# QOS-toezicht en -markering met Catalyst 4000/4500 IOS-gebaseerde Supervisor Engine

## Inhoud



## Inleiding

De controlemodule bepaalt of het verkeersniveau binnen het gespecificeerde profiel (contract) valt. Met de controlemodule kan het out-of-profile verkeer worden weggelaten of kan het verkeer worden afgedrukt op een andere DSCP-waarde (Differential Services Code Point) om gecontracteerd serviceniveau af te dwingen. DSCP is een maat voor het QoS-niveau (Quality of Service) van het pakket. Samen met DSCP worden IP-voorrang en serviceklasse (CoS) ook gebruikt om het QoS-niveau van het pakket over te brengen.

Toezicht moet niet worden verward met traffic shaping, alhoewel beide ervoor zorgen dat het verkeer binnen het profiel blijft (contract). Toezicht buffert het verkeer niet, zodat de transmissievertraging niet wordt beïnvloed. In plaats van buiten-profiel pakketten te bufferen, zal de politie ze laten vallen of met een ander QoS-niveau (DSCP-markering) markeren. Traffic Shaping buffert buiten profiel verkeer en zorgt voor een vlotte doorbraak, maar beïnvloedt de vertraging en de vertragingsvariatie. Shaping kan slechts op een uitgaande interface worden toegepast, terwijl de controle op zowel inkomende als uitgaande interfaces kan worden toegepast.

Catalyst 4000/4500 met Supervisor Engine 3, 4 en 2+ (SE3, SE4, SE2+ van nu af in dit document) ondersteunt toezicht in inkomende en uitgaande richtingen. Verkeersvormingen worden ook ondersteund. Dit document heeft echter alleen betrekking op toezicht en markering. Markeren is een proces om het QoS-pakketniveau aan de hand van een beleid te wijzigen.

## 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.

## QoS-toezicht- en markeerparameters

Het toezicht wordt ingesteld door de QoS-beleidskaarten te definiëren en ze toe te passen op havens (op poorten gebaseerde QoS) of VLAN's (op VLAN's gebaseerde QoS). De politie wordt gedefinieerd door parameters voor snelheid en uitbarsting, evenals acties voor in-profile en out-of-profile verkeer.

Er worden twee soorten politiemensen ondersteund: geaggregeerd en per interface. Elke politieman kan worden toegepast op meerdere poorten of VLAN's.

De verzamelpolitie handelt op het verkeer over alle gebruikte poorten/VLAN's. Bijvoorbeeld, wij passen de verzamelpolitie toe om het Transformer File Transfer Protocol (TFTP)-verkeer op VLAN's 1 en 3 te beperken tot 1 Mbps. Een dergelijke politieman zal 1 Mbps TFTP-verkeer in VLAN's 1 en 3 samen toestaan. Als we een per-interface politieman toepassen, zal het TFTP verkeer op VLANs 1 en 3 tot 1 Mbps elk beperken.

**Opmerking:** Als zowel de instap- als het toezicht op de uitgang op een pakje is toegepast, wordt de ernstigste beslissing genomen. Dat wil zeggen, als de ingangspolitieagent specificeert om het pakket te laten vallen en de ress politieagent aangeeft om het pakket te markeren, wordt het pakje ingetrokken. Tabel 1 vat de QoS-actie op het pakket samen wanneer het wordt behandeld door zowel het ingangsbeleid als het toegangsbeleid.

**Tabel 1:** QoS-actie afhankelijk van inDRUK- en Egress-beleid

| | **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$_e$ | Markdown$_e$ |
| **Mark$_e$** | Mark$_e$ | Drop | Mark$_e$ | Mark$_e$ |

