# QoS-toezicht op Catalyst 6500/6000 Series Switches

## Inhoud



## Inleiding

QoS-toezicht op een netwerk bepaalt of het netwerkverkeer binnen een bepaald profiel (contract) valt. Dit kan ertoe leiden dat buiten-profiel verkeer daalt of wordt gemarkeerd naar een andere DSCP-waarde (gedifferentieerd servicecopoint) om een contractueel serviceniveau af te dwingen. (DSCP is een maat voor het QoS-niveau van het kader.)

Verwar traffic policing niet met traffic shaping. Beiden verzekeren dat het verkeer binnen het profiel (contract) blijft. Je buffert geen buiten-profiel pakketten wanneer je het verkeer controleert. Daarom heeft u geen invloed op de transmissievertraging. U laat het verkeer vallen of mark het met een lager QoS-niveau (DSCP-markering). In tegenstelling tot, met traffic shaping, buffer je out-of-profile verkeer en bevrijd je de verkeerscrisis. Dit beïnvloedt de vertraging en vertragingsvariatie. U kunt alleen traffic shaping op een uitgaande interface toepassen. U kunt toezicht op zowel inkomende als uitgaande interfaces toepassen.

Catalyst 6500/6000 beleidsfunctiekaart (PFC) en PFC2 ondersteunen alleen inbraaktoezicht. De PFC3 ondersteunt innerings- en noodpolitie. Traffic Shaping wordt alleen ondersteund op bepaalde WAN-modules voor de Catalyst 6500/7600 Series, zoals de optische servicesmodules (OSM's) en FlexWAN-modules. Raadpleeg de Cisco 7600 Series routermodule Configuration voor meer informatie

## Voorwaarden

### Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

### Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

### Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

## QoS-parameters voor toezicht

Om beleid in te stellen, definieert u de beleidsmakers en past u ze toe op poorten (op poorten gebaseerde QoS) of op VLAN's (op VLAN gebaseerde QoS). Elke politieman definieert een naam, type, snelheid, uitbarsting en acties voor in-profile en out-of-profile verkeer. Beleidsgegevens op Supervisor Engine II ondersteunen ook parameters voor buitensporige snelheden. Er zijn twee soorten politiemensen: microflow en aggregaat.

- **Microflow**-politieverkeer voor elke toegepaste poort/VLAN afzonderlijk op een per-flow basis.
- Geaggregeerd-politieverkeer over alle toegepaste poorten/VLAN's.

Elke politieman kan worden toegepast op meerdere poorten of VLAN's. De stroom wordt gedefinieerd met behulp van deze parameters:

- IP-adres bron
- IP-adres van bestemming
- Layer 4 Protocol (zoals User Datagram Protocol [UDP])
- bronpoortnummer
- bestemming poortnummer

U kunt zeggen dat pakketten die overeenkomen met een bepaalde reeks gedefinieerde parameters tot dezelfde stroom behoren. (Dit is in wezen hetzelfde stroomconcept als dat van NetFlow-switching.)

Als u bijvoorbeeld een microflow-politieer configureren om het TFTP-verkeer te beperken tot 1 Mbps op VLAN 1 en VLAN 3, dan is 1 Mbps toegestaan voor elke stroom in VLAN 1 en 1 Mbps voor elke stroom in VLAN 3. Met andere woorden, als er drie stromen in VLAN 1 en vier stromen in VLAN 3 zijn, staat de microflow-agent elk van deze stromen 1 Mbps toe. Als u een verzamelpolitie vormt, beperkt het TFTP-verkeer voor alle stromen die op VLAN 1 en VLAN 3 tot 1 Mbps worden gecombineerd.

