Políticas de QoS nos switches Catalyst 6500/6000 Series

Contents

Introduction

A Política de QoS em uma rede determina se o tráfego de rede está dentro de um perfil especificado (contrato). Isto pode fazer com que o tráfego fora de perfil reduza ou seja marcado como reduzido para outros valores de Differentiated Services Code Point (DSCP) para reforçar um nível de serviço contratado. (O DSCP é uma medida de nível de QoS do frame.)

Não confunda a vigilância de tráfego com a modelagem de tráfego. Ambos garantem que o tráfego permaneça dentro do perfil (contrato). Você não faz o buffer de pacotes fora de perfil quando policia o tráfego. Portanto, você não afeta o atraso de transmissão. Você descarta o tráfego ou o marca com um nível de QoS mais baixo (marcação DSCP). Em contraste, com a modelagem de tráfego, você coloca em buffer o tráfego fora de perfil e suaviza as intermitências de tráfego. Isso afeta a variação de retardo e retardo. Você só pode aplicar a modelagem de tráfego em uma interface de saída. Você pode aplicar políticas em interfaces de entrada e saída.

A Placa de Recurso de Política (PFC - Policy Feature Card) do Catalyst 6500/6000 e o PFC2 suportam somente vigilância de entrada. O PFC3 suporta policiamento de entrada e saída. A modelagem de tráfego é suportada apenas em determinados módulos de WAN para a série Catalyst 6500/6000, como os módulos OSMs e FlexWAN. Consulte as Notas de Configuração do Cisco 7600 Series Router Module para obter mais informações

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Conventions

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

Parâmetros das políticas de QoS

Para configurar o policiamento, defina os vigilantes e aplique-os às portas (QoS baseada em porta) ou às VLANs (QoS baseada em VLAN). Cada vigilante define um nome, um tipo, uma taxa, uma intermitência e ações para tráfego dentro do perfil e fora do perfil. Os vigilantes no Supervisor Engine II também suportam os parâmetros de taxa de excesso. Existem dois tipos de vigilantes: microfluxo e agregado.

- **Microfluxo** —policia o tráfego para cada porta/VLAN aplicada separadamente por fluxo.
- **Agregar**—policia o tráfego em todas as portas/VLANs aplicadas.

Cada policer pode ser aplicado a várias portas ou VLANs. O fluxo é definido usando estes parâmetros:

- endereço IP origem
- endereço IP destino
- Protocolo da camada 4 (como User Datagram Protocol [UDP])
- número da porta de origem
- número da porta de destino

Você pode dizer que os pacotes que correspondem a um conjunto específico de parâmetros definidos pertencem ao mesmo fluxo. (Esse é essencialmente o mesmo conceito de fluxo que o switching do NetFlow usa.)

Por exemplo, se você configurar um vigilante de microfluxo para limitar o tráfego TFTP a 1 Mbps na VLAN 1 e na VLAN 3, então 1 Mbps é permitido para cada fluxo na VLAN 1 e 1 Mbps para cada fluxo na VLAN 3. Em outras palavras, se houver três fluxos na VLAN 1 e quatro fluxos na VLAN 3, o vigilante de microfluxo permitirá cada um desses fluxos de 1 Mbps. Se você configurar um vigilante agregado, ele limitará o tráfego TFTP para todos os fluxos combinados na VLAN 1 e na VLAN 3 a 1 Mbps.

