Catalyst 6500 switches - QoS-probleemoplossing

Inhoud

Inleiding

Dit document bevat de basisstappen voor het opsporen en verhelpen van problemen, de kwaliteit van de service (QoS)-beperkingen en informatie voor het oplossen van problemen met betrekking tot gemeenschappelijke QoS-problemen in de Catalyst 6500-switches. In dit document worden ook QoS-kwesties besproken die zich voordoen bij de classificatie en het markeren en controleren.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Catalyst 6500 Series-switches.

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.

Achtergrondinformatie

QoS is een netwerkfunctie die het verkeer classificeert en deterministische leveringsservices aanbiedt. Deze punten verklaren de verschillende stappen in het QoS-proces:

- **Invoerplanning**: het wordt door hardwarepoort en ASIC's verwerkt en het is een Layer 2 QoS-handeling. Er is geen beleidsfunctiekaart (PFC) nodig.
- **Classificatie**-Het wordt behandeld door de toezichthouder en/of PFC via de ACL-motor (Access Control List, ACL). De toezichthouder behandelt de handeling van Layer 2 QoS. PFC behandelt Layer 2 en Layer 3 QoS.
- **Toezicht**-Het wordt door PFC via Layer 3 verzendmotor verwerkt. PFC is vereist en het handvat Layer 2 en Layer 3 QoS werking.
- **Packet herschrijven**-Het wordt verwerkt door hardwarepoort ASIC's. Het is een Layer 2 en Layer 3 QoS bewerking op basis van de eerder uitgevoerde classificatie.
- **Uitvoerplanning** - het wordt verwerkt door hardwarepoort ASIC's. Het is een Layer 2 en Layer 3 QoS bewerking op basis van de eerder uitgevoerde classificatie.

QoS voor probleemoplossing

QoS werkt in Catalyst 6500 switches anders dan in de routers. De QoS-architectuur is behoorlijk complex in Catalyst 6500 switches. Het wordt aanbevolen om de functiekaart voor meerlaagse switch (MSFC), PFC en de architectuur van Supervisor Engine in Catalyst 6500 te begrijpen. Configuratie van QoS in Hybrid OS vereist meer begrip van Layer 2 CatOS functionaliteit en Layer 3 MSFC met Cisco IOS® functionaliteit. Het wordt aanbevolen deze documenten diepgaand te lezen voordat u QoS configureren:

- PFC QoS configureren - native IOS
- QoS configureren - CatOS

Stap voor stap Problemen oplossen

Deze sectie bevat de basisprocedure voor het opsporen en verhelpen van problemen voor QoS om het probleem voor verdere probleemoplossing te isoleren.

1. **Schakel QoS in**—De **opdracht Mls qos** tonen de politiestatistieken en de status van QoS, of deze nu aan- of uitgeschakeld zijn.

```
Switch#show mls qos
  QoS is enabled globally
  QoS ip packet dscp rewrite enabled globally
  Input mode for GRE Tunnel is Pipe mode
  Input mode for MPLS is Pipe mode
  Vlan or Portchannel(Multi-Earl)policies supported: Yes
  Egress policies supported: Yes


 ----- Module [5] -----
  QoS global counters:
    Total packets: 244
    IP shortcut packets: 0
    Packets dropped by policing: 0
    IP packets with TOS changed by policing: 5
    IP packets with COS changed by policing: 4
    Non-IP packets with COS changed by policing: 0
    MPLS packets with EXP changed by policing: 0
```

2. **Classificatie van inkomende verkeer met vertrouwenspoort**-Deze classificatie categoriseert het inkomende verkeer in een van de zeven klassen van de dienst (CoS) waarden. Het inkomende verkeer kan de CoS waarde hebben die reeds door de bron wordt toegewezen. In dit geval, moet u de haven vormen om de waarde van CoS van het inkomende verkeer te vertrouwen. Met vertrouwen kan de switch de CoS- of ToS-waarden (type service) van het ontvangen frame behouden. Deze opdracht toont hoe de status van het havenvertrouwen moet worden geverifieerd:

```
Switch#show queueing int fa 3/40
  Port QoS is enabled
Trust state: trust CoS
  Extend trust state: not trusted [CoS = 0]
  Default CoS is 0

!--- Output suppressed.
```

