# QoS op Catalyst 6000 Series Switches begrijpen

---

## Inhoud



---

## Inleiding

Dit document verklaart de Quality of Service (QoS) mogelijkheden die beschikbaar zijn in Catalyst 6000 Series switches. Dit document behandelt de mogelijkheden van QoS-formaties en geeft een aantal voorbeelden van de manier waarop QoS kan worden geïmplementeerd.

Dit document hoeft geen configuratiehandleiding te zijn. Configuratievoorbeelden worden in dit document gebruikt om te helpen bij de uitleg van de QoS-functies van de Catalyst 6000-familie hardware en -software. Raadpleeg voor syntax verwijzing voor QoS-commandostructuren de volgende configuratie en opdrachtgidsen voor de Catalyst 6000-familie:

- Catalyst 6500 Series Switches

## Layer 2 QoS definiëren

Hoewel velen kunnen denken dat QoS in Layer 2 (L2) switches simpelweg over het prioriteren van Ethernet frames bestaat, realiseren velen zich dat dit veel meer betekent. L2 QoS houdt het volgende in:

1. **Wachttijden voor invoerwachtrij:** wanneer het kader de poort ingaat, kan het aan één van een aantal op haven gebaseerde wachtrijen worden toegewezen alvorens aan op een uitgang wordt gepland. Meestal worden er meerdere wachtrijen gebruikt waar het verschillende verkeer verschillende serviceniveaus vereist, of waar de switch latentie tot een minimum moet worden beperkt. IP-gebaseerde video- en spraakgegevens vereisen bijvoorbeeld een lage latentie, zodat er mogelijk een switch nodig is van deze gegevens

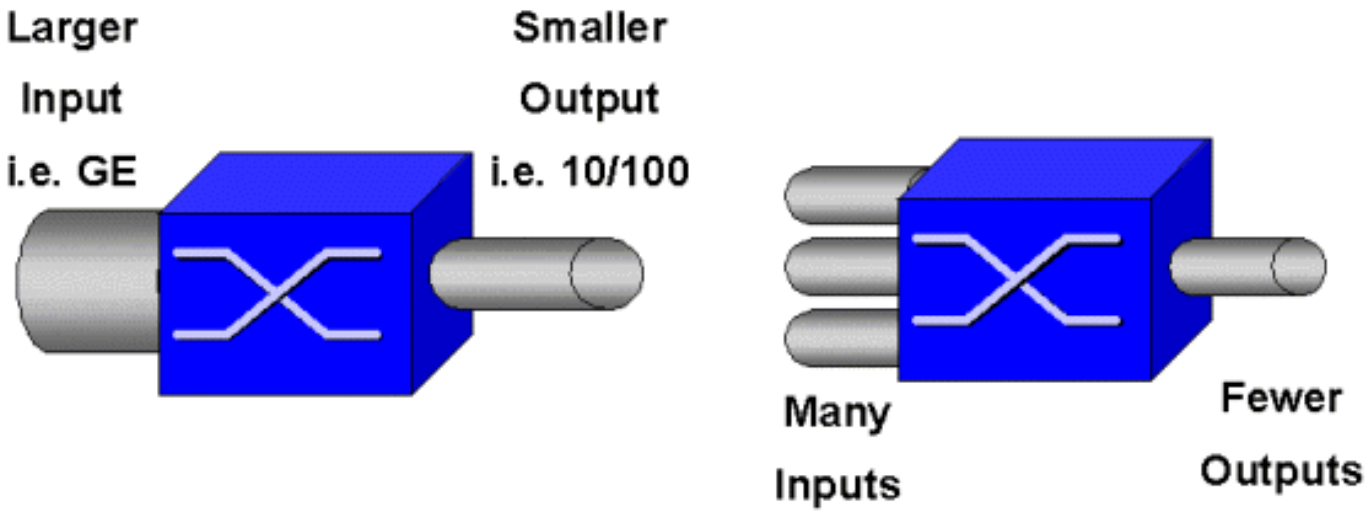
voordat er wordt overgeschakeld op andere gegevens, zoals File Transfer Protocol (FTP), web, e-mail, telnet enzovoort.

2. **Indeling:** het proces van classificatie omvat het inspecteren van verschillende velden in de Ethernet L2-header, naast velden in de IP-header (Layer 3 (L3) en de TCP/UDP-header (Transmission Control Protocol/UDP) met hulp bij het bepalen van het serviceniveau dat zal worden toegepast op het frame wanneer deze de switch doorgeeft.
3. **Toezicht:** Toezicht is het proces om een Ethernet frame te inspecteren om te zien of het binnen een bepaald tijdsbestek een vooraf bepaald verkeersvolume heeft overschreden (dit tijdpad is doorgaans een vast interne nummer van de switch). Als dat frame buiten profiel is (dat wil zeggen, maakt het deel uit van een gegevensstroom die de vooraf ingestelde snelheidslimiet overschrijdt), kan deze worden ingetrokken of kan de waarde voor serviceklasse (CoS) worden afgedrukt.
4. **Herschrijven:** Het herschrijfproces is de mogelijkheid van de switch om de CoS in de Ethernet header of de Type of Service (ToS) bits in de IPV4-header aan te passen.
5. **Wachttijden voor uitvoerwachtrij:** na de herschrijfprocessen zal de switch het Ethernet frame in een geschikte uitgaande (egress) wachtrij voor switching plaatsen. De switch zal bufferbeheer op deze wachtrij uitvoeren door ervoor te zorgen dat de buffer niet overstroomt. Dit gebeurt doorgaans door gebruik te maken van een Random Early Discard (RED)-algoritme, waarbij willekeurige frames worden verwijderd (ingetrokken) uit de wachtrij. Weighted RED (WRED) is een derivaat van ROOD (gebruikt door bepaalde modules in de Catalyst 6000-familie), waarbij de CoS-waarden worden geïnspecteerd om te bepalen welke frames zullen worden ingetrokken. Wanneer de buffers vooraf bepaalde drempels bereiken, worden de lagere prioriteitskaders normaal gedaald, die de hogere prioriteitsframes in de rij houden.

In dit document wordt elk van de bovengenoemde mechanismen en de wijze waarop zij betrekking hebben op de Catalyst 6000-familie in de volgende delen nader toegelicht.

## De noodzaak van QoS in een Switch

Grote backplanes, miljoenen switched pakketten per seconde en niet-blokkerende switches zijn vandaag de dag allemaal synoniem voor veel switches. Waarom QoS nodig is? Het antwoord komt door congestie.




Een switch kan de snelste switch ter wereld zijn, maar als je één van de twee scenario's hebt die in bovenstaande afbeelding worden getoond, dan zal die switch congestie ervaren. Als de functies

voor congestiebeheer niet aanwezig zijn, worden pakketten niet gedemonteerd. Wanneer pakketten worden ingetrokken, worden er opnieuw verzonden. Wanneer terugzendingen plaatsvinden, kan de netwerklading toenemen. In netwerken die al overbelast zijn, kan dit bestaande prestatiekwesties verergeren en de prestaties mogelijk verder degraderen.

Dankzij convergerende netwerken is het congestiebeheer nog kritischer. Latentie-gevoelig verkeer zoals spraak en video kan ernstig worden beïnvloed als er vertragingen optreden. Door eenvoudigweg meer buffers aan een switch toe te voegen, zullen de congestieproblemen niet noodzakelijkerwijs worden verlicht. Het Latency gevoelige verkeer moet zo snel mogelijk geschakeld worden. Eerst moet je dit belangrijke verkeer identificeren door middel van classificatietechnieken, en dan bufferbeheertechnieken toepassen om te voorkomen dat het prioriteitsverkeer tijdens de congestie daalt. Tenslotte moet u planningstechnieken integreren om belangrijke pakketten uit rijen zo snel mogelijk te switches. Zoals u in dit document zult lezen, implementeert de Catalyst 6000 familie al deze technieken. Daardoor is het QoS-subsysteem één van de meest uitgebreide in de huidige industrie.

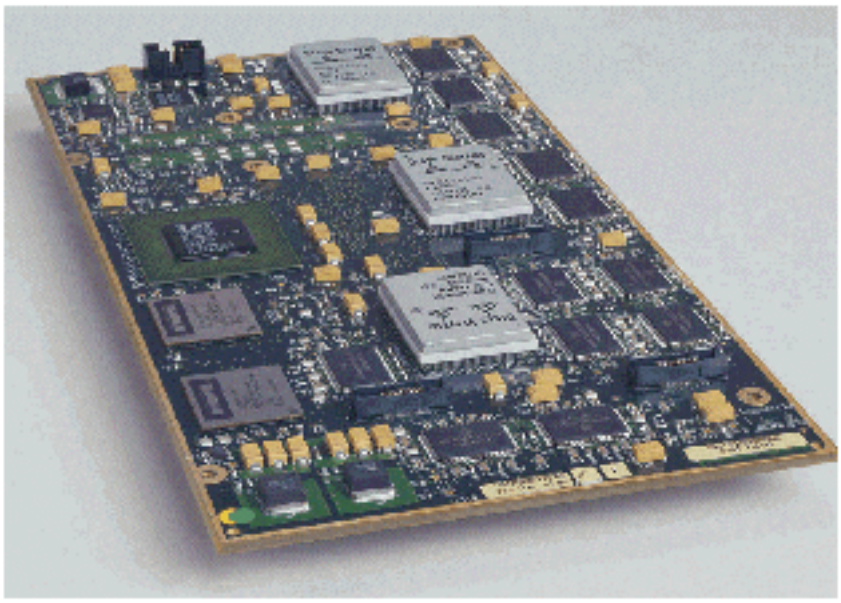
Alle QoS-technieken die in de vorige sectie zijn beschreven, zullen in dit document nader worden onderzocht.

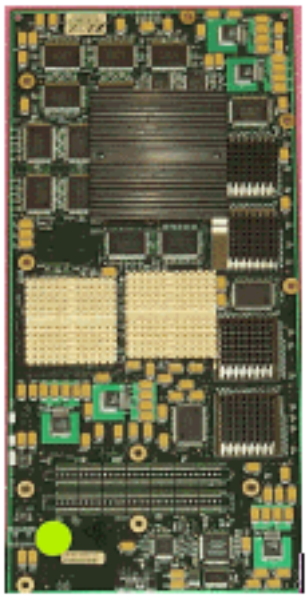
# Hardware ondersteuning voor QoS in de Catalyst 6000-reeks

Om QoS in de Catalyst 6000-familie te ondersteunen, is enige hardwareondersteuning vereist. De hardware die QoS ondersteunt, omvat de functiekaart voor meerlaagse Switch (MSFC), de beleidsfunctiekaart (PFC) en de Port Application Specific Integrated Circuits (ASIC's) op de lijnkaarten zelf. Dit document zal de QoS-mogelijkheden van de MSFC niet verkennen, maar zich wel concentreren op de QoS-functies van de PFC en de ASIC's op de lijnkaarten.

## PFC

PFC versie 1 is een dochterkaart die op supervisor I (SupI) en de Supervisor IA (SupIA) van de Catalyst 6000 familie zit. PFC2 is een hercentrifugeren van de PFC1 en schepen met de nieuwe Supervisor II (SupII) en enige nieuwe aan boord ASICs. Hoewel zowel de PFC1 als PFC2 voornamelijk bekend zijn om hun hardwareversnelling van L3-switching, is QoS een van hun andere doeleinden. De PFC's worden hierna weergegeven.





Hoewel PFC 1 en PFC2 in wezen hetzelfde zijn, zijn er enkele verschillen in QoS-functionaliteit. Namelijk voegt PFC2 het volgende toe:

1. De mogelijkheid om het QoS-beleid naar een Distributed Forwarding Card (DFC) te duwen.

2. De beleidsbeslissingen zijn iets anders. Zowel de PFC1 als PFC2 ondersteunen normaal toezicht, waarbij frames worden ingetrokken of gemarkeerd als een aggregaat of microflow beleid een buiten-profiel beslissing teruggeeft. Het PFC2 voegt echter steun toe voor een te hoge rente, wat een tweede politieniveau aangeeft dat beleidsmaatregelen kunnen worden genomen op.

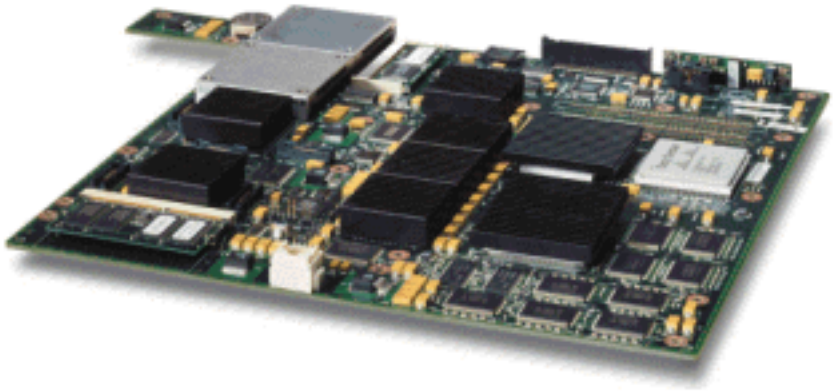
Wanneer een overtollig aantal politieagenten wordt gedefinieerd, kunnen de pakketten worden gedropt of gemarkeerd wanneer ze de overtollige snelheid overschrijden. Als een te hoog politieniveau is ingesteld, wordt de overtollige DSCP-afbeelding gebruikt om de oorspronkelijke DSCP-waarde te vervangen door een gemarkeerde waarde. Als slechts een normaal politieniveau is ingesteld, wordt de normale DSCP mapping gebruikt. Het buitensporige politieniveau heeft voorrang bij het selecteren van kaartenregels als beide politieniveaus worden ingesteld.

Het is belangrijk op te merken dat de in dit document beschreven QoS-functies die door de

genoemde ASIC's worden uitgevoerd, hoge prestatieniveaus opleveren. De QoS-prestaties in een basis Catalyst 6000-familie (zonder module van switch) leveren 15 MPPS op. Er kan voor QoS aanvullende prestatiewinst worden behaald indien DFC's worden gebruikt.

## DFC

De DFC kan als optie aan de WS-X6516-GBIC worden gekoppeld. Dit is echter een standaardfixatie op de WS-X6816-GBIC-kaart. Kan ook worden ondersteund op andere toekomstige fabric-lijnkaarten zoals de onlangs geïntroduceerde fabric 10/100 (WS-X6548-RJ45) lijnkaart, fabric RJ21 lijnkaart (WS-X6548-RJ21) en de 100FX lijnkaart (WS-X652) 4-MM-FX). De DFC wordt hierna weergegeven.



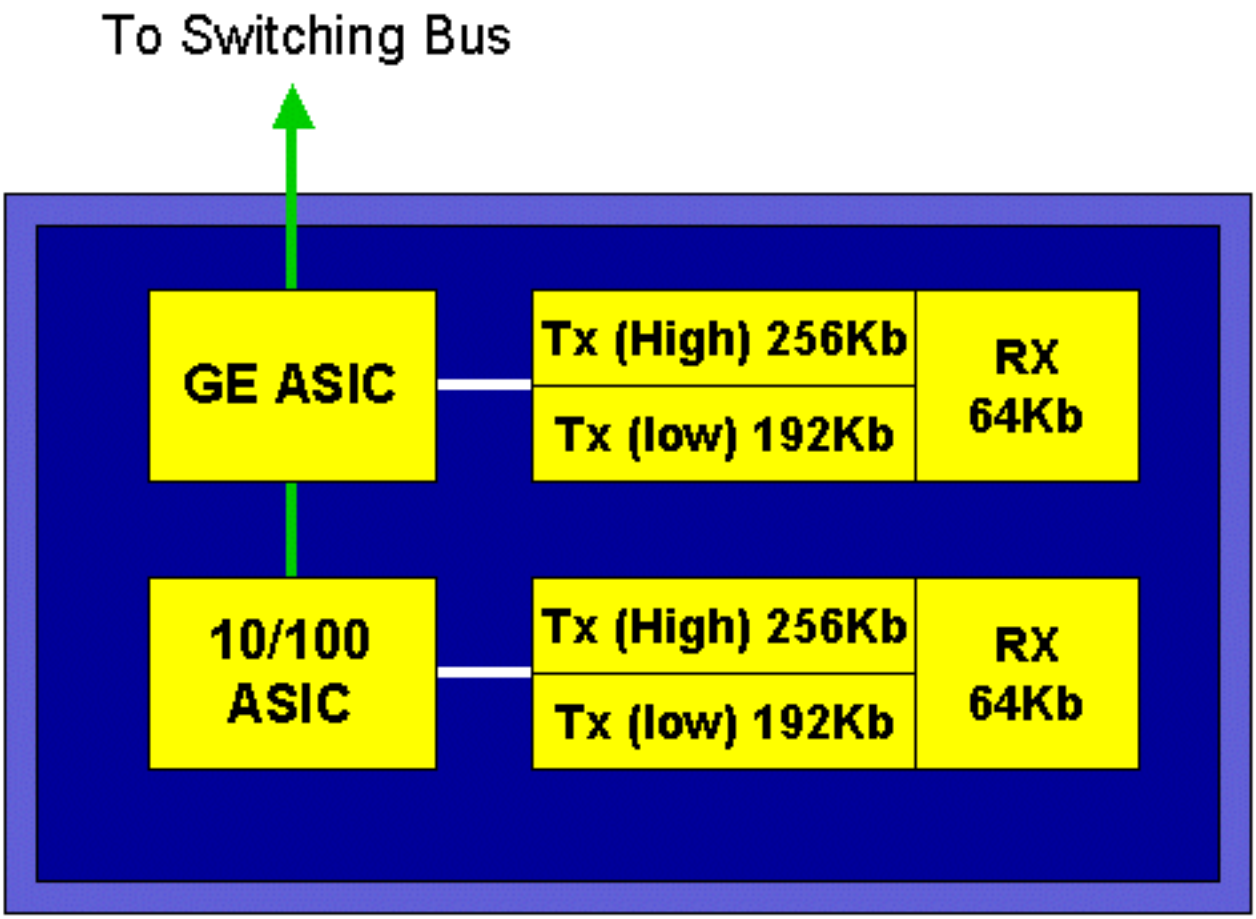
Met DFC kan de fabric-lijnkaart (cross-bar aangesloten) worden uitgevoerd voor lokale switching. Om dit te bereiken moet het ook elk QoS-beleid ondersteunen dat voor de switch is gedefinieerd. De beheerder kan de DFC niet rechtstreeks configureren; in plaats daarvan valt het onder de controle van de master MSFC/PFC op de actieve toezichthouder. Het primaire PFC zal een Forwarding Information Base (FIB)-tabel omlaag drukken, wat de DFC zijn L2- en L3-verzendtabellen geeft. Het zal ook een exemplaar van het QoS-beleid omlaag drukken zodat dit ook lokaal is naar de lijnkaart. Hierna kunnen lokale switching beslissingen in de lokale context een verwijzing naar de lokale kopie van elk QoS-beleid dat hardware QoS-verwerkingssnelheden biedt en hogere prestatieniveaus oplevert via gedistribueerde switching.

## Poortgebaseerde ASIC's

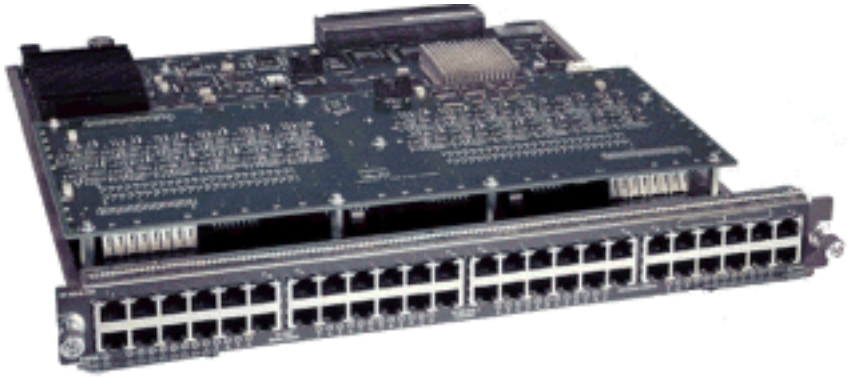
Om het hardwarebeeld te voltooien, implementeert elk van de lijnkaarten een aantal ASIC's. Deze ASIC's implementeren de wachtrijen, buffering en drempels die gebruikt worden voor de tijdelijke opslag van frames tijdens het doorvoeren van de switch. Op de 10/100 kaarten wordt een combinatie van ASIC's gebruikt om de 48 10/100 poorten te leveren.

### Originele 10/100 lijnkaarten (WS-X6348-RJ45)

De 10/100 ASIC's voorzien in een reeks ontvangers (RX) en transmissietransen (TX) voor elke 10/100 poort. ASIC's bieden 128.000 buffers per 10/100 poorten. Raadpleeg de aantekeningen bij vrijgave voor meer informatie over welke buffering per poort op elke lijnkaart beschikbaar is. Elke poort op deze lijnkaart ondersteunt één Rx-rij en twee TX-wachtrijen die hoog en laag zijn aangegeven. Dit wordt in het onderstaande schema weergegeven.