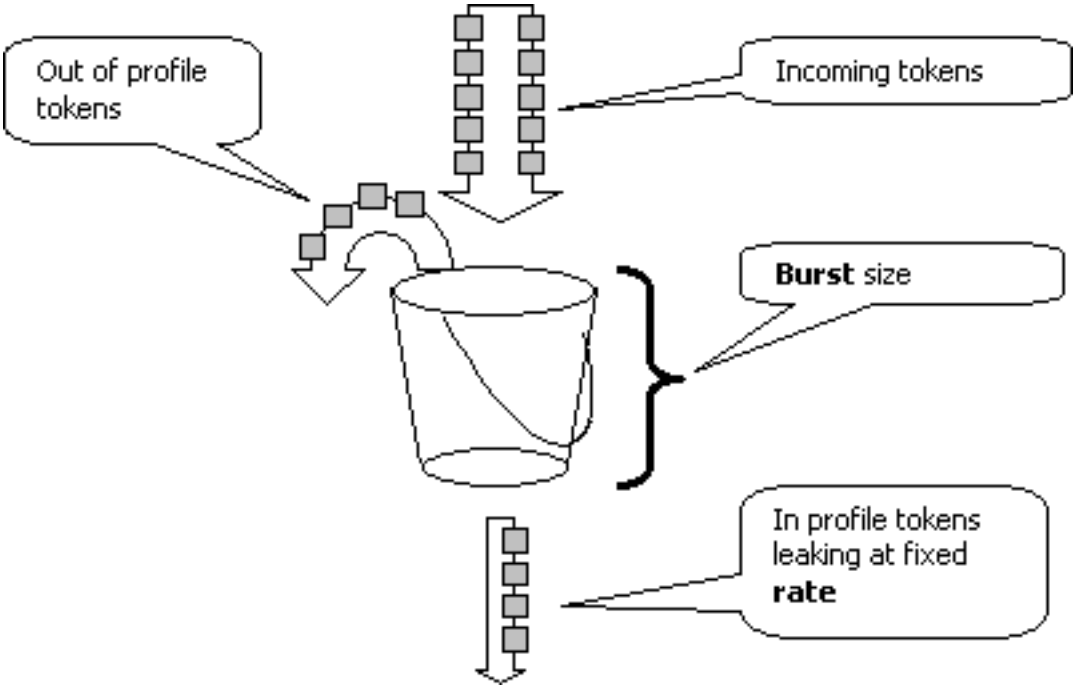
Se você aplicar os vigilantes de agregação e de microfluxo, o QoS sempre executará a ação mais grave especificada pelos vigilantes. Por exemplo, se um vigilante especifica para descartar o pacote, mas outro especifica para anotá-lo, o pacote será descartado.

Por padrão, os vigilantes de microfluxo funcionam somente com tráfego roteado (Camada 3 [L3]). Para policiar também o tráfego de ponte (Camada 2 [L2]), você precisa ativar o policiamento de microfluxo interligado. No Supervisor Engine II, você precisa habilitar a vigilância de microfluxo interligado mesmo para a vigilância de microfluxo L3.

A vigilância é baseada em protocolo. Todo o tráfego é dividido em três tipos:

- IP
- Internetwork Packet Exchange (IPX)
- Outro

O policiamento é implementado no Catalyst 6500/6000 de acordo com o conceito de "vazamento de bucket". Tokens correspondentes a pacotes de tráfego de entrada são colocados em um bucket. (Cada token representa um bit, de modo que um pacote grande é representado por mais tokens do que um pacote pequeno.) Em intervalos regulares, um número definido de tokens é removido do bucket e enviado em seu caminho. Se não houver lugar no bucket para acomodar pacotes de entrada, os pacotes serão considerados fora de perfil. Eles são descartados ou marcados para baixo de acordo com a ação de vigilância configurada.



Observação: o tráfego não é colocado em buffer no bucket, como pode aparecer na imagem acima. O tráfego real não passa pelo balde; o bucket é usado somente para decidir se o pacote está no perfil ou fora do perfil.