De CoS-waarde wordt alleen geleverd door Inter-Switch Link (ISL) en Pad1q frames. Niet-gelabelde frames dragen geen CoS-waarden. Niet-gelabelde frames dragen ToS waarden die zijn afgeleid van IP-voorrang of gedifferentieerd servicescoderingspunt (DSCP) van de IP-pakketheader. Om de ToS waarde te vertrouwen, moet u de poort configureren om IP voorrang of DSCP te vertrouwen. DSCP is achterwaarts compatibel met IP-voorrang. Als u bijvoorbeeld een switchpoort hebt ingesteld als Layer 3 poort, hebben deze geen punt1q of ISL-frames. In dit geval, moet u deze poort configureren om DSCP of IP voorrang te vertrouwen.

```
Switch#show queueing interface gigabitEthernet 1/1
Interface GigabitEthernet1/1 queueing strategy:  Weighted Round-Robin
  Port QoS is enabled
  Trust state: trust DSCP
  Extend trust state: not trusted [COS = 0]
  Default CoS is 0

!--- Output suppressed.
```

3. **Classificatie van inkomende verkeer met ACL en ACE** -U kunt ook de schakelaar configureren om het verkeer te classificeren en te markeren. De stappen die zijn meegeleverd om classificatie en markering te configureren zijn: om toegangslijsten, class-map en beleids-map te maken en de **service-beleid** input opdracht uit te geven om de beleidskaart in de interface toe te passen. U kunt de statistieken voor de beleidskaarten zoals hieronder aangegeven verifiëren:

```
Switch#show policy-map interface fa 3/13
 FastEthernet3/13

  Service-policy input: pqos2

    class-map: qos1 (match-all)
      Match: access-group 101
      set precedence 5:
      Earl in slot 5 :
        590 bytes
       5 minute offered rate 32 bps
        aggregate-forwarded 590 bytes

    Class-map: class-default (match-any)
      36 packets, 2394 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any

Switch#show mls qos ip ingress
 QoS Summary [IPv4]:      (* - shared aggregates, Mod - switch module)

      Int Mod Dir  Class-map DSCP  Agg  Trust Fl   AgForward-By   AgPoliced-By
                                   Id         Id
-------------------------------------------------------------------------------
    Fa3/13  5  In       qos1   40    1     No  10            590              0

       All  5   -    Default    0    0*    No  0          365487              0
```

Merk op dat de tellers **AgForward-By** die overeenkomen met de class-map qos1 toename geven. Als u de statistieken voor de corresponderende class-map niet ziet, controleer dan de toegangslijst die aan de class-map is toegevoegd.

4. **Invoerplanning**-PFC is niet vereist om invoerplanning te configureren. U kunt de **rcv-wachtrijdrempel** niet configureren of **qos** vervolgopdrachten op één poort van 10/100 instellen. Dit komt doordat de dienstregeling wordt beheerd door de ASIC-havens van de kustlijn die twaalf 10/100 havens bevatten. Daarom moet u het invoerschema configureren in sets van 12 poorten, zoals 1-12, 13-24, 25-36, 37-48.De wachtende architectuur wordt ingebouwd in de ASIC en kan niet opnieuw worden geconfigureerd. Geef de **fastnetsleuf/poort op voor** de **wachtrij van de toonbank | omvat type** opdracht om de wachtrijstructuur van een LAN poort te zien.

```
Switch#show queueing interface fastEthernet 3/40
Queueing Mode In Rx direction: mode-cos
    Receive queues [type = 1q4t]:         <--------- 1 Queue 4 Threshold
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       1         Standard            4


    queue tail-drop-thresholds
    --------------------------
    1     50[1] 60[2] 80[3] 100[4]  <------ Threshold levels 50%, 60%, 80% and 100%


  Packets dropped on Receive:
    BPDU packets:  0

    queue thresh    dropped  [cos-map]
    ---------------------------------------------------
    1     1               0  [0 1 ]
    1     2               0  [2 3 ]
    1     3               0  [4 5 ]
    1     4               0  [6 7 ]
```

```
!--- Output suppressed.
```

Standaard zijn alle vier de drempels 100%. U kunt de **rcv-wachtrijdrempel** uitgeven *<Wachtrij ID> <Drempel 1> <Drempel 2> <Drempel 3> <Drempel 14>* opdracht om de drempelniveaus te configureren. Op deze manier worden de hogere CoS-waardengegevens niet achtergelaten voordat de lagere CoS-waardengegevens tijdens de congestie achterblijven.

```
Switch(config)#interface range fa 3/37 - 48
Switch(config-if-range)#rcv-queue threshold 1 50 60 80 100
```

