QoS-classificatie en markering op Catalyst 6500/6000 Series Switches die Cisco IOS-software uitvoeren

Inhoud

Inleiding

Dit document onderzoekt wat er gebeurt met betrekking tot de markering en classificatie van een pakket op verschillende fasen in het Cisco Catalyst 6500/6000 chassis dat Cisco IOS®-software draait. Dit document beschrijft speciale gevallen en beperkingen, en geeft korte casestudy's.

Dit document bevat geen limitatieve lijst van alle IOS-softwarecoopdrachten van Cisco die betrekking hebben op QoS of markering. Raadpleeg voor meer informatie over de Cisco IOS-softwarerelease interface (CLI) het configureren van PFC QoS.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardwareversies:

- Catalyst 6500/6000 Series switches die Cisco IOS-software uitvoeren en een van deze Supervisor Engine gebruiken:Een Supervisor Engine 1a met een beleidsfunctiekaart (PFC) en een functiekaart voor meerlaagse Switch (MSFC)Een Supervisor Engine 1A met een PFC en een MSFC2Een Supervisor Engine 2 met een PFC2 en een MSFC2

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.

Terminologie

De lijst bevat de terminologie die in dit document wordt gebruikt:

- Gedifferentieerd services coderpunt (DSCP) - de eerste zes bits van het type service-byte (ToS) in de IP-header. DSCP is alleen aanwezig in het IP-pakket.**Opmerking:** de switch wijst ook een interne DSCP aan elk pakje toe, of het nu om IP of niet-IP gaat. In het gedeelte Vier MOGELIJKE bronnen voor interne DSCP van dit document wordt deze interne DSCP-toewijzing gedetailleerd.
- IP voorrang-de eerste drie bits van de ToS-byte in de IP-header.
- Serviceklasse (CoS) - het enige veld dat kan worden gebruikt om een pakket te markeren op Layer 2 (L2). CoS bestaat uit één van deze drie bits:De drie IEEE 802.1p-bits in de IEEE 802.1Q-tag (dot1q) voor het dot1q-pakket.**N.B.:** Standaard labelen Cisco-switches geen inheemse VLAN-pakketten.De drie bits genaamd "User Field" in de Inter-Switch Link (ISL) header voor een door ISL ingekapseld pakket.**Opmerking:** CoS is niet aanwezig in een niet-punt1q of een ISL-pakket.
- Classificatie—Het proces dat wordt gebruikt om het te markeren verkeer te selecteren.
- Marking-het proces dat een Layer 3 (L3) DSCP-waarde in een pakket instelt. In dit document wordt de definitie van markering uitgebreid tot de instelling van L2 CoS-waarden.

Catalyst 6500/6000 Series switches kunnen classificaties maken op basis van deze drie

parameters:

- DSCP
- IP-voorrang
- CoS

De Catalyst 6500/6000 Series switches voeren in verschillende fasen classificatie en markering uit. Dit gebeurt op verschillende plaatsen:

- Invoerpoort (ingress applicatie-specifieke geïntegreerde schakeling [ASIC])
- Switching Engine (PFC)
- Uitvoer (stress-ASIC)

Invoerpoortbehandeling

De belangrijkste configuratieparameter voor de ingangshaven, wat de classificatie betreft, is de `vertrouwensstaat` van de haven. Elke haven van het systeem kan één van deze `vertrouwensstaten` hebben:

- `trust-ip-voorrang`
- `trust-dscp`
- `vertrouwenskosten`
- `onbetrouwbaar`

Als u de status `van het` poortvertrouwen wilt instellen of wijzigen, geeft u deze opdracht voor Cisco IOS-software uit in de interfacemodus:

```
6k(config-if)#mls qos trust ?
  cos            cos keyword
  dscp           dscp keyword
  ip-precedence  ip-precedence keyword
  <cr>
```

Opmerking: Standaard zijn alle poorten in de `onvertrouwde` toestand geplaatst als QoS is ingeschakeld. Om QoS op Catalyst 6500 in te schakelen dat Cisco IOS-software draait, geeft u de opdracht **mls qos** uit in de hoofdconfiguratiemodus.

Op het niveau van de ingangspoort kunt u ook een standaard CoS per poort toepassen. Hierna volgt een voorbeeld:

```
6k(config-if)#mls qos cos cos-value
```

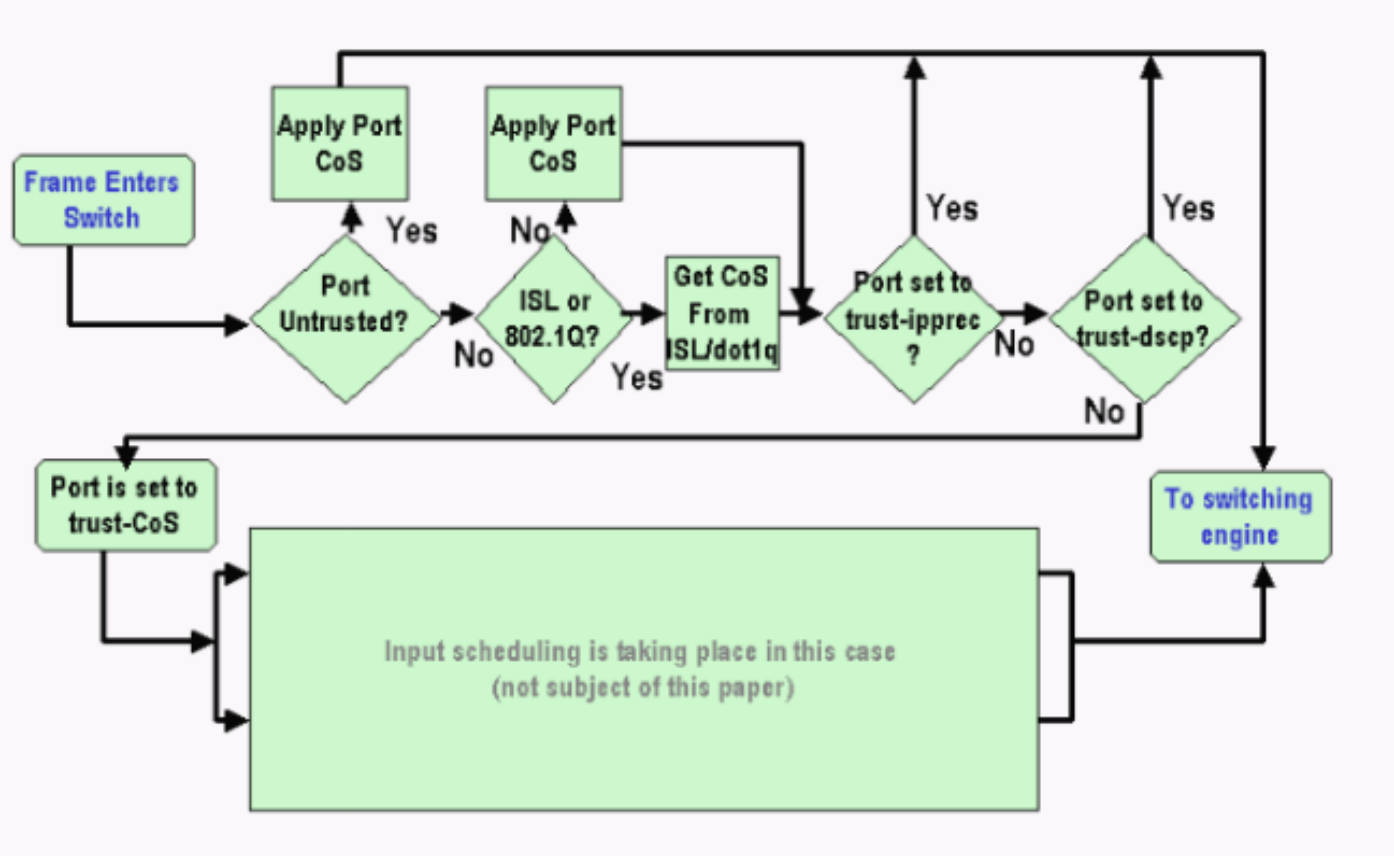
Deze standaard CoS is van toepassing op alle pakketten, zoals IP en Internetwork Packet Exchange (IPX). U kunt de standaard CoS op elke fysieke poort toepassen.