Calcular parâmetros

Vários parâmetros controlam a operação do token bucket, como mostrado aqui:

- **Rate** — define quantos tokens são removidos em cada intervalo. Isso define efetivamente a taxa de vigilância. Todo o tráfego abaixo da taxa é considerado em perfil.
- **Intervalo** — define a frequência com que os tokens são removidos do bucket. O intervalo é fixado em 0,00025 segundos, portanto os tokens são retirados do bucket 4.000 vezes por segundo. O intervalo não pode ser alterado.
- **Intermitência** — define o número máximo de tokens que o bucket pode conter a qualquer momento. Para manter a taxa de tráfego especificada, a intermitência não deve ser menor que a taxa vezes que o intervalo. Outra consideração é que o pacote de tamanho máximo deve caber no bucket.

Para determinar o parâmetro de intermitência, use esta equação:

- Intermitência = (Taxa [bps]) * 0.00025 [seg/intervalo]) *ou* (tamanho máximo do pacote [bits]), o que for maior.

Por exemplo, se você quiser calcular o valor mínimo de intermitência necessário para sustentar uma taxa de 1 Mbps em uma rede Ethernet, a taxa é definida como 1 Mbps e o tamanho máximo do pacote Ethernet é de 1518 bytes. A equação é:

- Intermitência = (1.000.000 bps * 0.00025) *ou* (1518 bytes * 8 bits/byte) = 250 *ou* 12144.

O resultado maior é de 12144, que pode ser arredondado para 13 kbps.

Observação: no Cisco IOS® Software, a taxa de vigilância é definida em bits por segundo (bps), ao contrário de kbps no Catalyst OS (CatOS). Também no Cisco IOS Software, a taxa de intermitência é definida em bytes, ao contrário dos kilobits no CatOS.

Observação: devido à granularidade da vigilância de hardware, a taxa exata e a intermitência são arredondadas para o valor suportado mais próximo. Certifique-se de que o valor de intermitência não seja inferior ao pacote de tamanho máximo. Caso contrário, todos os pacotes maiores que o tamanho da intermitência são cancelados.

Por exemplo, se você tentar definir a intermitência como 1518 no Cisco IOS Software, ela será arredondada para 1000. Isso faz com que todos os quadros maiores que 1000 bytes sejam descartados. A solução é configurar o burst para 2000.

Ao configurar a taxa de intermitência, leve em consideração que alguns protocolos (como o TCP) implementam um mecanismo de controle de fluxo que reage à perda de pacotes. Por exemplo, o TCP reduz o janelamento pela metade para cada pacote perdido. Consequentemente, quando policiada para uma determinada taxa, a utilização efetiva do link é inferior à taxa configurada. É possível aumentar a intermitência para obter melhor utilização. Um bom começo para esse tráfego é dobrar o tamanho da intermitência. (Neste exemplo, o tamanho da intermitência é aumentado de 13 kbps para 26 kbps). Depois, monitore o desempenho e efetue os ajustes necessários.

Pelo mesmo motivo, não é recomendável fazer o benchmark da operação do vigilante usando tráfego orientado a conexão. Isso geralmente mostra um desempenho menor do que o permitido pelo vigilante.

Ações da polícia

Como mencionado na Introdução, o vigilante pode fazer uma das duas coisas em um pacote fora de perfil:

- descartar o pacote (o parâmetro `drop` na configuração)
- marque o pacote para um DSCP mais baixo (o parâmetro `policed-dscp` na configuração)

Para marcar o pacote para baixo, você deve modificar o mapa de DSCP policiado. O DSCP policiado é definido por padrão para remarcar o pacote para o mesmo DSCP. (Nenhuma marca desconectada ocorre.)

Observação: se os pacotes "fora de perfil" forem marcados para um DSCP mapeado em uma fila de saída diferente do DSCP original, alguns pacotes poderão ser enviados fora de ordem. Por esse motivo, se a ordem dos pacotes for importante, é recomendável marcar pacotes fora de perfil para um DSCP que é mapeado para a mesma fila de saída dos pacotes no perfil.

No Supervisor Engine II, que suporta a taxa excedente, são possíveis dois disparadores:

- Quando o tráfego excede a taxa normal

- Quando o tráfego excede a taxa excedente

Um exemplo da aplicação da taxa de excesso é marcar os pacotes que excedem a taxa normal e descartar os pacotes que excedem a taxa de excesso.

