De betekenis van QoS-toezicht en -markering op Catalyst 3550

Inhoud

Inleiding

De politiefunctie bepaalt of het verkeersniveau binnen het gespecificeerde profiel of contract valt en u kunt in staat zijn om of out-of-profile verkeer uit te schakelen of het te markeren met een andere DSCP-waarde (Differential Services Code Point). Dit voert een contractueel serviceniveau in.

DSCP is een maat voor het QoS-niveau (Quality of Service) van het pakket. Samen met DSCP worden IP-voorrang en serviceklasse (CoS) ook gebruikt om het QoS-niveau van het pakket over te brengen.

Toezicht moet niet worden verward met traffic shaping, alhoewel beide zorgen dat het verkeer binnen het profiel of contract blijft.

Toezicht buffert het verkeer niet, dus toezicht heeft geen invloed op de transmissievertraging. In plaats van buiten-profiel pakketten te bufferen, laat de politie deze vallen of tekent ze met verschillende QoS-niveaus (DSCP markering).

Traffic Shaping buffert buiten-profiel verkeer en zorgt voor een vlotte verkeersuitbarsting, maar beïnvloedt de vertraging en de vertragingsvariatie. Shaping kan slechts op de uitgaande interface worden toegepast, terwijl controle op zowel de inkomende als de uitgaande interface kan worden toegepast.

Catalyst 3550 ondersteunt toezicht voor zowel inkomende als uitgaande richtingen. Traffic Shaping wordt niet ondersteund.

Het markeren verandert het pakket QoS niveau in overeenstemming met een beleid.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Hardware en softwareversies

Toezicht en markering op Catalyst 3550 wordt ondersteund met alle softwareversies. De meest recente configuratiehandleiding is hier weergegeven. Raadpleeg deze documentatie voor alle ondersteunde functies.

- QoS configureren

QoS-toezicht- en markeerparameters

Om toezicht op te zetten moet u de QoS-beleidskaarten definiëren en ze op havens toepassen. Dit staat verder bekend als op poorten gebaseerde QoS.

Opmerking: Op VLAN gebaseerde QoS wordt momenteel niet ondersteund door Catalyst 3550.

De politie wordt gedefinieerd door parameters voor snelheid en uitbarsting, evenals actie voor verkeer dat buiten profiel valt.

Deze twee soorten politieagenten worden ondersteund:

- samenvoegen
- individu

De politie treedt op in alle gevallen waarin ze wordt toegepast. De individuele politieagent treedt afzonderlijk op bij het verkeer in elke instantie waar het wordt toegepast.

Opmerking: Op Catalyst 3550 kan de totale politieagent alleen worden toegepast op verschillende

klassen van hetzelfde beleid. Geaggregeerd toezicht op meerdere interfaces of beleid wordt niet ondersteund.

Bijvoorbeeld, pas de globale politier toe om het verkeer van klasse klant1 en klasse customer2 in de zelfde beleidskaart tot 1 Mbps te beperken. Zo'n politieman staat 1 Mbps van verkeer in klasse klant1 en klant2 samen toe. Als u de individuele politieagent toepast, beperkt de politieagent het verkeer voor klasse klant1 tot 1 Mbps en voor klasse Customer2 tot 1 Mbps. Daarom is elk geval van de politieagent afzonderlijk.

Deze tabel geeft een samenvatting van de QoS-actie op het pakket wanneer deze wordt behandeld door zowel het ingangsbeleid als het toegangsbeleid:

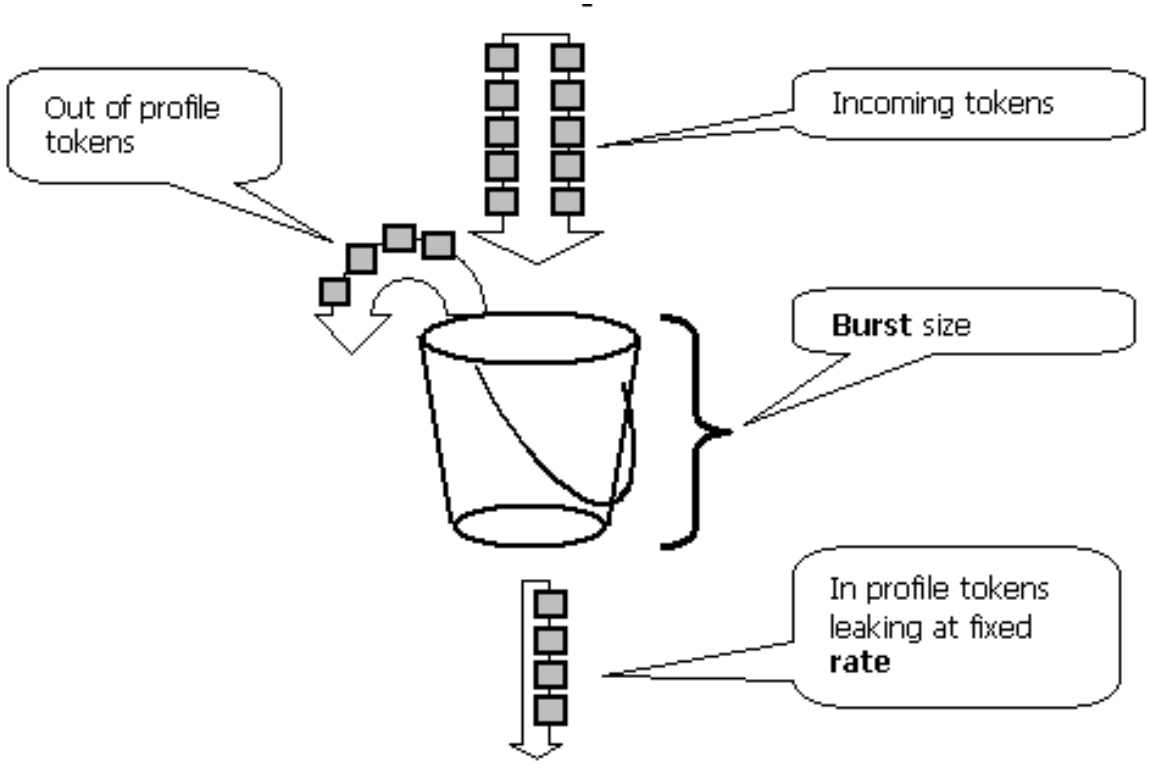
	Ingress policy			
Egress policy	Transmit	Drop	$Markdown_i$	$Mark_i$
Transmit	Transmit	Drop	$Markdown_i$	$Mark_i$
Drop	Drop	Drop	Drop	Drop
$Markdown_e$	$Markdown_e$	Drop	$Markdown_i$ then $Markdown_e$	$Mark_i$ then $Markdown_e$

Opmerking: Het is mogelijk om binnen dezelfde verkeersklasse van hetzelfde beleid een markering en markering te aanbrengen. In dat geval wordt al het verkeer voor de betreffende klasse als eerste gemarkeerd. Toezicht en markering vinden plaats op reeds gemarkeerd verkeer.

QoS-toezicht in Catalyst 3550 voldoet aan dit concept van lekkage emmer:

het aantal penningen dat evenredig is aan de inkomende pakketgrootte, wordt in een pennenemmer geplaatst; het aantal penningen is gelijk aan de grootte van het pakket . Op regelmatige tijdstippen wordt een bepaald aantal penningen, afgeleid van de geconfigureerde snelheid, uit de emmer verwijderd. Als er geen plaats in de emmer is om een inkomend pakje aan te passen, wordt het pakje als buiten profiel beschouwd en wordt het volgens de ingestelde politieactie ingetrokken of gemarkeerd.