In het bovenstaande schema biedt elke 10/100 ASIC een uitsplitsing voor 12 10/100 poorten. Voor elke 10/100 poort worden 128 K buffers geleverd. De 128 K buffers worden verdeeld tussen elk van de drie wachtrijen. De cijfers in de bovenstaande rij zijn niet de standaardinstellingen, maar eerder een weergave van wat anders zou kunnen worden geconfigureerd. De enkele Rx-wachtrij krijgt 16 K en het resterende geheugen (112 K) wordt verdeeld tussen de twee TX-rijen. Standaard (in CatOS) krijgt de hoge rij 20 procent van deze ruimte en de lage rij 80 procent. In Catalyst IOS is het standaard om de hoge rij 10 procent en de lage rij 90 procent te geven.

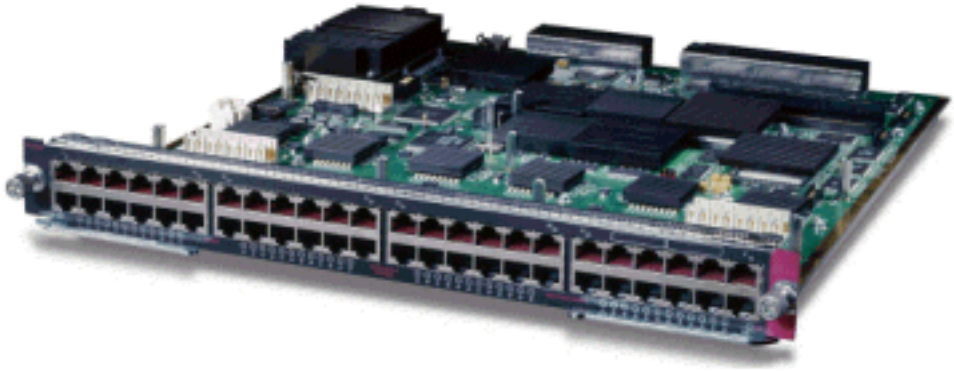


Terwijl de kaart tweefasenbuffers biedt, is er slechts 10/100 ASIC-gebaseerde buffering beschikbaar om tijdens de QoS-configuratie te worden gemanipuleerd.

### Fabric 10/100 lijnkaarten (WS-X6548-RJ45)

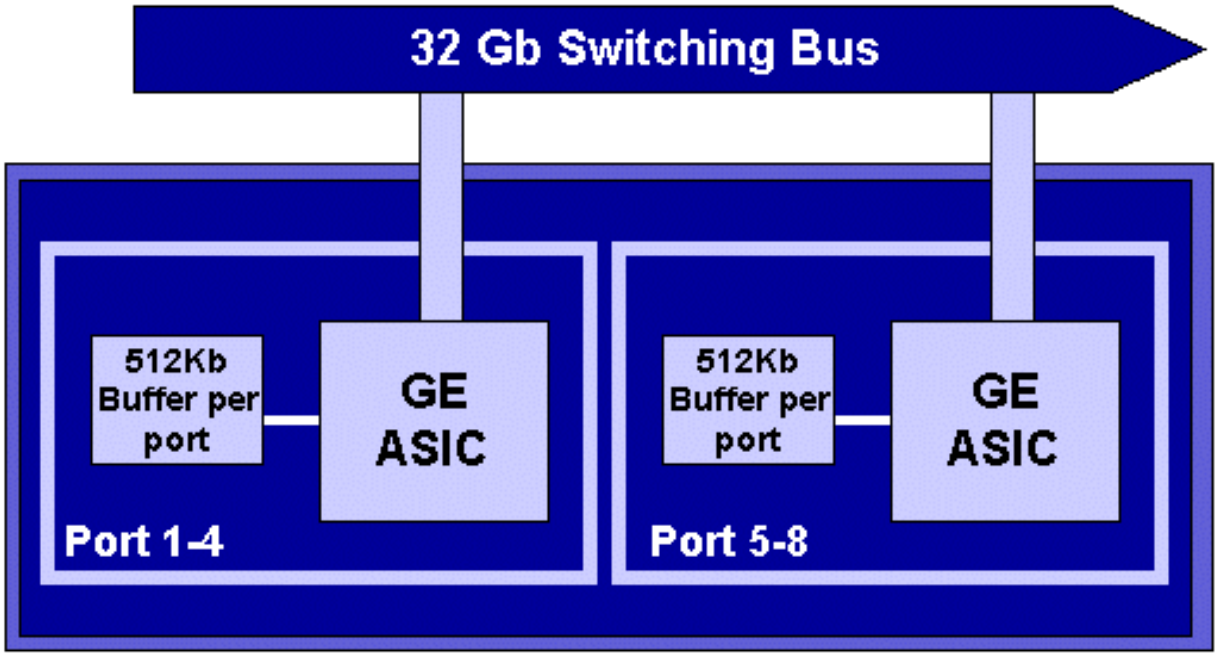
De nieuwe 10/100 ASIC's bieden een reeks Rx- en TX-wachtrijen voor elke 10/100 poort. De ASIC's bieden een gedeelde pool van geheugen beschikbaar over de 10/100 poorten. Raadpleeg de aantekeningen bij vrijgave voor meer informatie over welke buffering per poort op elke lijnkaart beschikbaar is. Elke poort op deze lijnkaart ondersteunt twee RX wachtrijen en drie TX wachtrijen.

Eén rij Rx en één rij TX worden elk aangeduid als een rij met absolute prioriteit. Dit fungeert als een lage latency wachtrij, die ideaal is voor latency gevoelig verkeer zoals Voice-over-IP (VoIP).

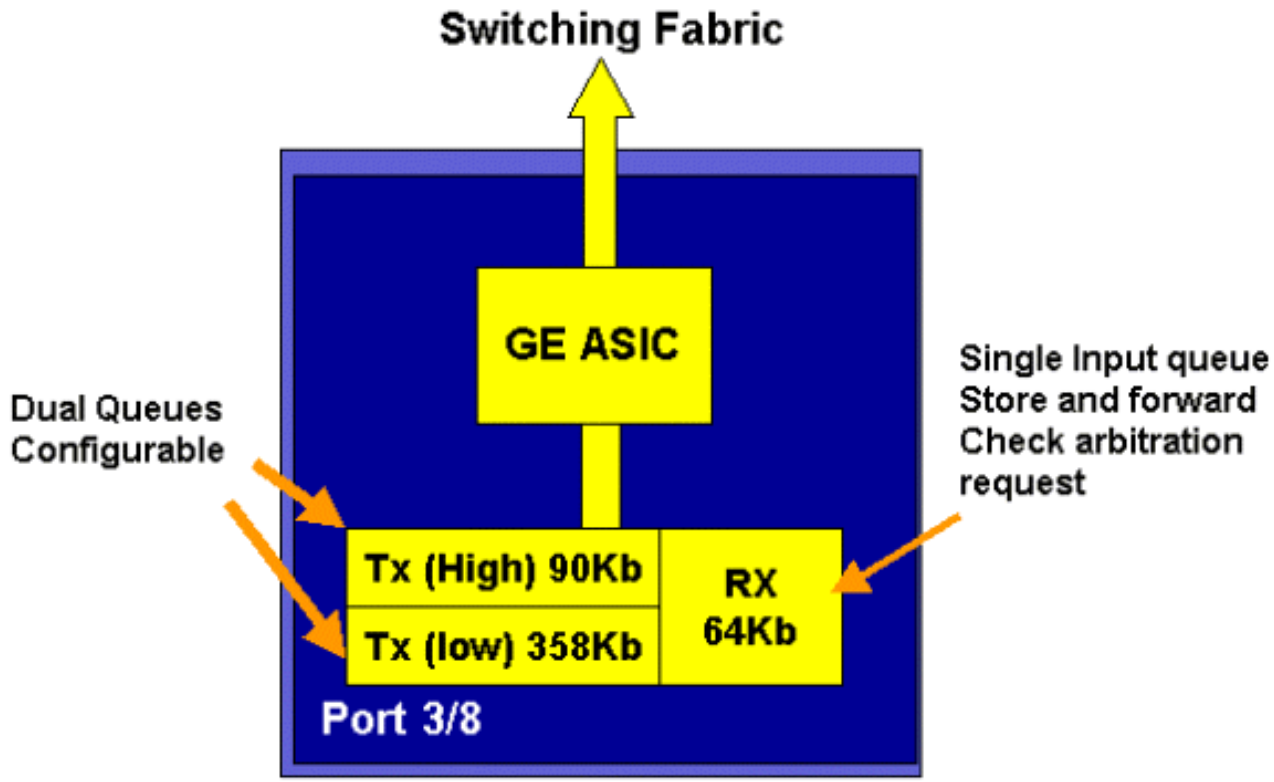


### GE-lijnkaarten (WS-X6408A, WS-X6516, WS-X6816)

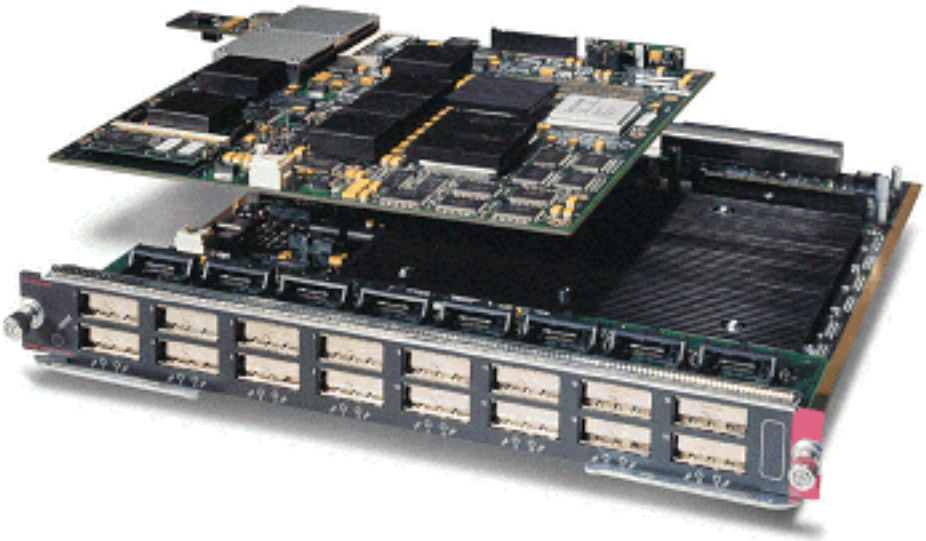
Voor GE lijnkaarten verstrekt ASIC 512K van per haven buffering. Een weergave van de acht-poorts GE lijnkaart wordt in het onderstaande schema weergegeven.




Net als bij de 10/100 poorten heeft elke GE poort drie wachtrijen, één x en twee TX wachtrijen. Dit is de standaardinstelling op de WS-X6408-GBIC lijnkaart en wordt in het onderstaande schema weergegeven.



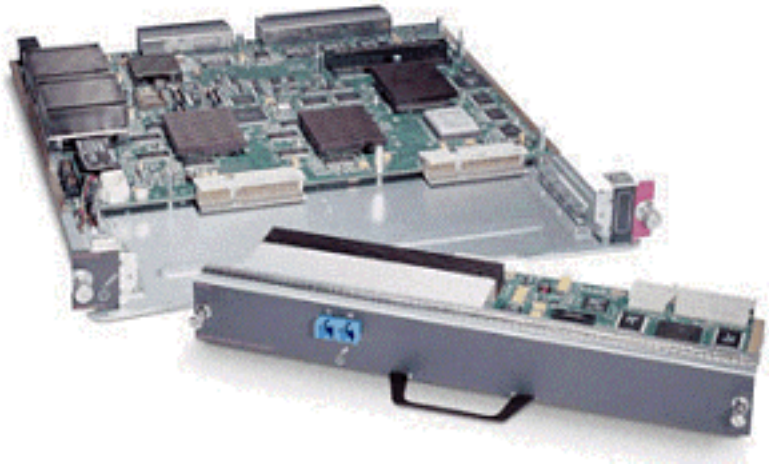

Op de nieuwere lijn 16-poorts GE-kaarten, worden de GBIC-poorten op SupIA en SupII, en de WS-X6408A-GBIC 8 poorten GE-kaart, twee extra strikte prioriteitswachtrijen (SP) geboden. De ene SP wachtrij wordt toegewezen als een Rx-wachtrij en de andere als een TX-wachtrij. Deze SP-wachtrij wordt voornamelijk gebruikt voor het in de wachtrij plaatsen van gevoelig verkeer zoals spraak. Met de SP-wachtrij worden alle in deze wachtrij geplaatste gegevens verwerkt vóór gegevens in de hoge en lage wachtrijen. Alleen wanneer de SP-wachtrij leeg is, worden de hoge en lage wachtrijen onderhouden.



### 10 GE lijnkaarten (WS-X6502-10 GE)

In de laatste helft van 2001 introduceerde Cisco een set van 10 GE lijnkaarten die één poort van 10 GE per lijnkaart leveren. Deze module neemt één sleuf in beslag van het 6000 chassis. De 10 GE lijnkaart ondersteunt QoS. Voor de poort van 10 GE biedt deze twee RX wachtrijen en drie TX wachtrijen. Eén Rx-wachtrij en één TX-wachtrij worden elk aangewezen als een SP-wachtrij.

Buffering is ook beschikbaar voor de poort, met in totaal 256 K Rx-buffering en 64 MB TX-buffering. Deze poort implementeert een 1p1q8t rijstructuur voor de RX kant en een 1p2q1t rijstructuur voor de TX kant. In dit document worden de structuren van de wachtrij later gedetailleerd beschreven.



### Catalyst 6000 Series QoS-hardwaresamenvatting

De hardwarecomponenten die de bovenstaande QoS-functies in de Catalyst 6000-familie uitvoeren, worden in de onderstaande tabel gespecificeerd.

| QoS Process | Catalyst 6500 Component that performs function |
|---|---|
| Input Scheduling | Performed by port ASIC's<br>L2 only with or without the PFC |
| Classification | Performed by Supervisor or PFC<br>L2 only is done by Supervisor<br>L2/3 is done by PFC |
| Policing | Done by PFC via L3 forwarding Engine |
| Packet Re-write | Done by port ASIC's<br>L2/L3 based on classification done in point 2 above |
| Output Scheduling | Done by port ASIC's<br>L2/L3 based on classification done in point 2 above |

## Catalyst 6000 Series softwareondersteuning voor QoS

De Catalyst 6000-familie ondersteunt twee besturingssystemen. Het oorspronkelijke softwareplatform, CatOS, werd afgeleid van de codebasis die op het Catalyst 5000-platform werd gebruikt. Recenter heeft Cisco geïntegreerd Cisco IOS ® (Native Mode) (voorheen bekend als Native IOS) geïntroduceerd, dat een codecoder gebruikt die is afgeleid van de Cisco IOS-router. Beide OS-platforms (CatOS en Integrated Cisco IOS (Native Mode) implementeren softwareondersteuning om QoS mogelijk te maken op het Catalyst 6000 switch familieplatform met behulp van de hardware die in de vorige secties is beschreven.

**Opmerking:** Dit document gebruikt configuratievoorbeelden van beide OS-platforms.

## Prioriteitsmechanismen in IP en Ethernet

Voor elke QoS-service die op gegevens moet worden toegepast, moet er een manier zijn om een IP-pakket of een Ethernet-kader te labelen of als prioriteit te definiëren. De ToS en de CoS velden worden gebruikt om dit te bereiken.

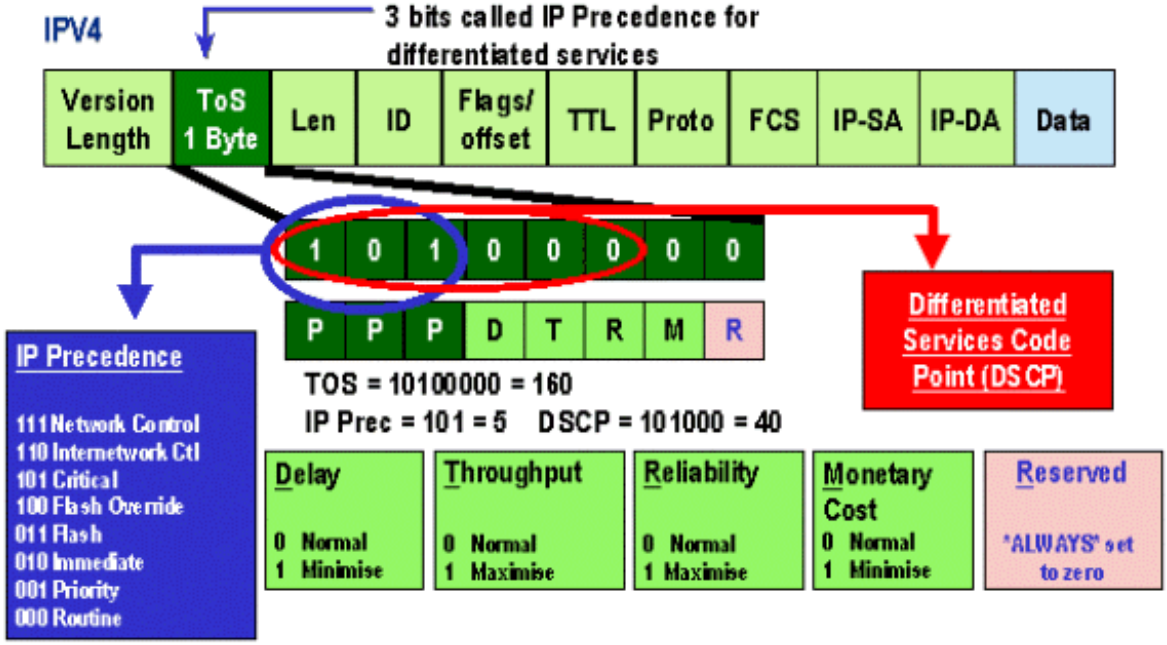
### Aan/uit

ToS is een veld van één byte dat in een IPV4-header bestaat. Het veld ToS bestaat uit acht bits, waarvan de eerste drie bits worden gebruikt om de prioriteit van het IP-pakket aan te geven. Deze eerste drie bits worden de IP-prioriteitsbits genoemd. Deze bits kunnen van nul tot zeven worden ingesteld, waarbij nul de laagste prioriteit is en zeven de hoogste prioriteit. Er is ondersteuning beschikbaar voor het instellen van IP-voorrang in IOS gedurende vele jaren. Ondersteuning van het opnieuw instellen van IP-voorrang kan worden verleend door de MSFC of door de PFC (onafhankelijk van de MSFC). Een vertrouwensinstelling van onvertrouwd kan ook elke IP-prioriteitsinstellingen op een inkomend frame wissen.

De waarden die kunnen worden ingesteld voor IP-voorrang zijn als volgt:

| IP Precedence bits | IP Precedence Value |
|---|---|
| 000 | Routine |
| 001 | Priority |
| 010 | Intermediate |
| 011 | Flash |
| 100 | Flash Override |
| 101 | Critical |
| 110 | Internetwork Control |
| 111 | Network Control |

In het onderstaande schema is een weergave van de IP-prioriteitsbits in de ToS-header. De drie meest significante bits (MSB) worden geïnterpreteerd als de IP-prioriteitsbits.



