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

Inhoud

Inleiding

Dit document onderzoekt wat er gebeurt met betrekking tot de markering en classificatie van een pakje op verschillende plaatsen tijdens de reis binnen het Catalyst 6000 chassis. Het vermeldt speciale gevallen, beperkingen en geeft korte casestudies.

Dit document is niet bedoeld als een limitatieve lijst van alle opdrachten van Catalyst OS (CatOS) met betrekking tot Quality of Service (QoS) of markering. Raadpleeg voor meer informatie over de

CatOS-opdrachtregel-interface (CLI) het volgende document:

- QoS configureren

N.B.: Dit document heeft alleen betrekking op IP-verkeer.

Voordat u begint

Conventies

Zie de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Voorwaarden

Er zijn geen specifieke voorwaarden van toepassing op dit document.

Gebruikte componenten

Dit document is geldig voor Catalyst 6000 Series switches die CatOS-software gebruiken en een van de volgende Supervisor Engine gebruiken:

- SUP1A + PFC
- SUP1A + PFC + MSFC
- SUP1A + PFC + MSFC2
- SUP2 + PFC2
- SUP2 + PFC2 + MSFC2

Alle voorbeeldopdrachten zijn echter op Catalyst 6506 met SUP1A/PFC-software versie 6.3 getest.

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als u in een levend netwerk werkt, zorg er dan voor dat u de potentiële impact van om het even welke opdracht begrijpt alvorens het te gebruiken.

Terminologie

Hieronder volgt een lijst van terminologie die in dit document wordt gebruikt:

- Gedifferentieerd servicescodepunt (DSCP): De eerste zes bits van het Type of Service (ToS)-byte in de IP-header. DSCP is alleen aanwezig in het IP-pakket.**N.B.:** U kent ook een interne DSCP toe aan elk pakket (IP of niet IP). Deze interne DSCP-toewijzing wordt later in dit document gedetailleerd weergegeven.
- 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 op Layer 2 (L2) te markeren. Het bestaat uit een van de volgende drie bits:De drie dot1p bits in de stip1q tag voor het IEEE dot1q-pakket.De drie bits genaamd "User Field" in de Inter-Switch Link (ISL) header voor een ingesloten ISL-pakket.Er is geen CoS aanwezig in een niet-punt1q of een ISL pakket.
- Indeling: Het proces voor het selecteren van het te markeren verkeer.

- Markeren: Het proces voor het instellen van een Layer 3 (L3) DSCP-waarde in een pakket. In dit document wordt de definitie van markering uitgebreid tot het instellen van L2 CoS-waarden.

Catalyst 6000-switches kunnen classificaties maken op basis van de volgende drie parameters:

- DSCP
- IP-voorrang
- CoS

De Catalyst 6000 switches maken classificatie en markering op verschillende plaatsen. Hier volgt een overzicht van wat er op deze verschillende plekken gebeurt:

- Invoerpoort (ingress Application-Specific Integrated Circuit (ASIC))
- Switching Engine (beleidsfunctiekaart (PFC)
- Uitvoer (stress-ASIC)

QoS inschakelen

Standaard is QoS uitgeschakeld aan Catalyst 6000 switches. QoS kan worden geactiveerd door het CatOS opdracht **set qos** uit te geven.

Wanneer QoS is uitgeschakeld, heeft de switch geen classificatie of markering uitgevoerd. Als zodanig verlaat elk pakje de switch met de DSCP/IP-voorrang die deze had toen u de switch invoerde.

Invoerpoortbehandeling

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

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

De rest van deze sectie beschrijft hoe de port trust status de uiteindelijke classificatie van het pakje beïnvloedt. De port trust state kan worden ingesteld of gewijzigd met de volgende CatOS opdracht:

stel port qos *mod/port* trust in | vertrouwenskosten | trust-ipprec | trust-dscp}