Dit concept wordt in dit voorbeeld getoond:



Opmerking: het verkeer wordt niet gebufferd in de emmer omdat het in dit voorbeeld kan verschijnen. Het werkelijke verkeer stroomt helemaal niet door de emmer; de emmer wordt alleen gebruikt om te bepalen of de verpakking in profiel of buiten profiel is.

Opmerking: Hardware implementatie van toezicht kan variëren, maar functioneel voldoet het nog steeds aan dit model.

Deze parameters regelen de werking van de politie:

- **Rate**-definieert hoeveel tokens elk interval worden verwijderd. Dit stelt in feite de politiekoers in. Alle verkeer onder het tarief wordt in profiel in aanmerking genomen. Ondersteunde snelheden variëren van 8 Kbps tot 2 Gbps en een stijging met 8 Kbps.
- **Interval**-definieert hoe vaak penningen uit de emmer worden verwijderd. Het interval is vastgesteld op 0,125 milliseconden (of 8000 keer per seconde). Dit interval kan niet worden gewijzigd.
- **Burst**—definieert de maximale hoeveelheid penningen die de emmer op elk moment kan bevatten. Ondersteunde bursts variëren van 8000 bytes tot 200000 bytes en van 64 bytes.

Opmerking: hoewel de opdrachtregel help strings een groot bereik van waarden tonen, kan de rate-bps optie niet hoger zijn dan de ingestelde poortsnelheid en kan de burst-byte optie niet hoger zijn dan 200000 bytes. Als u een grotere waarde invoert, wijst de switch de beleidskaart af wanneer u deze aan een interface vastlegt.

Om het gespecificeerde verkeerstarief te kunnen handhaven, mag de uitbarsting niet minder bedragen dan de som van deze vergelijking:

```
Burstmin (bits) = Rate (bps) / 8000 (1/sec)
```

Bereken bijvoorbeeld de minimale barstwaarde om een snelheid van 1 Mbps te behouden. Het tarief wordt gedefinieerd als 1000 Kbps, zodat de benodigde minimale uitbarsting de som van deze vergelijking is:

```
1000 (Kbps) / 8000 (1/sec) =125 (bits)
```

De minimum ondersteunde burst size is 8000 bytes, die meer is dan de minimum berekende burst.

Opmerking: Vanwege de granulariteit van het hardware-toezicht worden de exacte snelheid en uitbarsting tot de dichtstbijzijnde ondersteunde waarde afgerond.

Wanneer u de burst rate configureren moet u er rekening mee houden dat sommige protocollen mechanismen implementeren die reageren op het pakketverlies. Bijvoorbeeld, Transmission Control Protocol (TCP) vermindert het venster met de helft voor elk verloren pakket. Dit veroorzaakt een "zaagtand"effect in het TCP verkeer wanneer TCP probeert te versnellen tot de lijnsnelheid en door de politieagent wordt gedraaid. Als het gemiddelde tarief voor het zaagtandverkeer wordt berekend, is dit veel lager dan het bewaakte tarief. U kunt echter de barst verhogen om een beter gebruik te bereiken. Een goed begin is om de burst gelijk te stellen aan tweemaal de hoeveelheid verkeer die met de gewenste snelheid tijdens de Ronde Trip Tijd (TCP RTT) wordt verzonden. Als RTT niet bekend is, kunt u de waarde van de burst parameter verdubbelen.

Om dezelfde reden wordt het niet aanbevolen om de politietoezicht te benchmarken met op verbindingen gericht verkeer. Dit scenario laat over het algemeen lagere prestaties zien dan toegestaan door de politieagent.

Het verkeer zonder verbindingen kan ook anders reageren op het toezicht. Network File System (NFS) gebruikt bijvoorbeeld blokken, die kunnen bestaan uit meer dan één User Datagram Protocol-pakket (UDP). Eén pakje dat is gevallen, kan veel pakketten, zelfs het gehele blok, activeren om opnieuw te worden verzonden.