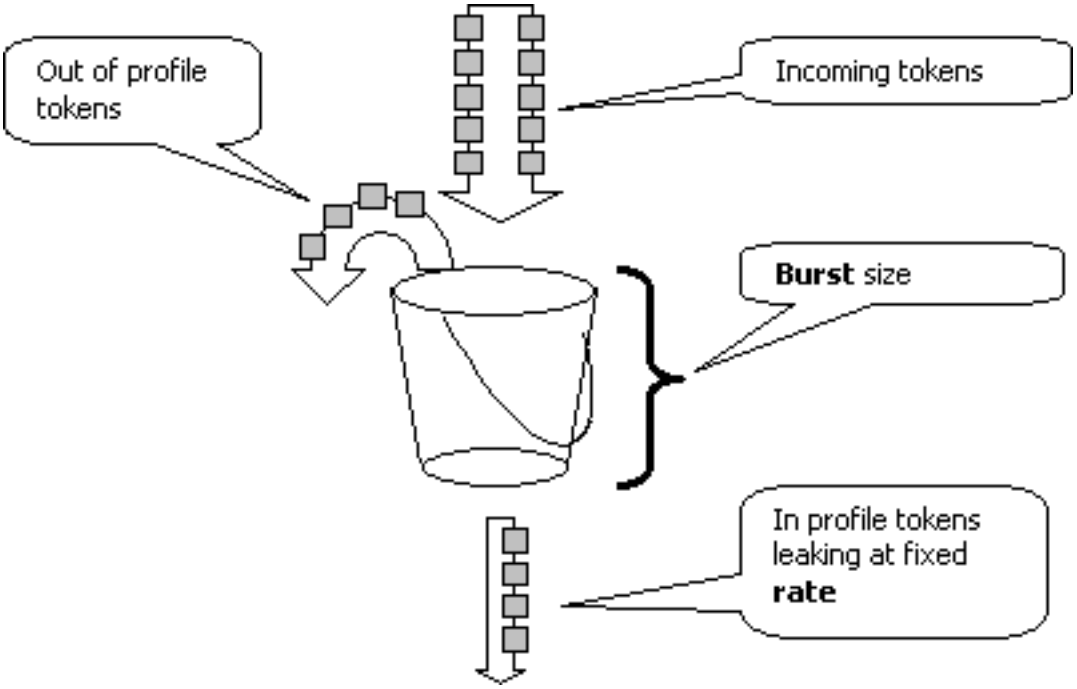
Als je zowel politie-agenten op basis van aggregaten als microflow toepast, neemt QoS altijd de ernstigste actie die door de politie wordt gespecificeerd. Als bijvoorbeeld een politieagent aangeeft het pakje te laten vallen maar een andere poster geeft aan om het pakje omlaag te halen, dan wordt het pakje ingetrokken.

Standaard werken microflow-politiemensen alleen met routeerd (Layer 3 [L3]) verkeer. Om ook het overbrugde verkeer (Layer 2 [L2]) te kunnen controleren moet u een overbrugd microflow-toezicht mogelijk maken. Op Supervisor Engine II moet u een overbrugging microflow-toezicht mogelijk maken, zelfs voor L3 microflow-toezicht.

Toezicht is protocol-bewust. Al het verkeer is verdeeld in drie types:

- IP
- Internetwork Packet Exchange (IPX)
- Other (Overig)

Toezicht wordt op Catalyst 6500/6000 uitgevoerd volgens een "lekkage emmer"-concept. Tokens die overeenkomen met inkomende verkeerspakketten worden in een emmer geplaatst. (Elke token vertegenwoordigt een beetje, dus een groot pakje wordt weergegeven door meer penningen dan een klein pakketje.) Op gezette tijden worden een bepaald aantal penningen uit de emmer verwijderd en onderweg verzonden. Als er geen plaats in de emmer is om binnenkomende pakketten op te nemen, worden de pakketten als buiten-profiel beschouwd. Ze worden volgens de ingestelde politieactie afgezet of gemarkeerd.




**Opmerking:** het verkeer is niet gebufferd in de emmer omdat het in de afbeelding hierboven kan verschijnen. het werkelijke verkeer gaat helemaal niet door de emmer; de emmer wordt alleen gebruikt om te bepalen of het pakje in profiel of buiten profiel is.