Als de poort in de `onvertrouwde` staat is, markeert u het frame met de poort-standaard CoS en geeft u de header door aan de switchingmachine (PFC). Als de poort is ingesteld op een van de `vertrouwde` staten, voert u een van deze twee opties uit:

- Als het frame geen ontvangen CoS (dot1q of ISL) heeft, past u de standaardpoort CoS toe.
- Voor dot1q en ISL frames bewaren de CoS zoals het is.

Geef het frame vervolgens door naar de wisselmachine.

Dit voorbeeld illustreert de invoerclassificatie en -markering. Het voorbeeld toont hoe een intern CoS aan elk kader toe te wijzen:



Opmerking: Zoals in dit voorbeeld wordt aangegeven, wordt aan elk frame een interne CoS toegewezen. De toewijzing is gebaseerd op de ontvangen CoS of de standaardpoort CoS. De interne CoS omvat niet-gelabelde frames die geen echte CoS dragen. De interne CoS wordt geschreven in een speciale pakketheader, die een gegevensbuskopader wordt genoemd, en verzonden over de gegevensbus naar de switchingmachine.

Switching Engine (PFC)

Wanneer de kop de wisselmachine bereikt, kent de wisselmachine Enhanced Address Recognition Logic (EARL) elk frame en interne DSCP toe. Deze interne DSCP is een interne prioriteit die aan het kader door PFC wordt toegewezen aangezien het kader de switch overbrengt. Dit is niet de DSCP in de IP versie 4 (IPv4) header. De interne DSCP is afgeleid van een bestaande CoS of ToS-instelling en wordt gebruikt om de CoS of ToS te resetten terwijl het frame de switch verlaat. Deze interne DSCP wordt toegewezen aan alle frames die door de PFC zijn geschakeld of routeerd, zelfs niet-IP frames.

In deze sectie wordt besproken hoe u een servicebeleid aan de interface kunt toewijzen om een markering te maken. In dit gedeelte wordt ook de laatste instelling van de interne DSCP besproken, die afhankelijk is van de haventrust state en het toegepaste servicepakket.

Configureer het servicebeleid om een pakket in Cisco IOS-softwarerelease 12.1(12c)E te classificeren of te markeren

Volg deze stappen om het servicebeleid te configureren:

1. Configureer een toegangscontrolelijst (ACL) om het verkeer te definiëren dat u wilt overwegen.ACL kan worden genummerd of genoemd en Catalyst 6500/6000 ondersteunt een uitgebreide ACL. Geef de opdracht **toegangslijst *xxx* Cisco IOS-software uit**, zoals dit voorbeeld laat zien:
   ```
   (config)#access-list 101 permit ip any host 10.1.1.1
   ```

2. Configureer een verkeersklasse (klassenkaart) om het verkeer aan te passen op basis van de ACL die u hebt gedefinieerd of op basis van de ontvangen DSCP.Geef de opdracht **class-map** Cisco IOS-software uit. PFC QoS ondersteunt niet meer dan één overeenkomende verklaring per class map. Bovendien ondersteunt PFC QoS alleen deze matchverklaringen:**match-ip access groupzie ip-puntzie ip-voorrangmatchprotocolOpmerking:** de opdracht **matchprotocol** maakt het gebruik van Network-Based Application Recognition (NBAR) mogelijk om het verkeer te koppelen.**Opmerking:** Van deze opties **worden** alleen verklaringen die een **gelijke** voorrang hebben op de **IP-NDSCP** en de **IP-prioriteitsverklaringen** ondersteund en gewerkt. Deze verklaringen zijn echter niet bruikbaar voor het merken of classificeren van de pakketten. U kunt deze verklaringen bijvoorbeeld gebruiken om toezicht te houden op alle pakketten die overeenkomen met een bepaalde DSCP. Deze actie valt echter buiten het toepassingsgebied van dit document.
   ```
   (config)#class-map class-name
   (config-cmap)#match {access-group | input-interface | ip dscp}
   ```
   Opmerking: Dit voorbeeld toont slechts drie opties voor de opdracht **match**. Maar u kunt veel meer opties instellen op deze opdrachtmelding.**N.B.:** Een van de opties in deze **overeenkomende** opdracht is gekozen voor matchcriteria en de andere opties zijn niet beschikbaar, afhankelijk van de inkomende pakketten.Hierna volgt een voorbeeld:

   ```
   class-map match-any TEST
    match access-group 101

   class-map match-all TEST2
    match ip precedence 6
   ```

3. Configureer een beleidskaart om een beleid toe te passen op een klasse die u eerder hebt gedefinieerd.Het beleidsplan bevat:Een naamEen reeks class statementsVoor elke klasseverklaring, de actie die voor die klasse moet worden ondernomenDe ondersteunde acties in PFC1 en PFC2 QoS zijn:**trust dscptrust ip - voorrangtrust cosip dscp** instellen in Cisco IOS-softwarerelease 12.1(12c)E1 en hoger**ip-voorrang** in Cisco IOS-softwarerelease 12.1(12c)E1 en hoger**politieOpmerking:** Deze actie valt buiten het toepassingsgebied van dit document.
   ```
   (config)#policy-map policy-name
   (config-pmap)#class class-name
   (config-pmap-c)#{police | set ip dscp}
   ```