Recursos de vigilância suportados pelo Catalyst 6500/6000

Conforme declarado na Introdução, o PFC1 no Supervisor Engine 1a e o PFC2 no Supervisor Engine 2 suportam somente a vigilância de entrada (interface de entrada). O PFC3 no Supervisor Engine 720 suporta a vigilância de entrada e saída (interface de saída).

O Catalyst 6500/6000 oferece suporte para até 63 vigilantes de microfluxo e para até 1023 vigilantes agregados.

O Supervisor Engine 1a suporta vigilância de entrada, começando com CatOS versão 5.3(1) e Cisco IOS Software Release 12.0(7)XE.

Observação: uma placa secundária PFC ou PFC2 é necessária para policiamento com o mecanismo de supervisor 1a.

O Supervisor Engine 2 suporta vigilância de entrada, começando com CatOS versão 6.1(1) e Cisco IOS Software Release 12.1(5c)EX. O Supervisor Engine II suporta o parâmetro de policiamento de taxa de excesso.

As configurações com DFCs (Distributed Forwarding Cards, placas de encaminhamento distribuído) suportam somente a vigilância baseada em portas. Além disso, o vigilante agregado conta apenas o tráfego por mecanismo de encaminhamento, não por sistema. O DFC e o PFC são ambos mecanismos de encaminhamento; se um módulo (placa de linha) não tiver um DFC, ele usará um PFC como mecanismo de encaminhamento.

Atualização de recursos de vigilância para o Supervisor Engine 720

Observação: se você não está familiarizado com o policiamento de QoS do Catalyst 6500/6000, leia as seções Parâmetros de Vigilância de QoS e Recursos de Policiamento Suportados pelo Catalyst 6500/6000 deste documento.

O Supervisor Engine 720 introduziu estes novos recursos de vigilância de QoS:

- **Policiamento de saída**. O Supervisor 720 suporta vigilância de entrada em uma porta ou interface de VLAN. Suporta vigilância de saída em uma porta ou interface roteada L3 (no caso do Cisco IOS System Software). Todas as portas na VLAN são vigiadas na saída, independentemente do modo de QoS da porta (seja QoS baseada em porta ou QoS baseada em VLAN). A vigilância de microfluxo não é suportada na saída. Exemplos de configurações são fornecidos na seção Configurar e Monitorar Vigilância no CatOS Software e Configurar e Monitorar Vigilância no Cisco IOS Software deste documento.
- **Política de microfluxo por usuário**. O Supervisor 720 suporta uma melhoria na vigilância de microfluxo conhecida como vigilância de microfluxo por usuário. Este recurso só é suportado com o Cisco IOS System Software. Ele permite que você forneça uma certa largura de banda para cada usuário (por endereço IP) por trás de determinadas interfaces. Isso é obtido

especificando uma máscara de fluxo dentro da política de serviço. A máscara de fluxo define quais informações são usadas para diferenciar os fluxos. Por exemplo, se você especificar uma máscara de fluxo somente de origem, todo o tráfego de um endereço IP será considerado um fluxo. Usando essa técnica, você pode policiar o tráfego por usuário em algumas interfaces (onde configurou a política de serviço correspondente); em outras interfaces, você continua a usar a máscara de fluxo padrão. É possível ter até duas máscaras de fluxo de QoS diferentes ativas no sistema em um determinado momento. Você pode associar apenas uma classe a uma máscara de fluxo. Uma política pode ter até duas máscaras de fluxo diferentes.