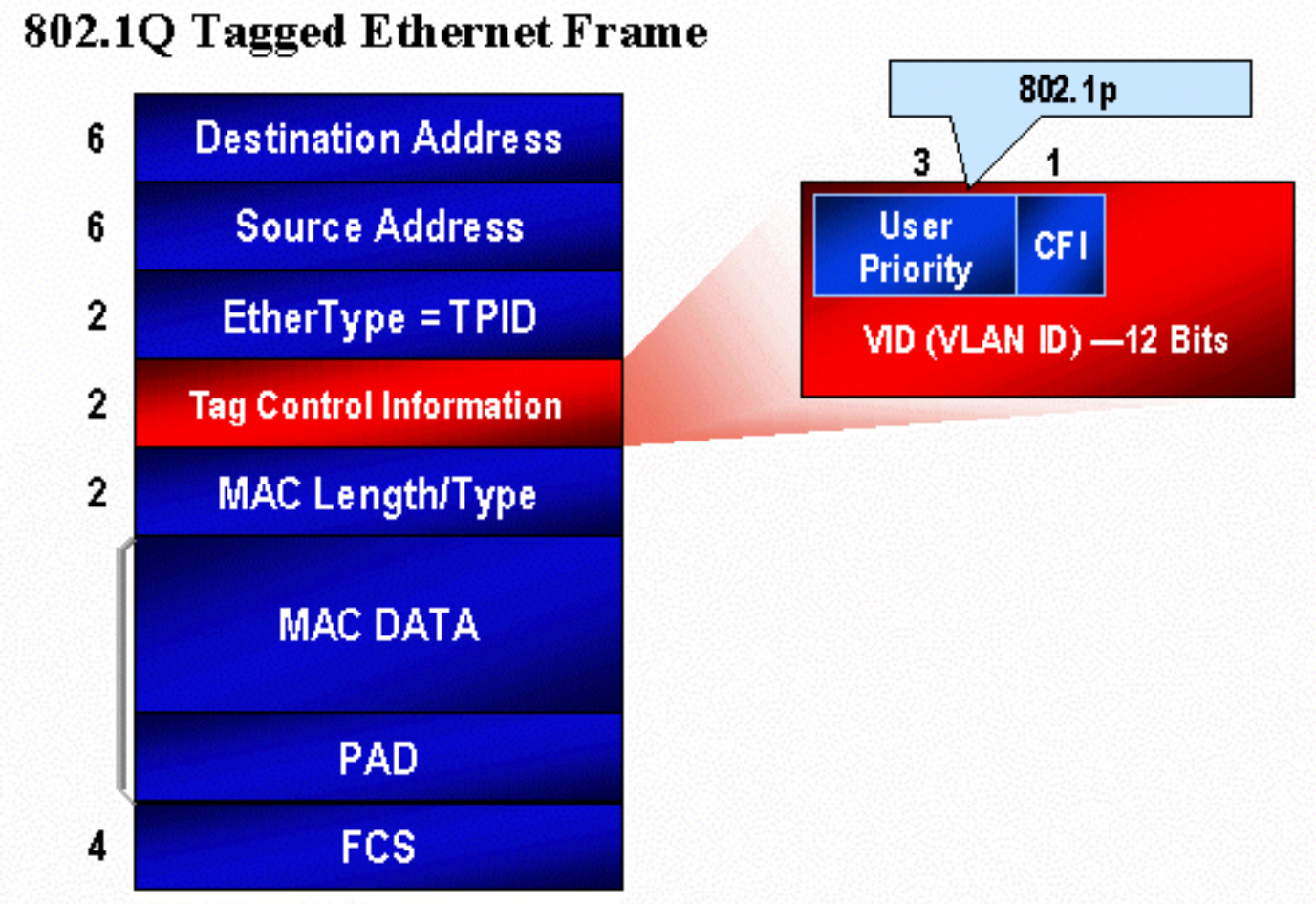

Recenter is het gebruik van het ToS-veld uitgebreid tot de zes MSB's, ook wel DSCP genoemd. DSCP levert 64 prioriteitswaarden (twee tot zes) op die aan het IP-pakket kunnen worden toegewezen.

De Catalyst 6000 familie kan de ToS manipuleren. Dit kan worden bereikt met zowel de PFC als/of de MSFC. Wanneer een kader in de switch komt, krijgt het een DSCP waarde toegewezen. Deze DSCP-waarde wordt intern in de switch gebruikt om serviceniveaus (QoS-beleid) aan te wijzen die door de beheerder worden gedefinieerd. DSCP kan al in een kader bestaan en gebruikt worden, of de DSCP kan afgeleid worden van de bestaande CoS, IP voorrang, of DSCP in het kader (zou de poort moeten worden vertrouwd). Een kaart wordt intern in de switch gebruikt om de DSCP af te leiden. Met acht mogelijke CoS/IP-prioriteitswaarden en 64 mogelijke DSCP-waarden zal de standaardkaart CoS/IPPrec 0 naar DSCP 0, CoS/IPPrec 1 naar DSCP 7, CoS/IPPrec 2 naar DSCP 15 enzovoort in kaart brengen. Deze standaardinstellingen kunnen door de beheerder worden overschreven. Wanneer het frame op een uitgaande poort is gepland, kan CoS opnieuw worden geschreven en wordt de DSCP-waarde gebruikt om de nieuwe CoS af te leiden.

## CoS

CoS verwijst naar drie bits in een ISL-kop of een 802.1Q-header die wordt gebruikt om de prioriteit van het Ethernet-frame aan te geven wanneer het door een geschakeld netwerk gaat. In dit document verwijzen we alleen naar het gebruik van de header van 802.1Q. De CoS-bits in de 802.1Q-header worden meestal de 802.1p-bits genoemd. Niet verrassend zijn er drie CoS bits, die het aantal bits aanpast voor IP-voorrang. In veel netwerken kan een pakje om QoS-end-to-end te onderhouden zowel voor L2- als voor L3-domeinen overlopen. Om QoS te onderhouden kunnen de ToS in kaart worden gebracht aan CoS, en kunnen CoS in kaart worden gebracht aan S.

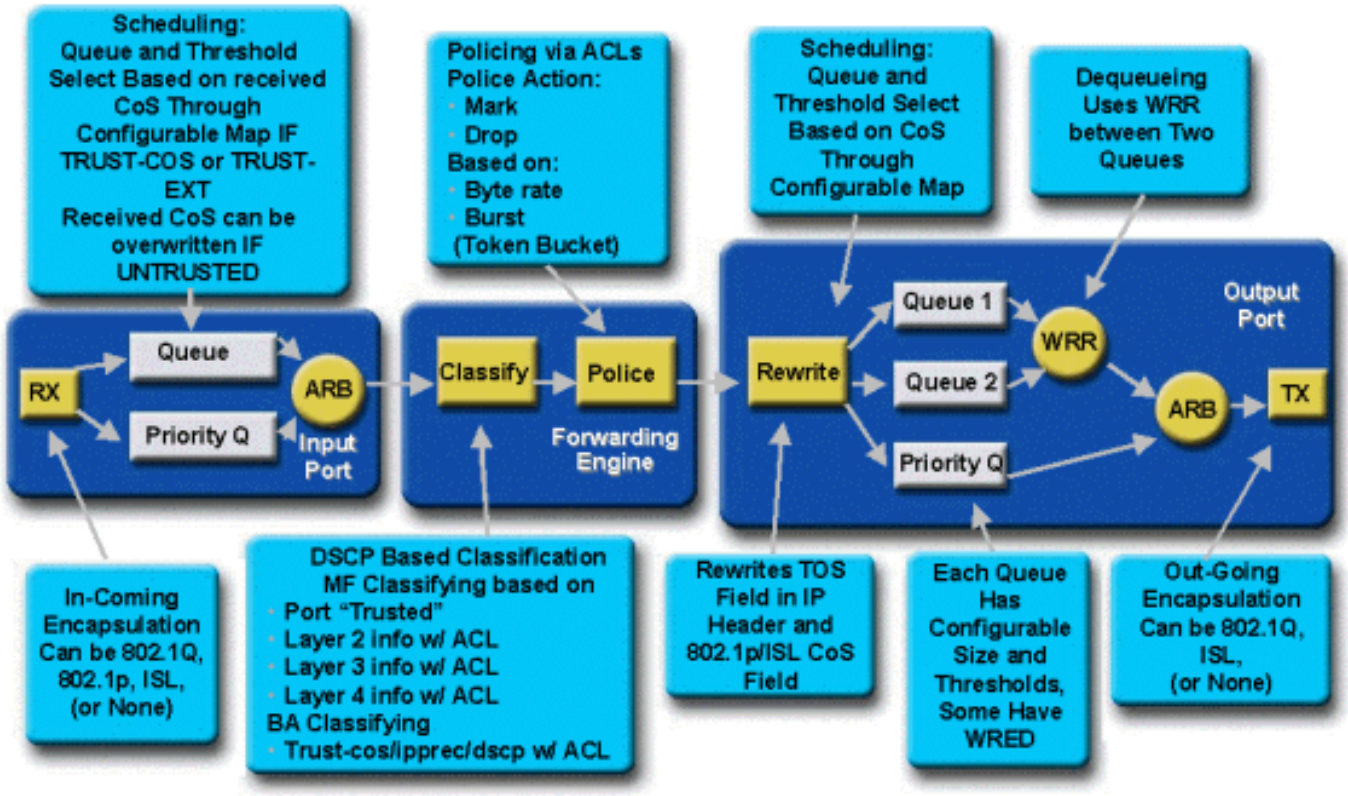
Het onderstaande schema is een Ethernet frame dat voorzien is van een 802.1Q-veld dat bestaat uit een Ethernet-type met twee bytes en een label met twee bytes. Binnen de twee-byte-tag worden de prioriteitsbits van de gebruiker (bekend als 802.1p) gebruikt.




## QoS-stroom in de Catalyst 6000-reeks

QoS in de Catalyst 6000-reeks is de meest uitgebreide implementatie van QoS in alle huidige Cisco Catalyst switches. De volgende secties beschrijven hoe de verschillende QoS processen op een kader worden toegepast aangezien het de switch overbrengt.

Eerder in dit document werd opgemerkt dat er een aantal QOS-elementen zijn die veel L2- en L3-switches kunnen bieden. Deze elementen zijn classificatie, schema's voor ingangslijsten, toezicht, herschrijven en schema's voor de uitvoerwachtrij. Het verschil met de Catalyst 6000-familie is dat deze QoS-elementen worden toegepast door een L2-motor die inzichten heeft in L3- en L4-gegevens en alleen in L2-headerinformatie. In het volgende schema wordt samengevat hoe de Catalyst 6000-familie deze elementen implementeert.




Een kader gaat de switch in en wordt eerst verwerkt door de poort ASIC die het kader heeft ontvangen. Het kader wordt in een rij Rx geplaatst. Afhankelijk van de Catalyst 6000 lijnkaart, zullen er een of twee RX wachtrijen zijn.

De poort ASIC gebruikt de CoS bits als een indicator waarvan de wachtrij voor het frame in (als er meerdere ingangswachtrijen aanwezig zijn) moet worden geplaatst. Als de poort als onbetrouwbaar is geclassificeerd, kan de port ASIC de bestaande CoS bits overschrijven op basis van een vooraf gedefinieerde waarde.

Het frame wordt vervolgens doorgegeven naar de L2/L3-verzendmotor (PFC), die het frame zal indelen en optioneel zal controleren (snelheidsbeperking). De classificatie is het proces om het kader een DSCP waarde toe te wijzen, die intern door de switch wordt gebruikt voor het verwerken van het frame. De DSCP wordt op een van de volgende manieren afgeleid:

1. Een bestaande DSCP-waarde ingesteld vóór het frame dat de switch invoert
2. De ontvangen IP-prioriteitsbits die al in de IPV4-header zijn ingesteld. Aangezien er 64 DSCP-waarden zijn en slechts acht IP-prioriteitswaarden, zal de beheerder een mapping configureren die door de switch wordt gebruikt om de DSCP af te leiden. Standaard toewijzingen zijn uitgevoerd indien de beheerder de kaarten niet aanpast.
3. De ontvangen CoS bits werden al ingesteld voorafgaand aan het frame dat de switch invoert. Overeenkomstig met IP-voorrang zijn er maximaal acht CoS-waarden, die elk aan een van 64 DSCP-waarden moeten worden gekoppeld. Deze kaart kan worden ingesteld of de switch kan de standaardkaart op zijn plaats gebruiken.
4. Stel dit kader in door gebruik te maken van een standaard DSCP-waarde die doorgaans wordt toegewezen aan een toegangscontrolelijst (ACL).

Nadat een DSCP-waarde is toegewezen aan het frame wordt de controle (snelheidsbeperking) toegepast indien er een politieconfiguratie bestaat. Toezicht zal de gegevensstroom door de PFC beperken door verkeer te laten vallen of omlaag te markeren dat niet meer in profiel is. Out-of-profile is een term die wordt gebruikt om aan te geven dat verkeer een limiet heeft overschreden

die door de beheerder is gedefinieerd als de hoeveelheid bits per seconde dat de PFC zal verzenden. Out-of-profile verkeer kan worden ingetrokken of de CoS-waarde kan worden gemarkeerd. PFC1 en PFC2 ondersteunen momenteel alleen invoercontrole (snelheidsbeperking). Ondersteuning voor input- en uitvoertoezicht is beschikbaar met de release van een nieuw PFC.

Het PFC zal het kader dan naar de gelijkmatige poort doorgeven voor verwerking. Op dit punt, wordt een herschrijfproces geactiveerd om de CoS-waarden in het frame en de ToS-waarde in de IPV4-header te wijzigen. Dit komt voort uit de interne DSCP. Het kader wordt dan in een verzendwachtrij geplaatst op basis van de CoS-waarde, klaar voor transmissie. Terwijl het kader in de rij staat, zal de haven ASIC de buffers controleren en WRED implementeren om de buffers van overstromen te vermijden. Een WRR-planningsalgoritme wordt dan gebruikt om frames op te plannen en door te geven vanaf de generatiepoort

In elk van de onderstaande secties wordt deze stroom gedetailleerder onderzocht, met configuratievoorbeelden voor elk van de bovengenoemde stappen.

# Wachtrijen, buffers, drempels en Mappingen

Voordat de QoS-configuratie in detail wordt beschreven, moeten bepaalde bepalingen verder worden uitgelegd om ervoor te zorgen dat u de QoS-configuratiefuncties van de switch volledig begrijpt.

### Wachtrijen

Elke poort op de switch heeft een reeks input- en uitvoerwachtrijen die worden gebruikt als tijdelijke opslaggebieden voor gegevens. Catalyst 6000 Series lijnkaarten implementeren verschillende getallen wachtrijen voor elke poort. De wachtrijen worden gewoonlijk in hardware-ASIC's voor elke poort geïmplementeerd. Op de lijnkaarten van de eerste generatie Catalyst 6000 familie was de typische configuratie één invoerrij en twee uitvoerrijen. Op nieuwere lijnkaarten (10/100 en GE) implementeert ASIC een extra set van twee wachtrijen (één ingangssignaal en één uitvoer), resulterend in twee ingangswachtrijen en drie uitvoerwachtrijen. Deze twee extra rijen zijn speciale SP rijen die voor latentiegevoelig verkeer zoals VoIP worden gebruikt. Onderhoud geschiedt op SP - wijze. Dat wil zeggen, als een kader in de SP wachtrij arriveert, worden planningsframes uit de lagere rijen niet meer verwerkt om het kader in de SP-wachtrij te verwerken. Alleen wanneer de SP wachtrij leeg is, wordt het plannen van pakketten uit de onderste rij(s) hervat.

Wanneer een kader bij een poort (voor invoer of uitvoer) aankomt op het moment van congestie, zal het in een rij worden geplaatst. De beslissing achter welke wachtrij van het kader wordt geplaatst, wordt doorgaans genomen op basis van de CoS-waarde in de Ethernet-kop van het inkomende frame.

Bij aanvang zal een planningsalgoritme worden gebruikt om de TX (output) wachtrij te verlaten. WRR is de techniek die wordt gebruikt om dit te bereiken. Voor elke rij wordt een weging gebruikt om te bepalen hoeveel gegevens uit de wachtrij zullen worden geleegd voordat ze naar de volgende wachtrij gaan. De door de beheerder toegewezen weging is een aantal van 1 tot 255 en wordt aan elke TX-wachtrij toegewezen.

### Buffers

Aan elke wachtrij wordt een bepaalde hoeveelheid bufferruimte toegewezen om doorvoergegevens op te slaan. Inwoonster in de haven is het geheugen, dat opgesplitst wordt en

per haven wordt toegewezen. Voor elke GE poort wijst GE ASIC 512 K bufferruimte toe. Voor 10/100 poorten behoudt de haven ASIC 64 K of 128 K (afhankelijk van de lijnkaart) van per poort buffering. Deze bufferruimte wordt dan verdeeld tussen de Rx (ingress) rij en de wachtrijen TX (egress).

### Drempelwaarden

Eén aspect van normale datatransmissie is dat wanneer een pakket wordt ingetrokken, dit resulteert in het opnieuw verzenden van dat pakket (TCP-stromen). Wanneer er sprake is van stremmingen, kan dit de lading op het netwerk vergroten en mogelijk leiden tot overbelasting van de buffers. Om ervoor te zorgen dat buffers niet overstromen, gebruikt de Catalyst 6000 familieswitch een aantal technieken om dit te voorkomen.

Drempelwaarden zijn denkbeeldige niveaus die door de switch (of de beheerder) zijn toegewezen die gebruikspunten definiëren waarmee het congestiebeheeralgoritme kan beginnen om gegevens uit de wachtrij te laten vallen. Op Catalyst 6000 familiepoorten zijn er meestal vier drempels die gekoppeld zijn aan ingangswachtrijen. Er zijn gewoonlijk twee drempels verbonden aan uitvoerrijen.

Deze drempels worden ook ingezet, in de context van QoS, als een manier om frames met verschillende prioriteiten aan deze drempels toe te wijzen. Aangezien de buffer begint te vullen en de drempelwaarden worden overschreden, kan de beheerder verschillende prioriteiten in kaart brengen aan verschillende drempelwaarden die de switch aangeven welke frames moeten worden verlaagd wanneer een drempelwaarde wordt overschreden.

### Maps

In de wachtrijen en de drempelsecties hierboven werd vermeld dat de CoS-waarde in het Ethernet-frame wordt gebruikt om te bepalen in welke wachtrij het frame wordt geplaatst en op welk punt van de buffervulling een kader dat in aanmerking komt om te vallen is. Dit is het doel van het in kaart brengen.

Wanneer QoS in de Catalyst 6000-familie is geconfigureerd zijn de standaardinstellingen geactiveerd die het volgende definiëren:

- bij welke drempelwaarden voor frames met specifieke CoS-waarden mogen worden verlaagd
- in welke rij een kader is geplaatst (op basis van de CoS-waarde)

Terwijl de standaardopmaak bestaat, kunnen deze standaardmappingen door de beheerder worden gecorrigeerd. Toewijzing bestaat voor de volgende:

- CoS-waarden op een inkomend frame naar een DSCP-waarde
- IP-prioriteitswaarden op een inkomend frame voor een DSCP-waarde
- DSCP-waarden voor een CoS-waarde voor een uitgaande frame
- CoS-waarden om drempelwaarden bij wachtrijen te verlagen
- CoS-waarden om drempels bij verzendrijen te verlagen
- DSCP-markeringswaarden voor frames die politieverklaringen overschrijden
- CoS-waarden naar een kader met een specifiek MAC-adres voor de bestemming

## WRED en WRR

WRED en WRR zijn twee uiterst krachtige algoritmen in de Catalyst 6000-familie. Zowel WRED als WRR gebruiken de Priority tag (CoS) binnen een Ethernet-kader om een verbeterd bufferbeheer en een uitgaande planning te bieden. B

## WRED

WRED is een bufferbeheeralgoritme die door de Catalyst 6000-familie wordt gebruikt om de impact van het afvallen van prioritair verkeer tijdens een congestie tot een minimum te beperken. WRED is gebaseerd op het RODE algoritme.

Om RED en WRED te begrijpen, herhaal het concept van TCP-stroombeheer. Het beheer van de stroom waarborgt dat de TCP zender niet overweldigt het netwerk. Het TCP vertraagde algoritme is een deel van de oplossing om dit aan te pakken. Het dicteert dat wanneer een stroom begint, één enkel pakket wordt verzonden vóór het voor een ontvangstbevestiging wacht. Twee pakketten worden dan verzonden voordat een ACK wordt ontvangen, geleidelijk aan vergroot het aantal pakketten die vóór elke ACK wordt ontvangen. Dit zal doorgaan tot de stroom een transmissieniveau bereikt (dwz, verstuur *x* aantal pakketten) dat het netwerk kan verwerken zonder de lading die congestie veroorzaakt. Als er opstopping optreedt, zal het algoritme vertraagde start de venstergrootte terugdraaien (dat wil zeggen, het aantal pakketten dat wordt verzonden voordat er op een ontvangstbevestiging wordt gewacht), waardoor de algemene prestaties voor die TCP-sessie (flow) worden verminderd.

RED zal een wachtrij bewaken bij het invullen. Zodra een bepaalde drempel is overschreden, worden pakketten willekeurig verzonden. Er wordt geen rekening gehouden met specifieke stromen; willekeurige pakketten worden eerder ingetrokken . Deze pakketten kunnen afkomstig zijn van stromen met een hoge of een lage prioriteit. Gedrukte pakketten kunnen deel uitmaken van één stroom of meerdere TCP stromen. Als meerdere stromen van invloed zijn, zoals hierboven beschreven, kan dit een aanzienlijke impact hebben op de omvang van elk stroomvenster.

In tegenstelling tot RED is WRED niet zo willekeurig bij het laten vallen van frames. WRED houdt rekening met de prioriteit van de frames (in Catalyst 6000-geval gebruikt het de CoS-waarde). Met WRED wijst de beheerder frames met bepaalde CoS-waarden toe aan specifieke drempels. Zodra deze drempels zijn overschreden, kunnen frames met CoS-waarden die aan deze drempels zijn gekoppeld, worden ingetrokken. Andere frames met aan de hogere drempels toegewezen CoS-waarden worden in de wachtrij gehouden. Dit proces maakt het mogelijk om de hogere prioriteitsstromen intact te houden, hun grotere venstergrootte intact te houden en de latentie te minimaliseren die nodig is om de pakketten van de zender naar de ontvanger te krijgen.