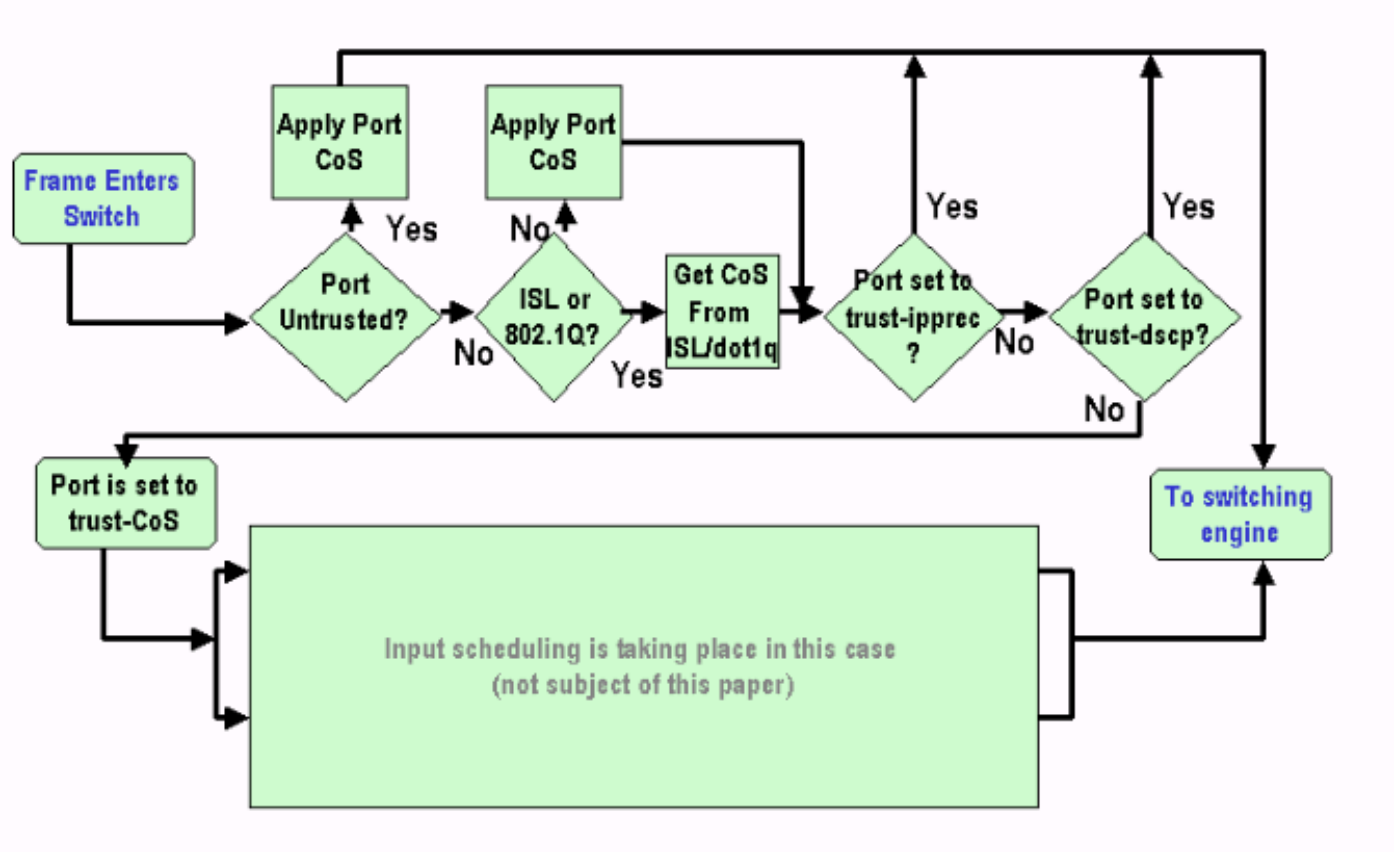
Opmerking: standaard zijn alle poorten in de onvertrouwde toestand wanneer QoS is ingeschakeld.

Op het niveau van de ingangspoort kunt u ook een standaard CoS per poort toepassen, zoals in het volgende voorbeeld:

set port qos *mod/*port cos *cos-waarde*

Als de poort is ingesteld op de onvertrouwde status, markeert u het frame met de standaard poort

CoS en geeft u de header door aan de wisselmachine (PFC). Als de poort is ingesteld op een van de vertrouwensstaten, gebruik dan de standaardpoort CoS (als het frame geen ontvangen CoS (dot1q of ISL) heeft, of houd CoS zoals het is (voor dot1q en ISL frames) en pas het kader aan de switchmotor door. De invoerclassificatie wordt geïllustreerd in het volgende stroomschema:



Opmerking: Zoals in het bovenstaande stroomschema wordt aangegeven, heeft elk frame een interne CoS toegewezen (ofwel de ontvangen CoS, ofwel de standaard poort CoS), inclusief niet-gelabelde frames die geen echte CoS aan boord hebben. Deze interne CoS en de ontvangen DSCP worden geschreven in een speciale pakketheader (een gegevensbus-header genaamd) en verzonden over de Data Bus naar de switchingmachine. Dit gebeurt op de ingress line card en op dit moment is nog niet bekend of deze interne CoS naar de gras ASIC zal worden vervoerd en in het uitgaande frame zal worden ingebracht. Dit hangt allemaal af van wat de PFC doet en verder wordt beschreven in de volgende sectie.

Switching Engine (PFC)

Zodra de kop de wisselmachine heeft bereikt, wordt elk frame aan een interne DSCP toegewezen via de overschakelmachine en de gecodeerde adresherkenning (EARL). Deze interne DSCP is een interne prioriteit die aan het kader door de PFC wordt toegewezen aangezien het de switch overbrengt. Dit is niet de DSCP in de IPv4 header. Hij is afgeleid van een bestaande CoS of ToS-instelling en wordt gebruikt om de CoS of ToS te herstellen 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.