5. **Toewijzing**-Als de poort is ingesteld om de CoS te vertrouwen, dan gebruikt u de CoS-DSCP kaarttabel om de ontvangen CoS-waarde in een interne DSCP-waarde in kaart te brengen.

```
Switch#show mls qos maps cos-dscp
   Cos-dscp map:
         cos:   0  1  2  3  4  5  6  7
      ---------------------------------
         dscp:   0  8 16 24 32 40 48 56
```

Als de poort is ingesteld om de trust IP-voorrang te vertrouwen, dan gebruik u de ip-prec-dscp-kaarttabel om de ontvangen IP-prioriteitswaarde in een interne DSCP-waarde in kaart te brengen.

```
Switch#show mls qos maps ip-prec-dscp
   IpPrecedence-dscp map:
      ipprec:   0  1  2  3  4  5  6  7
      ---------------------------------
         dscp:   0  8 16 24 32 40 48 56
```

Als de poort is ingesteld om de DSCP te vertrouwen, dan wordt de ontvangen DSCP-waarde gebruikt als de interne DSCP-waarde.Deze tabellen moeten op alle switches in uw netwerk hetzelfde zijn. Als een van de switches een tabel met verschillende afbeeldingen heeft, ontvangt u het gewenste resultaat niet. U kunt deze tabelwaarden als volgt wijzigen:

```
Switch(config)#mls qos map cos-dscp 0 8 16 24 40 48 48 56
Switch(config)#mls qos map ip-prec-dscp 0 8 16 24 40 48 48 56
```

6. **Toezicht**-Er zijn twee soorten toezicht beschikbaar in Catalyst 6500 switches:**Geaggregeerd** toezicht **op** - Geaggregeerd toezicht controleert de bandbreedte van een stroom in de switch. De opdracht **show mls qos aggregal-politier** toont alle geconfigureerde totale politieagent die op de schakelaar is ingesteld. Dit zijn de politiestatistieken:

```
Switch#show mls qos ip fastEthernet 3/13
   [In] Policy map is pqos2   [Out] Default.
 QoS Summary [IPv4]:      (* - shared aggregates, Mod - switch module)

      Int Mod Dir  Class-map DSCP  Agg  Trust Fl   AgForward-By   AgPoliced-By
                                   Id         Id
-------------------------------------------------------------------------------
    Fa3/13  5  In       qos1    0    1*  dscp  0          10626         118860
    Fa3/13  5  In class-defa   40    2     No  0           3338              0

Switch#show mls qos
  QoS is enabled globally
  QoS ip packet dscp rewrite enabled globally
  Input mode for GRE Tunnel is Pipe mode
  Input mode for MPLS is Pipe mode
  Vlan or Portchannel(Multi-Earl) policies supported: Yes
  Egress policies supported: Yes


 ----- Module [5] -----
  QoS global counters:
    Total packets: 163
```

```
    IP shortcut packets: 0
    Packets dropped by policing: 120
    IP packets with TOS changed by policing: 24
    IP packets with COS changed by policing: 20
    Non-IP packets with COS changed by policing: 3
    MPLS packets with EXP changed by policing: 0
```