Hoe weet je of je lijnkaart WRED ondersteunt? Geef de volgende opdracht uit. Controleer in het uitvoerdocument het gedeelte dat ondersteuning voor WRED op die poort aangeeft.

```
Console> show qos info config 2/1
QoS setting in NVRAM:
QoS is enabled
Port 2/1 has 2 transmit queue with 2 drop thresholds (2q2t).
Port 2/1 has 1 receive queue with 4 drop thresholds (1q4t).
Interface type:vlan-based
ACL attached:
The qos trust type is set to untrusted.
Default CoS = 0
Queue and Threshold Mapping:
Queue Threshold CoS
```

```
----- --------- ---------------
1     1         0 1
1     2         2 3
2     1         4 5
2     2         6 7
Rx drop thresholds:
Rx drop thresholds are disabled for untrusted ports.
Queue #  Thresholds - percentage (abs values)
-------  ----------------------------------
1        50% 60% 80% 100%
TX drop thresholds:
Queue #  Thresholds - percentage (abs values)
-------  ----------------------------------
1        40% 100%
2        40% 100%
TX WRED thresholds:
WRED feature is not supported for this port_type.
!-- Look for this. Queue Sizes: Queue # Sizes - percentage (abs values) ------- ----------------
-------------------- 1 80% 2 20% WRR Configuration of ports with speed 1000MBPS: Queue # Ratios
(abs values) ------- ----------------------------------- 1 100 2 255 Console> (enable)
```

Indien WRED niet beschikbaar is in een haven, gebruikt de haven een staart-valmethode van bufferbeheer. De val van de riem, zoals zijn naam impliceert, laat eenvoudigweg de inkomende frames vallen nadat de buffers volledig zijn gebruikt.

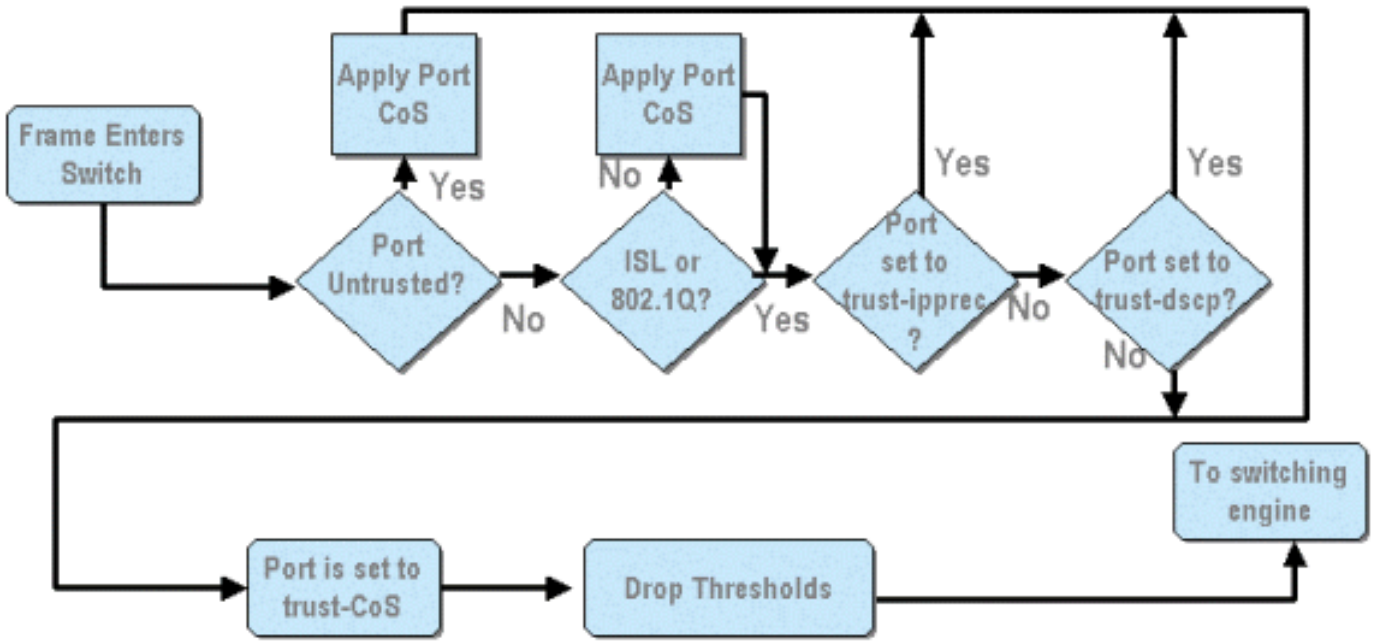
### WRR

WRR wordt gebruikt om stress verkeer te plannen vanaf TX wachtrijen. Een normaal ronde robin algoritme wisselt tussen de rijen van TX die een gelijk aantal pakketten van elke rij verzenden alvorens naar de volgende rij te bewegen. Met het gewogen aspect van WRR kan de planningsalgoritme een weging inspecteren die aan de wachtrij is toegewezen. Dit geeft gedefinieerde wachtrijen toegang tot meer van de bandbreedte. Het WRR-planningsalgoritme zal meer gegevens uit geïdentificeerde wachtrijen dan andere wachtrijen uitwissen, waardoor een voorkeur wordt gegeven voor toegewezen wachtrijen.

De configuratie van het WRR en de andere aspecten van de hierboven beschreven aspecten worden in de volgende secties beschreven.

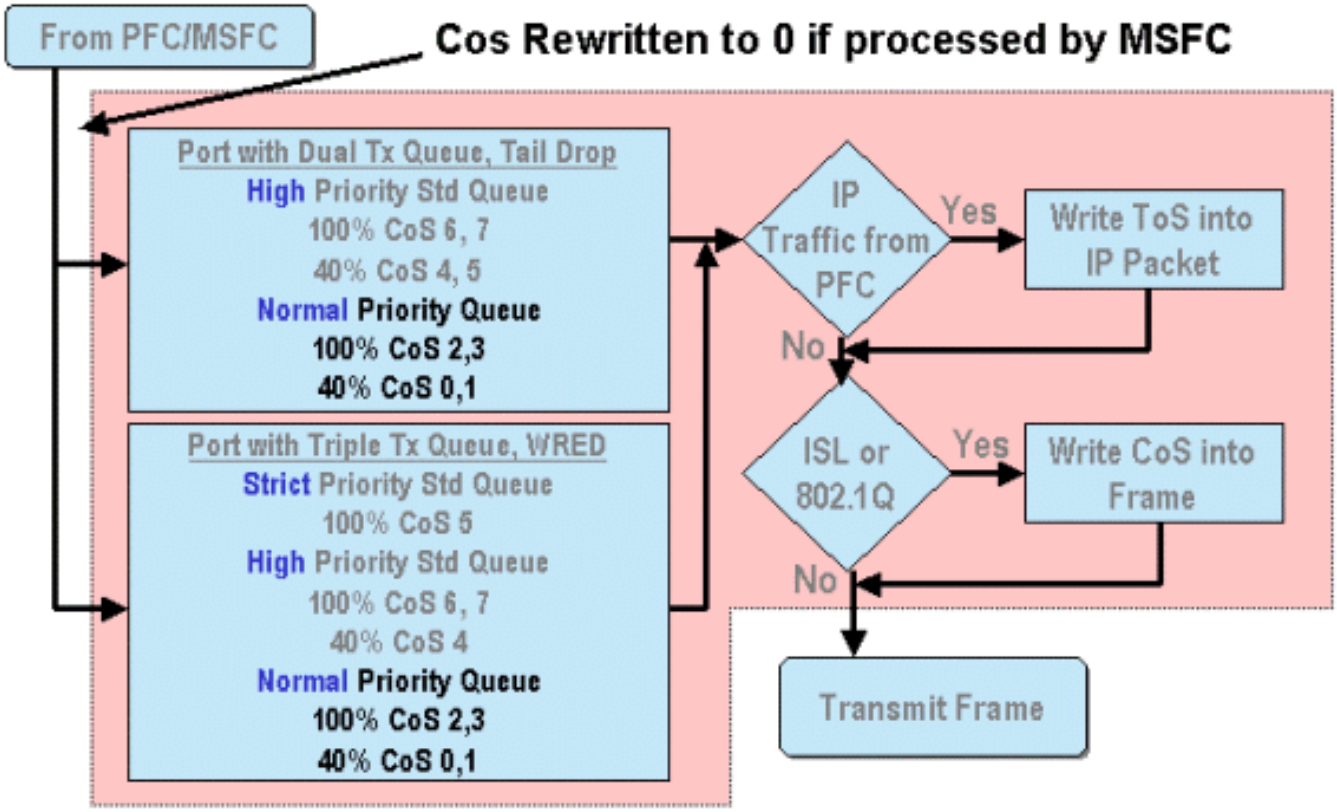
## Het configureren van poort op ASIC gebaseerde QoS op Catalyst 6000 reeks

QoS-configuratie heeft de poort-ASIC of de PFC opdracht om een QoS-actie uit te voeren. De volgende secties zullen de QoS-configuratie voor beide processen bekijken. Op de haven ASIC, beïnvloedt de QoS configuratie zowel inkomende als uitgaande verkeersstromen.




In het bovenstaande schema is te zien dat de volgende QoS-configuratieprocessen van toepassing zijn:

1. vertrouwensstaten in havens
2. toepassing van op poorten gebaseerde CoS
3. Toewijzing van minimale RX-waarde
4 CoS-to-RX-drop-drempelkaarten




Wanneer een kader door MSFC of de PFC wordt verwerkt, wordt het doorgegeven naar de uitgaande poort ASIC voor verdere verwerking. Alle frames die door de MSFC zijn verwerkt, worden de CoS-waarden teruggezet op nul. Hiermee moet rekening worden gehouden bij de QoS-

verwerking in uitgaande havens.

In het bovenstaande schema is aangegeven welke QoS-verwerking door de poort-ASIC is uitgevoerd voor uitgaande verkeer. Enkele van de processen die bij uitgaande QoS-verwerking worden ingeroepen zijn:

1. Toewijzing van TX-staart en WRED-drempels
2. CoS to TX tail drop en WRED maps

Ook, dat niet in het bovenstaande schema is weergegeven, is het proces om de CoS met behulp van een DSCP naar CoS-kaart aan het uitgaande frame toe te wijzen.

De volgende secties onderzoeken de QoS configuratiemogelijkheden van de op poort gebaseerde ASICs in meer detail.

**Opmerking:** Een belangrijk punt om te maken is dat wanneer QoS-opdrachten worden opgeroepen met behulp van CatOS, deze doorgaans van toepassing zijn op alle poorten met het gespecificeerde rijtype. Bijvoorbeeld, als een WRED-valdrempel wordt toegepast op poorten met wachtrijtype 1p2q2t, wordt deze WRED-drempel toegepast op alle poorten op alle lijnkaarten die dit rijtype ondersteunen. Met Cat IOS worden QoS-opdrachten doorgaans op het interfaceniveau toegepast.

## QoS inschakelen

Voordat er enige QOS-configuratie kan plaatsvinden in de Catalyst 6000-familie, moet QoS eerst op de switch zijn ingeschakeld. Dit wordt bereikt door het volgende opdracht uit te geven:

### CatOS

```
Console> (enable) set qos enable
!-- QoS is enabled. Console> (enable)
```

### Geïntegreerde Cisco IOS (native modus)

```
Cat6500(config)# mls qos
```

Wanneer QoS in de Catalyst 6000 familie is ingeschakeld, stelt de switch een serie QoS standaardinstellingen voor de switch in. Deze standaardinstellingen zijn de volgende instellingen:

| QoS Feature | Default setting |
|---|---|
| Trust state of each port | Un-trusted |
| Receive Queue drop threshold percentages | Threshold 1 – 50%<br>Threshold 2 – 60%<br>Threshold 3 – 80%<br>Threshold 4 – 100% |
| Transmit Queue drop threshold percentages | Low priority queue threshold 1 – 80%<br>Low priority queue threshold 2 – 100%<br>High priority queue threshold 1 – 80%<br>High priority queue threshold 2 – 100% |
| CoS value to Drop threshold mapping | Receive queue 1/drop threshold 1: CoS 0 and 1<br>Transmit queue 1/drop threshold 1: CoS 0 and 1<br>Receive queue 1/drop threshold 2: CoS 2 and 3<br>Transmit queue 1/drop threshold 2: CoS 2 and 3<br>Receive queue 1/drop threshold 3: CoS 4 and 5<br>Transmit queue 2/drop threshold 1: CoS 4 and 5<br>Receive queue 1/drop threshold 4: CoS 6 and 7 |
| | Transmit queue 2/drop threshold 2: CoS 6 and 7 |
| CoS to DSCP Mapping<br>(DSCP set from CoS value) | CoS 0 = DSCP 0<br>CoS 1 = DSCP 8<br>CoS 2 = DSCP 16<br>CoS 3 = DSCP 24<br>CoS 4 = DSCP 32<br>CoS 5 = DSCP 40<br>CoS 6 = DSCP 48<br>CoS 7 = DSCP 56 |
| IP Precedence to DSCP Map<br>(DSCP set from IP Precedence value) | IP precedence 0 = DSCP 0<br>IP precedence 1 = DSCP 8<br>IP precedence 2 = DSCP 16<br>IP precedence 3 = DSCP 24<br>IP precedence 4 = DSCP 32<br>IP precedence 5 = DSCP 40<br>IP precedence 6 = DSCP 48<br>IP precedence 7 = DSCP 56 |
| DSCP to CoS map<br>(CoS set from DSCP values) | DSCP 0-7 = CoS 0<br>DSCP 8-15 = CoS 1<br>DSCP 16-23 = CoS 2<br>DSCP 24-31 = CoS 3<br>DSCP 32-39 = CoS 4<br>DSCP 40-47 = CoS 5<br>DSCP 48-55 = CoS 6<br>DSCP 56-63 = CoS 7 |

## Trusted en onvertrouwde poorten

Elke poort op Catalyst 6000-familie kan worden geconfigureerd als vertrouwd of VN-vertrouwd The trust state of the port dicteert hoe het het frame markeert, classificeert en organiseert terwijl het de switch passeert. Standaard staan alle poorten in de onvertrouwde staat.

### Onvertrouwde poorten (standaardinstelling voor poorten)

Als de poort wordt geconfigureerd als een onbetrouwbare poort dan wordt in een frame dat de poort invoert, de CoS- en ToS-waarde door de poort ASIC op nul gezet. Dit betekent dat het frame de laagste prioritaire dienst krijgt op zijn pad door de switch.

In plaats hiervan kan de beheerder de CoS-waarde van een Ethernet-frame dat een onvertrouwde poort ingaat, ook terugstellen naar een vooraf bepaalde waarde. De configuratie van dit item wordt in een later gedeelte besproken.

Als u de poort instelt als onbetrouwbaar, wordt de switch geïnstrueerd geen congestievermijding uit te voeren. Congestievermijding is de methode die wordt gebruikt om frames op basis van hun CoS-waarden te laten vallen zodra ze de voor die wachtrij gedefinieerde drempels overschrijden. Alle frames die deze poort binnengaan, zullen ook in aanmerking komen om te vallen als de buffers 100% bereiken.

In CatOS kan een 10/100 of GE poort worden ingesteld als onbetrouwbaar door de volgende opdracht uit te geven:

### CatOS

```
Console> (enable) set port qos 3/16 trust untrusted
!-- Port 3/16 qos set to untrusted. Console> (enable)
```

Deze opdracht stelt poort 16 op module 3 in op een toestand van onbetrouwbaar.

**Opmerking:** Voor Geïntegreerde Cisco IOS (Native Mode) ondersteunt de software momenteel alleen het instellen van vertrouwen voor GE-poorten.

### Geïntegreerde Cisco IOS (native modus)

```
Cat6500(config)# interface gigabitethernet 1/1
Cat6500(config-if)# no mls qos trust
```

In het voorbeeld hierboven, gaan we de interfaceconfiguratie in en passen de **geen** vorm van de opdracht toe om de poort in te stellen als onbetrouwbaar aangezien het IOS is.

### Trusted poorten

Soms worden Ethernet-frames die een switch invoeren, voorzien van een CoS- of ToS-instelling waarvan de beheerder de switch wil handhaven terwijl het frame de switch doorvoert. Voor dit verkeer kan de beheerder de vertrouwenstatus van een haven instellen waar dat verkeer in de switch als vertrouwde op komt.

Zoals eerder vermeld gebruikt de switch intern een DSCP-waarde om een vooraf bepaald serviceniveau aan dat frame toe te wijzen. Aangezien een kader een vertrouwde poort ingaat, kan de beheerder de poort configureren om te kijken naar de bestaande CoS, IP voorrang of DSCP waarde om de interne DSCP waarde in te stellen. In plaats hiervan kan de beheerder een vooraf gedefinieerde DSCP instellen op elk pakje dat de poort ingaat.

U kunt de vertrouwensstatus van een poort naar vertrouwd instellen door de volgende opdracht uit te geven:

### CatOS

```
Console> (enable) set port qos 3/16 trust trust-cos
!-- Port 3/16 qos set to trust-COs Console> (enable)
```

Deze opdracht is van toepassing op de WS-X6548-RJ45 lijnkaart en stelt de vertrouwensstatus van poort 3/16 in op vertrouwd. De switch gebruikt de CoS-waarde die in het inkomende frame is ingesteld om de interne DSCP in te stellen. De DSCP is afgeleid van een standaard map die is aangemaakt toen QoS op de switch was ingeschakeld of anders van een kaart die door de beheerder is gedefinieerd. In plaats van het sleutelwoord van het vertrouwen-COs, kan de beheerder de sleutel van het trust-dscp of van het vertrouwens-ipprec ook gebruiken.

Op eerdere 10/100 lijnkaarten (WS-X6348-RJ45 en WS-X6248-RJ45) moet het poortvertrouwen worden ingesteld door de **ingestelde qos-**opdracht uit te geven. In deze opdracht kan een vertrouwensstaat worden toegewezen door een subparameter van de **set qos acl** opdracht. Het instellen van trust CoS op poorten op deze lijnkaarten wordt niet ondersteund, zoals hieronder wordt getoond.

```
Console> (enable) set port qos 4/1 trust trust-COs
Trust type trust-COs not supported on this port.
!-- Trust-COs not supported, use acl instead. Rx thresholds are enabled on port 4/1. !-- Need to
turn on input queue scheduling. Port 4/1 qos set to untrusted. !-- Trust-COs not supported, so
port is set to untrusted.
```

De bovenstaande opdracht geeft aan dat dit vereist is om een planning voor de invoerwachtrij mogelijk te maken. Voor 10/100 poorten op WS-X6248-RJ45 en WS-X6348-RJ45 lijnkaarten moet de opdracht **set port qos x/y trust-CO's** dus nog steeds worden geconfigureerd, hoewel om vertrouwensstatus in te stellen, moet ACL worden gebruikt.

Met Geïntegreerde Cisco IOS (Native Mode) kan de instelling van vertrouwen worden uitgevoerd op een GE-interface en 10/100 poorten op de nieuwe WS-X6548-RJ45 lijnkaart.

### Geïntegreerde Cisco IOS (native modus)

```
Cat6500(config)# interface gigabitethernet 5/4
Cat6500(config-if)# mls qos trust ip-precedence
Cat6500(config-if)#
```

Dit voorbeeld stelt de vertrouwensstatus van GE poort 5/4 in om vertrouwd te worden. De IP-prioriteitswaarde van het frame wordt gebruikt om de DSCP-waarde af te leiden.

## Invoerclassificatie en instellen van poortgebaseerde CoS

Bij toegang tot een switch poort kan een Ethernet frame zijn CoS laten veranderen als het aan een van de volgende twee criteria voldoet:

1. de poort is ingesteld als onbetrouwbaar, of
2. het Ethernet-frame heeft geen bestaande CoS-waarde die al is ingesteld

Als u de CoS van een inkomend Ethernet-frame wilt opnieuw configureren, dient u de volgende

opdracht uit te voeren:

### CatOS

```
Console> (enable) set port qos 3/16 cos 3
!-- Port 3/16 qos set to 3. Console> (enable)
```

Deze opdracht stelt de CO's van inkomende Ethernet frames in op poort 16 op module 3 in op een waarde van 3 wanneer een niet-gemarkeerd frame arriveert of als de poort op onbetrouwbaar is ingesteld.