Vier mogelijke bronnen voor interne DSCP

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

1. Een bestaande DSCP-waarde, ingesteld voordat het kader de switch invoert.
2. De ontvangen IP-prioriteitsbits die al in de IPv4-header zijn ingesteld. Aangezien er 64 DSCP-waarden zijn en slechts acht IP-prioriteitswaarden, zal de beheerder een mapping configureren die door de switch wordt gebruikt om de DSCP af te leiden. Standaard toewijzingen zijn uitgevoerd indien de beheerder de kaarten niet aanpast.
3. De ontvangen CoS bits werden al ingesteld voordat het frame dat de switch invoert, of vanaf de standaard CoS van de inkomende poort als er geen CoS in het inkomende frame was. Zoals bij IP-voorrang, zijn er maximaal acht CoS-waarden, die elk aan een van de 64 DSCP-waarden moeten worden gekoppeld. Deze kaart kan worden ingesteld of de switch kan de standaardkaart gebruiken die al op zijn plaats is.
4. De DSCP kan voor het frame worden ingesteld met behulp van een DSCP-standaardwaarde die doorgaans wordt toegewezen aan een ACL-item (toegangscontrolelijst).

Voor nrs. 2 en 3 in de bovenstaande lijst wordt de statische mapping standaard als volgt toegepast:

- DSCP afgeleid is gelijk aan acht keer CoS, voor CoS aan DSCP mapping.
- DSCP afgeleid is gelijk aan acht keer IP voorrang, voor IP voorrang aan DSCP mapping.

Deze statische afbeelding kan door de gebruiker worden overbrugd door de volgende opdrachten uit te geven:

qos ipprec-dscp-map instellen <dscp1> <dscp2>...<DSCP8>

qos cos-dscp-map instellen <dscp1> <dscp2>...<DSCP8>

De eerste waarde van de DSCP die correspondert met de mapping voor de CoS (of IP-voorrang) is "0", de tweede voor de CoS (of IP-voorrang) is "1", en wordt in dat patroon voortgezet.

Welke van de vier mogelijke bronnen voor interne DSCP zal worden gebruikt?

In dit gedeelte worden de regels beschreven die bepalen welke van de vier mogelijke bronnen hierboven worden gebruikt voor elk pakje. Dat hangt af van de volgende parameters:

1. Welke QoS ACL zal op het pakket worden toegepast? Dit wordt bepaald door de volgende regels:**Opmerking:** elk pakket gaat door een ACL-ingang.Als er geen ACL aan de inkomende poort of VLAN is toegevoegd, pas de standaard ACL toe.Als er een ACL aan de inkomende poort of VLAN is toegevoegd en als het verkeer één van de ingangen in ACL aanpast, gebruik deze ingang.Als er een ACL is toegevoegd aan de inkomende poort of VLAN en als het verkeer *niet* overeenkomt met een van de items in de ACL, gebruikt u de standaard ACL-ACL.
2. Elke ingang bevat een classificatietrefwoord. Hieronder vindt u een lijst met mogelijke zoekwoorden en de beschrijvingen ervan:trust-ipprec: De interne DSCP zal afgeleid worden van de ontvangen IP voorrang volgens de statische afbeelding, ongeacht wat de haventrust staat zou kunnen zijn.trust-dscp: De interne DSCP zal worden afgeleid van de ontvangen DSCP ongeacht wat de havenstaat kan zijn.vertrouwenskos: De interne DSCP zal worden afgeleid van de ontvangen CoS volgens de statische mapping, als de haventrust state wordt vertrouwd (trust-cos, trust-dscp, trust-ipprec). Als de port trust status trust-xx is, zal DSCP afgeleid worden van de standaard poort CoS volgens dezelfde statische mapping.DSCP *xx*: De interne DSCP zal afhangen van de volgende inkomende havenvertrouwenstaten:Als de poort niet wordt vertrouwd, wordt de interne DSCP ingesteld op *xx*.Als de poort op trust-dscp

is, wordt de interne DSCP het DSCP dat in het inkomende pakket wordt ontvangen.Als de poort op trust-CoS is, zal de interne DSCP van het ontvangen pakket worden afgeleid.Als de poort op trust-ipprec is, zal de interne DSCP afgeleid worden van de IP voorrang van het ontvangen pakket.

3. Elke QoS ACL kan op een poort of op een VLAN worden toegepast, maar er is een extra configuratieparameter om rekening te houden met; het ACL-poorttype. Een poort kan worden ingesteld om VLAN-gebaseerd of op poort gebaseerd te zijn. Hieronder volgt een beschrijving van de twee soorten configuraties:Een poort die om op VLAN gebaseerd wordt gevormd zal slechts op ACL kijken die op het VLAN wordt toegepast waarop de haven hoort. Als er ACL aan de poort is toegevoegd, zal ACL worden genegeerd voor het pakket dat op die poort komt.Als een haven die tot een VLAN behoort als haven-gebaseerd wordt gevormd, zelfs als er ACL aan dat VLAN is verbonden zal het niet in overweging worden genomen voor het verkeer dat van die haven binnenkomt.