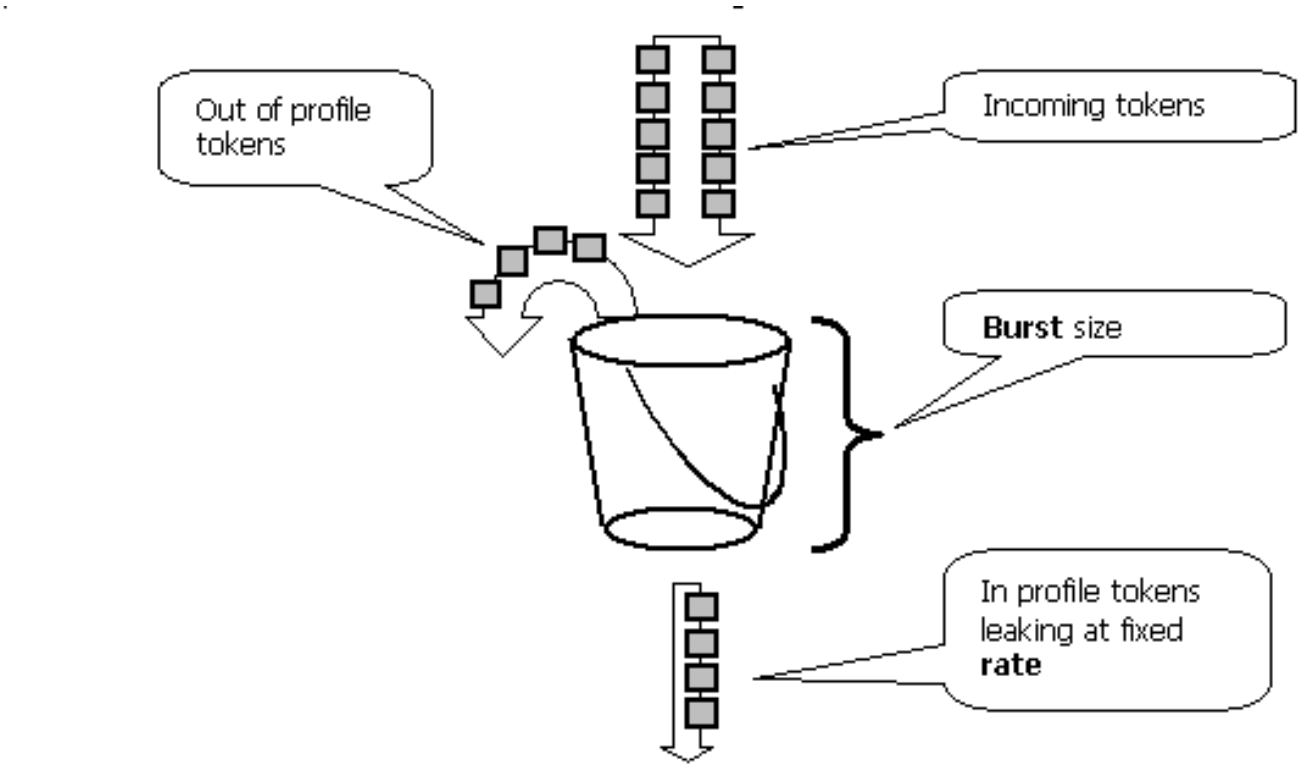
De hardware van Catalyst 4000 SE3, SE4, SE2+ QoS wordt op dusdanige wijze geïmplementeerd dat de echte markering van het pakje pas na de noodpolitie optreedt. Dit betekent dat zelfs als het ingangsbeleid het pakje opmerkingen (door de politie-markering of de normale markering), het persbeleid nog steeds pakketten ziet die gemarkeerd zijn met het oorspronkelijke QoS-niveau. Het striktiebeleid zal het pakket zien alsof het niet is gemarkeerd met het toegangsbeleid. Dit betekent het volgende:

- Bovenmaatse markering staat bovenaan de markering.
- Het voedingsbeleid kan niet op nieuwe QoS-niveaus worden afgestemd die worden gewijzigd door het aanbrengen van een markering.

Andere belangrijke implicaties zijn:

- Het is niet mogelijk om binnen dezelfde verkeersklasse in hetzelfde beleid een markering en markering aan te brengen.
- Geaggregeerde politiemensen zijn per richting. Als er dus een totale politieagent wordt toegepast op zowel de intrede als de uitgang, dan zullen er twee geaggregeerde politiemensen zijn, één op de input en één op de productie.
- Wanneer een geaggregeerd beleid binnen het beleid op VLAN's en op de fysieke interface wordt toegepast, zullen er in feite twee geaggregeerde politiers zijn - één voor de VLAN-interfaces en één voor fysieke interfaces. Op dit moment is het niet mogelijk om VLAN-interfaces en fysieke interfaces samen te controleren.