   Opmerking: Dit voorbeeld toont slechts twee opties, maar u kunt veel meer opties bij deze `(configuratie-kaart-c)#` opdrachtprompt configureren.Hierna volgt een voorbeeld:

   ```
   policy-map test_policy
    class TEST
      trust ip precedence
    class TEST2
      set ip dscp 16
   ```

4. Configuratie van een input van het de dienstbeleid om een beleidslijn toe te passen die u

eerder aan één of meer interface definieerde.**N.B.:** U kunt een servicebeleid toevoegen aan de fysieke interface of aan de switched virtuele interface (SVI) of VLAN-interface. Als u een servicebeleid aan een VLAN-interface toevoegt, zijn de enige poorten die dit servicebeleid gebruiken poorten die aan dat VLAN behoren en zijn geconfigureerd voor VLAN-gebaseerde QoS. Als de poort niet is ingesteld voor VLAN-gebaseerde QoS, gebruikt de poort nog steeds de standaard poort-gebaseerde QoS en kijkt alleen naar het servicebeleid dat aan de fysieke interface is gekoppeld.Dit voorbeeld past het de `test_policy` op de haven Gigabit Ethernet 1/1 toe:

```
(config) interface gigabitethernet 1/1
(config-if)#service-policy input test_policy
```

Dit voorbeeld past het de `test_policy` op alle poorten in VLAN 10 toe die een VLAN-gebaseerde configuratie uit het QoS-standpunt hebben:

```
(config) interface gigabitethernet 1/2
(config-if)#switchport mode access
(config-if)#switchport access vlan 10
(config-if)#mls qos vlan-based
(config-if)#exit
(config-if)#interface vlan 10
(config-if)#service-policy input test_policy
```

Opmerking: U kunt Stap 2 en Stap 3 van deze procedure combineren als u de specifieke definitie van de klasse overslaat en de ACL direct in de definitie van de beleidskaart plaatst. In dit voorbeeld, waar de klasse `TEST politie` niet is gedefinieerd voorafgaand aan de configuratie van de beleidskaart, wordt de klasse gedefinieerd in de beleidskaart:

```
(config)#policy-map policy-name
(config-pmap)#class class_name {access-group acl_index_or_name | dscp dscp_1 [dscp_2
[dscp_N]] | precedence ipp_1 [ipp_2 [ipp_N]]}
!--- Note: This command should be on one line.

policy-map TEST
class TEST police access-group 101
```

Configureer het servicebeleid om een pakket in Cisco IOS-softwarereleases eerder te classificeren of te markeren dan Cisco IOS-softwarerelease 12.1(12c)E

In Cisco IOS-softwarerelease eerder dan Cisco IOS-softwarerelease 12.1(12c)E1, kunt u de **ingestelde IP-**DSCP niet gebruiken of **IP-**prioriteitsactie in een beleidskaart **instellen**. Om deze reden is de enige manier om een markering van specifiek verkeer te maken die een klasse definieert een politieman met een zeer hoog tempo aan te passen. Dit percentage moet bijvoorbeeld ten minste gelijk zijn aan het lijntarief van de haven of iets wat hoog genoeg is om al het verkeer dat politieagent treft, te laten passeren. Gebruik vervolgens **set-dscp-ongeveer *xx* als** de conforme actie. Volg deze stappen om deze configuratie in te stellen:

1. Configureer een ACL om het verkeer te definiëren dat u wilt overwegen.ACL kan worden genummerd of genoemd en Catalyst 6500/6000 ondersteunt een uitgebreide ACL. Geef de opdracht **toegangslijst *xxx* Cisco IOS-software uit**, zoals dit voorbeeld laat zien:

   ```
   (config)#access-list 101 permit ip any host 10.1.1.1
   ```

2. Configureer een verkeersklasse (class map) om het verkeer aan te passen op basis van de ACL die u hebt gedefinieerd of op basis van de ontvangen DSCP.Geef de opdracht **class-**

map Cisco IOS-software uit. PFC QoS ondersteunt niet meer dan één overeenkomende verklaring per class map. Bovendien ondersteunt PFC QoS alleen deze matchverklaringen:**match-ip access groupzie ip-puntzie ip-voorrangmatchprotocolOpmerking:** De opdracht **matchprotocol** maakt het gebruik van NBAR mogelijk om verkeer aan te passen.**Opmerking:** Van deze verklaringen worden alleen de **overeenkomende ip-npp** en **IP-voorrang** verklaringen ondersteund en gewerkt. Deze verklaringen zijn echter niet nuttig voor het merken of classificeren van de pakketten. U kunt deze verklaringen bijvoorbeeld gebruiken om toezicht te houden op alle pakketten die overeenkomen met een bepaalde DSCP. Deze actie valt echter buiten het toepassingsgebied van dit document.

```
(config)#class-map  class-name
(config-cmap)#match {access-group | input-interface | ip dscp}
```

Opmerking: Dit voorbeeld toont slechts drie opties voor de opdracht **match**. Maar u kunt veel meer opties instellen op deze opdrachtmelding.Hierna volgt een voorbeeld:

```
class-map match-any TEST
 match access-group 101

class-map match-all TEST2
 match ip precedence 6
```

3. Configureer een beleidskaart om een beleid toe te passen op een klasse die u eerder hebt gedefinieerd.Het beleidsplan bevat:Een naamEen reeks class statementsVoor elke klasseverklaring, de actie die voor die klasse moet worden ondernomenDe ondersteunde acties in PFC1 of PFC2 QoS zijn:**trust dscptrust ip - voorrangtrust cospolitie**Je moet de **politie** statement gebruiken omdat de **ingestelde ip dscp** en de **ip voorrang** acties niet ondersteunen. Omdat je het verkeer niet echt wil controleren, maar gewoon om het te markeren, gebruik je een politieagent die gedefinieerd is om al het verkeer mogelijk te maken. Daarom moet u de politieagent met een grote snelheid configureren en barsten. U kunt bijvoorbeeld de politieagent met de maximaal toegestane snelheid configureren en barsten. Hierna volgt een voorbeeld:

```
policy-map test_policy
 class TEST
   trust ip precedence
 class TEST2
   police  4000000000 31250000 conform-action
   set-dscp-transmit 16 exceed-action policed-dscp-transmit
```