Dit voorbeeld berekent de burst voor een TCP sessie met een politieresnelheid van 64 Kbps en gegeven TCP RTT is, 0,05 seconden:

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

In dit voorbeeld is `<burst>` voor één TCP-sessie. Schaal dit cijfer om het verwachte aantal sessies te gemiddeld te nemen die door de politieagent reizen.

Opmerking: Dit is slechts een voorbeeld, in elk geval moet je verkeers- en toepassingsvereisten en gedrag ten opzichte van beschikbare bronnen evalueren om te kunnen kiezen uit parameters voor toezicht.

De politieactie kan worden ondernomen om het pakket te laten vallen of om de DSCP van het pakket te wijzigen (markering). Om het pakket te markeren, moet een gepolieerde DSCP kaart worden aangepast. Een standaard geïnspireerde DSCP kaart plaatst het pakje op dezelfde DSCP. Daarom treedt geen markering op.

Packets kunnen uit bestelling worden verzonden wanneer een out-of-profiel pakket is gemarkeerd naar een DSCP die in een andere uitvoerwachtrij is geplaatst dan de oorspronkelijke DSCP. Als de volgorde van de pakketten belangrijk is, kunt u de buiten-profiel pakketten op de DSCP markeren die in kaart zijn gebracht in dezelfde wachtrij zoals in-profiel pakketten.

Toezicht- en markeringsfuncties die worden ondersteund door Catalyst 3550

Deze tabel bevat een samenvatting van de functies voor toezicht en markering die door Catalyst 3550 worden ondersteund, uitgesplitst naar richting:

	Direction	
Feature	Ingress	Egress
Individual policers	Yes, totally 128 for GE and 8 for FE including ingress aggregate policers	Yes, totally 8 including egress aggregate policers
Aggregate policers	Yes, totally 128 for GE and 8 for FE including ingress individual policers	Yes, totally 8 including egress individual policers
Marking	Yes	No
Policer Markdown	Yes	Yes
Match with ACL	Yes	**No**
Match DSCP	Yes	**Yes**
Match IP precedence	Yes	No
Match COS	Yes, for non-IP traffic	No
Trust DSCP	Yes	No
Trust COS	Yes	No
Trust IP precedence	Yes	No

Eén overeenkomende verklaring wordt per class-map ondersteund. Dit zijn geldige matchverklaringen voor het integratiebeleid:

- match-toegangsgroep
- zie ip-punt
- zie ip-voorrang

Opmerking: Op Catalyst 3550 wordt de **opdracht**matchinterface niet ondersteund en is slechts één match-opdracht toegestaan in een class-map. Daarom is het lastig om al het verkeer dat binnenkomt door een interface te classificeren en al het verkeer met één enkel politieagent te controleren. Zie Hoe u al het interfaceverkeer kunt classificeren met één sectie van dit document.

Dit is de geldige matchverklaring voor het noodbeleid:

- zie ip-punt

Dit zijn geldige beleidsmaatregelen voor het integratiebeleid:

- politie
- ip dscp instellen (markering)
- ip - voorrang instellen (markering)
- trust dscp
- trust ip-precedent
- trust cos

In deze tabel wordt de ondersteunde QoS-beleidsmatrixprinter weergegeven:

Trust I/F	Match DSCP[1]	Match ACL	Trust Class[2]	Set DSCP[3]	Police	Result
						Traffic is assigned default QOS level of the port (0 by default)
√						QOS level of incoming traffic is preserved, according to what is trusted
	√		√		√	IP Traffic is matched by DSCP and then trusted then policed, excess traffic dropped or marked down
	√		√			IP Traffic is matched by DSCP/IP precedence and its QOS level is preserved
	√			√		IP Traffic is matched by DSCP/IP precedence then marked
	√			√	√	IP Traffic is matched by DSCP/IP precedence then marked then policed
		√	√		√	Traffic is matched by access list, QOS level of the matched traffic is preserved, then traffic is policed
		√	√			Traffic is matched by access list and its QOS level is preserved according to what is trusted
		√		√	√	Traffic is matched by access list then marked and then policed
		√		√		Traffic is matched by ACL then marked with specified DSCP/IP precedence
		MAC ACL w/COS	√			Match non-IP traffic by MAC EtherType and COS and preserve QOS level
		MAC ACL w/COS	√		√	Match non-IP IP traffic by MAC EtherType and COS and preserve QOS level then police
		MAC ACL w/COS		√		Match non-IP IP traffic by MAC EtherType and COS then mark matched traffic
		MAC ACL W/COS		√	√	Match non-IP IP traffic by MAC EtherType and COS then mark and then police