Outra alteração importante na vigilância no Supervisor Engine 720 é que ele pode contar o tráfego pelo comprimento L2 do quadro. Isso difere do Supervisor Engine 2 e do Supervisor Engine 1, que contam quadros IP e IPX pelo comprimento L3. Com alguns aplicativos, o comprimento de L2 e L3 pode não ser consistente. Um exemplo é um pequeno pacote L3 dentro de um grande quadro L2. Nesse caso, o Supervisor Engine 720 pode exibir uma taxa de tráfego policiado ligeiramente diferente em comparação com o Supervisor Engine 1 e o Supervisor Engine 2.

Configurar e monitorar policiamento no software CatOS

A configuração de vigilância para CatOS consiste em três etapas principais:

1. Defina um vigilante—a taxa de tráfego normal, a taxa de excesso (se aplicável), a intermitência e a ação de vigilância.
2. Crie uma ACL de QoS para selecionar o tráfego para a polícia e anexe um vigilante a essa ACL.
3. Aplique a ACL de QoS às portas ou VLANs necessárias.

Este exemplo mostra como policiar todo o tráfego para a porta UDP 111 na porta 2/8.

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 drop !--- This defines a
policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip
udp_qos_port dscp 0 aggregate udp_1mbps udp any any eq
111 !--- This creates QoS ACL to select traffic and
attaches !--- the policer to the QoS ACL. commit qos acl
all !--- This compiles the QoS ACL. set qos acl map
udp_qos_port 2/8 !--- This maps the QoS ACL to the
switch port.
```

O próximo exemplo é o mesmo. entretanto, neste exemplo, você conecta o vigilante a uma VLAN. A porta 2/8 pertence à VLAN 20.

Observação: você precisa alterar a QoS da porta para o modo `baseado em vlan`. Faça isso com o comando **set port qos**.

Este vigilante avalia o tráfego de todas as portas nessa VLAN configurada para QoS baseada em VLAN:

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 drop !--- This defines a
policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip
udp_qos_vlan dscp 0 aggregate udp_1mbps udp any any eq
111 !--- This creates the QoS ACL to select traffic and
attaches !--- the policer to QoS ACL. commit qos acl all
!--- This compiles the QoS ACL. set port qos 2/8 vlan-
based !--- This configures the port for VLAN-based QoS.
set qos acl map udp_qos_vlan 20 !--- This maps QoS ACL
to VLAN 20.
```

Em seguida, em vez de descartar pacotes fora de perfil com DSCP 32, marque-os para um DSCP de 0 (melhor esforço).

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 policed-dscp !--- This
defines a policer. For the calculation of rate and
burst, !--- refer to Calculate Parameters. set qos acl
ip udp_qos_md trust-ipprec aggregate udp_1mbps udp any
any eq 111 dscp-field 32 !--- Note: The above command
should be on one line. !--- This creates the QoS ACL to
select traffic and attaches !--- the policer to the QoS
ACL.

commit qos acl all
!--- This compiles the QoS ACL. set qos policed-dscp-map
32:0 !--- This modifies the policed DSCP map to mark
down DSCP 32 to DSCP 0. set port qos 2/8 vlan-based !---
This configures the port for VLAN-based QoS. set qos acl
map udp_qos_md 20 !--- This maps the QoS ACL to VLAN 20.
```

Este exemplo mostra a configuração para vigilância de saída somente para o Supervisor Engine 720. Ele mostra como policiar todo o tráfego IP de saída na VLAN 3 a 10 Mbps agregada.

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
egress_10mbps rate 10000 burst 20 drop !--- This defines
a policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip egress_pol
trust-ipprec aggregate egress_10mbps ip any any !---
This creates the QoS ACL to select traffic and attaches
!--- the policer to the QoS ACL. commit qos acl all !---
This compiles the QoS ACL. set qos acl map egress_pol 3
output !--- This maps the QoS ACL to VLAN 3 in the
output direction.
```

Use **show qos maps runtime policed-dscp-map** para ver o mapa DSCP policed atual.

Usar **show qos policer runtime {*nome_do_policer* | all}** para verificar os parâmetros do vigilante.