Toezicht in Catalyst 4000 SE3, SE4, SE2+ voldoet aan het concept van lekkage emmer, zoals wordt geïllustreerd in het onderstaande model. Tokens die overeenkomen met binnenkomende verkeerspakketten worden in een emmer geplaatst (# penningen = grootte van het pakket). Op regelmatige tijdstippen wordt een bepaald aantal penningen (afgeleid van de geconfigureerde snelheid) uit de emmer verwijderd. Als er geen plaats in de emmer is om een inkomend pakje aan te passen, wordt het pakje als buiten profiel beschouwd en volgens de ingestelde politieactie afgezet of gemarkeerd.




Er zij op gewezen dat het verkeer niet in de emmer gebukt gaat, zoals het in het bovenstaande model kan voorkomen. Het echte verkeer stroomt helemaal niet via de emmer. De emmer wordt alleen gebruikt om te bepalen of het pakje in profiel of buiten profiel is.

Merk op dat de exacte hardwareimplementatie van toezicht anders kan zijn, functioneel voldoet het aan het bovenstaande model.

De volgende parameters regelen de werking van de politie:

- Rate definieert hoeveel penningen met 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. Interval wordt vastgesteld op 16 nanoseconden (16 sec *10-9). Interval kan niet worden gewijzigd.

- Burst definieert de maximale hoeveelheid penningen die de emmer op elk moment kan bevatten.

Raadpleeg het gedeelte Vergelijkende controle en markering op Catalyst 6000 en Catalyst 4000/4500 IOS gebaseerde Supervisor Engine aan het eind van dit document voor verschillen in uitbarsting tussen Catalyst 6000 en Catalyst 4000 SE3, SE4, SE2+.

De politieagent zorgt ervoor dat als u een periode (van nul tot oneindig) onderzoekt, de agent nooit meer dan

```
<rate> * <period> + <burst-bytes> + <1 packet> bytes
```

van het verkeer door de politieagent in die periode.

De hardware van Catalyst 4000 SE3, SE4, SE2+ QoS heeft bepaalde granulariteit voor het toezicht. Afhankelijk van de ingestelde snelheid is de maximale afwijking van de snelheid 1,5% van de snelheid.

Bij het configureren van burst rate moet u er rekening mee houden dat sommige protocollen (zoals TCP) flow-control mechanismen implementeren die op pakketverlies reageren. TCP vermindert bijvoorbeeld het venster met de helft voor elk verloren pakket. Wanneer u een bepaalde snelheid hebt aangehouden, is de effectieve benutting van de link lager dan de ingestelde snelheid. We kunnen de barsten verhogen om een beter gebruik te bereiken. Een goede start voor dergelijk verkeer zou zijn om de burst in te stellen op tweemaal de hoeveelheid verkeer die tijdens de Ronde Trip Time (RTT) met de gewenste snelheid wordt verstuurd. Om dezelfde reden wordt het niet aanbevolen om de politietoezicht te benchmarken met op verbindingen gericht verkeer, omdat de prestaties doorgaans lager zijn dan toegestaan door de politieagent.

**Opmerking:** ook het verkeer zonder verbindingen kan op politiewerk anders reageren. Network File System (NFS) gebruikt bijvoorbeeld blokken, die kunnen bestaan uit meer dan één User Datagram Protocol-pakket (UDP). Een pakje dat is gevallen, kan veel pakketten (een volledig blok) laten oplopen om opnieuw te worden verzonden.

Bijvoorbeeld, het volgende is een berekening van de burst voor een TCP sessie, met een politiesnelheid van 64 Kbps en een TCP RTT van 0,05 seconden:

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

**Opmerking: <**burst**>** is voor één TCP-sessie, dus moet het worden geschaald om het verwachte aantal sessies via de politieagent te gemiddeld. Dit is slechts een voorbeeld, dus in elk geval moet je de verkeers-/toepassingsvereisten en het gedrag in vergelijking met de beschikbare middelen evalueren om te kunnen kiezen voor parameters voor toezicht.

De politieactie is om het pakje te laten vallen (of te laten vallen) of de DSCP van het pakje te wijzigen (of af te sluiten). Om het pakket te markeren, moet de gepolitie DSCP map worden aangepast. De standaard gecontroleerde DSCP opmerkingen van het pakje aan dezelfde DSCP, dat wil zeggen dat er geen markering onderaan staat.