1. Deze optie heeft ook betrekking op de IP-voorrang van de partijen.
2. Deze optie bestrijkt het vertrouwen van CoS, IP voorrang, en DSCP.
3. Deze optie heeft ook betrekking op het instellen van de IP-voorrang.

Dit is de geldige beleidsactie voor het noodbeleid:

- politie

In deze tabel wordt de ondersteunde matrixprinter voor progressief QoS-beleid weergegeven:

Match DSCP	Police	Result
		Traffic is sent out with COS and IP precedence according to QOS maps and internal DSCP after ingress QOS processing
√	√	Traffic is matched by DSCP and policed

Met markering kunt u het QoS-niveau van het pakket wijzigen op basis van classificatie of toezicht. De classificatie verdeelt verkeer in verschillende klassen voor QoS-verwerking op basis van de gedefinieerde criteria.

De QoS-verwerking is gebaseerd op de interne DSCP; de maat van het QoS-niveau van het pakket. De interne DSCP wordt afgeleid volgens de configuratie van het vertrouwen. Het systeem ondersteunt het vertrouwen van CoS, DSCP, IP voorrang, en onvertrouwde interfaces. Vertrouwen specificeert het veld waaruit de interne DSCP voor elk pakje is afgeleid, en wel als volgt:

- Wanneer u CoS vertrouwt, komt het QoS-niveau voort uit Layer 2 (L2) header van het Inter-Switch Link Protocol (ISL) of het ingesloten 802.1Q pakket.
- Wanneer het vertrouwen op DSCP of IP voorrang wordt, leidt het systeem het QoS niveau af van het DSCP of IP prioriteitsveld van het pakket.

Het stremmen van CoS is slechts betekenisvol op trunking interfaces, en het vertrouwen van DSCP (of IP voorrang) is slechts voor IP pakketten zinvol.

Wanneer een interface niet wordt vertrouwd, wordt de interne DSCP afgeleid van de configureerbare standaard CoS voor de corresponderende interface. Dit is de standaard toestand wanneer QoS is ingeschakeld. Als geen standaard CoS is ingesteld is de standaardwaarde nul.

Als de interne DSCP eenmaal is ingesteld, kan deze door markering en toezicht worden gewijzigd of behouden.

Nadat het pakket de QoS-verwerking heeft ondergaan, worden de velden QoS-niveau (binnen het IP/DSCP-veld voor IP en in de ISL/802.1Q-header, indien aanwezig) bijgewerkt vanaf de interne DSCP. Er zijn deze speciale QoS-kaarten die relevant zijn voor de politie:

- **DSCP-to-pluggable DSCP**-gebruikt om de gepolitie DSCP af te leiden wanneer u het pakket markeert.
- **DSCP-to-CoS**-gebruikt om het CoS-niveau af te leiden van de interne DSCP om het uitgaande pakket ISL/802.1Q-header bij te werken.
- **CoS-to-DSCP**-gebruikt om de interne DSCP van de inkomende CoS (ISL/802.1Q header) af te leiden wanneer de interface in de vertrouwde CoS-modus is.

