Vigilância de QoS nos Switches das Séries Catalyst 6500/6000

Índice

Introdução

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 o Policiamento de tráfego com o modelagem de tráfego. Ambos asseguram-se de que o tráfego fique dentro do perfil (contrato). Você não protege pacotes de fora de perfil quando você policia o tráfego. Consequentemente, você não afeta o retardo de transmissão. Você deixa cair o tráfego ou identifica-o por meio de um nível mais baixo de QoS (mapa de DSCP). Ao contrário, com modelagem de tráfego, você protege o tráfego fora de perfil e alisa as intermitências de tráfego. Isto afeta o atraso e a variação de retardo. Você pode somente aplicar o modelagem de tráfego em uma interface externa. Você pode aplicar o policiamento em ambos da interface de entrada e saída.

O Policy Feature Card do Catalyst 6500/6000 (PFC) e somente policiamento do ingresso do apoio PFC2. O PFC3 apoia o ingresso e o policiamento da 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. Refira as notas de configuração do módulo do Cisco 7600 Series Router para mais informação

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Convenções

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

Parâmetros de vigilância de QoS

Para estabelecer o policiamento, você define os vigilantes e aplica-os às portas (QoS com base na porta) ou a VLAN (QoS com base 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** — a polícia trafica para cada port/VLAN aplicado separadamente em uma base do por-fluxo.
- **Agregado** — policie o tráfego através de todas as portas aplicadas/VLAN.

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

- endereço IP de origem
- endereço IP de destino
- Protocolo da camada 4 (tal como o [UDP] do protocolo de datagrama de usuário)
- número de porta de origem
- número de porta de destino

Você pode dizer que os pacotes que combinam um conjunto específico de parâmetro definido pertencem ao mesmo fluxo. (Este é essencialmente o mesmo conceito de fluxo que aquele que o Netflow Switching usa.)

Como um exemplo, se você configura uma vigilância de microfluxo para limitar o tráfego TFTP ao 1 Mbps no VLAN1 e no VLAN3, a seguir o 1 Mbps é permitido cada fluxo no VLAN1 e 1 Mbps para cada fluxo em VLAN 3. ou seja se há três fluxos no VLAN1 e quatro fluxos no VLAN3, a vigilância de microfluxo permite cada um deste 1 Mbps dos fluxos. Se você configura um policer agregado, limita o tráfego TFTP para todos os fluxos combinados no VLAN1 e no VLAN3 ao 1 Mbps.

Se você aplica o agregado e as vigilâncias de microfluxo, QoS toma sempre a maioria de ação séria especificada pelos vigilantes. Por exemplo, se um vigilante especifica para deixar cair o pacote, mas outro especifica para marcar abaixo do pacote, o pacote é deixado cair.

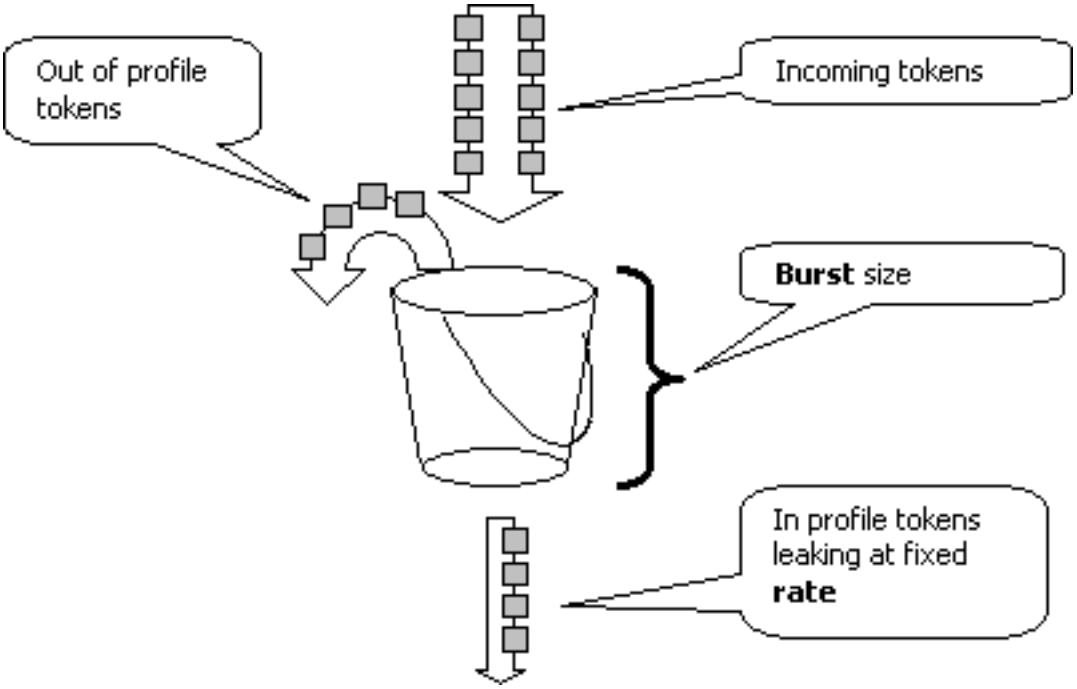
Àrevelia, as vigilâncias de microfluxo trabalham somente com (camada 3 [L3]) tráfego roteado. Para policiar construiu uma ponte sobre (camada 2 [L2]) o tráfego também, você precisa de