## Berekenen parameters

Er zijn verschillende parameters die de werking van de symbolische emmer regelen, zoals hieronder wordt aangegeven:

- **Rate**-definieert hoeveel tokens elk interval worden verwijderd. Dit stelt in feite de politiekoers in. Alle verkeer onder de snelheid wordt in profiel beschouwd.
- **Interval**-definieert hoe vaak penningen uit de emmer worden verwijderd. De interval is vastgesteld op 0,00025 seconden, dus worden penningen uit een emmer van 4,000 keer per seconde verwijderd. Het interval kan niet worden gewijzigd.
- **Burst**—definieert het maximale aantal penningen dat de emmer op ieder moment kan bevatten. Om de opgegeven verkeerssnelheid te kunnen handhaven, moet de barst niet minder zijn dan de snelheidstijden van het interval. Een andere overweging is dat het pakje met een maximale grootte in de emmer moet passen.

Om de burst parameter te bepalen, gebruikt u deze vergelijking:

- Burst = (Snelheid [bps]) * 0,00025 [sec/interval] *of* (maximale pakketgrootte [bits]), welke

groter is.

Bijvoorbeeld, als u de minimum burst waarde wilt berekenen nodig om een tarief van 1 Mbps op een netwerk Ethernet te handhaven, wordt het tarief gedefinieerd als 1 Mbps en de maximum Ethernet pakketgrootte is 1518 bytes. De vergelijking is:

- Burst = (1.000.000 bps * 0.0025) *of* (1518 bytes * 8 bits/bytes) = 250 *of* 12144.

Het grotere resultaat is 12144, wat je tot 13 kbps doet.

**Opmerking:** In Cisco IOS® Software is de politiesnelheid gedefinieerd in bits per seconde (bps), in tegenstelling tot kbps in Catalyst OS (CatOS). Ook in Cisco IOS-software is de barstsnelheid gedefinieerd in bytes, in tegenstelling tot kilobits in CatOS.

**Opmerking:** Vanwege de granulariteit van het hardware-toezicht worden de exacte snelheid en uitbarsting tot de dichtstbijzijnde ondersteunde waarde afgerond. Verzeker dat de burst waarde niet minder is dan het maximum groote pakje. Anders worden alle pakketten die groter zijn dan de barstgrootte, verbroken.

Als u bijvoorbeeld probeert de barst in Cisco IOS-software op 1518 in te stellen, wordt deze afgerond op 1000. Hierdoor worden alle frames die groter zijn dan 1000 bytes gevallen. De oplossing is om de barst aan 2000 te configureren.

Wanneer u de burst rate configureren houdt u er rekening mee dat sommige protocollen (zoals TCP) een flow-control mechanisme implementeren dat op pakketverlies reageert. TCP bijvoorbeeld verlaagt het venster met de helft voor elk verloren pakket. Als de controle in een bepaald tempo wordt uitgevoerd, is de effectieve benutting van de link dus lager dan het geconfigureerde percentage. Je kan de barst verhogen om beter gebruik te maken. Een goede start voor dit soort verkeer is het verdubbelen van de barstgrootte. (In dit voorbeeld, wordt de burst grootte verhoogd van 13 kbps tot 26 kbps). Daarna moet u de prestaties controleren en indien nodig verdere aanpassingen uitvoeren.

Om dezelfde reden wordt het niet aanbevolen om de politieverwerking te benchmarken met op verbindingen gericht verkeer. Dit laat over het algemeen een lagere prestatie zien dan de politieagent toestaat.

## Politieacties

Zoals in de Inleiding vermeld, kan de politieagent één van twee dingen doen aan een out-of-profile pakket:

- laat het pakje vallen (de parameter in de configuratie `laten vallen`)
- mark het pakket naar een lagere DSCP (de parameter `met` behulp `van een` gepolitie-`dscp` in de configuratie)

Om het pakket te markeren, moet u de gepolitie DSCP map wijzigen. De politie-DSCP is standaard ingesteld om het pakket naar dezelfde DSCP terug te brengen. (Er is geen markering opgetreden.)