Dit zijn belangrijke uitvoeringsspecifieke overwegingen:

- Het servicebeleid voor ingangen kan niet aan de interface worden gekoppeld wanneer de interface is ingesteld om een van de QoS-parameters te vertrouwen, zoals CoS/DSCP of IP-voorrang. Om op DSCP/IP voorrang en politie op toegang te vergelijken, moet u vertrouwen voor de specifieke klasse binnen het beleid vormen, niet op de interface. Om op DSCP/IP voorrang te geven, moet er geen vertrouwen worden ingesteld.
- Alleen IPv4-verkeer zonder IP-opties en Ethernet II Advanced Research Projects Agency

(ARPA) wordt vanuit het hardware- en QoS-standpunt als IP-verkeer beschouwd. Al het andere verkeer wordt beschouwd als niet-IP, inclusief IP met opties, zoals SubNetwork Access Protocol (SNAP) ingekapselde IP en IPv6.
- Voor niet IP-pakketten is "match access group" de enige methode van classificatie omdat u geen DSCP voor niet-IP verkeer kunt aanpassen. Daartoe wordt een toegangslijst (MAC) (ACL) gebruikt; De pakketten kunnen worden aangepast op basis van het bron MAC-adres, het bestemming MAC-adres en EtherType. Het is niet mogelijk het IP-verkeer aan te passen aan MAC ACL, aangezien de switch een onderscheid maakt tussen IP- en niet-IP-verkeer.

Toezicht configureren en bewaken

Deze stappen zijn nodig om toezicht in Cisco IOS te configureren:

1. Een polisator definiëren (voor geaggregeerde polisers)
2. Criteria definiëren voor het selecteren van verkeer voor toezicht
3. Defineert een class-map voor het selecteren van verkeer aan de hand van gedefinieerde criteria
4. Defineer een service-beleid met een klas en pas een politieagent op de gespecificeerde klasse toe
5. Pas een service-beleid op een poort toe

Deze twee soorten politieagenten worden ondersteund:

- Benoemd aggregaat
- individu

De genoemde agent controleert het verkeer dat is gecombineerd van alle klassen binnen hetzelfde beleid naar de plaats van toepassing. Geaggregeerd toezicht op verschillende interfaces wordt niet ondersteund.

Toelichting: De totale politieagent kan niet op meer dan één beleid worden toegepast. Als dit zo is, wordt deze foutmelding weergegeven:

```
QoS: Cannot allocate policer for policy map <policy name>
```

Neem dit voorbeeld:

Er is een verkeersgenerator aangesloten op poort Gigabit Ethernet0/3 die ongeveer 17 Mbps van UDP verkeer met de bestemming poort 111 verstuurt. Er is ook TCP verkeer van poort 20. U wilt dat deze twee verkeersstromen tot 1 Mbps worden gecontroleerd, en er moet excessief verkeer vallen. Dit voorbeeld laat zien hoe dit gebeurt:

```
!--- Globally enables QoS. mls qos !--- Defines the QoS policer, sets the burst !--- to 16000
for better TCP performance. mls qos aggregate-policer pol_1mbps 1000000 16000 exceed-action drop
!--- Defines the ACLs to select traffic. access-list 123 permit udp any any eq 111
access-list 145 permit tcp any eq 20 any
!--- Defines the traffic classes to be policed. class-map match-all cl_udp111 match access-group
123
class-map match-all cl_tcp20
  match access-group 145
!--- Defines the QoS policy, and attaches !--- the policer to the traffic classes. policy-map
po_test
```

```
  class cl_udp111
    police aggregate pol_1mbps
  class cl_tcp20
    police aggregate pol_1mbps
!--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport switchport
access vlan 2 service-policy input po_test
!
```