Toezicht microflow-microflow controle bandbreedte van een stroom per interface in de switch. Standaard beïnvloeden microflow-politiemensen alleen routeverkeer. Geef de **mls qos** een **overbrugde** opdracht in de interface van VLAN uit om microflow controle voor overbrugd verkeer mogelijk te maken. Dit is de verificatie van de microflow-politiestatistieken:

```
Switch#show mls ip detail
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f         :AdjPtr
---------------------------------------------------------------------------
Pkts         Bytes         Age   LastSeen  Attributes
-----------------------------------------------

Mask Pi R CR Xt Prio Dsc IP_EN OP_EN Pattern Rpf FIN_RDT FIN/RST
----+--+-+--+--+----+---+-----+-----+-------+---+-------+-------
Ig/acli Ig/aclo Ig/qosi Ig/qoso Fpkt Gemini MC-hit Dirty Diags
-------+-------+-------+-------+----+------+------+-----+------

    QoS     Police Count Threshold    Leak     Drop Bucket  Use-Tbl Use-Enable
-----------+------------+---------+-----------+----+-------+-------+-----------+
10.175.50.2     10.175.51.2     icmp:8      :0        --               :0x0
43           64500         84    21:37:16   L3 - Dynamic
1    1  0  0  1  0    0    1     1     0       0     0      0
0          0       0       0      0    0       0     0     0
  0x0          0               0        0       NO   1518      NO       NO
10.175.50.2     10.175.51.2     icmp:0      :0        --               :0x0
43           64500         84    21:37:16   L3 - Dynamic
1    1  0  0  1  0    0    1     1     0       0     0      0
0          0       0       0      0    0       0     0     0
  0x0          664832          0        0       NO   1491      NO       NO
0.0.0.0         0.0.0.0         0   :0      :0        --               :0x0
1980         155689        1092  21:37:16   L3 - Dynamic
0    1  0  0  1  0    0    1     1     0       0     0      0
0          0       0       0      0    0       0     0     0
  0x0          0               0        0       NO   0         NO       NO

Switch#show mls qos
  QoS is enabled globally
  QoS ip packet dscp rewrite enabled globally
  Input mode for GRE Tunnel is Pipe mode
  Input mode for MPLS is Pipe mode
  Vlan or Portchannel(Multi-Earl) policies supported: Yes
  Egress policies supported: Yes


 ----- Module [5] -----
  QoS global counters:
    Total packets: 551
    IP shortcut packets: 0
    Packets dropped by policing: 473
    IP packets with TOS changed by policing: 70
    IP packets with COS changed by policing: 44
    Non-IP packets with COS changed by policing: 11
    MPLS packets with EXP changed by policing: 0
```

Opmerking: de **opdracht Mls qos ip *type mod/number* opdracht toont de** microflow-politiestatistieken niet. Het geeft alleen de totale politiestatistieken weer.Als u de gewenste politiestatistieken niet ziet, controleert u de configuratie van het toezicht. Raadpleeg het QoS-

toezicht op Catalyst 6500/6000 Series-switches om het configuratievoorbeeld te zien. Raadpleeg ook de QoS-richtlijnen en -beperkingen voor Catalyst 6500 switches in dit document.

7. Controleer de releaseopmerkingen van uw versie van het besturingssysteem en controleer of er geen insecten zijn verbonden aan uw QoS-configuratie.
8. Let op uw model van de schakelaar toezichthouder, PFC-model, MSFC-model en Cisco IOS/CatOS-versie. Zie de QoS-richtlijnen en -beperkingen voor Catalyst 6500 switches met betrekking tot uw specificaties. Zorg ervoor dat de configuratie van toepassing is.

QoS-richtlijnen en -beperkingen voor Catalyst 6500 switches

Er zijn QoS-beperkingen waar u zich bewust van moet zijn voordat u QoS op Catalyst 6500-switches configureren:

- Algemene richtsnoeren
- PFC3-richtsnoeren
- PFC2-richtsnoeren
- Beperkingen van klasse-kaartopdracht
- Beperkingen in beleidsmap
- Beperkingen van klasse van beleidskaarten
- Wachtrij en Drop Drempel Toewijzing en beperkingen
- trust-kos in ACL-toegangsbeperkingen
- Beperkingen van de WS-X6248-xx, WS-X624-xx en WS-X6348-xx lijnkaarten
- PFC of PFC2 bieden geen QoS voor het WAN-verkeer. Met PFC of PFC2, verandert PFC QoS niet de ToS byte in het WAN-verkeer.
- Het ingegraven LAN-verkeer dat Layer 3 is ingeschakeld, gaat niet door MSFC of MSFC2 en behoudt de CoS-waarde die wordt toegewezen door Layer 3-switchmotor.
- QoS voert geen invoerpoortcongestievermijding uit op de poorten die zijn geconfigureerd met de zoekwoorden **onbetrouwbaar**, **trust-impprec** of **trust-dscp**. Het verkeer gaat rechtstreeks naar de wisselmachine.
- De schakelaar gebruikt de munt-daling drempel voor het verkeer dat de waarden CoS draagt die slechts aan de rij in kaart worden gebracht. De schakelaar gebruikt de WRED-daling drempels voor het verkeer dat de CoS waarden draagt die aan de rij en een drempel in kaart worden gebracht.
- Classificatie met een Layer 3-switchingmotor gebruikt de Layer 2-, 3- en 4-waarden. Markeren met een Layer 3-switchingmotor maakt gebruik van Layer 2 CoS-waarden en Layer 3 IP-voorrang of DSCP-waarden.
- Een vertrouwenwekkende ACL kan de ontvangen CoS in het verkeer van de onvertrouwde poorten niet herstellen. Het verkeer van de onvertrouwde havens heeft altijd de port CoS waarde.