**N.B.:** Als "out-of-profile" pakketten gemarkeerd zijn naar een DSCP die in een andere uitvoerwachtrij dan de oorspronkelijke DSCP is verdeeld, kunnen sommige pakketten uit bestelling worden verzonden. Om deze reden, als de volgorde van pakketten belangrijk is, wordt het aanbevolen om buiten-profiel pakketten te markeren naar een DSCP die in kaart wordt gebracht aan de zelfde uitvoerrij zoals in-profiel pakketten.

Op Supervisor Engine II, die overbelasting ondersteunt, zijn twee triggers mogelijk:

- Als het verkeer groter is dan het normale tarief
- Als het verkeer groter is dan de

Een voorbeeld van de toepassing van overtollige snelheid is om pakketten te markeren die de normale snelheid overschrijden en pakketten te laten vallen die de overtollige snelheid overschrijden.

## Bedieningsfuncties die worden ondersteund door Catalyst 6500/6000

Zoals in de Inleiding vermeld, steunt PFC1 op de Supervisor Engine 1a en PFC2 op Supervisor Engine 2 alleen inbraakinterface-toezicht (inkomende interface). PFC3 op Supervisor Engine 720 ondersteunt zowel inloop als stress (uitgaande interface) toezicht.

De Catalyst 6500/6000 ondersteunt tot 63 microflow-politiers en tot 1023 geaggregeerde politiers.

De Supervisor Engine 1a ondersteunt inbraaktoezicht, te beginnen met CatOS versie 5.3(1) en Cisco IOS-softwarerelease 12.0(7)XE.

**Opmerking:** Er is een PFC- of PFC2-dochterkaart vereist voor het toezicht op Supervisor Engine 1a.

Supervisor Engine 2 ondersteunt inbraaktoezicht, te beginnen met CatOS versie 6.1(1) en Cisco IOS-softwarerelease 12.1(5c)EX. De Supervisor Engine II ondersteunt de overtollige snelheidsparameter.

Configuraties met Distributed Forwarding Cards (DFC's) ondersteunen alleen poortgebaseerd toezicht. Bovendien telt de agent alleen het verkeer per expediteur, niet per systeem. DFC en PFC zijn beide verzendingsmotoren; als een module (lijnkaart) geen DFC heeft, gebruikt zij een PFC als een verzendende motor.

## Functies voor toezicht bijwerken voor Supervisor Engine 720

**N.B.:** Als u niet bekend bent met Catalyst 6500/6000 QoS toezicht, zorg er dan voor dat u de QoS controle parameters en functies voor toezicht leest die worden ondersteund door Catalyst 6500/6000 delen van dit document.

De Supervisor Engine 720 introduceerde deze nieuwe QoS politie-functies:

- **Garnalen**. De supervisor 720 ondersteunt inbraaktoezicht op een poort of VLAN-interface. Het ondersteunt toezicht op stress op een poort of L3 routed Interface (in het geval van Cisco IOS System Software). Alle poorten in het VLAN worden gecontroleerd op stress ongeacht de poort-QoS-modus (of op poort gebaseerde QoS of VLAN-gebaseerde QoS). Toezicht op microflow wordt niet ondersteund op stress. Samsung-configuraties worden geleverd in de sectie Configureren en controleren van de functies in het vak CatOS-software en Toezicht instellen en bewaken in het gedeelte Cisco IOS-software van dit document.
- **Toezicht per gebruiker**. De supervisor 720 ondersteunt een verbetering om te microflow-toezicht, gekend als microflow-toezicht per gebruiker. Deze optie wordt alleen ondersteund