**Opmerking:** pakketten kunnen zonder bestelling worden verzonden als een out-of-profiel pakket is gemarkeerd naar een DSCP in een andere wachtrij dan de oorspronkelijke DSCP. Om deze reden, als het bestellen van pakketten belangrijk is, wordt het aanbevolen om buiten-profiel pakketten aan DSCP te markeren die aan de zelfde uitvoerrij zoals in-profielpakketten in kaart zijn gebracht.

# Toezicht- en markeringsfuncties die worden ondersteund door Catalyst 4000/4500 IOS-gebaseerde Supervisor Engine

Zowel de ingang (inkomende interface) als de spanning (uitgaande interface) worden ondersteund op Catalyst 4000 SE3, SE4, SE2+. De switch ondersteunt 1024 ingangen en 1024 politieagenten. Het systeem gebruikt twee indringers en twee politieagenten die de politie standaard niet controleren.

Merk op dat wanneer de geaggregeerde politieagent binnen het beleid op een VLAN en een fysieke interface wordt toegepast, een extra ingang van de hardwarepolitieagent wordt gebruikt. Op dit moment is het niet mogelijk om VLAN-interfaces en fysieke interfaces samen te controleren. Dit zou kunnen veranderen in toekomstige softwarereleases.

Alle softwareversies bieden ondersteuning voor toezicht. De Catalyst 4000 ondersteunt maximaal 8 geldige overeenkomende verklaringen per klasse en maximaal 8 klassen worden ondersteund per beleidskaart. Geldige matchverklaringen zijn als volgt:

- match-toegangsgroep
- zie ip-punt
- zie ip-voorrang
- gelijk maken

**Opmerking:** Voor niet-IP V4-pakketten is de **matchip**-verklaring de enige manier om te classificeren, mits de pakketten in trunking poorten **ontvangen** die **vertrouwen** op CoS. Laat niet misleid worden door het sleutelwoord ip in het commando **overeenkomende ip dscp**, omdat interne DSCP gelijk is aan dit op alle pakketten van toepassing is, niet slechts IP. Wanneer een poort is ingesteld om CoS te vertrouwen, wordt deze laatste afgeleid uit het L2 (802.1Q of ISL gelabeld) frame en geconverteerd naar interne DSCP met behulp van een CoS naar DSCP QoS-kaart. Deze interne DSCP-waarde kan dan in het beleid worden aangepast met behulp van **een match-ip-dscp**.

Geldige beleidsmaatregelen zijn:

- politie
- ip-dscp instellen
- ip-voorrang instellen
- trust dscp
- trust cos

Met markering kunt u het QoS-niveau van het pakket wijzigen op basis van classificatie of toezicht. De classificatie verdeelt verkeer in verschillende klassen voor QoS-verwerking op basis van gedefinieerde criteria. Om IP-voorrang of DSCP aan te passen, moet de corresponderende inkomende interface op de vertrouwde modus worden ingesteld. De switch ondersteunt het vertrouwen van CoS, het vertrouwen van DSCP en onvertrouwde interfaces. Vertrouwen specificeert het veld waaruit het QoS-niveau van het pakket zal worden afgeleid.

Wanneer u CoS vertrouwt, zal het QoS-niveau worden afgeleid van de L2-header van het ingesloten pakket van ISL of 802.1Q. Wanneer de switch DSCP vertrouwt, zal hij het QoS-niveau afleiden van het DSCP-veld van het pakket. Het vertrouwen van CoS is slechts betekenisvol op trunking interfaces, en het vertrouwen van DSCP is geldig voor IP V4 pakketten.

Wanneer een interface niet wordt vertrouwd (dit is de standaardstatus wanneer QoS is

ingeschakeld), zal interne DSCP van de configureerbare standaard-CoS of DSCP voor de corresponderende interface worden afgeleid. Als geen standaard CoS of DSCP is ingesteld, wordt de standaardwaarde nul (0). Zodra het oorspronkelijke QoS-niveau van het pakket is bepaald, wordt het in kaart gebracht in de interne DSCP. Interne DSCP kan door markering of toezicht behouden of gewijzigd worden.