Opmerking: PFC QoS detecteert het gebruik van niet-ondersteunde opdrachten niet totdat u een beleidskaart aan een interface toevoegt.

QoS_CAM-beperking

De Ternary CAM (TCAM) is een gespecialiseerd geheugen dat voor snelle tabelraadpleging is ontworpen, op basis van pakketten die door de switch worden doorgegeven, uitgevoerd door de ACL-motor op PFC, PFC2 en PFC3. ACL's worden verwerkt in hardware in Cisco Catalyst 6500

Series-switches die TCAM worden genoemd. Wanneer u ACL vormt, in kaart brengen ACL op QoS en wanneer u het QoS beleid op de interface toepast, de schakelaar programma's TCAM. Als u al de beschikbare CAM-ruimte op de switch voor QoS hebt gebruikt, krijgt u deze foutmelding:

```
Switch(config)#interface vlan 52
Switch(config-if)#service-policy input test
Switch(config-if)#
3w0d: %QM-4-TCAM_ENTRY: Hardware TCAM entry capacity exceeded
```

Dit toont de opdrachtoutput van tcam aan dat de TCAM entry maskers 95% gebruikt zijn. Daarom, wanneer u het QoS-beleid op de interface toepast, ontmoet u de `%QM-4-TCAM_ENTRY:` foutmelding.

```
Switch#show tcam count
           Used        Free        Percent Used       Reserved
           ----        ----        ------------       --------
 Labels:(in) 43        4053             1
 Labels:(eg)  2        4094             0

ACL_TCAM
--------
  Masks:     19        4077             0                   72
Entries:     95       32673             0                  576

QOS_TCAM
--------
  Masks:   3902         194            95                   18
Entries:  23101        9667            70                  144

    LOU:      0         128             0
  ANDOR:      0          16             0
  ORAND:      0          16             0
    ADJ:      3        2045             0
```

TCAM-items en ACL-labels zijn beperkte resources. Daarom, afhankelijk van uw ACL configuratie, zou u voorzichtig moeten zijn om de beschikbare middelen niet uit te putten. Bovendien kunt u met grote VACL-configuraties (QoS ACL en VLAN Access Control List) ook non-Volatile Random Access Geheugen (NVRAM) overwegen. De beschikbare hardwarebronnen verschillen op supervisor 1a met PFC, supervisor 2 met PFC2 en supervisor 720 met PFC3.

Supervisor Module	QoS-TCAM	ACL-labels
supervisor 1a en PFC	2K-maskers en 16K patronen gedeeld tussen routertoegangscontrolelijsten (RACL's), VACL's en QoS ACL's	512 ACL-labels die worden gedeeld tussen RACL's, VACL's en QoS ACL's
Supervisor 2 en PFC2	4K-maskers en 32K-patronen voor QoS ACL's	512 ACL-labels die worden gedeeld tussen RACL's, VACL's en QoS ACL's
supervisor	4K-maskers en 32K-patronen voor QoS ACL's	512 ACL-labels die worden gedeeld

720 en PFC3		tussen RACL's, VACL's en QoS ACL's

Opmerking: Ongeacht de 512 ACL-labellimiet is er een extra softwarerelease in Cisco CatOS van 250 QoS ACL's voor het hele systeem wanneer u de standaard (binaire) configuratiemodus gebruikt. Deze beperking wordt in de tekstconfiguratie modus verwijderd. Geef het opdracht **de** ingestelde **configuratiemodus** uit om de configuratiemodus in de tekstmodus te wijzigen. De tekstmodus gebruikt doorgaans minder NVRAM of Flash geheugenruimte dan de binaire configuratie modus gebruikt. U moet het opdracht **schrijfgeheugen** uitgeven terwijl u in tekstmodus werkt om de configuratie in NVRAM op te slaan. Geef de **ingestelde configuratiewijze tekst auto-save-**opdracht uit om de tekstconfiguratie in NVRAM automatisch op te slaan.