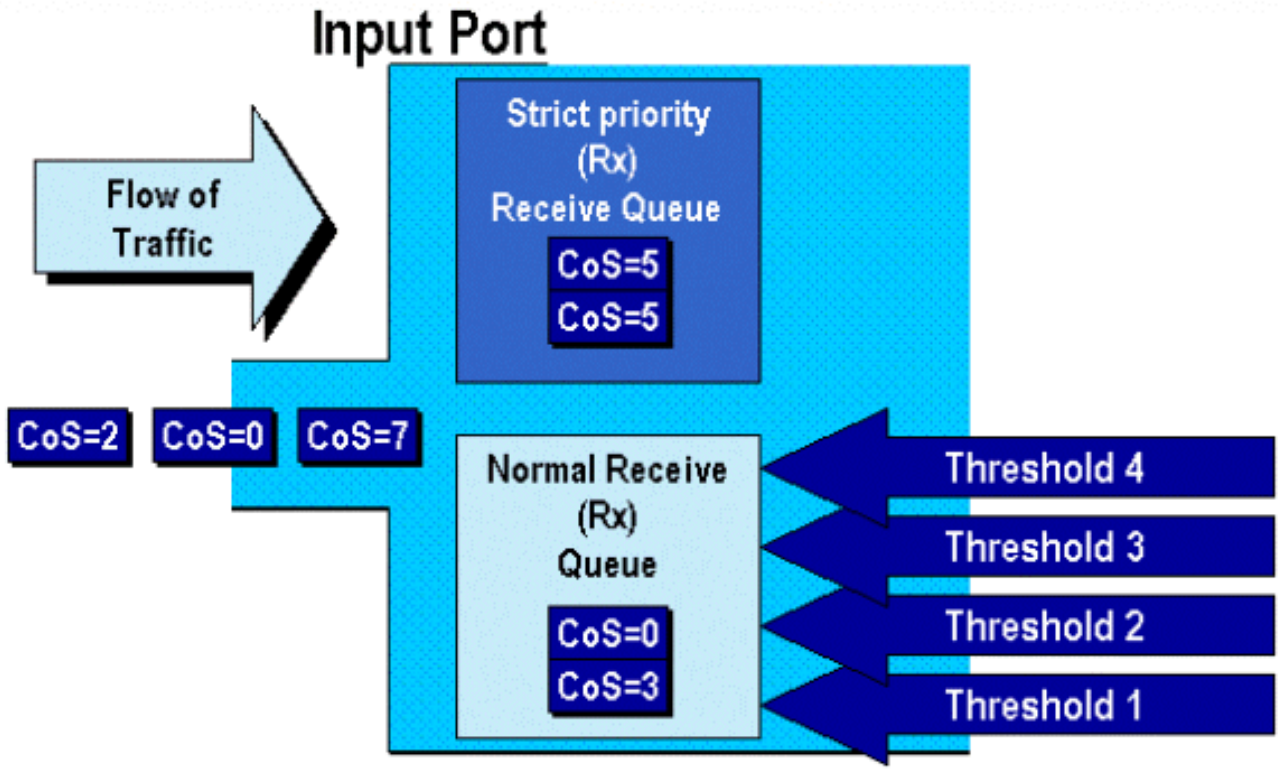
### Geïntegreerde Cisco IOS (native modus)

```
Cat6500(config)# interface fastethernet 5/13
Cat6500(config-if)# mls qos COs 4
Cat6500(config-if)#
```

Deze opdracht stelt de CO's van inkomende Ethernet frames in op poort 13 op module 5 in op een waarde van 4 wanneer een niet-gemarkeerd frame arriveert of als de poort op onbetrouwbaar is ingesteld.

## RX-drempels instellen

Bij toegang tot de poort van de switch wordt het kader in een rij Rx geplaatst. Om bufferoverstromen te voorkomen, implementeert de port ASIC vier drempels op elke Rx-rij en gebruikt deze drempels om frames te identificeren die kunnen worden gedropt zodra deze drempels zijn overschreden. De poort ASIC gebruikt de frames die CO's-waarde instellen om te identificeren welke frames kunnen worden gedropt wanneer een drempelwaarde wordt overschreden. Deze mogelijkheid maakt het mogelijk om hogere prioriteitsframes langer in de buffer te blijven als er opstopping optreedt.




Zoals in het bovenstaande diagram wordt getoond, arriveren de frames en worden deze in de wachtrij geplaatst. Aangezien de rij begint te vullen, worden de drempels gecontroleerd door de haven ASIC. Wanneer een drempel wordt overschreden, worden frames met door de beheerder geïdentificeerde CO2-waarden willekeurig uit de wachtrij geplaatst. De standaard drempeltoewijzingen voor een 1q4t wachtrij (gevonden op WS-X6248-RJ45 en WS-X6348-RJ45 lijnkaarten) zijn als volgt:

- drempelwaarde 1 is op 50% ingesteld en de CO's 0 en 1 worden aan deze drempelwaarde toegewezen
- drempelwaarde 2 is op 60% ingesteld en de CO2-waarden 2 en 3 worden aan deze drempelwaarde toegewezen
- drempelwaarde 3 is vastgesteld op 80% en de CO's 4 en 5 worden aan deze drempelwaarde toegewezen
- drempelwaarde 4 is ingesteld op 100% en de CO's 6 en 7 worden aan deze drempelwaarde toegewezen

Voor een 1P1q4t (gevonden op GE poorten) rij, zijn de standaardmappings als volgt:

- drempelwaarde 1 is op 50% ingesteld en de CO's 0 en 1 worden aan deze drempelwaarde toegewezen
- drempelwaarde 2 is op 60% ingesteld en de CO2-waarden 2 en 3 worden aan deze drempelwaarde toegewezen
- drempelwaarde 3 is ingesteld op 80% en CO2-waarden 4 worden aan deze drempelwaarde toegewezen
- drempelwaarde 4 is ingesteld op 100% en de CO's 6 en 7 worden aan deze drempelwaarde toegewezen
- CO's Waarde van 5 wordt in de wachtrij geplaatst met strikte prioriteit

Voor een 1p1q0t (gevonden op 10/100 poorten op de WS-X6548-RJ45 lijnkaart), zijn de standaardinstellingen als volgt:

- Frames met COs 5 gaan naar de SP Rx-wachtrij (wachtrij 2), waar de switch alleen inkomende frames laat vallen wanneer de SP-ontvangstwachtrij 100% vol is.
- Frames met CO's 0, 1, 2, 3, 4, 6 of 7 gaan naar de standaard RX-wachtrij. De switch laat inkomende frames vallen als de Rx-wachtrij buffer 100% vol is.

Deze dalingsdrempels kunnen door de beheerder worden gewijzigd. Ook kunnen de standaard CO's-waarden die aan elke drempelwaarde zijn gekoppeld, worden gewijzigd. Verschillende lijnkaarten implementeren verschillende Rx-rijimplementaties. Hieronder vindt u een samenvatting van de wachtrijtypen.

### CatOS

```
Console> (enable) set qos drop-threshold 1q4t rx queue 1 20 40 75 100
!-- Rx drop thresholds for queue 1 set at 20%, 40%, 75%, and 100%. Console> (enable)
```

Deze opdracht stelt de drempelwaarden voor alle ingangspoorten met één rij en vier drempels (punten 1q4t) in op 20%, 40%, 75% en 100%.

De opdracht die in Geïntegreerd Cisco IOS (Native Mode) wordt verstrekt, wordt hieronder weergegeven.

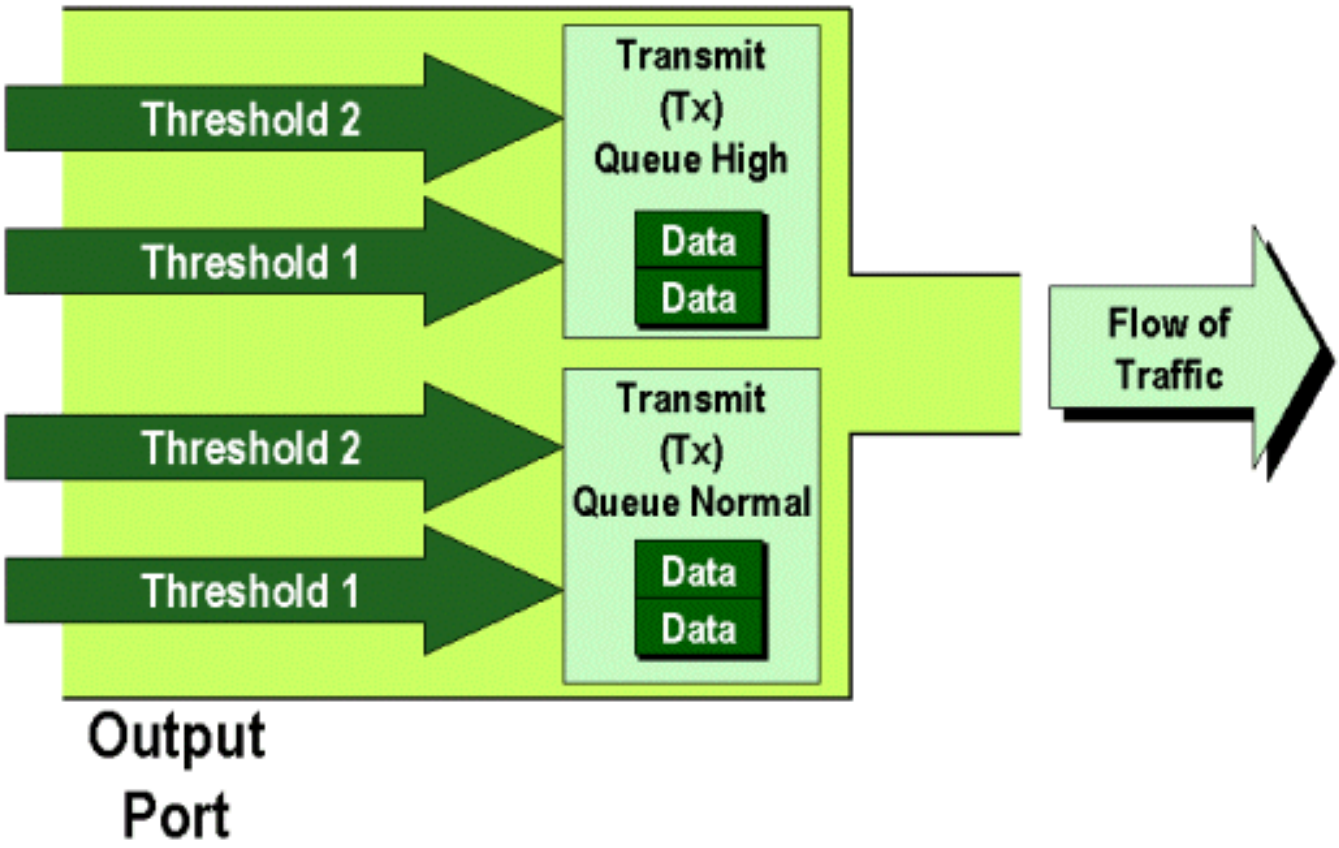
### Geïntegreerde Cisco IOS (native modus)

```
Cat6500(config-if)# wrr-queue threshold 1 40 50
Cat6500(config-if)# wrr-queue threshold 2 60 100

!-- Configures the 4 thresholds for a 1q4t rx queue and. Cat6500(config-if)# rcv-queue threshold
1 60 75 85 100

!-- Configures for a 1p1q4t rx queue, which applies to !-- the new WS-X6548-RJ45 10/100 line
card.
```

Rx-dalingsdrempels moeten door de beheerder worden ingeschakeld. Op dit moment moet de **ingestelde** poort qos x/y trust-COs opdracht worden gebruikt om de Rx-valdrempels in te stellen (waarbij *x* het modulenummer is en *y* de poort op die module).

## TX-drop-drempels configureren

Op een vrijhaven zal de haven twee X drempels hebben die als deel van het mechanisme van congestievermijding, rij 1 en rij 2 worden gebruikt. Wachtrij 1 wordt aangeduid als de standaard rij met lage prioriteit, en rij 2 wordt aangeduid als de standaard rij met hoge prioriteit. Afhankelijk van de gebruikte lijnkaarten, zullen zij of een munt of een WRED drempelbeheeralgoritme gebruiken. Beide algoritmen gebruiken twee drempels voor elke TX-wachtrij.




De beheerder kan deze drempels handmatig als volgt instellen:

### CatOS

```
Console> (enable) set qos drop-threshold 2q2t TX queue 1 40 100
!-- TX drop thresholds for queue 1 set at 40% and 100%. Console> (enable)
```

Deze opdracht stelt de TX-drempels voor wachtrij 1 in voor alle uitvoerpoorten met twee wachtrijen en twee drempels (punten 2q2t) op 40% en 100%.

```
Console> (enable) set qos wred 1p2q2t TX queue 1  60 100
!-- WRED thresholds for queue 1 set at 60% 100% on all WRED-capable 1p2q2t ports. Console>
(enable)
```

Deze opdracht stelt de WRED-drempels voor wachtrij 1 in voor alle uitvoerpoorten met één SP-wachtrij, twee normale wachtrijen en twee drempels (1p2q2t) op 60% en 100%. Wachtrij 1 wordt gedefinieerd als de normale rij met lage prioriteit en heeft de laagste prioriteit. Wachtrij 2 is de hoge prioriteit van de normale wachtrij en heeft een hogere prioriteit dan rij 1. Wachtrij 3 is de SP-wachtrij en wordt vóór alle andere wachtrijen op die haven onderhouden.

De equivalente opdracht uitgegeven in Geïntegreerd Cisco IOS (Native Mode) wordt hieronder weergegeven.

### Geïntegreerde Cisco IOS (native modus)

```
Cat6500(config-if)# wrr-queue random-detect max-threshold  1 40 100
```

```
Cat6500(config-if)#
```

Dit stelt de WRED-drempels in voor een 1p2q2t-poort in om 1 tot 40% in de rij te staan voor drempel 1 (TX) en 100% voor drempel 2 (TX).

WRED kan ook worden uitgeschakeld indien vereist in Geïntegreerd Cisco IOS (Native Mode). De methode die wordt gebruikt om dit te doen is de **n"** vorm van de opdracht te gebruiken. Een voorbeeld van het uitschakelen van WRED wordt als volgt weergegeven:

### Geïntegreerde Cisco IOS (native modus)

```
Cat6500(config-if)# no wrr-queue random-detect queue_id
```

## MAC-adres aan CO's-waarden toewijzen

Naast het instellen van CO's op basis van een mondiale poortdefinitie, staat de switch de beheerder toe om CO's-waarden in te stellen op basis van het MAC-adres van de bestemming en VLAN-id. Dit maakt het mogelijk dat voor specifieke doelstellingen bestemde frames worden getagd met een vooraf bepaalde CO2-waarde. Deze configuratie kan worden bereikt door de volgende opdracht uit te geven:

### CatOS

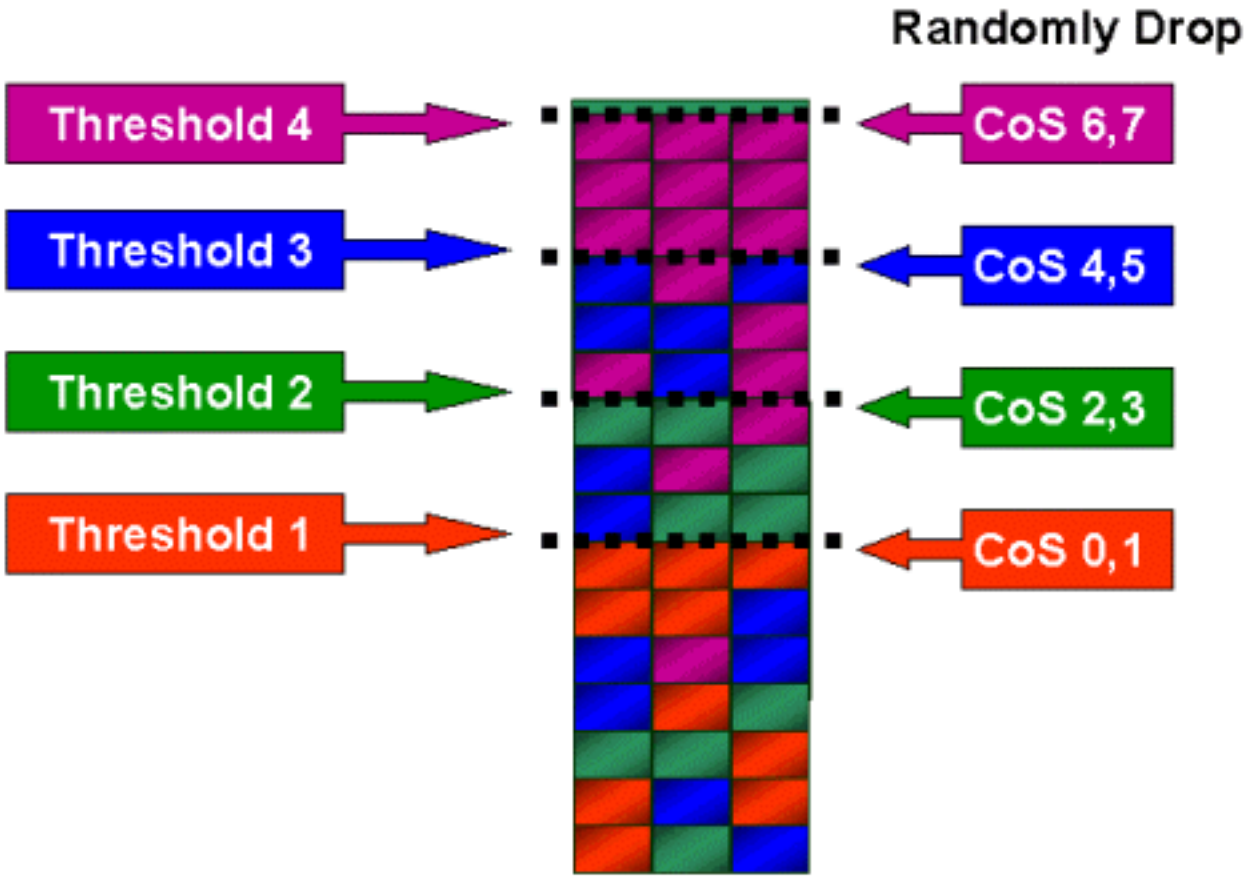
```
Console> (enable) set qos Mac-COs 00-00-0c-33-2a-4e 200 5
!-- COs 5 is assigned to 00-00-0c-33-2a-4e VLAN 200. Console> (enable)
```

Deze opdracht stelt een COs van 5 in voor elk frame waarvan het doel-MAC-adres 00-00-0c-33-2a-4e is dat van VLAN 200.

Er is geen gelijkwaardig bevel in Geïntegreerd Cisco IOS (Modus). Dit komt doordat deze opdracht alleen wordt ondersteund wanneer er geen PFC is en wanneer Geïntegreerde Cisco IOS (Native Mode) een PFC nodig heeft om te kunnen functioneren.

## CO's aan drempels toewijzen

Nadat de drempels zijn ingesteld, kan de beheerder dan de CO's-waarden aan deze drempels toewijzen, zodat wanneer de drempel is overschreden, frames met specifieke CO's-waarden kunnen worden ingetrokken. Gewoonlijk zal de beheerder lagere prioriteitsframes aan de lagere drempels toewijzen, zodat hoger prioritair verkeer in de rij behouden blijft indien zich opstopping voordoet.




Bovenstaande figuur laat een input-wachtrij met vier drempels zien, en hoe de CO's-waarden aan elke drempel zijn toegewezen.