door Cisco IOS-systeemsoftware. Het staat u toe om een bepaalde bandbreedte voor elke gebruiker (per IP-adres) achter bepaalde interfaces te bieden. Dit wordt bereikt door een stroommasker binnen het servicebeleid op te geven. Het stroommasker definieert welke informatie wordt gebruikt om onderscheid te maken tussen de stromen. Bijvoorbeeld, als u een bron-slechts stroommasker specificeert, wordt al verkeer van één IP adres als één stroom beschouwd. Met behulp van deze techniek kunt u het verkeer per gebruiker op bepaalde interfaces controleren (waar u het corresponderende servicebeleid hebt ingesteld); op andere interfaces, blijft u het standaardstroommasker gebruiken. Het is mogelijk om op een bepaald moment maximaal twee verschillende QoS-stroommaskers actief in het systeem te hebben. U kunt slechts één klasse associëren met één stroommasker. Een beleid kan tot twee verschillende stromingsmaskers hebben.

Een andere belangrijke verandering in het toezicht op Supervisor Engine 720 is dat het verkeer kan tellen met de L2 lengte van het frame. Dit verschilt van Supervisor Engine 2 en Supervisor Engine 1, die IP en IPX frames tellen door hun L3 lengte. Bij sommige toepassingen zijn L2 en L3 length mogelijk niet consistent. Een voorbeeld is een klein L3 pakje in een groot L2 frame. In dit geval kan Supervisor Engine 720 een enigszins verschillend verkeerstarief weergeven in vergelijking met Supervisor Engine 1 en Supervisor Engine 2.

## Toezicht instellen en bewaken in CatOS-software

De politieconfiguratie van CatOS bestaat uit drie belangrijke stappen:

1. Defineer een politieagent—de normale verkeerssnelheid, de overtollige snelheid (indien van toepassing), de barst, en de politieactie.
2. Maak een QoS ACL om verkeer aan politie te selecteren en voeg een politieman aan deze ACL toe.
3. Pas QoS ACL op de gewenste poorten of VLAN's toe.

Dit voorbeeld laat zien hoe je al het verkeer naar UDP-poort 111 op poort 2/8 moet controleren.

**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.
```

Het volgende voorbeeld is hetzelfde. in dit voorbeeld, hecht u de politieagent aan een VLAN. Port 2/8 behoort tot VLAN 20.

**Opmerking:** U moet de poort-QoS naar de `VLAN-gebaseerde` modus wijzigen. Doe dit met de **ingestelde poort qos** opdracht.

Deze politieagent evalueert verkeer van alle havens in dat VLAN dat voor op VLAN gebaseerde QoS wordt gevormd:

**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.
```

Daarna, in plaats van buiten-profiel pakketten met DSCP 32 te laten vallen, markeert ze terug naar een DSCP van 0 (best inspanning).

**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.
```

Dit voorbeeld toont de configuratie voor spanning slechts voor Supervisor Engine 720. Het toont hoe om al het uitgaande IP-verkeer op VLAN 3 tot 10 Mbps te controleren samen.

**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.
```

Gebruik **Show qos maps uit meerdere** gebieden **met toezicht-dscp-map** om de huidige gepolitieerde DSCP-kaart te zien.

Gebruik **show qos politierelentime {*politier_name* | alle )** om de parameters van de politieagent te verifiëren. U kunt ook QoS ACL zien waaraan de politieagent is bevestigd.

**Opmerking:** Met Supervisor Engine 1 en 1a is het niet mogelijk om politiestatistieken te hebben voor individuele geaggregeerde politieagenten. Om de politiestatistieken per systeem te bekijken, gebruikt u deze opdracht:

```
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
```

Gebruik deze opdracht voor het controleren van politiestatistieken van microflow:

```
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)
```

Met Supervisor Engine II kan je geaggregeerde politiestatistieken per beleidsbasis bekijken met de **opdracht** om **qos statistieken samen te voegen-politieman**.

Bijvoorbeeld, wordt een verkeersgenerator aangesloten aan haven 2/8. Het verstuurt 17 Mbps van UDP verkeer met bestemmingspoort 111. U verwacht dat de politieman 16/17 van het verkeer zal laten vallen, zodat 1 Mbps door moet:

```
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
```

**Opmerking:** Let op dat het aantal toegestane pakketten gestegen is met 65 en het aantal te grote pakketten gestegen is met 1090. Dit betekent dat de politieagent 1090 pakketten heeft laten vallen en 65 door heeft laten gaan. Je kunt berekenen dat 65 / (1090 + 65) = 0,056, of grofweg 1/17. Daarom werkt de politieagent correct.