Dit is het werkkader voor de TCAM-kwestie:

- Als u de opdracht **service-beleid** op veel Layer 2 interfaces hebt geïmplementeerd die tot één VLAN behoren, kunt u VLAN-gebaseerd toezicht uitvoeren in plaats van op switchpoort gebaseerd. Dit is een voorbeeld:
```
Switch(config)#interface range fastethernet x/y - Z
Switch(config-if)#mls qos vlan-based
Switch(config-if)#exit
Switch(config)#interface vlan 100
Switch(config-if)#service-policy input Test_Policy
```

- QoS-markeringsstatistieken uitschakelen. Met de opdracht **geen mls qos markeringsstatistieken** kan de max van 1020 AgIDs niet worden geïmplementeerd. Dit komt doordat de standaardpolitie wordt toegewezen aan vaste DSCP-beleidsmakers. Het negatieve effect hiervan is dat er geen statistieken zijn voor de specifieke politieagent omdat ze allemaal de standaardpolitie delen.
```
Switch(config)#no mls qos marking statistics
```

- Gebruik indien mogelijk dezelfde ACL's op meerdere interfaces om de contentopslag van TCAM te beperken.

NBAR-beperking

Network-Based Application Recognition (NBAR) is een classificatiemodule die een brede reeks toepassingen herkent, die web-gebaseerde en andere moeilijk te classificeren protocollen omvat die dynamische TCP/UDP-poorttaken gebruiken. Wanneer een toepassing door NBAR wordt herkend en geclassificeerd, kan een netwerk voor die specifieke toepassing een beroep doen op diensten. NBAR classificeert pakketten en past dan QoS op het gerubriceerde verkeer toe om ervoor te zorgen dat de netwerkbandbreedte efficiënt wordt gebruikt. Er zijn enige beperkingen in hoe QoS moet worden geïmplementeerd wanneer u NBAR gebruikt:

- PFC3 ondersteunt NBAR niet.
- Met een Supervisor Engine 2, PFC2 en MSFC2:U kunt NBAR op Layer 3 interfaces configureren in plaats van PFC QoS.PFC2 biedt hardwareondersteuning voor ingangsACL's op poorten waar u NBAR vormt.Wanneer PFC QoS is geactiveerd, het verkeer door havens waar u NBAR vormt passeert door de ingangen en de stress wachtrijen en daalt drempels.Wanneer PFC QoS is geactiveerd, stelt MSFC2 grotere CoS in gelijk aan IP voorrang in NBAR-verkeer.Nadat al het verkeer door een ingangsrij passeert, wordt het in

software op MSFC2 op interfaces verwerkt waar u NBAR vormt.

De co-map opdrachten ontbreekt in supervisor 2

Onder Native IOS-softwarereleases 12.1(8a)EX-12.1(8b)EX5 en 12.1(11b)E en later zijn de standaard QoS CoS-mappings voor Gigabit uplinks op Supervisor2 gewijzigd. Alle CoS waarden zijn toegewezen aan rij 1 en drempel 1, en kunnen niet worden gewijzigd.

Deze opdrachten kunnen niet worden ingesteld op een Sup2 Gigabit uplink-poort op deze releases:

```
rcv-queue cos-map
priority-queue
wrr-queue cos-map
```

QoS-configuraties zijn beperkt en de strikte prioriteitswachtrij kan niet worden gebruikt. Dit beïnvloedt alleen de Gigabit poorten die fysiek op de Supervisor 2 Engine zijn geplaatst. Gigabit-poorten op andere lijnkaartmodules worden niet beïnvloed.

Er is een firmware upgrade die dit probleem oplost. Deze upgrade kan via software worden uitgevoerd. Neem contact op met technische ondersteuning als een upgrade van de firmware is vereist. Merk op dat een firmware-upgrade alleen nodig is als de HW versie van Supervisor2 kleiner is dan 4.0. Als de HW versie van Supervisor2 4.0 of hoger is, dient QoS toegestaan te zijn op de Gigabit uplink-poorten zonder de firmware-upgrade. U kunt de opdracht **Module tonen** uitgeven om het niveau firmware te vinden. Dit probleem wordt geïdentificeerd in Cisco bug-ID CSCdw89764 (alleen geregistreerde klanten).

Beperkingen in servicesbeleid

Om beleid-kaart op de interface toe te passen, geef de **dienst-beleid** opdracht uit. Als u een niet-ondersteunde opdracht in beleid-map hebt, nadat u deze met de opdracht **service-beleid** hebt toegepast, leidt de switch de foutmeldingen op de console. Deze punten moeten in overweging worden genomen bij de problemen **met** uw **servicebeleid**.