De volgende output toont hoe de CO's-waarden in kaart kunnen worden gebracht in drempels:

### CatOS

```
Console> (enable) set qos map 2q2t 1 1 COs 0 1
!-- QoS TX priority queue and threshold mapped to COs successfully. Console> (enable)
```

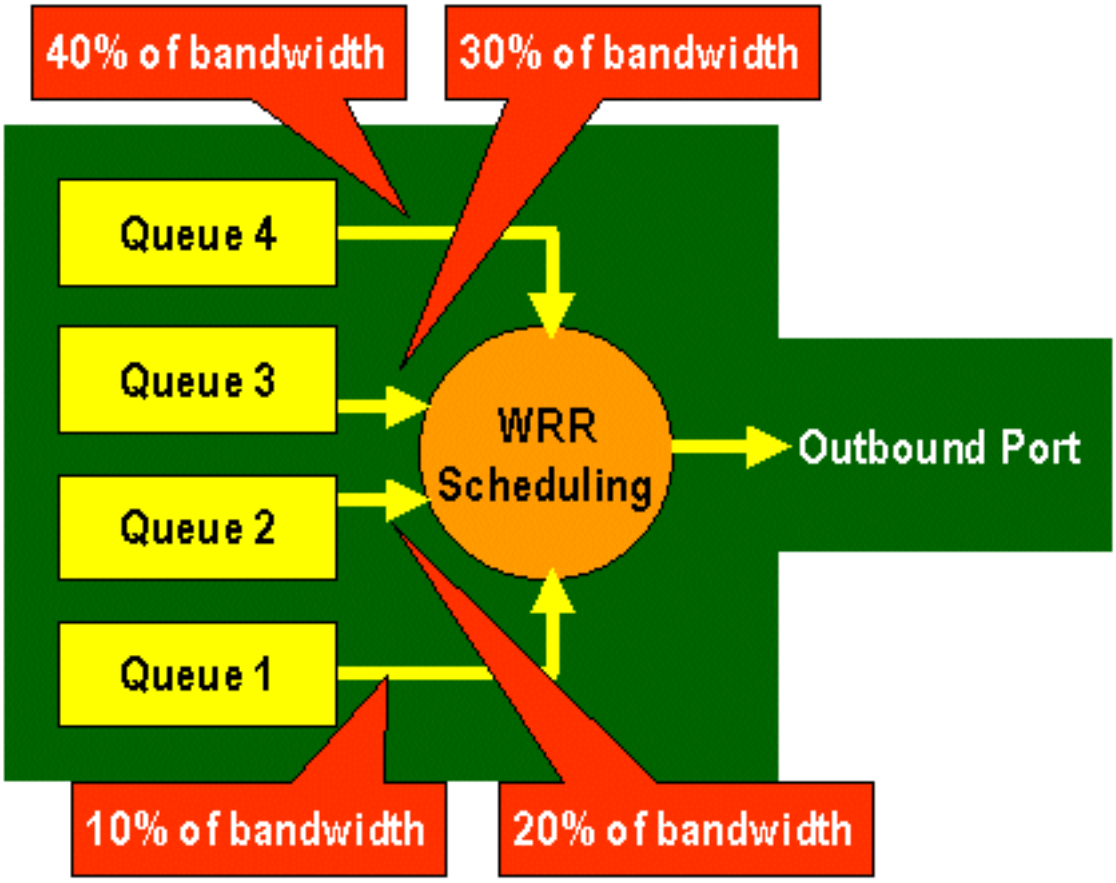
Deze opdracht wijst CO's-waarden van 0 en 1 toe aan wachtrij 1, drempel 1. De gelijkwaardige opdracht in Geïntegreerd Cisco IOS (Native Mode) wordt hieronder weergegeven.

### Geïntegreerde Cisco IOS (native modus)

```
Cat6500(config-if)# wrr-queue COs-map  1  1  0  1
Cat6500(config-if)#
```

## Bandbreedte instellen op TX-wachtrijen

Wanneer een kader in een uitvoerwachtrij wordt geplaatst, wordt het doorgegeven met behulp van een uitvoerplanningsalgoritme. Het uitvoerplannerproces gebruikt WRR om frames uit de uitvoerwachtrijen te verzenden. Afhankelijk van de hardware die op de lijnkaart wordt gebruikt, zijn er twee, drie of vier verzendrijen per poort.




Op de WS-X6248 en WS-X6348 lijnkaarten (met 2q2t rijstructuren) worden twee TX-rijen door het WRR-mechanisme gebruikt voor het plannen. Op de WS-X6548 lijnkaarten (met een 1p3q1t rijstructuur) zijn er vier TX wachtrijen. Van deze vier TX-wachtrijen worden drie TX-wachtrijen onderhouden door het WRR-algoritme (de laatste TX-wachtrij is een SP-wachtrij). Op GE-lijnkaarten zijn er drie TX-wachtrijen (met behulp van een 1p2q2t-rijstructuur); een van deze wachtrijen is een SP wachtrij zodat het WRR-algoritme alleen twee TX-wachtrijen biedt.

Meestal wijst de beheerder een gewicht aan de TX-wachtrij toe. WRR werkt door te kijken naar de weging die is toegewezen aan de havenrij, die intern door de switch wordt gebruikt om te bepalen hoeveel verkeer zal worden verzonden alvorens naar de volgende rij te gaan. Een wegingswaarde tussen 1 en 255 kan aan elke havenwachtrij worden toegewezen.

### CatOS

```
Console> (enable) set qos wrr 2q2t 40 80
!-- QoS wrr ratio set successfully. Console> (enable)
```

Deze opdracht wijst een weging van 40 toe aan rij 1 en 80 aan rij 2. Dit betekent effectief een verhouding van twee tot één (80 tot 40 = 2 tot 1) toegewezen bandbreedte tussen de twee wachtrijen. Deze opdracht wordt van kracht op alle poorten met twee rijen en twee drempels op havens.

De equivalente opdracht uitgegeven in Geïntegreerd Cisco IOS (Native Mode) wordt hieronder weergegeven.

### Geïntegreerde Cisco IOS (native modus)

```
Cat6500(config-if)# wrr-queue bandwidth 1 3
Cat6500(config-if)#
```

Het bovenstaande staat voor een verhouding van drie tot één tussen de twee rijen. U merkt dat de Cat IOS versie van deze opdracht alleen van toepassing is op een specifieke interface.

## Toewijzing van DSCP naar CO's

Wanneer het frame in de bovenlooppoort is geplaatst, gebruikt de poort-ASIC de toegewezen CO's om congestievermijding (dat wil zeggen, WRED) uit te voeren en gebruikt het OCR-systeem ook om de planning van het frame (dat wil zeggen, het frame doorgeven) te bepalen. Op dit punt zal de switch een standaardkaart gebruiken om de toegewezen DSCP in kaart te brengen en die terug naar een COs-waarde in kaart te brengen. Deze standaardmap wordt in deze tabel weergegeven.

In plaats hiervan kan de beheerder een map maken die door de switch gebruikt zal worden om de toegewezen interne DSCP-waarde te nemen en een nieuwe CO2-waarde voor het frame te maken. Voorbeelden van hoe u CatOS en Geïntegreerd Cisco IOS (Modus) zou gebruiken om dit te bereiken worden hieronder weergegeven.

### CatOS

```
Console> (enable) set qos dscp-cos--map 20-30:5 10-15:3 45-52:7
!-- QoS dscp-cos-map set successfully. Console> (enable)
```

De bovenstaande opdracht geeft DSCP-waarden 20 tot 30 in kaart aan een COs-waarde van 5, DSCP-waarden 10 tot 15 in een COs van 3 en DSCP-waarden 45 tot 52 in een COs-waarde van 7. Alle andere DSCP-waarden gebruiken de standaardkaart die is gemaakt wanneer QoS op de switch is ingeschakeld.

De equivalente opdracht uitgegeven in Geïntegreerd Cisco IOS (Native Mode) wordt hieronder weergegeven.

### Geïntegreerde Cisco IOS (native modus)

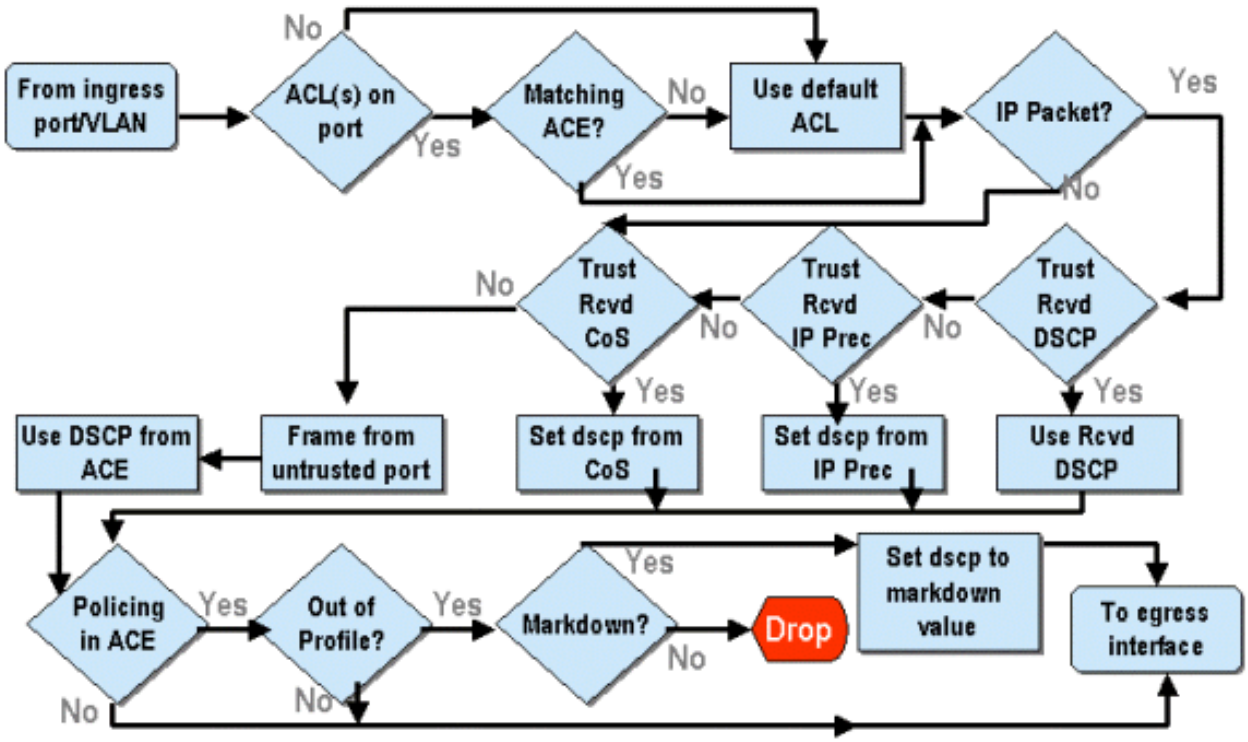
```
Cat6500(config)# mls qos map dscp-cos 20 30 40 50 52 10 1 to 3
Cat6500(config)#
```

Hiermee worden DSCP-waarden van 20, 30, 40, 50, 52, 10 en 1 ingesteld op een CO-waarde van 3.

# Classificatie en toezicht met de PFC

De PFC ondersteunt de classificatie en het toezicht op frames. De classificatie kan ACL gebruiken om (merk) een inkomend kader met een prioriteit (DSCP) toe te wijzen. Door te controleren kan een verkeersstroom worden beperkt tot een bepaalde hoeveelheid bandbreedte.

De volgende secties zullen deze mogelijkheden op de PFC vanuit het perspectief van zowel het CatOS als de Geïntegreerde platforms van Cisco IOS (Native Mode) OS beschrijven. De door de PFC toegepaste processen worden in het volgende schema weergegeven:




## Toezicht configureren op de Catalyst 6000 reeks met CatOS

De functie van het toezicht wordt opgesplitst in twee delen, één voor CatOS en één voor Geïntegreerde Cisco IOS (Native Mode). Beiden bereiken hetzelfde eindresultaat, maar worden op verschillende manieren geconfigureerd en geïmplementeerd.

### Toezicht

De PFC ondersteunt de mogelijkheid om grensverkeer (of politie) naar de switch te verplaatsen en kan de verkeersstroom naar een van te voren vastgestelde limiet beperken. Het verkeer dat deze grenswaarde overschrijdt kan worden ingetrokken of de DSCP waarde in het frame is gemarkeerd naar een lagere waarde.

Output (egress)-snelheidsbeperking wordt momenteel niet ondersteund in PFC1 of PFC2. Dit zal worden toegevoegd in een nieuwe herziening van de PFC die gepland is voor de tweede helft van 2002 en die uitvoertoezicht (of noodtoezicht) zal ondersteunen.

Toezicht wordt ondersteund in zowel het CatOS als het nieuwe Geïntegreerde Cisco IOS (Native Mode), hoewel de configuratie van deze functies zeer verschillend is. In de volgende secties wordt de configuratie van de politiebewaking in beide OS-platforms beschreven.

### Aggregaten en microstromen (CatOS)

Aggregaten en Microflow zijn termen die worden gebruikt om het bereik van het toezicht te definiëren dat de PFC uitvoert.

Een microflow definieert het toezicht op één stroom. Een stroom wordt gedefinieerd door een sessie met een uniek MAC-adres, SA/DA IP-adres en TCP/UDP-poortnummers. Voor elke nieuwe stroom die door een poort van een VLAN wordt geïnitieerd, kan de microflow worden gebruikt om de hoeveelheid gegevens te beperken die voor die stroom door de switch worden ontvangen. In de definitie van microflow kunnen pakketten die de voorgeschreven snelheidsgrens overschrijden gedemonteerd worden of hun DSCP waarde verlaagd worden.

Overeenkomstig met een microflow kan een aggregaat worden gebruikt om limietverkeer te meten. Niettemin, is het geaggregeerde tarief van toepassing op al verkeer binnenkomend op een haven of VLAN dat een gespecificeerde QoS ACL aanpast. U kunt het aggregaat bekijken als het toezicht op cumulatief verkeer dat overeenkomt met het profiel in het Access Control Entry (ACE).

Zowel het aggregaat als de microflow definiëren de hoeveelheid verkeer die in de switch kan worden geaccepteerd. Zowel een aggregaat als een microflow kunnen tegelijkertijd aan een poort of een VLAN worden toegewezen.

Bij het definiëren van microstromen kunnen maximaal 63 daarvan worden gedefinieerd en kunnen maximaal 1023 aggregaten worden gedefinieerd.

### Toegangscontrolelijsten en QoS ACL's (CatOS)

Een QoS ACL bestaat uit een lijst van ACEs die een reeks QoS regels definieert die de PFC gebruikt om inkomende frames te verwerken. Aces zijn vergelijkbaar met een routertoegangscontrolelijst (RACL). ACE definieert classificatie, markering en politiecriteria voor een inkomend frame. Als een inkomend frame voldoet aan de criteria die in het ACE zijn ingesteld, verwerkt de QoS-motor het frame (zoals geacht door het ACE).

Alle QoS-verwerkingsstappen worden uitgevoerd op hardware, zodat QoS-toezicht geen invloed heeft op de prestaties van de switch.

De PFC2 ondersteunt momenteel maximaal 500 ACL's en deze ACL's kunnen uit maximaal 32000 Aces (in totaal) bestaan. Feitelijke ACE-nummers zullen afhangen van andere services die gedefinieerd zijn en beschikbaar geheugen in de PFC.

Er zijn drie soorten apparaten die kunnen worden gedefinieerd. Ze zijn IP, IPX en MAC. Zowel IP als IPX Aces inspecteren L3 header informatie, terwijl MAC-gebaseerde Aces alleen L2 header informatie inspecteren. Ook moet worden opgemerkt dat MAC Aces alleen kan worden toegepast op niet-IP en niet-IPX verkeer.

### Toezichtregels maken

Het proces van het creëren van een politieregel houdt in dat er een aggregaat (of microflow) wordt gemaakt, om dat aggregaat (of de microflow) in kaart te brengen naar een ACE.

Als, bijvoorbeeld, de vereiste was om al het inkomende IP-verkeer op poort 5/3 te beperken tot een maximum van 20 MB, moeten de twee bovengenoemde stappen worden geconfigureerd.

Eerst wordt in het voorbeeld gevraagd om al het inkomende IP-verkeer te beperken. Dit houdt in dat een geaggregeerde politieagent moet worden gedefinieerd. Een voorbeeld hiervan kan zijn:

```
Console> (enable) set qos policer aggregate test-flow rate 20000 burst 13 policed-dscp
!-- Hardware programming in progress !-- QoS policer for aggregate test-flow created
successfully. Console> (enable)
```

We hebben samengevoegd, testflow genoemd. Het definieert een percentage van 20000 KBPS (20 MBPS) en een uitbarsting van 13. Het politie-dscp sleutelwoord geeft aan dat elke gegevens die dit beleid overschrijden, zijn DSCP waarde gemarkeerd hebben zoals gespecificeerd in een DSCP markeerkaart (een standaard is er of dit kan worden gewijzigd door de beheerder). Een afwisselend aan het gebruiken van het politied-dscp sleutelwoord is het druppelsleutelwoord te gebruiken. Het uitrolsleutelwoord zal eenvoudig al het out-of-profile verkeer laten vallen (verkeer dat buiten de toegewezen barstwaarde valt).

De politie-eenheid werkt op een emmer-systeem met een lekkagetoken, in die zin dat je een uitbarsting definieert (wat de hoeveelheid gegevens in bits per seconde is die je accepteert binnen een bepaald (vast) tijdsinterval), en dan het percentage (dat wordt gedefinieerd als de hoeveelheid gegevens die je in één seconde uit die emmer zal leeghalen). Alle gegevens die dit emmer overstromen, worden ingetrokken of de DSCP is gemarkeerd. De opgegeven tijdsperiode (of interval) hierboven is 0,00025 seconden (of 1/4000ste seconde) en is vastgemaakt (dwz, u kunt geen configuratieopdrachten gebruiken om dit nummer te wijzigen).

Het getal 13 uit het bovenstaande voorbeeld vertegenwoordigt een emmer die maximaal 13.000 bits gegevens per 1/4000ste van een seconde zal accepteren. Dit heeft betrekking op 52 MB a seconde (13K * (1 / 0.00025) of 13K * 4000). U moet er altijd voor zorgen dat de barst is ingesteld op of hoger dan het tempo waarin u gegevens wilt verzenden. Met andere woorden, de uitbarsting dient groter te zijn dan of gelijk aan de minimale hoeveelheid gegevens die u gedurende een bepaalde periode wilt verzenden. Als de uitbarsting een lager getal oplevert dan wat u hebt opgegeven als uw tarief, zal de tarieflimiet gelijk zijn aan de uitbarsting. Met andere woorden, als je een snelheid van 20 MBPS definieert en een uitbarsting die berekent tot 15 MBPS, zal je snelheid nooit hoger zijn dan 15 MBPS. De volgende vraag die je misschien stelt is waarom 13? Onthoud dat de burst de diepte van de symbolische emmer definieert, of met andere woorden, de diepte van de emmer die gebruikt wordt om elke 1/4000th van een seconde binnenkomende gegevens te ontvangen. De burst zou dus een gegeven kunnen zijn dat ondersteund wordt door een aankomsdata van 20 MB of meer. De minimale uitbarsting die je zou kunnen gebruiken voor een snelheidslimiet van 20 MB is 2000/4000 = 5.

Bij het verwerken van de politieagent begint de algoritme van het toezicht door de token op te vullen met een volledige aanvulling op penningen. Het aantal penningen is gelijk aan de waarde van de uitbarsting. Dus, als de waarde 13 is, is het aantal penningen in de emmer gelijk aan 13.000. Voor elke 1/4000ste van een seconde zal de algoritme van de politie een hoeveelheid gegevens sturen die gelijk is aan het gedefinieerde percentage gedeeld door 4000. Voor elk bit (binair cijfer) aan verzonden gegevens, verbruikt het één token uit de emmer. Aan het eind van het interval zal het de emmer met een nieuwe set penningen aanvullen. Het aantal penningen dat wordt vervangen wordt gedefinieerd aan de hand van het tarief / 4000. Bekijk het voorbeeld hierboven om dit te begrijpen:

```
Console> (enable) set qos policer aggregate test-flow rate 20000 burst 13
```

Stel dat dit een haven van 100 MBPS is en we sturen een constante stroom van 100 MBPS naar de haven. We weten dat dit gelijk zal zijn aan een inkomend tempo van 100.000.000 bits per seconde. De parameters hier zijn een percentage van 20000 en een uitbarsting van 13. Op het tijdstip t0 is er een volledige aanvulling van penningen in de emmer (dat is 13.000). Op tijd interval t0, zullen de eerste reeks gegevens in de haven aankomen. Voor dit tijdsinterval zal het aankomstpercentage 100.000.000 / 4000 = 25.000 bits per seconde zijn. Omdat onze penningmeester maar een diepte heeft van 13.000 penningen, komen slechts 13.000 bits van de 25.000 bits die in deze tussenpoos de haven binnenkomen in aanmerking voor verzending en worden 12.000 bits laten vallen.

Het gespecificeerde tarief definieert een verzendingssnelheid van 20.000.000 bits per seconde, wat gelijk is aan 5.000 bits verzonden per 1/4000ste interval. Voor elke 5.000 verzonden bits worden er 5.000 gebruikte penningen gebruikt. Op tijdinterval T1 komen nog eens 25.000 bits data aan, maar de emmer daalt 12.000 bits. De emmer wordt aangevuld met penningen die worden gedefinieerd als het percentage / 4000 (dat staat voor 5000 nieuwe penningen). De algoritme stuurt dan de volgende aanvulling van data, wat overeenkomt met nog eens 5000 bits data (wat nog eens 5000 penningen verbruikt) en zo verder voor elk interval.

Gegevens die meer dan de diepte van de emmer (gedefinieerde uitbarsting) binnenkomen,

worden in wezen ingetrokken. Gegevens die na verzending van gegevens zijn achtergebleven (overeenkomend met de opgegeven frequentie) worden ook ingetrokken, zodat plaats wordt gemaakt voor de volgende verzameling aankomende gegevens. Een onvolledig pakket is er een dat niet volledig binnen het tijdsinterval is ontvangen, wordt niet gedropt maar bewaard totdat het volledig in de poort is ontvangen.