Het volgende is een syntaxis om een QoS ACL te maken om IP-verkeer te markeren:

qos acl ip ***acl_name*** **[dscp xx] instellen | vertrouwenskosten | trust-dscp | trust-ipprec]** ***acl-toegangsregel***

Op basis van onderstaande ACL wordt al het IP-verkeer naar host 1.1.1.1 gemarkeerd met een DSCP van "40" en is er een trust-dscp voor al het andere IP-verkeer:

qos acl TEST_ACL dscp 40 ip elke host 1.1.1

qos acl TEST_ACL trust-dscp instellen

Zodra ACL is gecreëerd moet u het in kaart brengen aan een haven of VLAN, kan dit door de volgende opdracht uit te geven worden gedaan:

qos acl map ***acl_name*** **instellen [module/poort | VLAN]**

Standaard is elke poort op basis van poort voor ACL, zodat als u ACL aan een VLAN wilt toevoegen, u de poorten van dit VLAN als op VLAN gebaseerd moet configureren. Dit kan worden gedaan door de volgende opdracht uit te geven:

stel port qos ***module/poort op*** **VLAN gebaseerd**

Kan ook worden teruggedraaid naar poortgebaseerde modus door de volgende opdracht uit te geven:

stel port qos ***module/poort*** **op poort gebaseerd**

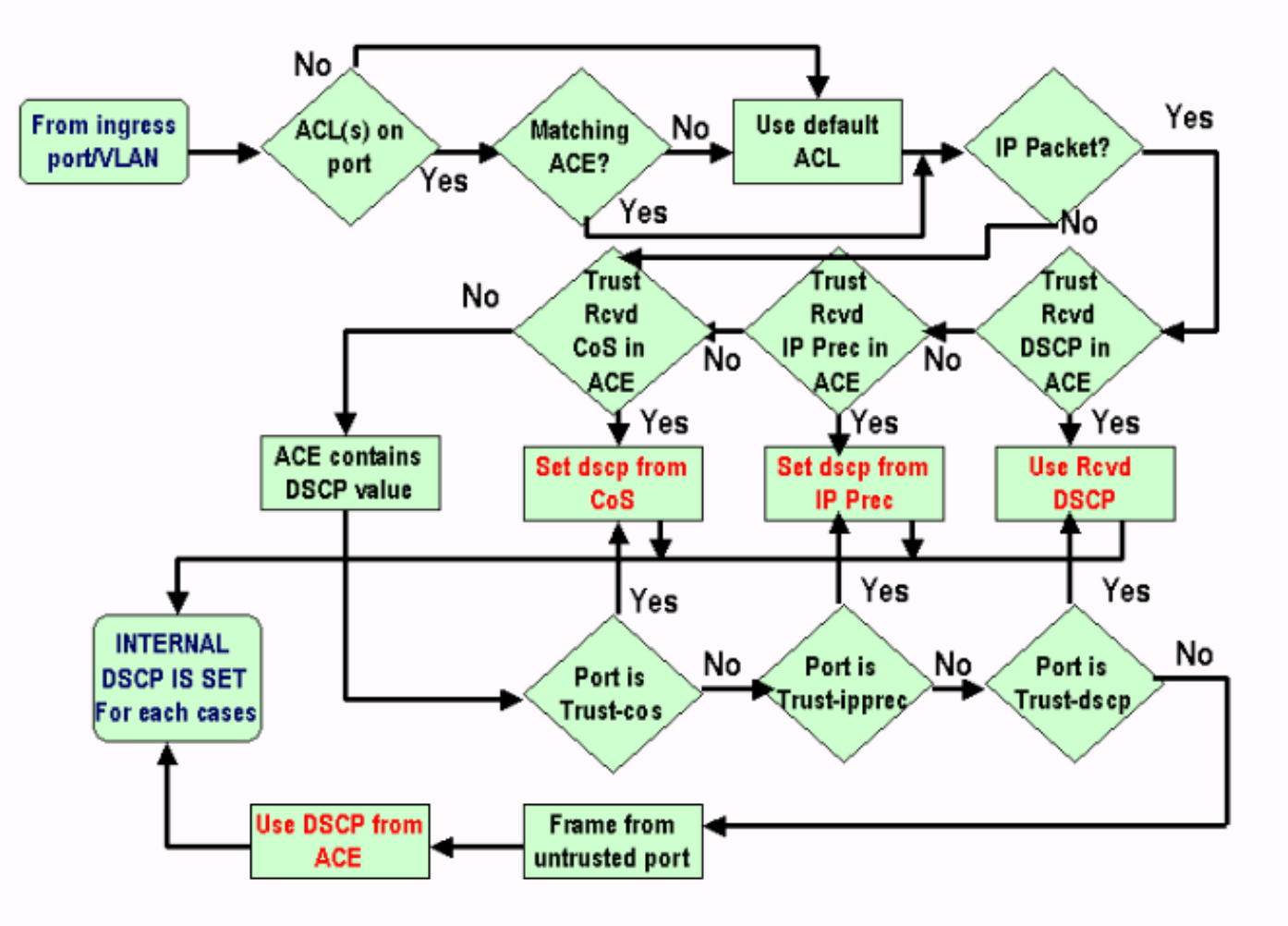
Samenvatting: Hoe wordt de interne DSCP geselecteerd?