- Sluit geen servicebeleid aan op een haven die lid is van een EtherChannel.
- Dankzij geïnstalleerde Distributed Forwarding Cards (DFC's) ondersteunt PFC2 op VLAN gebaseerde QoS niet. U kunt de **mls qos op VLAN gebaseerde** opdracht niet geven of **het** servicebeleid aan VLAN-interfaces toevoegen.
- PFC QoS ondersteunt het uitvoersleutelwoord alleen met PFC3 en alleen op Layer 3 interfaces (LAN poorten die zijn geconfigureerd als Layer 3 interfaces of VLAN-interfaces). Met PFC3 kunt u zowel een ingang als een uitvoerbeleidskaart aan een Layer 3-interface toevoegen.
- VLAN-gebaseerde of op poort gebaseerde PFC QoS op Layer 2-poorten zijn niet relevant voor beleid dat aan Layer 3-interfaces met het uitvoersleutelwoord is gekoppeld.
- Het beleid dat met het uitvoersleutelwoord wordt verbonden steunt geen toezicht op microflow.
- U kunt geen beleidskaart toevoegen die een vertrouwensstaat vormt met de opdrachtoutput **van het service-beleid**.
- PFC QoS ondersteunt invoermarkering niet met striktere of lagere waarde bij lagere

markering.

Uitvoer van Service-beleid De verklaringen tonen niet omhoog in de uitvoer van het in werking stellen-configuratie bevel

Wanneer u QoS op de multilink op de FlexWAN-module vormt, kunt u de opdrachtoutput **van het service-beleid** niet zien in de opdrachtoutput van de **show-run-**instelling. Dit gebeurt wanneer de switch Cisco IOS-versies eerder dan 12.2SX draait. FlexWAN voor Cisco 7600 Series ondersteunt dLLQ op niet-gebundelde interfaces. Het ondersteunt dLLQ niet op MLPPP bundelinterfaces. Deze ondersteuning is beschikbaar bij Cisco IOS-softwarerelease 12.2S.

De tijdelijke versie om deze beperking te omzeilen is het service-beleid aan ontbundelde interfaces toe te voegen of de Cisco IOS versie aan 12.2SX of later te verbeteren, waar de functie wordt ondersteund.

Beperking toezicht

Controle wordt uitgevoerd in hardware op PFC zonder de impact van switchprestaties. Toezicht kan niet plaatsvinden op het 6500-platform zonder PFC. In Hybrid OS moet de controle in het CatOS worden geconfigureerd. Deze punten moeten in overweging worden genomen bij het controleren van problemen met uw probleemoplossing:

- Wanneer u zowel inbraakpolitie- als toegangscontrole op hetzelfde verkeer toepast, moeten zowel het invoerbeleid als het uitvoerbeleid het verkeer markeren of het verkeer verminderen. PFC QoS ondersteunt invoermarkering niet met striktere of lagere waarde bij lagere markering.
- Wanneer u een politieman maakt die niet het sleutelwoord gebruikt en de maximum_burst_bytes parameter is gelijk aan de normaalwaarde_burst_bytes parameter (wat het geval is als u niet de maximum_burst_bytes parameter) ingaat, de veel-actie gepolitied-dscp-transmissie sleutelwoorden PFC QoS om verkeer te markeren zoals bepaald door de politie-dscp max-burst markering.
- Wanneer de overschrijdingsactie laat is, negeert PFC QoS elke geconfigureerde gewelddadige actie.
- Wanneer u droog vormt als de conforme actie, daalt de PFC QoS-configuratie als de hoger gelegen actie en de violette actie.
- De vereisten voor het vloeiingmasker van microflow-toezicht, NetFlow, en NetFlow Data Exporteren (NDE) kunnen conflicteren.

Rate-Limit voor problemen met toezicht met MSFC in hybride OS

Op Catalyst 6500 switches die Hybrid OS draaien, geeft de configuratie van de snelheidsbeperking niet de gewenste uitvoer. Als u bijvoorbeeld de opdracht **rate-limit** configureren onder de opdracht **interface-VLAN** op de MSFC, dan beperkt dit het verkeer feitelijk niet.

```
interface Vlan10
 rate-limit input 256000 2000 2000 conform-action transmit exceed-action drop
 rate-limit output 256000 2000 2000 conform-action transmit exceed-action drop
```

Of:

```
interface Vlan10
service-policy input Test_Policy
```

De reden achter dit is dat MSFC alleen de controle functies verzorgt, maar dat het daadwerkelijke doorsturen van verkeer plaatsvindt op PFC ASICs op de supervisor. De MSFC verzamelt de FIB- en nabijheidstabellen, evenals andere controlemateriaal, en downloads het tot PFC om in hardware te implementeren. Met de configuratie die u hebt gemaakt, beperkt u alleen de software die is overgeschakeld, en deze is minimaal (of geen).