Dit burst nummer veronderstelt een constante verkeersstroom. In netwerken in de echte wereld zijn gegevens echter niet constant en wordt zijn stroom bepaald door de grootte van het TCP-venster, die de TCP-erkenning in de transmissievolgorde verwerkt. Om rekening te houden met de kwesties van de grootte van het TCP-venster wordt aangeraden om de barstwaarde te verdubbelen. In het bovenstaande voorbeeld wordt de voorgestelde waarde van 13 in werkelijkheid ingesteld op 26.

Een ander belangrijk punt dat ik naar voren moet brengen is dat op time-interval 0 (dat wil zeggen het begin van een politiecyclus) de pennenzak vol tokens zit.

Dit geaggregeerde beleid moet nu worden opgenomen in een kwantitatieve versoepeling. De ACE is waar de specificatie wordt gemaakt om een reeks criteria aan een inkomend frame te koppelen. Neem het volgende voorbeeld. U wilt het aggregaat toepassen dat boven op al IP verkeer wordt gedefinieerd, maar specifiek voor verkeer dat van Subnet 10.5.x.x wordt afgeleid en voorbestemd voor Subnet 203.100.45.x. ACE zou er als volgt uitzien:

```
Console> (enable) set qos acl ip test-acl trust-dscp aggregate test-flow tcp 10.5.0.0
203.100.45.0
!-- Test-acl editbuffer modified. Issue the commit command to apply changes.
Console> (enable)
```

De bovenstaande opdracht heeft een IP ACE gecreëerd (aangegeven door het gebruik van de **ingestelde qos acl ip**-opdracht), dat nu wordt gekoppeld aan een QoS ACL genaamd testgalg. Latere Aces die zijn gemaakt en gekoppeld aan de ACL-testband worden toegevoegd aan het einde van de ACE-lijst. De ACE-ingang heeft de bijbehorende totale teststroom. Om het even welke TCP stromen met een bronsubnet van 10.5.0.0 en bestemmingssubnet van 203.100.45.0 zal dit beleid op het van toepassing zijn hebben.

ACL's (en de bijbehorende Aces) bieden een zeer granulair niveau van configuratieflexibiliteit die beheerders kunnen gebruiken. ACL kan uit één of een aantal bronnen bestaan, en bron- en/of doeladressen kunnen worden gebruikt evenals L4 poortwaarden om bepaalde stromen te identificeren die moeten worden gecontroleerd.

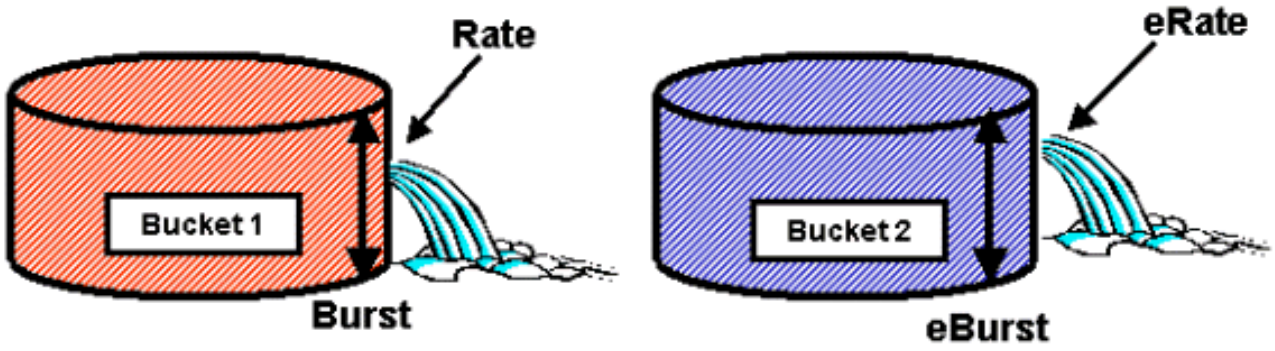
Maar voordat er daadwerkelijk toezicht wordt uitgeoefend, moet ACL in kaart worden gebracht met een fysieke poort of een VLAN.

### PFC2-beleidsbeslissingen

Voor de PFC2 is een verandering aangebracht in CatOS 7.1 en CatOS 7.2, die een dubbel lekkage emmer algoritme voor controle introduceerden. Met dit nieuwe algoritme, voegt het de volgende twee nieuwe niveaus toe:

1. **Normaal toezicht:** dit is gelijk aan het eerste emmer en definieert parameters die de diepte van de emmer (breuk) en de snelheid aangeven waartegen gegevens uit de emmer moeten worden verzonden (snelheid).
2. **Overtollige mate van toezicht:** dit is gelijk aan een tweede emmer en definieert parameters die de diepte van de emmer ( eburst ) en de snelheid aangeven waartegen

gegevens uit de emmer moeten worden verzonden ( erate ) .




De manier waarop dit proces werkt, is dat data het eerste emmer invullen. De PFC2 accepteert een inkomende gegevensstroom die kleiner is dan of gelijk is aan de diepte (burst value) van het eerste emmer. Gegevens die overstromen van het eerste emmer kunnen worden gemarkeerd en worden doorgegeven aan het tweede emmer. Het tweede emmer kan een inkomend gegevensstroom uit emmer één accepteren tegen een waarde die gelijk is aan of lager is dan de waarde van de uitbarsting. Gegevens uit het tweede emmer worden verzonden tegen een snelheid die wordt bepaald door de erate parameter minus de snelheidsparameter. Gegevens die van het tweede emmer overstromen, kunnen ook worden gemarkeerd of ingetrokken.

Een voorbeeld van een tweevoudige leksechte emmer-agent is als volgt:

```
Console> (enable) set qos policer aggregate AGG1 rate 10000 policed-dscp erate 12000 drop burst
13 eburst 13
```

Dit voorbeeld stelt een aggregaat in dat AGG1 wordt genoemd met een verkeerssnelheid van meer dan 10 MBPS, en zal worden gemarkeerd volgens de bewaakte DSCP-kaart. Verkeer meer dan het vorige (ingesteld op 12 MBPS) zal gedaald worden volgens het uitrolsleutelwoord.

### Geaggregeerde beleidsmakers toepassen op DFC-enabled-modules

Er zij op gewezen dat de toepassing van geaggregeerde politiemensen op niet-DFC lijnkaarten kan worden verwezenlijkt door de wijze waarop de 6000 een gecentraliseerde expediteur (PFC) gebruikt voor het doorsturen van verkeer. De implementatie van een centrale expediteur stelt het in staat om verkeersstatistieken voor een bepaald VLAN bij te houden. Dit proces kan worden gebruikt om een geaggregeerde politieagent op een VLAN toe te passen.

Op een DFC-enabled lijnkaart, echter, worden de verzendende besluiten aan die lijnkaart verdeeld. De DFC is alleen op de hoogte van de havens op haar directe lijnkaart en is niet op de hoogte van de verkeersbeweging op andere lijnkaarten. Om deze reden, als een geaggregeerde politieman wordt toegepast op een VLAN dat aangesloten poorten over meerdere DFC modules heeft, kan de politieman inconsistente resultaten produceren. De reden hiervoor is dat de DFC alleen de plaatselijke havenstatistieken kan bijhouden en geen rekening houdt met havenstatistieken op andere lijnkaarten. Om deze reden zal een geaggregeerde politier die op een VLAN met aangesloten poorten op een DFC-enabled lijnkaart wordt toegepast, in het DFC politieverkeer resulteren om de gespecificeerde limiet voor VLAN-poorten die alleen op de DFC-lijnkaart staan te controleren.

### DSCP-markeerkaarten (CatOS)

DSCP-markeerkaarten worden gebruikt als de politieagent is gedefinieerd om buiten profiel verkeer te markeren in plaats van het te laten vallen. Out-of-profile verkeer is gedefinieerd als het verkeer dat de gedefinieerde burst-instelling overschrijdt.

Een standaard DSCP markeerkaart is ingesteld wanneer QoS is ingeschakeld. Deze standaardindellageerkaart is in deze tabel opgenomen eerder in het document. Met de Opdrachtlijn Interface (CLI) kan een beheerder de standaardinstelmap wijzigen door de **ingestelde qo's** uit **te** geven **met** behulp **van een** dscp-map. Hieronder wordt een voorbeeld gegeven.

```
Cat6500(config)# set qos policed-dscp-map 20-25:7 33-38:3
```

In dit voorbeeld wordt de getrainde DSCP-map aangepast om aan te geven dat de DSCP-waarden 20 tot en met 25 worden gemarkeerd naar een DSCP-waarde van 7, en dat de DSCP-waarden van 33 tot en met 38 worden gemarkeerd naar een DSCP-waarde van 3.

## Toewijzing van beleid aan VLAN's en poorten (CatOS)

Zodra een ACL is gebouwd, moet het dan in kaart worden gebracht aan of een haven of een VLAN zodat die ACL van kracht wordt.

Eén interessante opdracht die veel onbewust vangt is de standaard QoS-instelling die alle QoS-poorten gebaseerd maakt. Als u een aggregaat (of microflow) op een VLAN toepast, zal het niet op een poort van kracht worden tenzij die poort is geconfigureerd voor VLAN-gebaseerde QoS.

```
Console> (enable) set port qos 2/5-10 vlan-based
!-- Hardware programming in progress  !-- QoS interface is set to vlan-based for ports 2/5-10.
Console> (enable)
```

Veranderen van op poort gebaseerde QoS naar op VLAN gebaseerde QoS ontspant onmiddellijk alle ACLs die aan die poort zijn toegewezen en wijst op om het even welke op VLAN gebaseerde ACLs aan die poort toe.

Toewijzing van ACL aan een poort (of VLAN) wordt gedaan door de volgende opdracht uit te geven:

```
Console> (enable) set qos acl map test-acl 3/5
!-- Hardware programming in progress  !-- ACL test-acl is attached to port 3/5. Console>
(enable) Console> (enable) set qos acl map test-acl 18
!-- Hardware programming in progress  !-- ACL test-acl is attached to VLAN 18. Console> (enable)
```

Zelfs na het in kaart brengen van ACL aan een haven (of VLAN), wordt ACL nog steeds niet van kracht tot ACL aan hardware wordt geëngageerd. Dit wordt beschreven in de volgende paragraaf. Op dit punt, ligt ACL in een tijdelijk bewerk buffer in geheugen. Terwijl in deze buffer, kan ACL worden gewijzigd.

Als u niet-geëngageerde ACL's wilt verwijderen die in de bewerkingsbuffer aanwezig zijn, geeft u de opdracht **terugdraaiing** uit. Deze opdracht verwijdert in wezen ACL uit de bewerkingsbuffer.

```
Console> (enable) rollback qos acl test-acl
!-- Rollback for QoS ACL test-acl is successful. Console> (enable)
```

## ACL's (CatOS) invoeren

Om QoS ACL toe te passen die u (hierboven) hebt bepaald, moet ACL aan hardware worden gecommitteerd. Het proces om ACL van de tijdelijke buffer aan de PFC hardware te binden. Zodra

hij in het PFC-geheugen verblijft, kan het beleid dat in QoS ACL is gedefinieerd worden toegepast op al het verkeer dat met de Aces overeenkomt

Voor gemak van configuratie geven de meeste beheerders een **vastlegging aan alle** opdracht uit. U kunt echter een specifieke ACL (een van de vele) plegen die momenteel in de bewerkingsbuffer kan voorkomen. Hieronder wordt een voorbeeld van de opdracht gecommitteerd.

```
Console> (enable) commit qos acl test-acl
!-- Hardware programming in progress  !-- ACL test-acl is committed to hardware. Console>
(enable)
```

Als u ACL uit een poort (of VLAN) wilt verwijderen, moet u de kaart wissen die ACL aan die poort (of VLAN) associeert door de volgende opdracht uit te geven:

```
Console> (enable) clear qos acl map test-acl 3/5
!-- Hardware programming in progress  !-- ACL test-acl is detached from port 3/5.
Console>(enable)
```

## Configureren van de Catalyst 6000-reeks met geïntegreerd Cisco IOS (native modus)

Het toezicht wordt ondersteund met Geïntegreerd Cisco IOS (Native Mode). De configuratie en uitvoering van de politiefunctie wordt echter met behulp van beleidskaarten bereikt. Elke beleidslijn maakt gebruik van meerdere beleidsklassen om een beleidskaart op te stellen en deze beleidsklassen kunnen worden gedefinieerd voor verschillende soorten verkeersstromen.

Beleids kaartklassen, wanneer het filteren, gebruik IOS gebaseerde ACL's en class matchen verklaringen om verkeer te identificeren dat moet worden gecontroleerd. Zodra het verkeer is geïdentificeerd kunnen de beleidsklassen geaggregeerde en microflow-politiemensen gebruiken om het politiebeleid op dat gematchte verkeer toe te passen.

De volgende secties verklaren de configuratie van het toezicht voor Geïntegreerd Cisco IOS (Modus van de Modus) in veel gedetailleerder detail.

### Aggregaten en Microflow (geïntegreerde Cisco IOS (native modus)

Aggregaten en microstromen zijn termen die worden gebruikt om de reikwijdte van het toezicht te definiëren dat de PFC uitvoert. Overeenkomstig met CatOS worden aggregaten en microstromen ook gebruikt in Geïntegreerde Cisco IOS (Native Mode).

Een microflow definieert het toezicht op één stroom. Een stroom wordt gedefinieerd door een sessie met een uniek MAC-adres, SA/DA IP-adres en TCP/UDP-poortnummers. Voor elke nieuwe stroom die door een poort van een VLAN wordt geïnitieerd, kan de microflow worden gebruikt om de hoeveelheid gegevens te beperken die voor die stroom door de switch worden ontvangen. In de definitie van microflow kunnen pakketten die de voorgeschreven snelheidsgrens overschrijden gedemonteerd worden of hun DSCP waarde verlaagd worden. Microstromen worden toegepast met de stroomopdracht van de politie die deel uitmaakt van een beleidskaartklasse.

Om microflow-toezicht in Geïntegreerd Cisco IOS (Native Mode) mogelijk te maken, moet dit mondiaal op de switch ingeschakeld zijn. Dit kan worden bereikt door de volgende opdracht uit te geven:

```
Cat6500(config)# mls qos flow-policing
```

Toezicht microflow kan ook worden toegepast op overbrugd verkeer, dat verkeer is dat niet L3 is geschakeld. Om de switch in staat te stellen om microflow-toezicht op overbrugd verkeer te ondersteunen geeft u de volgende opdracht uit:

```
Cat6500(config)# mls qos bridged
```

Deze opdracht maakt het ook mogelijk microflow-toezicht te houden op multicast verkeer. Als multicast verkeer een microflow-politieagent op het moet hebben toegepast, moet deze opdracht ( **mls qos brugd**) worden geactiveerd.

Overeenkomstig met een microflow kan een aggregaat worden gebruikt om limietverkeer te meten. Niettemin, is het geaggregeerde tarief van toepassing op al verkeer binnenkomend op een haven of VLAN dat een gespecificeerde QoS ACL aanpast. U kunt het aggregaat bekijken als het toezicht op cumulatief verkeer dat overeenkomt met een gedefinieerd verkeersprofiel.

Er zijn twee vormen van aggregaten die in Geïntegreerd Cisco IOS (inheemse modus) kunnen worden gedefinieerd, als volgt:

- per interface
- genaamd verzamelpolitie

Per interface worden de aggregaten toegepast op een individuele interface door de **politie**-opdracht uit te geven binnen een beleidskaartklasse. Deze kaartklassen kunnen op meerdere interfaces worden toegepast, maar de politieagent controleert elke interface afzonderlijk. Benoemde aggregaten worden op een groep havens en politieverkeer over alle interfaces cumulatief toegepast. Benoemde aggregaten worden toegepast door de opdracht van de **mls qos** als **verzamelaar** uit te geven.

Bij het definiëren van microstromen kunnen maximaal 63 daarvan worden gedefinieerd en kunnen maximaal 1023 aggregaten worden gedefinieerd.

### Toezichtregels maken (geïntegreerd Cisco IOS (native modus)

Het proces van het creëren van een politieregel houdt in dat er een aggregaat (of microflow) wordt gecreëerd via een beleidsplan en dat de beleidskaart vervolgens aan een interface wordt bevestigd.

Neem hetzelfde voorbeeld dat voor CatOS is gemaakt. Het vereiste was om al het inkomende IP-verkeer op poort 5/3 te beperken tot een maximum van 20 MBPS.

In de eerste plaats moet er een beleidskaart worden gemaakt. Maak een beleidskaart met de naam limietverkeer. Dit gebeurt als volgt:

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)#
```

U zal onmiddellijk opmerken dat de switch direct verandert om te reflecteren dat u in de configuratiemodus bent voor het maken van een map class. Denk eraan dat een beleidsplan meerdere klassen kan bevatten. Elke klasse bevat een afzonderlijke reeks beleidsacties die op

verschillende verkeersstromen kunnen worden toegepast.

We zullen een verkeersklasse creëren om het inkomende verkeer specifiek te beperken tot 20 MBPS. We noemen deze klasse limiet tot 20, zoals hieronder wordt aangegeven.

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20
Cat6500(config-pmap-c)#
```

De melding verandert opnieuw om aan te geven dat u nu in de configuratie van de map-klasse staat (weergegeven met de -c aan het eind van de melding). Als u de snelheidsbeperking wilt toepassen om specifiek inkomend verkeer aan te passen, kunt u ACL configureren en dit op de klassennaam toepassen. Als u de 20 MBPS limiet wilt toepassen op verkeer dat afkomstig is van netwerk 10.10.1.x, geeft u de volgende ACL uit:

```
Cat6500(config)# access-list 101 permit ip 10.10.1.0  0.0.0.255 any
```

U kunt dit ACL aan de klassennaam als volgt toevoegen:

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20 access-group 101
Cat6500(config-pmap-c)#
```

Zodra je de klassenkaart hebt gedefinieerd, kun je nu individuele politieagenten in die klasse definiëren. U kunt aggregaten maken (met het sleutelwoord van de politie) of microstromen (met het trefwoord van de politie). Maak het aggregaat, zoals hieronder wordt getoond.

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20 access-group 101
Cat6500(config-pmap-c)# police 20000000 13000 confirm-action transmit exceed-action drop
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

De klassenverklaring hierboven (politieopdracht) definieert een snelheidsgrens van 20000 k (20 MBPS) met een barst van 52 MBPS (13000 x 4000 = 52 MB). Als het verkeer overeenkomt met het profiel en binnen de opgegeven limiet valt, moet de actie worden ingesteld door de bevestiging-actie verklaring om het in-profile verkeer door te geven. Als het verkeer buiten profiel is (in ons voorbeeld boven de limiet van 20 MB) is de overtollige-actiestatement ingesteld om het verkeer te laten vallen (in ons voorbeeld is dat alle verkeer boven de 20 MB gevallen).

Bij het configureren van een microflow wordt er een soortgelijke actie ondernomen. Als we de limiet van alle stromen in een haven wilden beperken die een bepaalde klassenkaart op 200 K elk aansloot, zou de configuratie van die stroom vergelijkbaar zijn met het volgende:

```
Cat6500(config)# mls qos flow-policing
Cat6500(config)# policy-map limit-each-flow
Cat6500(config-pmap)# class limit-to-200
```

```
Cat6500(config-pmap-c)# police flow 200000 13000 confirm-action transmit exceed-action drop
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
```

### DSCP-markeringskaarten

DSCP-markeerkaarten worden gebruikt als de politieagent is gedefinieerd om buiten profiel verkeer te markeren in plaats van het te laten vallen. Out-of-profile verkeer is gedefinieerd als het verkeer dat de gedefinieerde burst-instelling overschrijdt.

Een standaard DSCP markeerkaart wordt ingesteld als QoS is ingeschakeld. Deze standaardindellakkaart is in deze tabel opgenomen. De CLI staat een beheerder toe om de standaardmarkeerkaart aan te passen door de **set qos politied-dscp-map** opdracht uit te geven. Hieronder wordt een voorbeeld gegeven.

```
Cat6500(config)#

mls qos map policed-dscp normal-burst 32 to 16
```

Dit voorbeeld definieert een aanpassing aan de standaard georiënteerde dSCP kaart die DSCP waarde van 32 zal worden gemarkeerd naar een DSCP waarde van 16. Voor een poort met deze politieagent die wordt gedefinieerd, zullen alle inkomende gegevens met deze DSCP waarde die deel uitmaken van een blok gegevens dat de vermelde barst overschrijdt, zijn DSCP waarde laten gemarkeerd naar 16.

### Toewijzing van beleid aan VLAN's en poorten (geïntegreerde Cisco IOS (native modus)

Zodra een beleid is gebouwd moet het dan in kaart worden gebracht in een haven of in een VLAN zodat dat beleid van kracht wordt. In tegenstelling tot het geëngageerde proces in CatOS, is er geen equivalent in Geïntegreerde Cisco IOS (Native Mode). Wanneer een beleid op een interface is afgestemd, is dat beleid van kracht. U geeft de volgende opdracht uit om het bovenstaande beleid in een interface in kaart te brengen:

```
Cat6500(config)# interface fastethernet 3/5
Cat6500(config-if)# service-policy input limit-traffic
```

Als een beleid aan een VLAN in kaart wordt gebracht, voor elke haven in VLAN die u het beleid van VLAN wilt van toepassing zijn op, moet u de interface meedelen dat QoS VLAN gebaseerd is door de op **mls qos VLAN gebaseerde** opdracht uit te geven.