Het eerste voorbeeld gebruikte de naam geaggregeerde politieagent. De individuele politieagent, in tegenstelling tot de genoemde politieagent, controleert afzonderlijk het verkeer op elke klasse waar het wordt toegepast. De individuele politieagent wordt gedefinieerd in de beleidskaartconfiguratie. In dit voorbeeld worden twee verkeersklassen gecontroleerd door twee afzonderlijke politieagenten; cl_udp111 wordt uitgevoerd op 1 Mbps per burst van 8 kW, en cl_tcp20 wordt uitgevoerd op 512 Kbps per 32 kHz:

```
!--- Globally enables QoS. mls qos !--- Defines the ACLs to select traffic. access-list 123
permit udp any any eq 111
access-list 145 permit tcp any eq 20 any
!--- Defines the traffic classes to be policed. class-map match-all cl_udp111
  match access-group 123
class-map match-all cl_tcp20
  match access-group 145
!--- Defines QoS policy, and creates and attaches !--- the policers to the traffic classes.
policy-map po_test2
  class cl_udp111
    police 1000000 8000 exceed-action drop
  class cl_tcp20
    police 512000 32000 exceed-action drop
!--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport switchport
access vlan 2 service-policy input po_test2
```

Deze opdracht wordt gebruikt om de politiehandeling te controleren:

```
cat3550#show mls qos interface g0/3 statistics
GigabitEthernet0/3
Ingress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
Others: 267718     0          267717     0          0
Egress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
Others: 590877        n/a        n/a      266303     0

WRED drop counts:
  qid  thresh1    thresh2   FreeQ
   1 : 0          0         1024
   2 : 0          0         1024
   3 : 0          0         8
   4 : 0          0         1024
```

Opmerking: standaard zijn er geen per-DSCP statistieken. Catalyst 3550 ondersteunt een verzameling per interface, per richting van statistieken voor maximaal acht verschillende DSCP-waarden. Dit wordt ingesteld wanneer u de **mls qos monitor** opdracht geeft. Om statistieken voor DSCPs 8, 16, 24 en 32 te controleren moet u deze opdracht **per-interface** uitgeven:

```
cat3550(config-if)#mls qos monitor dscp 8 16 24 32
```

Opmerking: de opdracht **mls qos monitor dscp 8 16 24 32** wijzigt de uitvoer van de opdracht **mls qos int g0/3 statistieken** hierdoor:

```
cat3550#show mls qos interface g0/3 statistics
GigabitEthernet0/3
Ingress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
    8 : 0          0          675053785  0          0
    16: 1811748    0          0          0          0         ? per DSCP statistics
    24: 1227820404 15241073   0          0          0
    32: 0          0          539337294  0          0
Others: 1658208    0          1658208    0          0
Egress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
    8 : 675425886     n/a        n/a       0          0
    16: 0             n/a        n/a       0          0         ? per DSCP statistics
    24: 15239542      n/a        n/a       0          0
    32: 539289117     n/a        n/a       536486430  0
Others: 1983055       n/a        n/a       1649446    0

WRED drop counts:
  qid  thresh1    thresh2   FreeQ
   1 : 0          0         1024
   2 : 0          0         1024
   3 : 0          0         6
   4 : 0          0         1024
```

Dit is een beschrijving van de velden in het voorbeeld:

- **Inkomend**-toont hoeveel pakketten uit elke richting aankomen
- **NO_change** - toont aan hoeveel pakketten werden vertrouwd (zoals QoS-niveau niet gewijzigd)
- **Gerubriceerd** - toont hoeveel pakketten aan deze interne DSCP na classificatie zijn toegewezen
- Toezicht-toont hoeveel pakketten door toezicht werden gemarkeerd; DSCP wordt voor de markering weergegeven.
- **Gedrukt** - toont hoeveel pakketten door toezicht werden gedropt

Let op deze uitvoeringsspecifieke overwegingen:

- Als acht DSCP-waarden worden ingesteld wanneer u de opdracht **mls qos monitor** geeft, **kunnen** de andere die worden gezien wanneer u de opdracht **show mls qos int statistics geeft**, ontoereikende informatie weergeven.
- Er is geen specifieke opdracht om het aangeboden of uitgaande verkeerstarief per agent te verifiëren.
- Aangezien de tellers achtereenvolgens van de hardware worden teruggewonnen, is het mogelijk dat de tellers niet correct samenvoegen. Bijvoorbeeld, de hoeveelheid gecontroleerde, geclassificeerde of ingetrokken pakketten kan lichtjes anders zijn dan het aantal inkomende pakketten.