De tijdelijke versie is om de CatOS opdrachtregel interface (CLI) te gebruiken om de snelheidsbeperking voor de supervisor te configureren. Raadpleeg CatOS QoS voor de gedetailleerde uitleg over de manier waarop u de QoS-toezicht in CatOS kunt configureren. U kunt ook QoS-toezicht op Catalyst 6500/6000 Series switches raadplegen om het configuratievoorbeeld te zien.

Gemiddelde commando vorm niet ondersteund in VLAN-interfaces van Cisco 7600

Wanneer u een servicebeleidsingang op een interface voor Cisco 7600 toepast, verschijnt deze foutmelding:

```
7600_1(config)#int Gi 1/40
7600_1(config-if)#service-policy input POLICY_1
shape average command is not supported for this interface
```

De **vorm gemiddelde** opdracht wordt niet ondersteund voor de VLAN-interfaces in Cisco 7600. In plaats daarvan moet je politie gebruiken.

```
7600_1(config)#policy-map POLICY_1
7600_1(config-pmap)#class TRAFFIC_1
7600_1(config-pmap-c)#police conform-action transmit exceed-action drop
```

Raadpleeg het Toezicht op Beleidslijn configureren voor meer informatie over het uitvoeren van toezicht op snelheidsbeperking voor verkeer.

Zoals u dit service-beleid aan een VLAN-interface (SVI) vastlegt, moet u VLAN-gebaseerde QoS inschakelen op al die Layer 2-poorten die tot dit VLAN behoren, waarin u wilt dat deze beleidskaart wordt toegepast.

```
7600_1(config)#interface Gi 1/40
7600_1(config-if)#mls qos vlan-based
```

Raadpleeg VLAN-gebaseerde PFC QoS op Layer 2 LAN-poorten voor meer informatie.

QoS-FOUT: Toevoeging/wijziging van de beleidskaart [tekens] en klasse [tekens] is ongeldig, opdracht wordt verworpen

```
QoS-ERROR: Addition/Modification made to policymap vtc-map and class voice-video is
not valid, command is rejected
```

Deze foutmelding geeft aan dat de acties die in de genoemde klasse zijn gedefinieerd, niet zijn toegestaan in Cisco Catalyst 6500 Series-switches. Er zijn enige beperkingen tijdens de configuratie van beleidslijnklasseacties.

- U kunt deze drie niet allemaal in een beleidskaartklasse doen:Verkeer markeren met de **ingestelde** opdrachtenDe vertrouwensstaat configurerenToezicht configurerenU kunt alleen verkeer met de **ingestelde** opdrachten markeren.OFConfigureer de truststaat en/of stel het toezicht in.
- Voor hardware-switched verkeer ondersteunt PFC QoS niet de opdrachten van de **bandbreedte**, **prioriteit**, **wachtrijlimiet** of **willekeurige** detectie van beleidskenmerken. U kunt deze opdrachten configureren omdat ze kunnen worden gebruikt voor software-switched verkeer.
- PFC QoS steunt de **ingestelde** opdrachten van de beleidskaartklasse niet van **qos-group**.

Raadpleeg de acties van de klasse Policy Map voor meer informatie over dergelijke beperkingen.

Gerelateerde informatie

- QoS-classificatie en markering op Catalyst 6500/6000 Series-switches die Cisco IOS-software uitvoeren
- QoS O-planning bij Catalyst 6500/6000 Series switches die Cisco IOS-systeemsoftware uitvoeren
- QoS-toezicht op Catalyst 6500/6000 Series-switches
- QoS-classificatie en markering op Catalyst 6500/6000 Series-switches met CatOS-software
- QoS O-planning bij Catalyst 6500/6000 Series switches die CatOS-systeemsoftware uitvoeren
- Productondersteuningspagina's voor LAN
- Ondersteuningspagina voor LAN-switching
- Technische ondersteuning en documentatie – Cisco Systems