Você também pode ver a ACL de QoS à qual o vigilante está conectado.

Observação: com o Supervisor Engine 1 e 1a, não é possível ter estatísticas de policiamento para vigilantes agregados individuais. Para exibir as estatísticas de policiamento por sistema, use este comando:

```
Cat6k> (enable) show qos statistics l3stats
Packets dropped due to policing: 1222086
IP packets with ToS changed: 27424
IP packets with CoS changed: 3220
Non-IP packets with CoS changed: 0
```

Para verificar estatísticas de vigilância de microfluxo, use este comando:

```
Cat6k> (enable) show mls entry qos short
Destination-IP  Source-IP Port  DstPrt SrcPrt Uptime  Age
--------------- --------------- ----- ------ ------ -------- --------

IP bridged entries:
239.77.77.77 192.168.10.200UDP   63 6300:22:02 00:00:00
Stat-Pkts : 165360
Stat-Bytes : 7606560
Excd-Pkts : 492240
Stat-Bkts : 1660
239.3.3.3192.168.11.200UDP  888 77700:05:38 00:00:00
Stat-Pkts : 42372
Stat-Bytes : 1949112
Excd-Pkts : 126128
Stat-Bkts : 1628

Only out of the profile MLS entries are displayed
Cat6k> (enable)
```

Com o Supervisor Engine II, você pode exibir estatísticas de policiamento agregado por vigilante com o comando **show qos statistics aggregate-policer**.

Para este exemplo, um gerador de tráfego é conectado à porta 2/8. Envia 17 Mbps de tráfego UDP com porta destino 111. Você espera que o vigilante descarte 16/17 do tráfego, portanto 1 Mbps deve passar por:

```
Cat6k> (enable) show qos statistics aggregate-policer udp_1mbps
QoS aggregate-policer statistics:
Aggregate policerAllowed packet Packets exceed Packets exceed
                count        normal rate       excess rate
------------------------------ ------------- ------------- -------------
udp_1mbps58243997321089732108

Cat6k> (enable) show qos statistics aggregate-policer udp_1mbps
QoS aggregate-policer statistics:
Aggregate policerAllowed packet Packets exceed Packets exceed
                count        normal rate       excess rate
------------------------------ ------------- ------------- -------------
udp_1mbps58250497331989733198
```

Observação: observe que os pacotes permitidos aumentaram em 65 e os pacotes em excesso aumentaram em 1090. Isso significa que o vigilante descartou 1090 pacotes e permitiu a passagem de 65. Você pode calcular que 65 / (1090 + 65) = 0,056, ou aproximadamente 1/17. Portanto, o vigilante funciona corretamente.

Configurar e monitorar políticas no software Cisco IOS

A configuração para vigilância no Cisco IOS Software envolve estas etapas:

1. Defina um vigilante.
2. Crie uma ACL para selecionar o tráfego a ser policiado.
3. Defina um mapa de classe para selecionar o tráfego com a ACL e/ou precedência de DSCP/IP.
4. Defina uma política de serviço que use classe e aplique o vigilante a uma classe especificada.
5. Aplique a política de serviço a uma porta ou VLAN.

Considere o mesmo exemplo fornecido na seção Configurar e monitorar policiamento no CatOS Software, mas agora com o Cisco IOS Software. Para este exemplo, você tem um gerador de tráfego conectado à porta 2/8. Envia 17 Mbps de tráfego UDP com porta destino 111:

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. mls qos aggregate-policer
udp_1mbps 1000000 2000 conform-action transmit exceed-
action drop !--- Note: The above command should be on
one line. !--- This defines a policer. For the
calculation of rate and burst, !--- refer to Calculate
Parameters. !--- Note: The burst is 2000 instead of
1518, due to hardware granularity.