De interne DSCP is afhankelijk van de volgende factoren:

- havenstaat
- ACL aan poort
- Standaard ACL
- Op VLAN gebaseerde of op haven gebaseerde gegevens met betrekking tot de ACL

Het volgende stroomschema vat samen hoe de interne DSCP afhankelijk van de configuratie

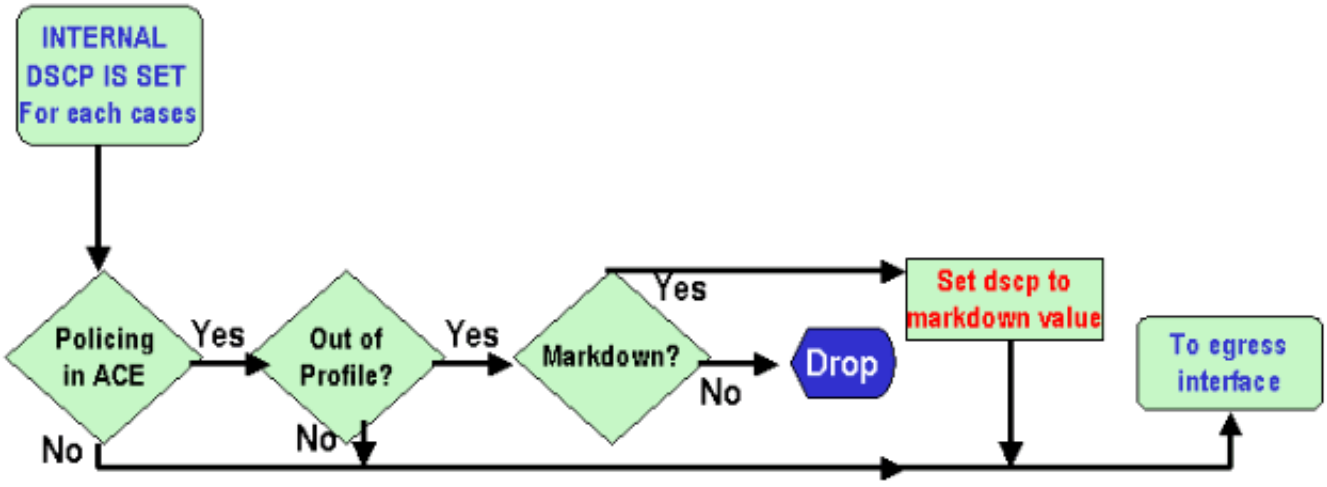
wordt geselecteerd:



De PFC kan ook toezicht houden. Dit zou uiteindelijk kunnen resulteren in een verlaging van de interne DSCP. Raadpleeg voor meer informatie over de controle het volgende document:

- QoS-toezicht op Catalyst 6000

In het volgende stroomschema wordt aangegeven hoe de toezichthouder wordt toegepast:



Uitvoer-poortverwerking

Er is niets dat op het niveau van de uitgang kan worden gedaan om de classificatie te veranderen, maar in deze sectie zult u het pakket volgens de volgende regels markeren:

- Als het pakket een IPv4-pakket is, kopieert u de interne DSCP die door de switchingmachine is toegewezen naar de ToS-poort van de IPv4-header.
- Als de uitvoerpoort is geconfigureerd voor een ISL- of dot1q-insluiting, gebruikt u een CoS die is afgeleid van de interne DSCP en kopieert u deze in het ISL- of dot1q-frame.

Opmerking: De CoS is afgeleid van de interne DSCP volgens een statische configuratie door de gebruiker die de volgende opdracht geeft:

Opmerking: **qos dscp-cos-map** ***dscp_list:cos_value instellen***

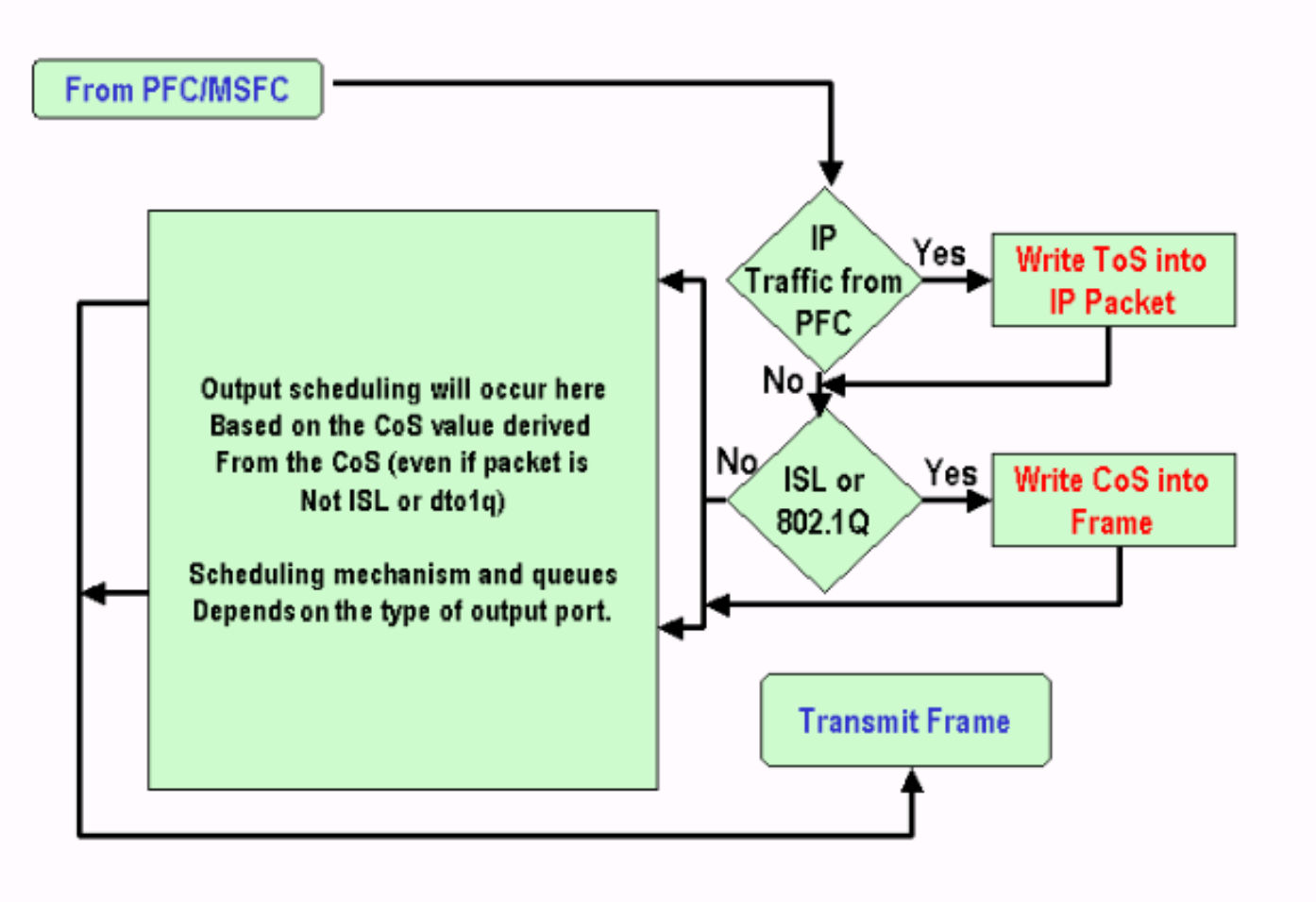
Opmerking: de standaardinstellingen zijn de volgende. Standaard zal CoS het integerdeel van de DSCP zijn, gedeeld door acht:

```
set qos dscp-cos-map 0-7:0
set qos dscp-cos-map 8-15:1
set qos dscp-cos-map 16-23:2
set qos dscp-cos-map 24-31:3
set qos dscp-cos-map 32-39:4
set qos dscp-cos-map 40-47:5
set qos dscp-cos-map 48-55:6
set qos dscp-cos-map 56-63:7
```

Zodra 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 zijn CoS (zelfs als het pakket geen punt1q of een ISL is). Raadpleeg voor meer informatie over het plannen van de uitvoerwachtrij het volgende document:

- QoS op Catalyst 6000 Series Switches: Uitvoerplanning op Catalyst 6000 met PFC of PFC 2 bij gebruik van CatOS-software

In het volgende stroomschema 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 gebruikt ACL "dscp 0" als classificatieslewoord. Dat betekent dat al het verkeer dat de switch via een onvertrouwde poort ingaat zal worden gemarkeerd met een DSCP van "0" als QoS is ingeschakeld. U kunt de standaard ACL voor de IP controleren door de volgende opdracht uit te geven:

```
Boris-1> (enable) show qos acl  info default-action  ip
set qos acl default-action
-------------------------
ip dscp 0
```

Standaard ACL kan ook worden gewijzigd door de volgende opdracht uit te geven:

standaard qos acl ip [dscp xx] | trust-CoS | trust-dscp | trust-ipprec)

trust-kos in ACL-toegangsbeperkingen

Er is een extra beperking die verschijnt wanneer u het trust-CoS sleutelwoord binnen een ingang gebruikt. CoS kan alleen in een boeking worden vertrouwd indien de ontvangende staat niet onbetrouwbaar is. Probeer een ingang met trust-CoS te configureren toont de volgende waarschuwing:

```
Telix  (enable) set qos acl ip test_2 trust-CoS ip any any
Warning: ACL trust-CoS should only be used with ports that are also configured with port
trust=trust-CoS
test_2 editbuffer modified. Use 'commit' command to apply changes.
```

Deze beperking is een gevolg van wat eerder in de sectie Invoerpoortbehandeling werd gezien. Zoals te zien is in het stroomschema van die sectie, als de poort niet vertrouwd is, wordt het frame onmiddellijk toegewezen de standaardpoort CoS. Daarom wordt de inkomende CoS niet bewaard en niet naar de switchingmotor gestuurd, waardoor de CoS niet kan vertrouwen, zelfs niet met een specifieke ACL.