# Toezicht configureren en bewaken in Cisco IOS-software

De configuratie voor toezicht in Cisco IOS-software omvat deze stappen:

1. Defineer een politieagent.
2. Maak een ACL om verkeer naar politie te selecteren.
3. Defineert een class map voor het selecteren van verkeer met ACL en/of DSCP/IP voorrang.
4. Defineer een dienstbeleid dat klasse gebruikt, en pas de politieman op een gespecificeerde klasse toe.
5. Pas het servicebeleid op een poort of VLAN toe.

Neem hetzelfde voorbeeld als dat in de sectie Toezicht instellen en bewaken in CatOS-software, maar nu met Cisco IOS-software. Bijvoorbeeld, u hebt een verkeersgenerator aangesloten aan haven 2/8. Het verstuurt 17 Mbps van UDP verkeer met bestemmingspoort 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.
```

Er zijn twee soorten geaggregeerde politiers in Cisco IOS-software: **genoemd** en **per interface**. De genoemde coördinator controleert het verkeer dat wordt gecombineerd van alle interfaces waarop het wordt toegepast. Dit is het type dat in het bovenstaande voorbeeld wordt gebruikt. De per-interface politieman controleert afzonderlijk verkeer op elke inkomende interface waarop het wordt toegepast. Een per-interface politieman wordt gedefinieerd in de beleidskaartconfiguratie. Neem dit voorbeeld, dat een per-interface geaggregeerde politieagent heeft:

**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.
```

Microflow-politiemensen worden gedefinieerd binnen de beleidskaartconfiguratie, evenals per-interface geaggregeerde politiemensen. In het onderstaande voorbeeld wordt elke stroom van host 192.168.2.2 die in VLAN 2 komt, aan 100 kbps gecontroleerd. Al het verkeer vanaf 192.168.2.2 wordt beperkt tot 500 kbps aggregaat. VLAN 2 omvat interfaces fa4/11 en 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.
```

Het voorbeeld hieronder toont een configuratie voor spanning toezicht voor Supervisor Engine 720. Het voert de bewaking van al het uitgaande verkeer op interface Gigabit Ethernet 8/6 tot 100 kbps in:

**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.
```

Het voorbeeld hieronder toont een configuratie voor per-gebruiker toezicht op de Supervisor Engine 720. Verkeersverkeer dat van gebruikers achter poort 1/1 naar Internet komt, wordt naar 1 Mbps per gebruiker gecontroleerd. Het verkeer dat van Internet naar de gebruikers komt wordt gecontroleerd tot 5 Mbps per gebruiker:

**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
```

U kunt toezicht houden op het toezicht op deze opdrachten:

```
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
```

**Opmerking:** toegestane pakketten zijn met 304 toegenomen en het aantal pakketten is met 5068 toegenomen. Dit betekent dat de politieagent 5068 pakketten heeft laten vallen en 304 heeft laten doorlopen. Gezien het invoertarief van 17 Mbps, zou de politieagent 1/17 van het verkeer moeten passeren. Als u de geworpen en verzonden pakketten vergelijkt, ziet u dat dit het geval is geweest: 304 / (304 + 5068) = 0,057, of grofweg 1/17. Een kleine variatie is mogelijk als gevolg van de granulariteit van de hardwarekwiniging.

Voor microflow politiestatistieken, gebruik de opdracht **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
```

**Opmerking:** het veld `Politieteller` toont het aantal politiepakketten per stroom.

# Gerelateerde informatie

- QoS configureren
- Inzicht op Quality-of-Service op Catalyst 6000 Series Switches
- LAN-productondersteuning
- Ondersteuning voor LAN-switching technologie
- Technische ondersteuning en documentatie – Cisco Systems