permitir a vigilância de microfluxo interligado. No Supervisor Engine II, você precisa de permitir a vigilância de microfluxo interligado mesmo para a vigilância de microfluxo L3.

Policiar está protocolo-ciente. Todo o tráfego é dividido em três tipos:

- IP
- Trocas de Pacote Entre Redes IPX (IPX)
- Outros

Policiar é executado no Catalyst 6500/6000 de acordo com um conceito do “vazamento de bucket”. Os tokens que correspondem aos pacotes do tráfego de entrada são colocados em uma cubeta. (Cada token representa um bit, assim que um grande pacote é representado por mais tokens do que um pacote pequeno.) Em intervalos regulares, um número definido de tokens é removido da cubeta e enviado sobre sua maneira. Se não há nenhum lugar na cubeta para acomodar pacotes de entrada, os pacotes estão considerados fora de perfil. São deixados cair ou marcados para baixo de acordo com a ação de vigilância configurada.



Nota: O tráfego não é protegido na cubeta, porque pode aparecer na imagem acima. O tráfego real não atravessa a cubeta de todo; a cubeta é usada somente para decidir se o pacote é em perfil ou fora de perfil.

Calcule parâmetros

Diversos parâmetros controlam o funcionamento do Token Bucket, como mostrado aqui:

- **Taxa** — 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 como os tokens são removidos frequentemente da cubeta. 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.
- **Explosão** — define o número máximo de tokens que a cubeta pode sustentar a qualquer altura. Para sustentar a taxa especificada de tráfego, a explosão deve ser nenhuma menos do que o tempo de taxa o intervalo. Outra consideração é que o pacote de tamanho máximo

deve caber no bucket.

Para determinar o parâmetro de intermitência, use esta equação:

- Explosão = ([bps] da taxa) * 0.00025 [sec/interval]) *ou* ([bits] do tamanho máximo do pacote), qualquer é maior.

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

- Explosão = (1,000,000 bps * 0.00025) *ou* (1518 bytes * 8 bit/byte) = 250 *ou* 12144.

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

Nota: No software de Cisco IOS®, a taxa de vigilância é definida nos bit por segundo (bps), ao contrário dos kbps no OS do catalizador (Cactos). Igualmente no Cisco IOS Software, a taxa de intermitência é definida nos bytes, ao contrário dos kilobits em Cactos.

Nota: Devido à granularidade de vigilância de hardware, à taxa exata e à explosão é arredondado ao valor suportado o mais próximo. Seja certo que o valor de intermitência é não menos que o pacote de tamanho máximo. Caso contrário, todos os pacotes maiores que o tamanho da intermitência são cancelados.

Por exemplo, se você tenta ajustar a explosão a 1518 no Cisco IOS Software, é arredondado a 1000. Isto faz com que a todos os quadros os de 1000 bytes maiores sejam deixados cair. A solução é configurar a explosão a 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 windowing pela metade para cada pacote perdido. Consequentemente, quando policiada a uma determinada taxa, a utilização de link eficaz é mais baixa do que a taxa configurada. É possível aumentar a intermitência para obter melhor utilização. Um bom começo para tal tráfego é dobrar o tamanho de intermitência. (Neste exemplo, o tamanho de intermitência é aumentado de 13 kbps a 26 kbps). Depois, monitore o desempenho e efetue os ajustes necessários.

Pela mesma razão, não se recomenda avaliar a operação de vigilância usando o tráfego orientado de conexão. Isto mostra geralmente o desempenho mais baixo do que as licenças do vigilante.

Ações policiais

Como mencionado na introdução, o vigilante pode fazer uma de duas coisas a um pacote de fora de perfil:

- deixe cair o pacote (o parâmetro da `gota na` configuração)
- marque o pacote a um DSCP mais baixo (o parâmetro policiar-`DSCP na` configuração)

Para marcar abaixo do pacote, você deve alterar o mapa dscp policiado. O DSCP policiado é ajustado à revelia para observar o pacote ao mesmo DSCP. (Nenhuma marca ocorre para baixo.)