Nadat het pakket QoS-verwerking ondergaat, worden de velden met QoS-niveau (binnen het IP DSCP-veld voor IP en in de ISL/802.1Q-header, indien aanwezig) bijgewerkt vanaf interne DSCP.

Er zijn speciale kaarten die worden gebruikt om de vertrouwde QoS-metriek van het pakket om te zetten naar een interne DSCP en vice versa. Deze kaarten zijn als volgt:

- DSCP naar Toegepaste DSCP; afleiden van een geïnspireerde DSCP bij het omlaag markeren van het pakket.
- DSCP naar CoS: Om het CoS-niveau af te leiden van interne DSCP om de uitgaande pakket ISL/802.1Q-header bij te werken.
- CoS naar DSCP: gebruikt om interne DSCP van inkomende CoS (ISL/802.1Q header) af te leiden wanneer de interface in trust CoS modus is.

Merk op dat wanneer een interface in de CoS-modus voor vertrouwen is, de uitgaande CoS altijd hetzelfde is als de inkomende CoS. Dit is specifiek voor QoS-implementatie in Catalyst 4000 SE3, SE4, SE2+.

## Toezicht configureren en bewaken

Het configureren van toezicht in IOS omvat de volgende stappen:

1. Een politieagent definiëren.
2. Criteria definiëren voor het selecteren van verkeer voor toezicht
3. Het definiëren van service-beleid dat klasse gebruikt en het toepassen van een politieman op een gespecificeerde klasse.
4. U kunt een servicesbeleid toepassen op een poort of VLAN.

Neem het volgende voorbeeld. Er is een verkeersgenerator aangesloten op poort 5/14 die ~17 Mbps UDP-verkeer verzenden met een bestemming van poort 111. We willen dat dit verkeer wordt beperkt tot 1 Mbps en dat excessief verkeer wordt gevallen.

```
! enable qos
qos
! define policer, for rate and burst values, see 'policing parameters
qos aggregate-policer pol_1mbps 1mbps 1000 conform-action transmit
exceed-action
drop
! define ACL to select traffic
access-list 111 permit udp any any eq 111
! define traffic class to be policed
class-map match-all cl_test
match access-group 111
! define QoS policy, attach policer to traffic class
policy-map po_test
class cl_test
police aggregate pol_1mbps
! apply QoS policy to an interface
interface FastEthernet5/14
```

```
switchport access vlan 2
! switch qos to vlan-based mode on this port
qos vlan-based
! apply QoS policy to an interface
interface Vlan 2
service-policy output po_test
!
```

Merk op dat wanneer een poort in een VLAN gebaseerde QoS-modus is, maar er geen servicebeleid is toegepast op het corresponderende VLAN, de switch het servicebeleid (indien van toepassing) zal volgen dat op een fysieke poort is toegepast. Dit maakt extra flexibiliteit mogelijk bij het combineren van op poort gebaseerde en VLAN-gebaseerde QoS.

Er worden twee soorten politiemensen ondersteund: genoemd aggregaat en per interface. Een benoemde politieagent zal het verkeer dat wordt gecombineerd controleren op alle interfaces waarop het wordt toegepast. Het bovenstaande voorbeeld gebruikte een genaamd politieagent. Een politieman per interface, anders dan een genoemde politieagent, zal het verkeer op elke interface afzonderlijk controleren waar het wordt toegepast. Een per-interface politieman wordt gedefinieerd in de beleidskaartconfiguratie. Overweeg het volgende voorbeeld met een per-interface geaggregeerde politier:

```
! enable qos
qos
! define traffic class to be policed
class-map match-all cl_test2
match ip precedence 3 4
! define QoS policy, attach policer to traffic class
policy-map po_test2
class cl_test2
! per-interface policer is defined inside the policy map
police 512k 1000 conform-action transmit exceed-action drop
interface FastEthernet5/14
switchport
! set port to trust DSCP - need this to be able to match to incoming IP precedence
qos trust dscp
! switch to port-based qos mode
no qos vlan-based
! apply QoS policy to an interface
service-policy input po_test2
```

De volgende opdracht wordt gebruikt om de politiehandeling te controleren:

```
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400026 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166067574 bytes Exceed: 5268602114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400138 packets
```

```
match: ip precedence 3 4
police: Per-interface
Conform: 1166088574 bytes Exceed: 5268693114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
```

De teller bij class-map telt het aantal pakketten dat overeenkomt met een corresponderende klasse.