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

Deze paragraaf heeft alleen betrekking op de volgende lijnkaarten:

- WS-X6224-100FX-MT : CATALYST 6000 24-POORTS 100 FX MULTI-MODE
- WS-X6248-RJ-45: CATALYST 6000 48-POORTS 10/100 RJ-45 MODULE
- WS-X6248-TEL : CATALYST 6000 48-POORTS 10/100 TELCO-MODULE
- WS-X6248A-RJ-45: CATALYST 6000 48-POORTS 10/100, UITGEBREIDE QOS-FUNCTIE
- WS-X6248A-TEL : CATALYST 6000 48-POORTS 10/100, UITGEBREIDE QOS-FUNCTIE
- WS-X6324-100FX-M: CATALYST 6000 24-POORTS 100FX, ENH QOS, MT
- WS-X6324-100FX-SM: CATALYST 6000 24-POORTS 100FX, ENH QOS, MT
- WS-X6348-RJ-45: CATALYST 6000 48-POORTS 10/100, UITGEBREIDE QO
- WS-X6348-RJ21V: CATALYST 6000 48-POORTS 10/100, INLINE VOEDING
- WS-X6348-RJ45V: CATALYST 6000 48-POORTS 10/100, ENH QOS, INLI-NETVOEDING

Deze lijnkaarten hebben echter wel enkele extra beperkingen:

- Op havenniveau, kunt u geen vertrouwen-dscp of vertrouwen-ipprec vertrouwen.
- Op het havenniveau, indien de havenstaat trust-CoS is, gelden de volgende verklaringen:De ontvangstdrempel voor invoerschema is ingeschakeld. Bovendien wordt de CoS in het ontvangstpakket gebruikt om pakketten op te stellen om de bus te bereiken.De CoS zal niet worden vertrouwd en zal niet worden gebruikt om de interne DSCP af te leiden, tenzij u ook ACL voor dat verkeer instelt om te vertrouwen-cos. Bovendien is het niet genoeg voor de lijnkaarten om te vertrouwen op de haven, u moet ook ACL hebben met vertrouwenscopen voor dat verkeer.
- Als de vertrouwensstaat van de haven niet wordt vertrouwd, zal er een normale markering plaatsvinden (zoals bij het standaardgeval). Dit hangt af van de ACL die op het verkeer wordt toegepast.

Elke poging om een vertrouwensstaat op een van deze poorten te configureren bevat een van de volgende waarschuwingsberichten:

```
telix (enable) set port qos 3/24 trust trust-ipprec
Trust type trust-ipprec not supported on this port.

telix (enable) set port qos 8/4 trust trust-dscp
Trust type trust-dscp not supported on this port.

telix (enable) set port qos 3/24 trust trust-cos
Trust type trust-cos not supported on this port.
Receive thresholds are enabled on port 3/24.
Port  3/24 qos set to untrusted.
```

Samenvatting van de classificatie

In de onderstaande tabellen wordt de resulterende DSCP weergegeven die als volgt is ingedeeld:

- De inkomende havenvertrouwenstatus.
- Het classificatietrefwoord binnen de toegepaste ACL.

Generic Table Summary voor alle poorten behalve WS-X62*xx* en WS-X63*xx*

ACL-sleutelwoord Poortvertrouwensstaat	DSCP xx	trust-dscp	trust-ipprec	trust-CoS
onbetrouwbaar	xx (1)	RX 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 ipprec	RX DSCP	afgeleid van RX ipprec	afgeleid van RX CoS of port CoS
trust-CoS	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.

Tabeloverzicht voor WS-X62*xx* of WS-X63*xx*

ACL-sleutelwoord Poortvertrouwensstaat	DSCP xx	trust-dscp	trust-ipprec	trust-CoS
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
trust-CoS	xx	RX DSCP	afgeleid van RX ipprec	afgeleid van Rx CoS of port CoS (2)

(2) Dit is de enige manier om de inkomende CoS te beschermen voor verkeer vanaf een lijnkaart van 62*xx* of 63*xx*.