Nota: Se os pacotes “fora de perfil” são marcados para baixo a um DSCP que esteja traçado em uma fila de saída diferente do que o DSCP original, alguns pacotes podem ser enviados a fora de serviço. Por este motivo, se a ordem de pacotes é importante, recomenda-se marcar abaixo dos

pacotes de fora de perfil a um DSCP que seja traçado à mesma fila de saída que pacotes em perfil.

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

- Quando o tráfego excede normal avalie
- Quando o tráfego excede a taxa excedente

Um exemplo do aplicativo da taxa excedente é marcar abaixo dos pacotes que excedem os pacotes normais da taxa e da gota que excedem a taxa excedente.

Recursos de vigilância apoiados pelo Catalyst 6500/6000

Como exposto na introdução, o PFC1 no Supervisor Engine 1A e o PFC2 no Supervisor Engine 2 apoiam somente o policiamento do ingresso (interface de entrada). O PFC3 no Supervisor Engine 720 apoia o ingresso e o policiamento da saída (interface externa).

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

O Supervisor Engine 1A apoia o ingresso que policia, começando com versão cactos 5.3(1) e Cisco IOS Software Release 12.0(7)XE.

Nota: Uma placa-filha PFC ou PFC2 é exigida policiando com o Supervisor Engine 1A.

O Supervisor Engine 2 apoia o ingresso que policia, começando com versão cactos 6.1(1) e Cisco IOS Software Release 12.1(5c)EX. O Supervisor Engine II apoia o parâmetro de vigilância da taxa excedente.

As configurações com os cartões de transmissão distribuídos (DFC) apoiam somente o policiamento com base na porta. Também, o policer agregado conta somente o tráfego em uma base do per-forwarding-engine, não por-sistema. O DFC e o PFC são ambos os motores da transmissão; se um módulo (placa de linha) não tem um DFC, usa um PFC como um Forwarding Engine.

Os recursos de vigilância atualizam para o Supervisor Engine 720

Nota: Se você é estranho com Regulamentação QoS do Catalyst 6500/6000, seja certo ler os parâmetros e os recursos de vigilância do Regulamentação QoS apoiados pelas seções do Catalyst 6500/6000 deste documento.

O Supervisor Engine 720 introduziu estas características novas do Regulamentação QoS:

- **Policiamento da saída**. O ingresso dos apoios do supervisor 720 que policia em uma porta ou em uma interface de VLAN. Apoia a saída que policia em uma porta ou em uma interface roteada L3 (no caso do software do sistema do Cisco IOS). Todas as portas no VLAN são policiadas na saída apesar do modo de QoS da porta (se QoS com base na porta ou QoS com base em VLAN). A vigilância de microfluxo não é apoiada na saída. As configurações de amostra são fornecidas configurar e monitoram o policiamento na seção do Cactos Software

e configuram e monitoram o policiamento na seção do Cisco IOS Software deste documento.

- **Por usuário vigilância de microfluxo**. O supervisor 720 apoia um realce à vigilância de microfluxo conhecida como a vigilância de microfluxo do usuário per. Esta característica é apoiada somente com software do sistema do Cisco IOS. Permite que você forneça uma determinada largura de banda para cada usuário (pelo endereço IP de Um ou Mais Servidores Cisco ICM NT) atrás das dadas interfaces. Isto é conseguido especificando uma máscara do fluxo dentro da política de serviços. A máscara do fluxo define que informação é usada para se diferenciar entre os fluxos. Por exemplo, se você especifica uma máscara do fluxo da fonte-somente, todo o tráfego de um endereço IP de Um ou Mais Servidores Cisco ICM NT é considerado um fluxo. Usando esta técnica, você pode policiar o tráfego pelo usuário em algumas relações (onde você configurou a política de serviços correspondente); em outras relações, você continua a usar a máscara do fluxo do padrão. É possível ter até duas máscaras diferentes do fluxo de QoS ativas no sistema em um dado momento. Você pode associar somente uma classe com a uma máscara do fluxo. Uma política pode ter até duas máscaras diferentes do fluxo.

Uma outra mudança importante no policiamento no Supervisor Engine 720 é que pode contar o tráfego pelo comprimento L2 do quadro. Isto difere do Supervisor Engine 2 e do Supervisor Engine 1, que contam quadros IP e IPX por seu comprimento L3. Com alguns aplicativos, comprimento L2 e L3 não pode ser consistente. Um exemplo é um pequeno pacote L3 dentro de um grande quadro L2. Neste caso, o Supervisor Engine 720 pode indicar uma taxa de tráfego policiada levemente diferente em comparação ao Supervisor Engine 1 e ao Supervisor Engine 2.