access-list 111 permit udp any any eq 111
!--- This defines the ACL to select traffic. class-map
match-all udp_qos match access-group 111 !--- This
defines the traffic class to police. policy-map
udp_policy class udp_qos police aggregate udp_1mbps !---
This defines the QoS policy that attaches the policer to
the traffic class. interface GigabitEthernet2/8
switchport service-policy input udp_policy !--- This
applies the QoS policy to an interface.
```

Há dois tipos de vigilantes agregados no software Cisco IOS: **nomeado e por interface.** O vigilante agregado nomeado policia o tráfego combinado de todas as interfaces às quais é aplicado. Esse é o tipo usado no exemplo acima. O vigilante por interface policia o tráfego separadamente em cada interface de entrada à qual ele é aplicado. Um vigilante por interface é definido na configuração de mapa de política. Considere este exemplo, que tem um vigilante agregado por interface:

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 111 permit udp any
any eq 111 !--- This defines the ACL to select traffic.
class-map match-all udp_qos match access-group 111 !---
This defines the traffic class to police. policy-map
udp_policy class udp_qos !--- This defines the QoS
policy that attaches the policer to the traffic class.
police 1000000 2000 2000 conform-action transmit exceed-
action drop !--- This creates a per-interface aggregate
!--- policer and applies it to the traffic class.
```

```
interface GigabitEthernet2/8 switchport service-policy
input udp_policy !--- This applies the QoS policy to an
interface.
```

Os vigilantes de microfluxo são definidos na configuração do mapa de política, assim como os vigilantes agregados por interface. No exemplo abaixo, cada fluxo do host 192.168.2.2 que entra na VLAN 2 é policiado para 100 kbps. Todo o tráfego de 192.168.2.2 é policiado para agregado de 500 kbps. A VLAN 2 inclui as interfaces fa4/11 e fa4/12:

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 1 permit 192.168.2.2
!--- This defines the access list to select traffic from
host 192.168.2.2. class-map match-all host_2_2 match
access-group 1 !--- This defines the traffic class to
police. policy-map host class host_2_2 !--- This defines
the QoS policy. police flow 100000 2000 conform-action
transmit exceed-action drop !--- This defines a
microflow policer. For the calculation of rate and !---
burst, refer to Calculate Parameters. police 500000 2000
2000 conform-action transmit exceed-action drop !---
This defines the aggregate policer to limit !--- traffic
from the host to 500 kbps aggregate. interface fa4/11
mls qos vlan-based interface fa4/12 mls qos vlan-based
!--- This configures interfaces in VLAN 2 for VLAN-based
QoS. interface vlan 2 service-policy input host !---
This applies the QoS policy to VLAN 2.
```

O exemplo abaixo mostra uma configuração para vigilância de saída para o Supervisor Engine 720. Ele estabelece a vigilância de todo o tráfego de saída na interface Gigabit Ethernet 8/6 a 100 kbps:

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 111 permit ip any any
!--- This defines the ACL to select traffic. All IP
traffic is subject to policing. class-map match-all
cl_out match access-group 111 !--- This defines the
traffic class to police. policy-map pol_out class cl_out
police 100000 3000 3000 conform-action transmit exceed-
action drop !--- This creates a policer and attaches it
to the traffic class. interface GigabitEthernet8/6 ip
address 3.3.3.3 255.255.255.0 service-policy output
pol_out !--- This attaches the policy to an interface.
```

O exemplo abaixo mostra uma configuração para vigilância por usuário para o Supervisor Engine 720. O tráfego que chega dos usuários por trás da porta 1/1 para a Internet é policiado para 1 Mbps por usuário. O tráfego proveniente da Internet em direção aos usuários é policiado para 5 Mbps por usuário:

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 111 permit ip any any
!--- This defines the ACL to select user traffic. class-
```