```
Cat6500(config)# interface fastethernet 3/5
Cat6500(config-if)# mls qos vlan-based
Cat6500(config-if)# exit
Cat6500(config)# interface vlan 100
Cat6500(config-if)# service-policy input limit-traffic
```

Aangenomen dat interface 3/5 deel uitmaakte van VLAN 100, zou het beleid genaamd limit-traffic die werd toegepast op VLAN 100 ook van toepassing zijn op interface 3/5.

## Classificatie op Catalyst 6000-reeks instellen met CatOS

PFC introduceert ondersteuning voor het classificeren van gegevens met ACL's die L2, L3 en L4 header informatie kunnen weergeven. Voor een SupI, of IA (zonder PFC) is de classificatie beperkt tot het gebruik van de trustsleutelwoorden op havens.

In de volgende sectie worden de QoS-configuratieonderdelen beschreven die door de PFC zijn gebruikt voor classificatie in het CatOS.

### CO's naar DSCP-toewijzing (CatOS)

Bij toegang tot de switch wordt een kader met een DSCP-waarde ingesteld door de switch. Als de poort in een vertrouwde status is, en de beheerder het trust-COs sleutelwoord heeft gebruikt, zal de COs waarde die in het frame is ingesteld worden gebruikt om de DSCP waarde te bepalen die voor het frame is ingesteld. Zoals eerder vermeld, kan de switch serviceniveaus aan het frame toewijzen terwijl deze de switch doorvoert op basis van de interne DSCP-waarde.

Dit sleutelwoord op sommige van de vroegere 10/100 modules (WS-X6248 en WS-X6348) wordt niet ondersteund. Voor die modules wordt het aanbevolen gebruik van ACL's om CO's-instellingen voor inkomende gegevens toe te passen.

Wanneer QoS is ingeschakeld, maakt de switch een standaardkaart. Deze kaart wordt gebruikt om de DSCP-waarde te identificeren die zal worden ingesteld op basis van de CO2-waarde. Deze kaarten zijn eerder in het document in deze tabel opgenomen. U kunt ook een unieke kaart instellen door de beheerder. Hieronder wordt een voorbeeld gegeven.

```
Console> (enable) set qos cos-dscp-map 20 30 1 43 63 12 13 8
!-- QoS cos-dscp-map set successfully. Console> (enable)
```

De bovenstaande opdracht stelt de volgende map in:

| CO | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| DSCP | 20 | 30 | 1 | 43 | 63 | 12 | 13 | 8 |

Hoewel het zeer onwaarschijnlijk is dat de bovenstaande kaart gebruikt zal worden in een real life netwerk, geeft deze een idee van wat er bereikt kan worden met deze opdracht.

### IP-voorrang voor DSCP-toewijzing (CatOS)

Overeenkomstig de CO's aan de DSCP-kaart kan een kader een DSCP-waarde hebben die wordt bepaald door de inkomende IP-prioriteitsinstelling. Dit komt nog steeds voor als de haven aan de beheerder wordt vertrouwd, en zij hebben het trust-ipprec sleutelwoord gebruikt.

Wanneer QoS is ingeschakeld, maakt de switch een standaardkaart. Deze kaart is eerder in deze tabel opgenomen in dit document. Deze kaart wordt gebruikt om de DSCP waarde te identificeren die zal worden ingesteld op basis van de IP-prioriteitswaarde. U kunt ook een unieke kaart instellen door de beheerder. Hieronder wordt een voorbeeld gegeven:

```
Console> (enable) set qos ipprec-dscp-map 20 30 1 43 63 12 13 8
!-- QoS ipprec-dscp-map set successfully. Console> (enable)
```

De bovenstaande opdracht stelt de volgende map in:

| IP-voorrang | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| DSCP | 20 | 30 | 1 | 43 | 63 | 12 | 13 | 8 |

Hoewel het zeer onwaarschijnlijk is dat de bovenstaande kaart gebruikt zal worden in een real life netwerk, geeft deze een idee van wat er bereikt kan worden met deze opdracht.

## Classificatie (CatOS)

Wanneer een kader voor verwerking aan de PFC wordt doorgegeven, wordt het classificatieproces op het frame uitgevoerd. De PFC zal een vooraf ingesteld ACL (of een standaard ACL) gebruiken om een DSCP aan het frame toe te wijzen. Binnen de ACE, wordt één van vier sleutelwoorden gebruikt om een DSCP waarde toe te wijzen. Het gaat om:

1. TRUST-DSCP (alleen IP ACL's)
2. TRUST-IPPREC (alleen IP ACL's)
3. TRUST-COS (alle ACL's behalve IPX en MAC op een PFC2)
4. DSCP

Het TRUST-DSCP sleutelwoord veronderstelt dat het kader dat in PFC aankomt reeds een waarde DSCP heeft die wordt ingesteld voordat het de switch ingaat. De switch behoudt deze DSCP-waarde.

Met TRUST-IPPREC zal de PFC een DSCP-waarde afleiden van de bestaande IP-prioriteitswaarde ingezeten in het ToS-veld. Het PFC zal IP voorrang aan DSCP kaarten gebruiken om de juiste DSCP toe te wijzen. Er wordt een standaardmap gemaakt wanneer QoS op de switch is ingeschakeld. In plaats hiervan kan een kaart die door de beheerder is gemaakt, ook worden gebruikt om de DSCP-waarde af te leiden.

Overeenkomstig met TRUST-IPREC, wordt het TRUS-COS sleutelwoord de PFC opgedragen een DSCP waarde af te leiden van de CO's in de framafkop. Er zal ook een COs aan DSCP kaart zijn (of een standaard van een beheerder toegewezen) om de PFC te helpen bij het afleiden van de DSCP.

Het DSCP-trefwoord wordt gebruikt wanneer een frame uit een onvertrouwde poort komt. Dit levert een interessante situatie op voor het afleiden van de DSCP. Op dit punt wordt de DSCP die in de ingestelde qos akl statement is ingesteld, gebruikt om de DSCP af te leiden. Op dit punt kunnen de ACL's echter worden gebruikt om een DSCP voor het verkeer af te leiden op basis van de in de ACE-index vastgestelde classificatiecriteria. Dit betekent dat in een ACE, men classificatiecriteria zoals IP bron en bestemmingsadres, TCP/UDP poortnummers, ICMP codes, IGMP type, IPX netwerk en protocol nummers, bron- en doeladressen van MAC, en Ethertypes (voor niet-IP en niet-IPX verkeer slechts) kan gebruiken om verkeer te identificeren. Dit betekent dat een ACE kan worden geconfigureerd om een specifieke DSCP-waarde toe te wijzen om HTTP-verkeer via FTP-verkeer te zeggen.

Neem het volgende voorbeeld:

```
Console> (enable) set port qos 3/5 trust untrusted
```

Als u een poort instelt als onbetrouwbaar, wordt de PFC opgedragen een ACE te gebruiken om de DSCP voor het frame af te leiden. Als ACE is ingesteld met classificatiecriteria, kunnen individuele stromen uit die haven met verschillende prioriteiten worden ingedeeld. Dit wordt geïllustreerd door de volgende cijfers:

```
Console> (enable) set qos acl ip abc dscp 32 tcp any any eq http
```

```
Console> (enable) set qos acl ip ABC dscp 16 tcp any any eq ftp
```

In dit voorbeeld hebben we twee ACE-verklaringen. De eerste identificeert elke TCP-stroom (het trefwoord wordt elk gebruikt om bron- en doelverkeer te identificeren) waarvan het poortnummer 80 (80 = HTTP) is om een DSCP-waarde van 32 toe te kennen. De tweede ACE identificeert verkeer dat is afgeleid van elke host en is bestemd voor elke host wiens TCP-poortnummer 21 (FTP) is toegewezen aan een DSCP-waarde van 16.

## Indeling op de Catalyst 6000-reeks met geïntegreerd Cisco IOS (native modus)

In het volgende gedeelte worden de QoS-configuratieonderdelen beschreven die gebruikt zijn om classificatie op de PFC te ondersteunen met behulp van Geïntegreerde Cisco IOS (Native Mode).

### Toewijzing van CO's naar DSCP (geïntegreerde Cisco IOS (native modus)

Bij toegang tot de switch wordt een kader met een DSCP-waarde ingesteld door de switch. Als de poort in een vertrouwde status is en de beheerder de mls qos trust-COs sleutelwoord (op GE poorten of 10/100 poorten op de WS-X6548 lijnkaarten) heeft gebruikt, zal de COs waarde die in het frame is ingesteld worden gebruikt om de DSCP waarde te bepalen die voor het frame is ingesteld. Zoals eerder vermeld, kan de switch serviceniveaus aan het frame toewijzen terwijl deze de switch doorvoert op basis van de interne DSCP-waarde.

Wanneer QoS is ingeschakeld, maakt de switch een standaardkaart. Raadpleeg deze tabel voor standaardinstellingen. Deze kaart wordt gebruikt om de DSCP-waarde te identificeren die zal worden ingesteld op basis van de CO2-waarde. U kunt ook een unieke kaart instellen door de beheerder. Hieronder wordt een voorbeeld gegeven.

```
Cat6500(config)# mls qos map cos-dscp 20 30 1 43 63 12 13 8
Cat6500(config)#
```

De bovenstaande opdracht stelt de volgende map in:

| CO | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| DSCP | 20 | 30 | 1 | 43 | 63 | 12 | 13 | 8 |

Hoewel het zeer onwaarschijnlijk is dat de bovenstaande kaart gebruikt zal worden in een real life netwerk, geeft deze een idee van wat er bereikt kan worden met deze opdracht.

### IP-voorrang voor DSCP-toewijzing (geïntegreerde Cisco IOS (native modus)

Overeenkomstig de CO's aan de DSCP-kaart kan een kader een DSCP-waarde hebben die wordt bepaald door de inkomende IP-prioriteitsinstelling. Dit komt nog steeds voor als de poort is ingesteld op vertrouwd door de beheerder en ze hebben het mls qos trust-ipprec sleutelwoord gebruikt. Dit sleutelwoord wordt alleen ondersteund op GE poorten en 10/100 poorten op de WS-X6548 lijnkaarten. Voor 10/100 poorten op de WS-X6348- en WS-X6248-lijnkaarten moeten ACL's worden gebruikt om ip-prioriteitsvertrouwen aan inkomende gegevens toe te wijzen.

Wanneer QoS is ingeschakeld, maakt de switch een standaardkaart. Raadpleeg deze tabel voor standaardinstellingen. Deze kaart wordt gebruikt om de DSCP waarde te identificeren die zal worden ingesteld op basis van de IP-prioriteitswaarde. U kunt ook een unieke kaart instellen door de beheerder. Hieronder wordt een voorbeeld gegeven.

```
Cat6500(config)# mls qos map ip-prec-dscp 20 30 1 43 63 12 13 8
Cat6500(config)#
```

De bovenstaande opdracht stelt de volgende map in:

| IP-voorrang | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| DSCP | 20 | 30 | 1 | 43 | 63 | 12 | 13 | 8 |

Hoewel het zeer onwaarschijnlijk is dat de bovenstaande kaart gebruikt zal worden in een real life netwerk, geeft deze een idee van wat er bereikt kan worden met deze opdracht.

### Classificatie (geïntegreerde Cisco IOS (native modus)

Wanneer een kader aan de PFC wordt doorgegeven, kan het proces van classificatie worden uitgevoerd om een nieuwe prioriteit aan een inkomend frame toe te wijzen. Voorhouden is dat dit alleen kan worden gedaan als het frame uit een onvertrouwde poort komt, of het frame is geclassificeerd als onbetrouwbaar.

Een beleidslijnklassenactie kan worden gebruikt om:

1. TRUST-CO's
2. TRUST IP-PRECEDENCE
3. TRUST DSCP
4. GEEN VERTROUWEN

Het sleutelwoord TRUST DSCP veronderstelt dat het kader dat in PFC aankomt reeds een waarde DSCP heeft die wordt geplaatst alvorens het de switch ingaat. De switch behoudt deze DSCP-waarde.

Met TRUST IP-PRECEDENCE zal de PFC een DSCP-waarde afleiden van de bestaande IP-prioriteitswaarde ingezeten in het ToS-veld. De PFC zal een IP voorrang aan DSCP kaart gebruiken om de juiste DSCP toe te wijzen. Er wordt een standaardmap gemaakt wanneer QoS op de switch is ingeschakeld. In plaats hiervan kan een kaart die door de beheerder is gemaakt, ook worden gebruikt om de DSCP-waarde af te leiden.

Overeenkomstig met TRUST IP-PRECEDENCE, wordt het sleutelwoord TRUST CO's de PFC opgedragen een DSCP-waarde af te leiden van de CO's in de kop van het frame. Er zal ook een COs aan DSCP kaart zijn (of een standaard van een beheerder toegewezen) om de PFC te helpen bij het afleiden van de DSCP.

Hieronder wordt een voorbeeld weergegeven van het afleiden van DSCP van een bestaande prioriteit (DSCP, IP-voorrang of CO's).

```
Cat6500(config)# policy-map assign-dscp-value
Cat6500(config-pmap)# class test
Cat6500(config-pmap-c)# trust COs
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

De bovenstaande class map leidt de DSCP-waarde af van de CO's in de Ethernet-header.

De NO TRUST vorm van het sleutelwoord wordt gebruikt wanneer een kader van een

onvertrouwde haven aankomt. Dit laat het kader toe om een DSCP waarde toegewezen te hebben tijdens het proces van toezicht.

Neem het volgende voorbeeld van hoe een nieuwe prioriteit (DSCP) kan worden toegewezen aan verschillende stromen die in het PFC komen te staan met behulp van de volgende beleidsdefinitie.

```
Cat6500(config)# access-list 102 permit tcp any any eq http
Cat6500(config)# policy-map new-dscp-for-flow
Cat6500(config-pmap)# class test access-group 102
Cat6500(config-pmap-c)# no trust
Cat6500(config-pmap-c)# police 1000 1 confirm-action set-dscp-transmit 24  Cat6500(config-pmap-
c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

Het bovenstaande voorbeeld toont het volgende:

1. Er wordt een ACL gecreëerd om http stromen te identificeren die de haven binnenkomen.
2. Een beleidskaart genaamd 'new-dscp-for-flow'.
3. Een class map (name test) die toegangslijst 102 gebruikt om het verkeer te identificeren waarvoor deze class map de handeling zal uitvoeren.
4. De class map test zal de trust status voor het inkomende frame op onvertrouwde positie instellen en een DSCP van 24 aan die stroom toewijzen.
5. Deze class map zal het totaal van alle http stromen ook beperken tot maximaal 1 MB.

# Gemeenschappelijk Open Policy Server (COPS)

COPS is een protocol dat Catalyst 6000-familie in staat stelt om QoS uit een externe host te laten configureren. Op dit moment wordt COPS alleen ondersteund met CatOS en maakt het deel uit van de intserv-architectuur voor QoS. Er is momenteel geen ondersteuning (vanaf de datum van dit document) voor COPS bij gebruik van Geïntegreerde Cisco IOS (Native Mode). Terwijl het COPS-protocol de QoS-configuratieinformatie naar de switch doorgeeft, is de bron van de QoS-configuratieinformatie niet voldoende. Gebruik van het COPS-protocol vereist dat een externe QoS-beheerder de QoS-configuraties voor de switch onderhoudt. De externe QoS-beheerder zal met behulp van het COPS-protocol de neerwaartse druk van deze configuraties op de switch inleiden. Cisco QoS Policy Manager (QPM) is een voorbeeld van een externe QoS Manager.

Het is niet de bedoeling van dit document om de werking van QPM te verklaren, maar om de configuratie uit te leggen die vereist is op de switch om externe QoS-configuraties te ondersteunen bij het gebruik van QPM.

## COPS-configuratie

COPS-ondersteuning wordt standaard uitgeschakeld. Als u COPS op de switch wilt gebruiken, moet deze functie zijn ingeschakeld. Dit kan worden bereikt door de volgende opdracht uit te geven:

```
Console> (enable) set qos policy-source cops
```

```
!-- QoS policy source for the switch set to COPS. Console> (enable)
```
Wanneer deze opdracht wordt gestart, worden bepaalde standaardwaarden voor de QoS-configuratie afgeleid van de COPS-server. Deze omvatten:

1. CO's in de wachtrij voor afbeeldingen
2. Toewijzing van in- en uitvoerwachtdrempels
3. WRR-bandbreedteopdrachten
4. Elk beleid op het gebied van aggregatie en microflow
5. DSCP naar CO2-kaarten voor toegangsverkeer
6. ACL's
7. Standaard CO's-toegewezen poorten

Wanneer QoS-configuraties worden uitgevoerd met behulp van COPS, is het belangrijk te begrijpen dat de toepassing van deze configuraties op een andere manier wordt toegepast. In plaats van de poorten direct te configureren wordt COPS gebruikt om de poort-ASIC te configureren. De poort-ASIC controleert doorgaans een groep poorten, zodat de COPS-configuratie tegelijkertijd wordt toegepast op een aantal poorten.

De poort-ASIC die wordt geconfigureerd is de GE ASIC. Op GE lijnkaarten zijn er vier poorten per GE (poorten 1-4, 5-8, 9-12, 13-16). Op deze lijnkaarten beïnvloedt de configuratie COPS elke groep poorten. Op 10/100 lijnkaarten (zoals eerder in dit document besproken) zijn er twee groepen ASIC's, de GE en de 10/100 ASIC's. Eén GE ASIC bestaat voor vier 10/100 ASIC' s. Elke 10/100 ASIC ondersteunt 12 10/100 poorten. COPS vormt de GE ASIC. Bij het toepassen van QoS-configuratie op 10/100 lijnkaarten via COPS is de configuratie dus van toepassing op alle 48 10/100 poorten.

Wanneer COPS-ondersteuning mogelijk wordt gemaakt door de **set qos-**opdracht voor **beleidsbronpolitie** uit te geven, wordt de QoS-configuratie via COPS toegepast op alle ASIC's in het switch chassis. Het is mogelijk de COPS-configuratie op specifieke ASIC's toe te passen. U kunt dit bereiken met de volgende opdracht:

```
Console> (enable) set port qos 5/4 policy-source cops
!-- QoS policy source set to COPS for port (s) 5/1-4. Console> (enable)
```
U kunt aan de toepassing van de bovenstaande opdracht zien dat deze opdracht is gegeven op een GE-module omdat vier poorten door de opdracht werden beïnvloed.

## Beleidsbeslissingspuntservers en domeinnamen

Beleidsbeslissingen Point Server (PDPS) zijn de externe beleidsmanagers die worden gebruikt om QoS-configuratiegegevens op te slaan die naar de switch zijn afgedrukt. Als COPS op de switch is ingeschakeld, moet de switch zijn ingesteld met het IP-adres van de externe beheerder die de QoS-configuratiegegevens aan de switch zal leveren. Dit is gelijk aan wanneer SNMP wordt ingeschakeld en het SNMP Manager IP-adres is gedefinieerd.

De opdracht om de externe PDPS te identificeren wordt uitgevoerd met behulp van het volgende:

```
Console> (enable) set cops server 192.168.1.1 primary
!-- 192.168.1.1 is added to the COPS diff-serv server table as primary server. !-- 192.168.1.1
is added to the COPS rsvp server table as primary server. Console> (enable)
```
Bovenstaande opdracht identificeert machine 192.168.1.1 als de primaire beslissingspuntserver.

Wanneer de switch met de PDPS communiceert, moet deze onderdeel zijn van een domein dat op de PDPS is gedefinieerd. In de PDPS wordt alleen gesproken met switches die deel uitmaken van het afgebakende domein, zodat de switch zo moet worden geconfigureerd dat hij het COPS-domein identificeert waartoe hij behoort. Dit gebeurt door de volgende opdracht uit te geven:

```
Console> (enable) set cops domain name remote-cat6k
!-- Domain name set to remote-cat6k. Console> (enable)
```

De bovenstaande opdracht toont de switch als zodanig geconfigureerd dat deze deel uitmaakt van het domein met de naam Remote-cat6k. Dit domein dient in QPM te worden gedefinieerd en de switch dient aan dat domein te worden toegevoegd.

---

## Gerelateerde informatie

- Productondersteuning voor switches
- Ondersteuning voor LAN-switching technologie
- Technische ondersteuning en documentatie – Cisco Systems

---