS, tal como o CoS/DSCP ou a Precedência IP. A fim combinar na precedência e na polícia DSCP/IP no ingresso, você deve configurar a confiança para a classe particular dentro da política, não na relação. A fim marcar baseou na precedência DSCP/IP, nenhuma confiança deve ser configurada.
- Somente o tráfego do IPv4 sem opções IP e encapsulamento do Advanced Research Projects Agency do Ethernet II (ARPA) é considerado tráfego IP do hardware e do ponto de

vista de QoS. Todo tráfego restante é considerado incluir não-IP, IP com opções, tais como o IP encapsulado do protocolo de acesso de sub-rede de comunicação (PRESSÃO) e o IPv6.
- Para pacotes não-IP, do “o grupo de acesso fósforo” é o único método de classificação porque você não pode combinar o DSCP para o tráfego não-IP. Uma lista de acesso (ACL) do Media Access Control (MAC) é usada para essa finalidade; os pacotes podem ser combinados com base no endereço MAC de origem, no endereço MAC de destino, e em Ethertype. Não é possível combinar o tráfego IP com o MAC ACL, desde que o interruptor faz uma distinção entre o IP e o tráfego não-IP.

Configurar e monitore o policiamento

Estas etapas são necessárias a fim configurar o policiamento no Cisco IOS:

1. Defina um vigilante (para policeres agregados)
2. Defina critérios para selecionar o tráfego para policiar
3. Defina um mapa de classe para selecionar o tráfego usando critérios definidos
4. Defina uma serviço-política usando a classe e aplicando um vigilante à classe especificada
5. Aplique uma serviço-política a uma porta

Estes dois tipos de vigilantes são apoiados:

- Agregado nomeado
- Individual

O vigilante agregado nomeado policia o tráfego combinado de todas as classes dentro da mesma política a onde é aplicado. O policiamento agregado através das relações diferentes não é apoiado.

Note: O policer agregado não pode ser aplicado a mais de uma política. Se é, este Mensagem de Erro está indicado:

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

Considere este exemplo:

Há um gerador de tráfego anexado para mover GigabitEthernet0/3 que envia aproximadamente o 17 Mbps do tráfego UDP com a porta do destino 111. Há igualmente um tráfego TCP da porta 20. Você quer estes dois fluxos de tráfego ser policiado para baixo ao 1 Mbps, e o tráfego excessivo deve ser deixado cair. Este exemplo mostra como este 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 onde é aplicado. O vigilante individual é definido dentro da configuração de mapa de política. Neste exemplo, duas classes de tráfego são policiadas por dois vigilantes individuais; cl_udp111 é policiado ao 1 Mbps pela explosão 8K, e cl_tcp20 é policiado a 512 kbps por 32K estourado:

```
!--- 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 a fim 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
```

Note: À revelia, não há nenhuma estatística por-DSCP. O Catalyst 3550 apoia uma interface per., coleta de estatística do por-sentido para até oito valores diferentes DSCP. Isto é configurado quando você emite o **comando mls qos monitor**. A fim monitorar estatísticas para DSCP 8, 16, 24, e 32, você deve emitir este **comando per-interface**:

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

Note: **O comando mls qos monitor dscp 8 16 24 32** muda a saída do **comando show mls qos int g0/3 statistics a** esta:

```
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:

- **Entrante** — mostra quantos pacotes chegam de cada sentido
- **NO_change** — mostra quantos pacotes foram confiados (como o nível de QoS não mudado)
- **Classificado** — mostra quanto pacotes foram atribuídos a este DSCP interno após a classificação
- **Policiado** — mostra quanto os pacotes foram marcados para baixo policiando; DSCP mostrado antes do markdown.
- **Deixado cair** — mostra quantos pacotes foram deixados cair policiando

Esteja ciente destas considerações específicas de implementação:

- Se oito valores DSCP são configurados quando você emite o **comando mls qos monitor**, o outro visto contra quando você emite o **comando show mls qos int statistics** poderia indicar a informação inadequada.
- Não há nenhum comando específico a fim verificar a taxa de tráfego por vigilante oferecida ou de saída.
- Desde que os contadores são recuperados do hardware sequencialmente, é possível que os contadores não adicionam acima corretamente. Por exemplo, a quantidade de policiado, classificada, ou os pacotes descartado podem ser levemente diferentes do que o número de pacotes recebidos.

Configurar e monitore a marcação

Estas etapas são necessárias a fim configurar a marcação:

1. Defina os critérios para classificar o tráfego
2. Defina as classes de tráfego a ser classificadas com os critérios definidos previamente
3. Crie um mapa de política que anexa ações e ações de vigilância da marcação às classes definidas
4. Configurar a interface correspondente para confiar o modo

5. Aplique o mapa de política a uma relação

Neste exemplo, você quer o tráfego IP recebido hospedar 192.168.192.168 identificado por meio de Precedência IP 6 e policiado para baixo ao 1 Mbps; o tráfego excedente deve ser marcado para baixo à Precedência IP 2:

```
!--- 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 a fim monitorar a marcação. O exemplo de saída e as implicações são documentados na seção deste documento.

Como classificar todo o tráfego da relação com um único vigilante

No Catalyst 3550, o **comando match interface** não é apoiado, e a somente é permitido um comando match pelo mapa de classe. Além disso, o Catalyst 3550 não permite que o tráfego IP seja combinado pelo MAC ACL. Assim o IP e o tráfego não-IP devem ser classificados com os dois mapas de classe separados. Isto fá-lo complicado para classificar todo o tráfego que entra uma relação e policia-o todo o tráfego com um único vigilante. A configuração de exemplo aqui deixa-o realizar este. Nesta configuração, o IP e o tráfego não-IP são combinados com os dois mapas de classe diferentes. Contudo, cada um usa um policer comum para ambos o tráfego.

```
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 QoS no Catalyst 3550
- Páginas do 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