```
map match-all cl_out match access-group 111 !--- This
defines the traffic class for policing. policy-map
pol_out class cl_out police flow mask src-only 1000000
32000 conform-act transmit exceed-act drop
!--- Only the source IP address is considered for flow
creation !--- on interfaces with this policy attached.
interface gigabit 1/1 !--- 1/1 is the uplink toward the
users. service-policy input pol_out !--- Traffic comes
in from users, so the policy is attached !--- in the
input direction. class-map match-all cl_in match access-
group 111 policy-map pol_in class cl_in police flow mask
dest-only 5000000 32000 conform-act transmit exceed-act
drop
!--- Only the destination IP address is considered for
flow creation !--- on interfaces with this policy
attached. interface gigabit 1/2 !--- 1/2 is the uplink
to the Internet. service-policy input pol_in
```

Para monitorar a vigilância, você pode usar estes comandos:

```
bratan# show mls qos
QoS is enabled globally
Microflow policing is enabled globally
QoS global counters:
Total packets: 10779
IP shortcut packets: 0
Packets dropped by policing: 2110223
IP packets with TOS changed by policing: 0
IP packets with COS changed by policing: 0
Non-IP packets with COS changed by policing: 0

bratan# show mls qos ip gigabitethernet 2/8
[In] Policy map is udp_policy [Out] Default.
QoS Summary [IP]: (* - shared aggregates, Mod - switch module)

Int   Mod Dir Class-map DSCP AgId Trust FlId AgForward-Pk AgPoliced-Pk
--------------------------------------------------------------------------------
Gi2/8 1   In  udp_qos   0    1*   No0 127451  2129602


bratan# show mls qos ip gigabitethernet 2/8
[In] Policy map is udp_policy [Out] Default.
QoS Summary [IP]: (* - shared aggregates, Mod - switch module)

Int   Mod Dir Class-map DSCP AgId Trust FlId AgForward-Pk AgPoliced-Pk
--------------------------------------------------------------------------------
Gi2/8 1   In  udp_qos   0    1*   No0 127755  2134670
```

Observação: os pacotes permitidos aumentaram em 304 e os pacotes em excesso aumentaram em 5068. Isso significa que o vigilante descartou 5068 pacotes e permitiu a passagem de 304. Dada a taxa de entrada de 17 Mbps, o vigilante deve passar 1/17 do tráfego. Se você comparar os pacotes descartados e encaminhados, verá que esse foi o caso: 304 / (304 + 5068) = 0,057, ou aproximadamente 1/17. Uma pequena variação é possível devido à granularidade da vigilância de hardware.

Para estatísticas de vigilância de microfluxo, use o comando **show mls ip detail**:

```
Orion# show mls ip detail
IP Destination IP Source        Protocol L4 Ports     Vlan Xtag L3-protocol
-------------+--------------+--------+-------------+----+----+-----------+
```

```
192.168.3.33192.168.2.2udp555 / 5550   1ip
192.168.3.3192.168.2.2udp63 / 630   1ip

[IN/OUT] Ports Encapsulation RW-Vlan RW-MACSourceRW-MACDestinationBytes
--------------+-------------+-------+--------------+-----------------+------------+
Fa4/11 - ----ARPA3    0030.7137.1000  0000.3333.3333314548
Fa4/11 - ----ARPA3    0030.7137.1000  0000.2222.2222314824

Packets     Age   Last SeenQoS      Police Count ThresholdLeak
------------+-----+---------+-----------+------------+---------+-----------+
6838     36   18:50:090x80  34619762*2^5 3*2^0
6844     36   18:50:090x80  34669562*2^5 3*2^0

Drop Bucket  Use-Tbl Use-Enable
----+-------+-------+----------+
YES   1968     NONO
YES   1937     NONO
```

Observação: o campo `Contagem de Polícia` mostra o número de pacotes policiados por fluxo.

Informações Relacionadas

- Configurando QoS
- Entendendo a qualidade do serviço nos Switches da família Catalyst 6000
- Suporte a Produtos de LAN
- Suporte de tecnologia de switching de LAN
- Suporte Técnico e Documentação - Cisco Systems