4. Configuratie van een input van het de dienstbeleid om een beleidslijn toe te passen die u eerder aan één of meer interfaces definieerde.**Opmerking:** het servicebeleid kan worden aangesloten op een fysieke interface of op de SVI- of VLAN-interface. Als een servicebeleid aan een interface van VLAN is gekoppeld, gebruiken alleen poorten die aan dat VLAN behoren en die zijn geconfigureerd voor VLAN-gebaseerde QoS dit servicebeleid. Als de poort niet is ingesteld voor VLAN-gebaseerde QoS, gebruikt de poort nog steeds de standaard poort-gebaseerde QoS en kijkt alleen naar een servicebeleid dat aan de fysieke interface is gekoppeld.Dit voorbeeld past het de `test_policy` op de haven Gigabit Ethernet 1/1 toe:

```
(config) interface gigabitethernet 1/1
(config-if)#service-policy input test_policy
```

Dit voorbeeld past het de `test_policy` op alle poorten in VLAN 10 toe die een VLAN-

gebaseerde configuratie uit het QoS-standpunt hebben:

```
(config) interface gigabitethernet 1/2
(config-if)#switchport mode access
(config-if)#switchport access vlan 10
(config-if)#mls qos vlan-based
(config-if)#exit
(config-if)#interface vlan 10
(config-if)#service-policy input test_policy
```

Vier mogelijke bronnen voor interne DSCP

De interne DSCP is afgeleid van een van de volgende factoren:

1. Een bestaande ontvangen DSCP-waarde die is ingesteld voordat het kader de switch ingaatEen voorbeeld is **trust dscp**.
2. De ontvangen IP-prioriteitsbits die al in de IPv4-header zijn ingesteldOmdat er 64 DSCP-waarden zijn en slechts acht IP-prioriteitswaarden, vormt de beheerder een afbeelding die de switch gebruikt om de DSCP af te leiden. Er zijn standaardinstellingen, voor het geval dat de beheerder de kaarten niet aanpast. Een voorbeeld is het **vertrouwen van ip voorrang**.
3. De ontvangen CoS bits die al zijn ingesteld voordat het frame de switch ingaat en die zijn opgeslagen in de gegevensbuskop, of als er geen CoS in het inkomende frame was, vanaf de standaard CoS van de inkomende poortZoals bij IP-voorrang, zijn er maximaal acht CoS-waarden, die elk aan een van de 64 DSCP-waarden moeten worden gekoppeld. De beheerder kan deze kaart vormen, of de switch kan de standaardkaart gebruiken die reeds op zijn plaats is.
4. Het servicebeleid kan de interne DSCP op een specifieke waarde instellen.

Voor de nummers 2 en 3 in deze lijst is de statische afbeelding standaard op deze manier:

- Voor CoS-to-DSCP mapping is de DSCP die is afgeleid gelijk aan acht keer de CoS.
- Voor IP voorrang-aan-DSCP-afbeelding is de DSCP die is afgeleid gelijk aan acht keer de IP-voorrang.

U kunt deze opdrachten uitgeven om deze statische mapping te omzeilen en te verifiëren:

- **mls qos map ip-prec-dscp** *dscp_1 dscp_2 dscp_3 dscp_4 dscp_5 dscp_6 dscp_7 dscp_8*
- **mls qos map cos-dscp** *dscp_1 dscp_2 dscp_3 dscp_4 dscp_5 dscp_6 dscp_7 dscp_8*

De eerste waarde van de DSCP die overeenkomt met de mapping voor de CoS (of IP-voorrang) is 0. De tweede waarde voor de CoS (of IP-voorrang) is 1, en het patroon gaat op deze manier verder. Bijvoorbeeld, deze opdracht verandert de mapping zodat de CoS 0 in kaart wordt gebracht op de DSCP van 0, en de CoS van 1 in kaart wordt gebracht aan de DSCP van 8, enzovoort:

```
Cat65(config)#mls qos map cos-dscp 0 8 16 26 32 46 48 54
Cat65#show mls qos maps
CoS-dscp map:
 cos:     0 1  2   3   4   5   6   7
  ---------------------------------
 dscp:    0 8 16  26  32  46  48  54
```

Hoe wordt de interne DSCP geselecteerd?

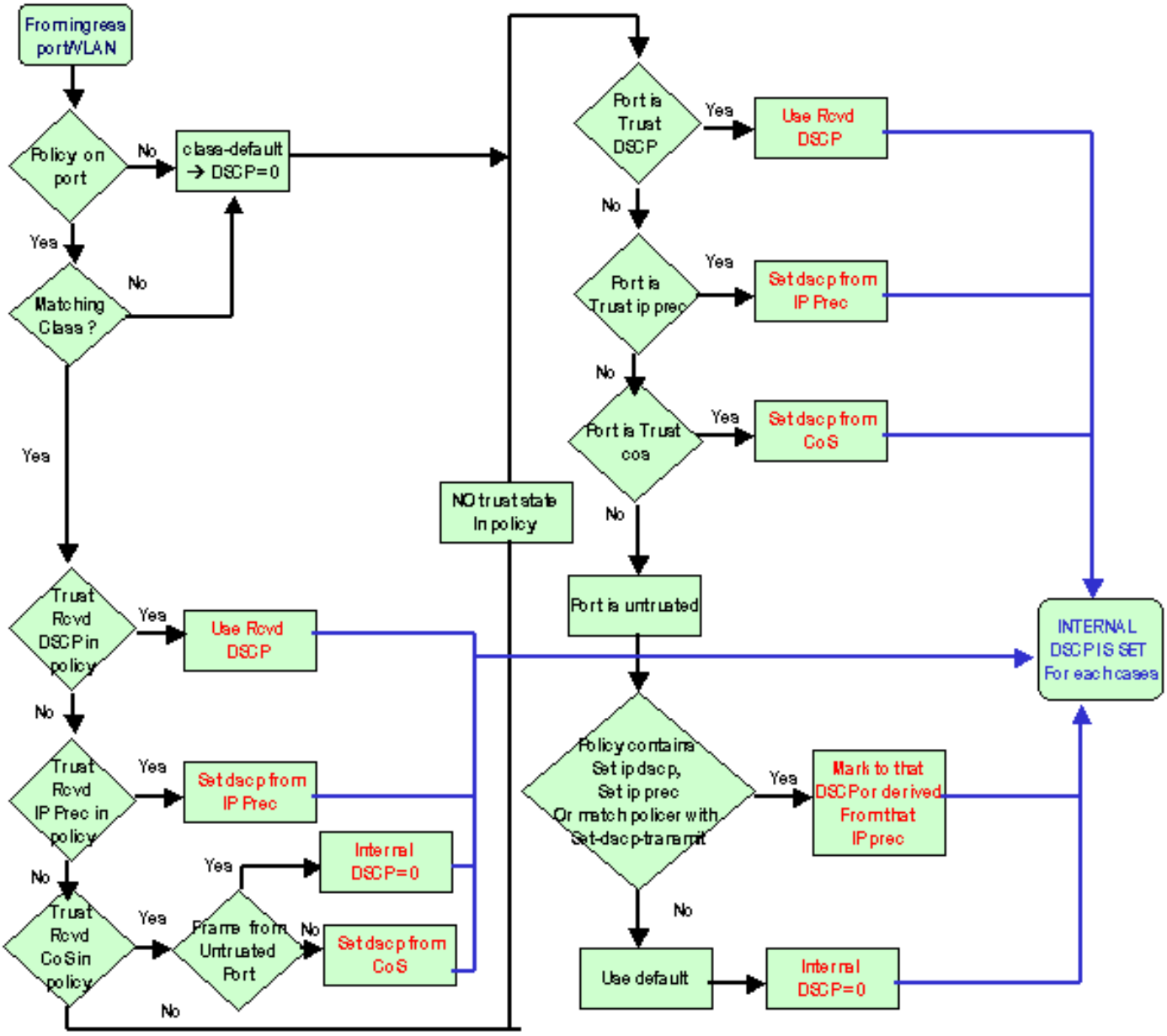
De interne DSCP wordt op basis van deze parameters geselecteerd:

- De QoS-beleidskaart die op het pakket wordt toegepastDe QoS-beleidskaart wordt door deze regels bepaald:Als er geen servicebeleid is aangesloten op de inkomende poort of VLAN, gebruikt u de standaardinstelling.**Opmerking:** deze standaardinstelling is om de interne DSCP op 0 in te stellen.Als een servicebeleid is gekoppeld aan de inkomende poort of VLAN en als het verkeer overeenkomt met een van de klassen die het beleid definieert, gebruikt u deze optie.Als een servicebeleid is gekoppeld aan de inkomende poort of VLAN en als het verkeer niet overeenkomt met een van de klassen die het beleid definieert, gebruikt u de standaardinstelling.
- De `vertrouwensstaat` van de haven en de actie van de beleidslijnWanneer de haven een specifieke `vertrouwensstaat` heeft en een beleid met een bepaalde markering (tegelijkertijd vertrouwende actie), zijn deze regels van toepassing:De **ingestelde ip dscp** of de DSCP die per politieagent in een beleidsplan wordt gedefinieerd worden slechts toegepast als de haven in de `onvertrouwde` staat wordt verlaten.Als de haven een `vertrouwensstaat` heeft, wordt deze staat van het vertrouwen gebruikt om de interne DSCP af te leiden. De status van het `havenvertrouwen` heeft altijd voorrang op de **ingestelde ip dscp-**opdracht.De opdracht **trust *xx* in een beleidskaart heeft voorrang op de** `haventrust` staat.Als de haven en het beleid een andere `vertrouwensstaat` bevatten, wordt de `vertrouwensstaat` die uit de beleidsplanning voortkomt in overweging genomen.

Daarom is de interne DSCP afhankelijk van deze factoren:

- De staat `van het` havenvertrouwen
- Het servicebeleid (met gebruik van ACL) dat aan de poort is toegevoegd
- De standaardbeleidsplanning**Opmerking:** de standaardinstelling is dat de DSCP wordt teruggebracht naar 0.
- Op VLAN gebaseerde of op poort gebaseerd met betrekking tot ACL

In dit schema wordt samengevat hoe de interne DSCP op basis van de configuratie wordt geselecteerd:



De PFC kan ook toezicht houden. Dit kan uiteindelijk resulteren in een markering van de interne DSCP. Raadpleeg voor meer informatie over toezicht QoS-toezicht op Catalyst 6500/6000 Series Switches.

Uitvoer-poortverwerking

U kunt niets doen op het niveau van de uitgang om de classificatie te veranderen. Op basis van deze regels wordt echter op de verpakking het volgende aangebracht:

- Als het pakket een IPv4-pakket is, kopieert u de interne DSCP die de switchmachine in de ToS-byte van de IPv4-header heeft toegewezen.
- Als de uitvoerpoort is geconfigureerd voor een ISL- of dot1q-insluiting, gebruikt u een CoS dat afkomstig is van de interne DSCP. Kopieer de CoS in het ISL of punt1q frame.

Opmerking: de CoS is op basis van een statische schatting afgeleid van de interne DSCP. Geef deze opdracht uit om het statische beeld te configureren:

```
Router(config)#mls qos map dscp-cos dscp1 [dscp2 [dscp3 [dscp4 [dscp5 [dscp6 [dscp7
```

```
[dscp8]]]]]]] to cos_value
!--- Note: This command should be on one line.
```

De standaardinstellingen worden hier weergegeven. Standaard is de CoS het integerdeel van de DSCP, gedeeld door acht. Geef deze opdracht uit om de afbeelding te zien en te controleren:

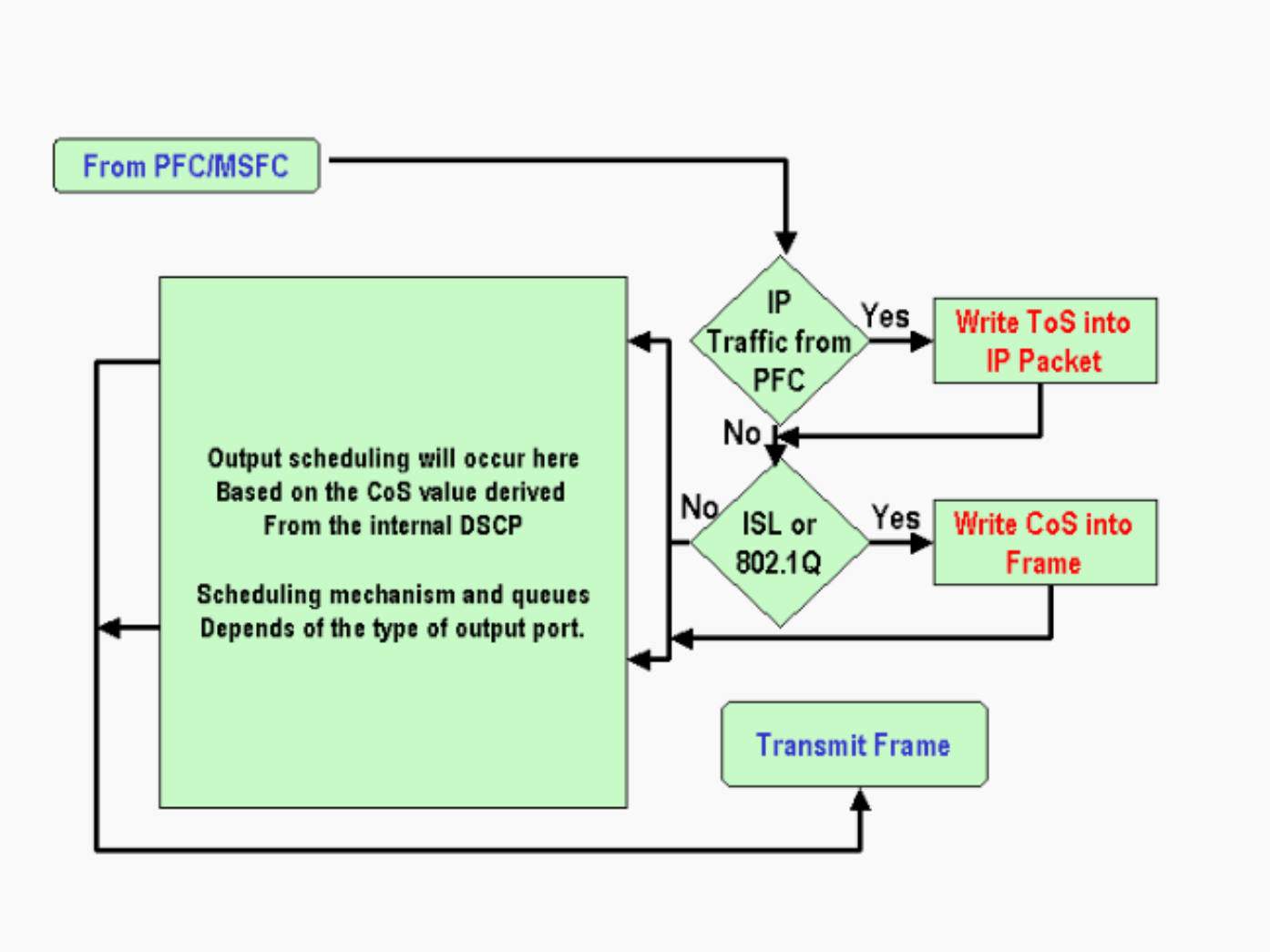
```
cat6k#show mls qos maps
...
  Dscp-cos map:                                     (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ------------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 02 02 02 02
      2 :    02 02 02 02 03 03 03 03 03 03
      3 :    03 03 04 04 04 04 04 04 04 04
      4 :    05 05 05 05 05 05 05 05 06 06
      5 :    06 06 06 06 06 06 07 07 07 07
      6 :    07 07 07 07
```

Geef deze configuratieopdracht in de normale configuratie-modus uit om deze afbeelding te wijzigen:

```
mls qos map dscp-cos 0 1 2 3 4 5 6 7 to 0
mls qos map dscp-cos 8 9 10 11 12 13 14 15 to 1
mls qos map dscp-cos 16 17 18 19 20 21 22 23 to 2
...
```

Nadat de DSCP in de IP-header is geschreven en de CoS afkomstig is van de DSCP, wordt het pakket verzonden naar een van de uitvoerwachtrijen voor uitvoerschema's op basis van de CoS. Dit gebeurt zelfs als het pakket geen punt1q of een ISL is. Voor meer informatie over het plannen van de uitvoerwachtrij kunt u QoS-uitvoerplanning raadplegen bij Catalyst 6500/6000 Series Switches die Cisco IOS-systeemsoftware uitvoeren.

In dit schema wordt een samenvatting gegeven van de verwerking van het pakket met betrekking tot het markeren in de uitvoerpoort:



Opmerkingen en beperkingen

De standaard ACL

Standaard ACL gebruikt "dscp 0" als classificatie-trefwoord. Al verkeer dat de switch door een onvertrouwde poort ingaat en geen ingang van het de dienstbeleid aanslaat wordt met een DSCP van 0 gemarkeerd als QoS wordt toegelaten. Op dit moment kunt u de standaard ACL niet wijzigen in Cisco IOS-software.

Opmerking: In Catalyst OS-software (CatOS) kunt u dit standaardgedrag configureren en wijzigen. Raadpleeg voor meer informatie het gedeelte *Standaard ACL*-Switches van QoS-classificatie en markering op Catalyst 6500/6000 Series die CatOS-software uitvoeren.

Beperkingen van de WS-X61x, WS-X6248-xx, WS-X624-xx en WS-X6348-xx lijnkaarten

Deze paragraaf heeft alleen betrekking op deze lijnkaarten:

- WS-X6224-100FX-MT: Catalyst 6000 24-poorts 100 FX multi-mode switch
- WS-X6248-RJ-45: Catalyst 6000 48-poorts 10/100 RJ-45 module
- WS-X6248-TEL: Catalyst 6000 48-poorts 10/100 telecommodule
- WS-X6248A-RJ-45: Catalyst 6000 48-poorts 10/100, uitgebreide QoS-module

- WS-X6248A-TEL: Catalyst 6000 48-poorts 10/100, uitgebreide QoS-module
- WS-X6324-100FX-M: Catalyst 6000 24-poorts 100 FX, uitgebreide QoS, MT
- WS-X6324-100FX-SM: Catalyst 6000 24-poorts 100 FX, uitgebreide QoS, MT
- WS-X6348-RJ-45: Catalyst 6000 48-poorts 10/100, uitgebreide QoS-module
- WS-X6348-RJ21V: Catalyst 6000 48-poorts 10/100, inline voeding
- WS-X6348-RJ45V: Catalyst 6000 48-poorts 10/100, uitgebreide QoS, inline voeding
- WS-X6148-RJ21V: Catalyst 6500 48-poorts 10/100 inline voeding
- WS-X6148-RJ45V: Catalyst 6500 48-poorts 10/100 inline voeding

Deze lijnkaarten hebben een beperking. Op poortniveau kunt u de `vertrouwde` status niet configureren met behulp van een van deze trefwoorden:

- `trust-dscp`
- `trust-ipprec`
- `vertrouwenskosten`

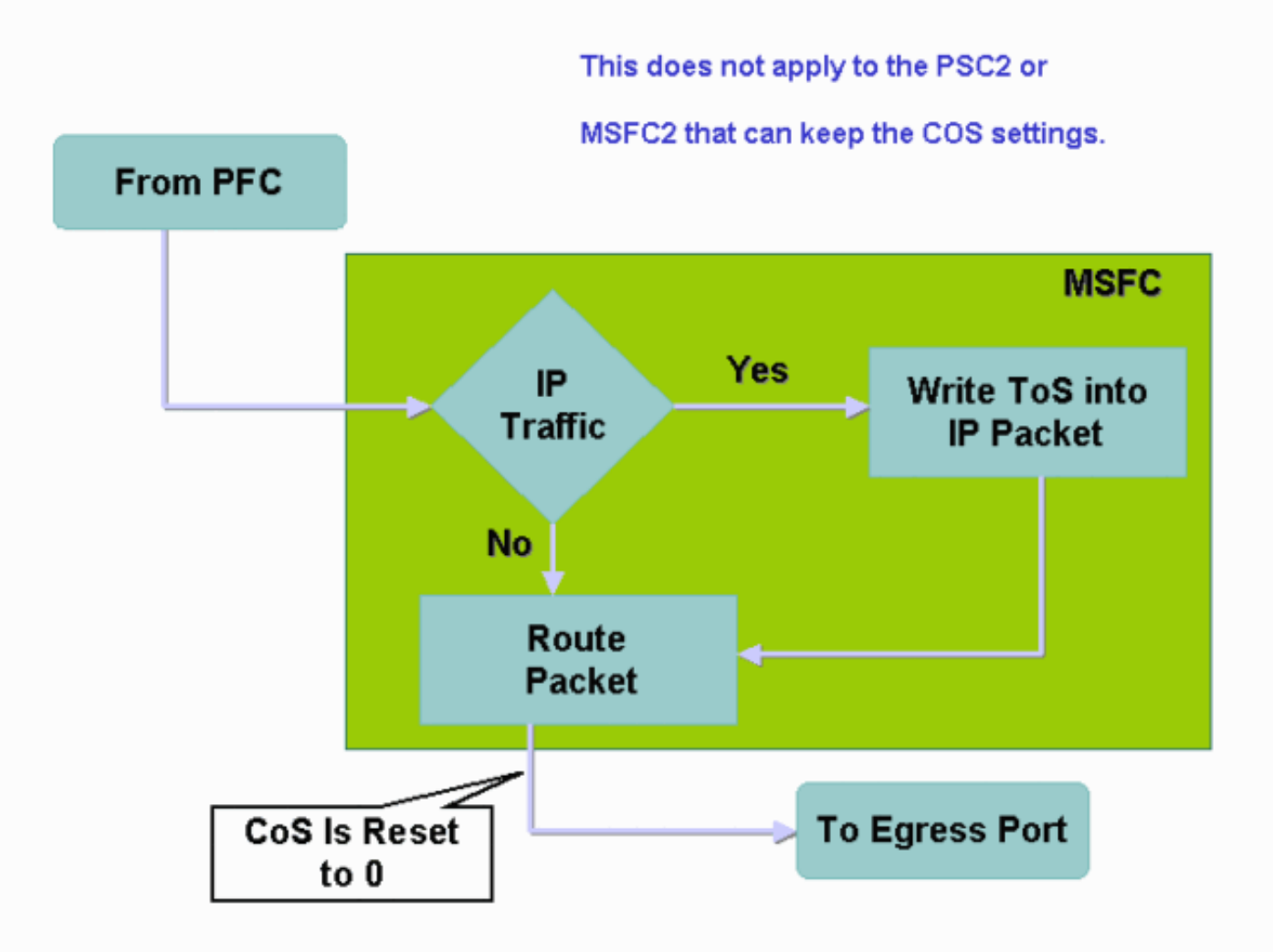
U kunt alleen de `onvertrouwde` staat gebruiken. Elke poging om een `vertrouwensstaat` op een van deze poorten te configureren geeft een van deze waarschuwingsberichten weer:

```
Tank(config-if)#mls qos trust ?
  extend  extend keyword
Tank(config-if)#mls qos trust
% Incomplete command.
Tank(config-if)#mls qos trust cos
                              ^
% Invalid input detected at '^' marker.
Tank(config-if)#mls qos trust ip-pre
                              ^
% Invalid input detected at '^' marker.
```

U moet een servicebeleid aan de poort of het VLAN toevoegen als u een betrouwbaar frame op zo'n lijnkaart wilt insluiten. Gebruik de methode in het geval 1: Markeren in het gedeelte Edge van dit document.

Packet die van MSFC1 of MSFC2 op Supervisor Engine 1A/PFC komen

Alle pakketten die afkomstig zijn van de MSFC1 of MSFC2 hebben een CoS van 0. Het pakket kan een software-routepakket zijn of een pakket dat door de MSFC wordt problemen. Dit is een beperking van de PFC omdat het de CoS van alle pakketten die van MSFC komen terug heeft. De DSCP- en IP-voorrang blijven behouden. De PFC2 heeft deze beperking niet. De bestaande CoS van PFC2 is gelijk aan de IP voorrang van het pakket.



Samenvatting van de classificatie

De tabellen in deze sectie tonen de DSCP die op basis van deze classificaties resulteert:

- De inkomende vertrouwensstaat
- Het indelingswoord binnen de toegepaste ACL

Deze tabel biedt een generieke samenvatting voor alle poorten behalve WS-X62xx en WS-X63xx:

Toetsenwoord voor beleidsschema Poortvertrouwensstaat	set-ip-dscp xx of set-dscp-send xx	trust-dscp	trust-ipprec	vertrouwenskosten
onbetrouwbaar	xx[1]	RX[2] DSCP	Afgeleid van RX ipprec	0
trust-dscp	RX DSCP	RX DSCP	Afgeleid van RX ipprec	afgeleid van RX CoS of Port CoS
trust-ipprec	Afgeleid van RX	RX DSCP	Afgeleid van	afgeleid van RX CoS of

	ipprec		RX ipprec	Port CoS
vertrouwenskosten	afgeleid van RX CoS of Port CoS	RX DSCP	Afgeleid van RX ipprec	afgeleid van RX CoS of Port CoS

[1] Dit is de enige manier om een nieuwe markering van een kader te maken.

[2] RX = ontvangen

Deze tabel biedt een samenvatting voor de WS-X61x-, WS-X62xx- en WS-X63x-poorten:

Toetsenwoord voor beleidsschema **Poortvertrouwensstaat**	**set-ip-dscp xx of set-dscp-send xx**	**trust-dscp**	**trust-ipprec**	**vertrouwenskosten**
onbetrouwbaar	xx	RX DSCP	Afgeleid van RX ipprec	0
trust-dscp	Niet ondersteund	Niet ondersteund	Niet ondersteund	Niet ondersteund
trust-ipprec	Niet ondersteund	Niet ondersteund	Niet ondersteund	Niet ondersteund
vertrouwenskosten	Niet ondersteund	Niet ondersteund	Niet ondersteund	Niet ondersteund

Configuratie bewaken en controleren

Controleer de poortconfiguratie

Geef de **opdracht** van de **show een interface** ***interface-id*** **uit** om de poortinstellingen en -configuraties te controleren.