Configurar e monitore o policiamento no Cactos Software

A configuração de vigilância para Cactos consiste em três etapas principal:

1. Defina um vigilante — a taxa de tráfego, a taxa excedente (se aplicável), a explosão, e a ação de vigilância normais.
2. Crie um QoS ACL para selecionar o tráfego para policiar, e anexe um vigilante a este ACL.
3. Aplique o QoS ACL às portas necessárias ou aos VLAN.

Este exemplo mostra como policiar todo o tráfego à porta 111 UDP 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 exemplo seguinte é o mesmo; contudo, neste exemplo, você anexa o vigilante a um VLAN. A porta 2/8 pertence ao VLAN20.

Nota: Você precisa de mudar a porta QoS ao modo VLAN-`baseado`. Faça isto com o **comando set port qos**.

Este vigilante avalia o tráfego de todas as portas nesse VLAN configurado para QoS com base 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 dos pacotes de fora de perfil deixando cair com DSCP 32, marque-os para baixo a 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 de saída que policia para o Supervisor Engine 720 somente. Mostra como policiar todo o tráfego IP que parte no VLAN3 ao agregado do 10 Mbps.

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.
```

Use o **policed-dscp-map do tempo de execução dos mapas dos qos da mostra** para ver o mapa dscp policiado corrente.

Use o **policer runtime dos qos da mostra {***policer_name* **| tudo}** para verificar os parâmetros do vigilante. Você pode igualmente ver o QoS ACL a que o vigilante é anexado.

Nota: Com Supervisor Engine 1 e 1a, não é possível ter o policiamento de policeres agregados das estatísticas de individual. Para ver o por-sistema que policia estatísticas, 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 ver o agregado que policia estatísticas em uma base do por-vigilante com o **comando show qos statistics aggregate-policer**.

Para este exemplo, um gerador de tráfego é anexado à porta 2/8. Envia o 17 Mbps do tráfego UDP com porta do destino 111. Você espera o vigilante deixar cair 16/17 do tráfego, assim que o 1 Mbps deve ir completamente:

```
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
```

Nota: Observe que os pacotes permitidos aumentaram por 65 e pacotes adicionais aumentaram por 1090. Isto significa que o vigilante deixou cair 1090 pacotes e 65 permitidos para passar completamente. Você pode calcular que 65/(1090 + 65) = 0.056, ou aproximadamente 1/17.

Consequentemente, o vigilante trabalha corretamente.

Configurar e monitore o policiamento no Cisco IOS Software

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

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

Considere o mesmo exemplo que isso fornecido na seção configura e monitora o policiamento no Cactos Software, mas agora com Cisco IOS Software. Para este exemplo, você tem um gerador de tráfego anexado à porta 2/8. Envia o 17 Mbps do tráfego UDP com porta do 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 policeres agregados no Cisco IOS Software: nomeado e por interface. O vigilante agregado nomeado policia o tráfego combinado de todas as relações a que é aplicado. Este é o tipo usado no exemplo acima. O per-interface policer policia o tráfego separadamente em cada interface de entrada a que é aplicado. Um vigilante por interface é definido na configuração de mapa de política. Considere este exemplo, que tem um policer agregado por interface:

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.
```

As vigilâncias de microfluxo são definidas dentro da configuração de mapa de política, como são policeres agregados por interface. No exemplo abaixo, cada fluxo do host 192.168.2.2 que entra o VLAN2 é policiado a 100 kbps. Todo o tráfego de 192.168.2.2 é policiado ao agregado de 500 kbps. O VLAN2 inclui as relações fa4/11 e fa4/12:

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.
```

O exemplo abaixo mostra uma configuração de saída que policia para o Supervisor Engine 720. Estabelece o policiamento de todo o tráfego de saída no Gigabit Ethernet da relação 8/6 a 100 kbps:

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.
```

O exemplo abaixo mostra uma configuração para o usuário per. que policia para o Supervisor Engine 720. Trafique que vem dentro dos usuários atrás da porta 1/1 para o Internet é policiado ao 1 Mbps pelo usuário. Trafique que vem do Internet para os usuários é policiado ao 5 Mbps

pelo 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 o policiamento, 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
```

Nota: Os pacotes permitidos aumentaram por 304 e os pacotes adicionais aumentaram por 5068. Isto significa que o vigilante deixou cair 5068 pacotes e 304 permitidos para passar completamente. Dado a taxa de entrada do 17 Mbps, o vigilante deve passar 1/17 do tráfego. Se você compara os pacotes deixados cair e enviados, você vê que este foi o caso: 304/(304 + 5068) = 0.057, ou aproximadamente 1/17. Alguma variação pequena é possível devido à granularidade de 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
```

Nota: `O campo de contagem da polícia` mostra o número de pacotes policiados pelo 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