Configuratie controleren en controleren

De poortconfiguratie controleren

De poortinstellingen en -configuraties kunnen worden geverifieerd door de volgende opdracht uit te geven:

toon port qos ***module/poort***

Door deze opdracht uit te geven, kunt u, naast andere parameters, de volgende classificatieparameters controleren:

- op basis van poort of VLAN
- type trust poort
- ACL aan poort

Het volgende is een voorbeeld van deze opdrachtoutput met belangrijke velden met betrekking tot de classificatie die gemarkeerd is:

```
tamer (enable) show port qos 1/1
QoS is enabled for the switch.
QoS policy source for the switch set to local.


Port  Interface Type Interface Type Policy Source Policy Source
      config         runtime        config        runtime
----- -------------- -------------- ------------- -------------
 1/1    port-based     port-based      COPS           local

Port  TxPort Type  RxPort Type  Trust Type   Trust Type    Def CoS Def CoS
                                config       runtime       config  runtime
----- ------------ ------------ ------------ ------------- ------- -------
 1/1     1p2q2t       1p1q4t     untrusted     untrusted      0       0

(*)Runtime trust type set to untrusted.

Config:
Port  ACL name                         Type
----- -------------------------------- ----
 1/1  test_2                           IP

Runtime:
Port  ACL name                         Type
----- -------------------------------- ----
 1/1  test_2                            IP
```

Opmerking: voor elk veld zijn er de geconfigureerde parameter en de parameter Runtime. Degene die op het pakje zal worden toegepast, is de parameter run.

De ACL controleren

U kunt ACL controleren dat in vorige opdrachten wordt toegepast en weergegeven door de

volgende opdracht uit te geven:

laat qos acl info *tap_name zien*

```
tamer (enable) show qos acl info run test_2
set qos acl IP test_2
------------------------------------------
1. dscp 32 ip any host 1.1.1.1
2. trust-dscp any
```

Steekproef-casestudy's

De volgende voorbeelden zijn voorbeeldconfiguraties van gemeenschappelijke gevallen die in een netwerk kunnen verschijnen.

Zaak 1 : Markeren aan de rand

Stel dat u een Catalyst 6000 configureren die gebruikt wordt als switch voor toegang met veel gebruikers die aangesloten zijn op sleuf 2, een WS-X6348 lijnkaart (10/100M). De gebruikers kunnen het volgende verzenden:

- Normaal gegevensverkeer: Dit is altijd in VLAN 100, en moet een DSCP van "0 krijgen."
- Spraakverkeer vanaf een IP-telefoon: Dit is altijd in de stemhulpbron VLAN 101, en moet een DSCP van "40 krijgen."
- Missiestkritische toepassingsverkeer: Dit komt ook in VLAN 100, en is gericht op de server 10.10.10.20. Dit verkeer moet een DSCP van "32 krijgen."

Niets van dit verkeer wordt door de toepassing gemarkeerd en daarom zal u de poort als onbetrouwbaar verlaten en zal u een specifieke ACL configureren om het verkeer in te delen. Eén ACL zal op VLAN 100 worden toegepast en één ACL zal op VLAN 101 worden toegepast. U moet ook alle poorten als VLAN-gebaseerd configureren. Het volgende is een voorbeeld van de resulterende configuratie:

```
set qos enable
set port qos 2/1-48 vlan-based
!--- Not needed, as it is the default. set port qos 2/1-48 trust untrusted set qos acl ip
Data_vlan dscp 32 ip any host 10.10.10.20 !--- Not needed, because if it is not present you
would !--- use the default ACL which has the same effect. Set qos acl ip Data_vlan dscp 0 ip any
any set qos acl ip Voice_vlan dscp 40 ip any any commit qos acl all set qos acl map Data_vlan
100 set qos acl map Voice_vlan 101
```

Zaak 2: Een kern met slechts een Gigabit-interface

Stel dat u een Catalyst 6000-kern configureren met alleen een Gigabit-interface in sleuf 1 en sleuf 2 (geen 62xx- of 63xx-lijnkaart in het chassis). Het verkeer is eerder correct gemarkeerd door de switches van de toegang, daarom hoeft u geen opmerkingen te maken, maar u moet ervoor zorgen dat u de inkomende DSCP wel vertrouwt. Dit is het makkelijkste geval, aangezien alle havens zullen worden aangeduid als trust-dscp en dat zou moeten volstaan:

```
set qos enable
set port qos 1/1-2 trust trust-dscp
set port qos 2/1-16 trust trust-dscp
...
```

Zaak 3: Strijken in de kern met een 62xx- of 63xx-poort in het chassis

Stel dat u een kern-/distributieapparaat configureren met een Gigabit-link op een WS-X6416-GBIC lijnkaart (in sleuf 2) en een 10/100 link op een WS-X6348 lijnkaart (in sleuf 3). U moet ook al het inkomende verkeer vertrouwen aangezien het eerder op het niveau van de switch van de toegang is gemarkeerd. Omdat u geen vertrouwen-DSCP kunt hebben op de 6348 lijnkaart, zou de makkelijkste methode in dit geval zijn om alle poorten als onbetrouwbaar te verlaten en de standaard ACL om te zetten in trust-dscp, zoals in het volgende voorbeeld:

```
set qos enable
set port qos 2/1-16 trust untrusted
set port qos 3/1-48 trust untrusted
set qos acl default-action ip trust-dscp
```

Gerelateerde informatie

- LAN-productondersteuning
- Ondersteuning voor LAN-switching technologie
- Technische ondersteuning - Cisco-systemen