Wees op de hoogte van de volgende specifieke implementatieoverwegingen:

- De pakketteller per klasse is niet per interface. Dat wil zeggen, het telt alle pakketten die de klasse uit alle interfaces aanpassen waar deze klasse binnen het dienstbeleid wordt toegepast.
- Toezicht houdt geen pakkettellers in, alleen byte-tellers worden ondersteund.
- Er is geen specifieke opdracht om het aangeboden of uitgaande verkeerstarief per agent te verifiëren.
- De tellers worden periodiek bijgewerkt. Als u de bovenstaande opdracht herhaaldelijk in sneltreinvaart uitvoert, kunnen er op een bepaald moment tellers verschijnen.

## Marking configureren en bewaken

De configuratie van de markering omvat de volgende stappen:

1. Definieer de criteria voor het classificeren van het verkeer - toegangslijst, DSCP, IP voorrang, enz.
2. Bepaal de te classificeren verkeersklassen aan de hand van eerder gedefinieerde criteria.
3. Een beleidsplan maken dat markeringsacties en/of politieacties aan de gedefinieerde klassen vastlegt.
4. De trustmodus instellen op de corresponderende interface(s).
5. Pas de beleidskaart op een interface toe.

Neem het volgende voorbeeld waar we inkomend verkeer met IP voorrang 3 willen om 192.168.196.3 UDP poort 777 in kaart te brengen aan IP voorrang 6. Alle andere IP voorrang 3 verkeer wordt beperkt tot 1 Mbps, en overmatig verkeer moet worden gemarkeerd tot IP voorrang 2.

```
! enable QoS globally
qos
! define ACL to select UDP traffic to 192.168.196.3 port 777
ip access-list extended acl_test4
permit udp any host 192.168.196.3 eq 777
! define class of traffic using ACL and ip precedence matching
class-map match-all cl_test10
match ip precedence 3
match access-group name acl_test4
! all the remaining ip precedence 3 traffic will match this class
class-map match-all cl_test11
match ip precedence 3
! define policy with above classes
policy-map po_test10
class cl_test10
```

```
! mark traffic belonging to class with ip precedence 6
set ip precedence 6
class cl_test11
! police and mark down all other ip precedence 3 traffic
police 1 mbps 1000 exceed-action policed-dscp-transmit
!
! adjust DSCP to policed DSCP map so to map DSCP 24 to DSCP 16
qos map dscp policed 24 to dscp 16
!
interface FastEthernet5/14
! set interface to trust IP DSCP
qos trust dscp
! apply policy to interface
service-policy input po_test10
!
```

De opdracht **beleidsinterface** van **sh** wordt gebruikt om de markering te controleren. De steekproefuitvoer en de implicaties worden gedocumenteerd in de bovenstaande configuratie van het toezicht.

## Vergelijking van toezicht en markering op Catalyst 6000 en Catalyst 4000/4500 IOS-gebaseerde Supervisor Engine

| Feature | Catalyst6000 | Catalyst4000 SE3 |
|---|---|---|
| Egress QoS policies | Not supported by Supervisor 1A and Superviso r2 hardware. | Supported. |
| Burst policing parameter calculation | Burst should be at least the same size as maximum frame supposed to pass via policer and no less then rate/interval, with the interval being 250 microseconds | No such restriction. |
| QoS policing L2 & L3 | By default, microflow policing is only enabled for L3 on the sup1a and is not enabled at all for Supervisor 2. A CLI command is available to enable it for L2 on sup1a and L2 & L3 for sup2. Aggregate policing for sup1a & Supervisor 2 is enabled by default for L2 & L3. | Always. |
| Egress CoS | Always derived from internal DSCP using DSCP to CoS QoS map. | If the ingress port is in trust CoS mode, the egress CoS will be the same as the ingress CoS. Otherwise, it will be derived from the internal DSCP. |
| Microflow policing | Supported. | Not supported. |
| QoS behavior when port is in VLAN-based QoS mode, but no policy is applied to the VLAN. | No policy applied. | Fallback to port-based QoS. Will apply policy attached to port. |

## Gerelateerde informatie

- QoS begrijpen en configureren
- Technische ondersteuning - Cisco-systemen