Markeren en bewaken

Deze stappen zijn nodig om de markering te configureren:

1. Bepaal de criteria voor de indeling van het verkeer

2. Verkeerscategorieën definiëren die moeten worden ingedeeld aan de hand van eerder vastgestelde criteria
3. Een beleidskaart maken die gemarkeerde acties en politieacties aan de gedefinieerde klassen hecht
4. Configureer de corresponderende interface(s) om de modus te vertrouwen
5. Pas de beleidskaart op een interface toe

In dit voorbeeld, wilt u inkomend IP verkeer om 192.168.192.168 te ontvangen die met IP voorrang 6 wordt gemarkeerd en tot 1 Mbps wordt gecontroleerd; overtollig verkeer moet worden gemarkeerd naar IP-voorrang 2:

```
!--- Globally enables QoS. mls qos !--- Defines the ACLs to select traffic. access-list 167
permit ip any host 192.168.192.168
!--- Defines the traffic class. class-map match-all cl_2host
  match access-group 167
!--- Defines QoS policy, and creates and attaches !--- the policers to the traffic classes.
policy-map po_test3
  class cl_2host
!--- Marks all the class traffic with the IP precedence 6. set ip precedence 6
!--- Polices down to 1 Mbps and marks down according to the QoS map. police 1000000 8000 exceed-
action policed-dscp-transmit
!--- Modifies the policed DSCP QoS map, so the !--- traffic is marked down from IP precedence 6
to 2. !--- In terms of DSCP, this is from 48 to 16 (DSCP=IPprec x8). mls qos map policed-dscp 48
to 16 !--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport
switchport access vlan 2 service-policy input po_test3
```

Het opdracht **mls qos interface statistics** wordt ook gegeven om de markering te controleren. De resultaten en implicaties van een steekproef worden in het gedeelte van dit document gedocumenteerd.

Hoe u al het interfaceverkeer kunt indelen met één automatische versterker

In Catalyst 3550 wordt de opdracht **overeenkomende interface** niet ondersteund en wordt slechts één match opdracht per class-map toegestaan. Bovendien staat Catalyst 3550 niet toe dat het IP-verkeer door de ACL's wordt gecompenseerd. IP- en niet-IP-verkeer moeten dus worden geclassificeerd met twee afzonderlijke class-maps. Dit maakt het lastig om al het verkeer dat in een interface komt in te delen en om al het verkeer met één enkel politieagent te controleren. Met de voorbeeldconfiguratie hier kun je dit realiseren. In deze configuratie worden IP- en niet-IP-verkeer gecombineerd met twee verschillende class-maps. Echter, elk gebruikt een gemeenschappelijke politieman voor zowel het verkeer.

```
access-list 100 permit ip any any

class-map ip
match access-group 100
!--- This class-map classifies all IP traffic. mac access-list extended non-ip-acl
permit any any

class-map non-ip
match access-group name non-ip-acl
!--- Class-map classifies all non-IP traffic only. mls qos aggregate-policer all-traffic 8000
8000 exceed-action drop
!--- This command configures a common policer that is applied for both IP and non-IP traffic.
policy-map police-all-traffic
```

```
class non-ip
police aggregate all-traffic
class ip
police aggregate all-traffic

interface gigabitEthernet 0/7
service-policy input police-all-traffic
!--- This command applies the policy map to the physical interface.
```

Gerelateerde informatie

- QoS configureren op Catalyst 3550
- Pagina's voor Quality-of-Service ondersteuning
- Ondersteuningspagina voor LAN-switching
- Productondersteuningspagina's voor LAN
- Technische ondersteuning en documentatie – Cisco Systems