Wanneer u deze opdracht geeft, kunt u deze classificatieparameters, naast andere parameters, controleren:

- Of op basis van poort of VLAN
- Het type trust poort
- ACL die aan de poort is bevestigd

Hier is een voorbeeld van deze opdrachtoutput. De belangrijke gebieden met betrekking tot de indeling zijn op vet weergegeven:

```
6500#show queuing interface gigabitethernet 3/2
Interface GigabitEthernet3/2 queuing strategy:  Weighted Round-Robin
  Port QoS is enabled
  Trust state: trust COS
  Default COS is 0
  Transmit queues [type = 1p2q2t]:
```

De output toont dat de configuratie van deze specifieke haven met `vertrouwenskosten` op havenniveau is. Bovendien is de standaardpoort CoS 0.

Gedefinieerde klassen controleren

Geef de opdracht **showclass-map uit** om de gedefinieerde klassen te controleren. Hierna volgt een voorbeeld:

```
Boris#show class-map
 Class Map match-all test (id 3)
   Match access-group  112

 Class Map match-any class-default (id 0)
   Match any
 Class Map match-all voice (id 4)
```

Controleer de beleidskaart die op een interface wordt toegepast

Geef deze opdrachten uit om de beleidskaart te controleren die in eerdere opdrachten wordt toegepast en weergegeven:

- **MLS qos ip interface-*id* tonen**
- **Beleids-kaart interface-*id* tonen**

Hier zijn voorbeelden van de uitvoer van deze opdrachten:

```
Boris#show mls qos ip gigabitethernet 1/1
   [In] Default.   [Out] Default.
 QoS Summary [IP]:      (* - shared aggregates, Mod - switch module)

 Int  Mod Dir  Class-map  DSCP AgId Trust FlId AgForward-Pk AgPoliced-k
 ---------------------------------------------------------------------
 Gi1/1 1  In   TEST       0    0*   No    0    1242120099             0
```

Opmerking: U kunt deze velden met betrekking tot classificatie bekijken:

- `Class-map`—Hiermee vertelt u welke klasse is gekoppeld aan het servicepakket dat aan deze interface is toegevoegd.
- `Vertrouwen` - vertelt je of de politie actie in die klas een vertrouwensopdracht bevat en wat in de klas vertrouwd is.
- `DSCP` - Vermeldt u de DSCP die voor de pakketten wordt verzonden die die klasse raken.

```
Tank#show policy-map interface fastethernet 4/4

 FastEthernet4/4

  service-policy input: TEST_aggre2
```

```
    class-map: Test_marking (match-all)
      27315332 packets
      5 minute offered rate 25726 pps
      match: access-group 101
      police :
        10000000 bps 10000 limit 10000 extended limit
        aggregate-forwarded 20155529 packets action: transmit
        exceeded 7159803 packets action: drop
        aggregate-forward 19498 pps exceed 6926 pps
```

Steekproef-casestudy's

Deze sectie verschaft voorbeeldconfiguraties van normale gevallen die in een netwerk kunnen verschijnen.

Zaak 1: Markeren aan de rand

Stel dat u een Catalyst 6000 configureren dat gebruikt wordt als switch voor toegang. Veel gebruikers verbinden met sleuven 2 van de switch, een WS-X6348 lijnkaart (10/100 Mbps). De gebruikers kunnen verzenden:

- Normaal gegevensverkeer-Dit verkeer is altijd in VLAN 100 en moet een DSCP van 0 krijgen.
- Spraakverkeer vanaf een IP-telefoon: dit verkeer bevindt zich altijd in de spraakassistent VLAN 101 en moet een DSCP van 46 krijgen.
- Mission-Critical Application Traffic-This traffic-is ook in VLAN 100 en is gericht op server 10.10.10.20. Dit verkeer moet een DSCP van 32 hebben.

De toepassing markeert geen van dit verkeer. Laat de poort daarom als `onbetrouwbaar` achter en stel een specifieke ACL in om het verkeer te classificeren. Eén ACL wordt toegepast op VLAN 100, en één ACL wordt toegepast op VLAN 101. U moet ook alle poorten configureren als VLAN-gebaseerd. Hier is een voorbeeld van de configuratie die het resultaat is:

```
Boris(config)#mls qos
Boris(config)#interface range fastethernet 2/1-48
Boris(config-if)#mls qos vlan-based
Boris(config-if)#exit
Boris(config)#ip access-list extended Mission_critical
Boris(config-ext-nacl)#permit ip any host 10.10.10.20
Boris(config)#ip access-list extended Voice_traffic
Boris(config-ext-nacl)#permit ip any any
Boris(config)#class-map voice

Boris(config-cmap)#match access-group Voice_traffic
Boris(config)#class-map Critical

Boris(config-cmap)#match access-group Mission_critical
Boris(config)#policy-map Voice_vlan
Boris(config-pmap)#class voice
Boris(config-pmap-c)#set ip dscp 46
Boris(config)#policy-map Data_vlan
Boris(config-pmap)#class Critical
Boris(config-pmap-c)#set ip dscp 32
Boris(config)#interface vlan 100
Boris(config-if)#service-policy input Data_vlan
Boris(config)#interface vlan 101
Boris(config-if)#service-policy input Voice_vlan
```

Zaak 2: Betrokken in de Core met Alleen Gigabit Ethernet-interfaces

Stel dat u een kern Catalyst 6000 met slechts een Gigabit Ethernet-interface in sleuf 1 en sleuf 2 vormt. De switches van de toegang markeerden eerder correct verkeer. U hoeft daarom geen opmerkingen te maken. U dient er echter voor te zorgen dat de switch van de kern de inkomende DSCP vertrouwt. Dit geval is gemakkelijker omdat alle havens zijn aangeduid als `trust-dscp`, wat voldoende zou moeten zijn:

```
6k(config)#mls qos
6k(config)#interface range gigabitethernet 1/1-2 , gigabitethernet 2/1-2
6k(config-if)#mls qos trust dscp
```

Gerelateerde informatie

- Inzicht op Quality-of-Service op Catalyst 6000 Series Switches
- QoS-classificatie en markering op Catalyst 6500/6000 Series Switches die CatOS-software uitvoeren
- LAN-productondersteuning
- Ondersteuning voor LAN-switching technologie
- Technische ondersteuning en documentatie – Cisco Systems