QoS-Klassifizierung und -Kennzeichnung für Catalyst Switches der Serien 6500 und 6000 mit CatOS-Software

Inhalt

Einführung

In diesem Dokument wird untersucht, was bei der Kennzeichnung und Klassifizierung eines Pakets an verschiedenen Stellen während der Reise innerhalb des Catalyst 6000-Chassis geschieht. Es werden Sonderfälle, Einschränkungen und kurze Fallstudien erwähnt.

Dieses Dokument ist nicht als vollständige Liste aller Catalyst OS (CatOS)-Befehle bezüglich Quality of Service (QoS) oder Kennzeichnung vorgesehen. Weitere Informationen zur CatOS-

Befehlszeilenschnittstelle (CLI) finden Sie im folgenden Dokument:

- Konfigurieren von QoS

Hinweis: Dieses Dokument behandelt nur IP-Datenverkehr.

Bevor Sie beginnen

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Voraussetzungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

Verwendete Komponenten

Dieses Dokument gilt für Catalyst Switches der Serie 6000 mit CatOS-Software und einer der folgenden Supervisor Engines:

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

Alle Beispielbefehle wurden jedoch mit einem Catalyst 6506 mit SUP1A/PFC mit der Softwareversion 6.3 ausprobiert.

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Terminologie

Im Folgenden finden Sie eine Liste der in diesem Dokument verwendeten Terminologie:

- Differentiated Services Code Point (DSCP): Die ersten sechs Bit des ToS-Bytes (Type of Service) im IP-Header. DSCP ist nur im IP-Paket vorhanden.**Hinweis:** Sie weisen jedem Paket (IP oder Nicht-IP) auch ein internes DSCP zu. Diese interne DSCP-Zuweisung wird später in diesem Dokument erläutert.
- IP-Rangfolge: Die ersten drei Bit des ToS-Bytes im IP-Header.
- Class of Service (CoS): Das einzige Feld, das verwendet werden kann, um ein Paket auf Layer 2 (L2) zu kennzeichnen. Es besteht aus einem der folgenden drei Bits:Die drei dot1p-Bits im dot1q-Tag für das IEEE dot1q-Paket.Die drei Bits mit der Bezeichnung "User Field" (Benutzerfeld) im ISL-Header (Inter-Switch Link) für ein gekapseltes ISL-Paket.In einem Nicht-dot1q- oder ISL-Paket ist keine CoS vorhanden.

- Klassifizierung: Der Prozess zur Auswahl des zu markierenden Datenverkehrs.
- Markierung: Der Prozess zum Festlegen eines Layer 3 (L3)-DSCP-Werts in einem Paket. In diesem Dokument wird die Definition der Kennzeichnung erweitert, sodass auch L2-CoS-Werte festgelegt werden.

Catalyst Switches der Serie 6000 können Klassifizierungen anhand der folgenden drei Parameter vornehmen:

- DSCP
- IP-Rangfolge
- CoS

Die Catalyst Switches der Serie 6000 führen Klassifizierungen und Markierungen an verschiedenen Stellen durch. Folgendes zeigt, was an diesen verschiedenen Orten geschieht:

- Eingangsport (ASIC (Ingress Application-Specific Integrated Circuit))
- Switching Engine (Policy Feature Card, PFC)
- Ausgangsport (Ausgangs-ASIC)

Aktivieren von QoS

QoS ist auf Catalyst 6000-Switches standardmäßig deaktiviert. QoS kann aktiviert werden, indem der CatOS-Befehl **set qos enable** ausgegeben wird.

Wenn QoS deaktiviert ist, erfolgt keine Klassifizierung oder Kennzeichnung durch den Switch. Daher verlässt jedes Paket den Switch mit der beim Eingeben des Switches geltenden DSCP/IP-Priorität.

Verarbeitung der Eingangsports

Der Hauptkonfigurationsparameter für den Eingangsport hinsichtlich der Klassifizierung ist der Vertrauensstatus des Ports. Jeder Port des Systems kann einen der folgenden Vertrauensstatus aufweisen:

- trust-ip-Rangfolge
- trust-dscp
- Treuhandkosten
- nicht vertrauenswürdig

Im verbleibenden Teil dieses Abschnitts wird beschrieben, wie der Status "port trust" die endgültige Klassifizierung des Pakets beeinflusst. Der Port-Vertrauensstatus kann mit dem folgenden CatOS-Befehl festgelegt oder geändert werden:

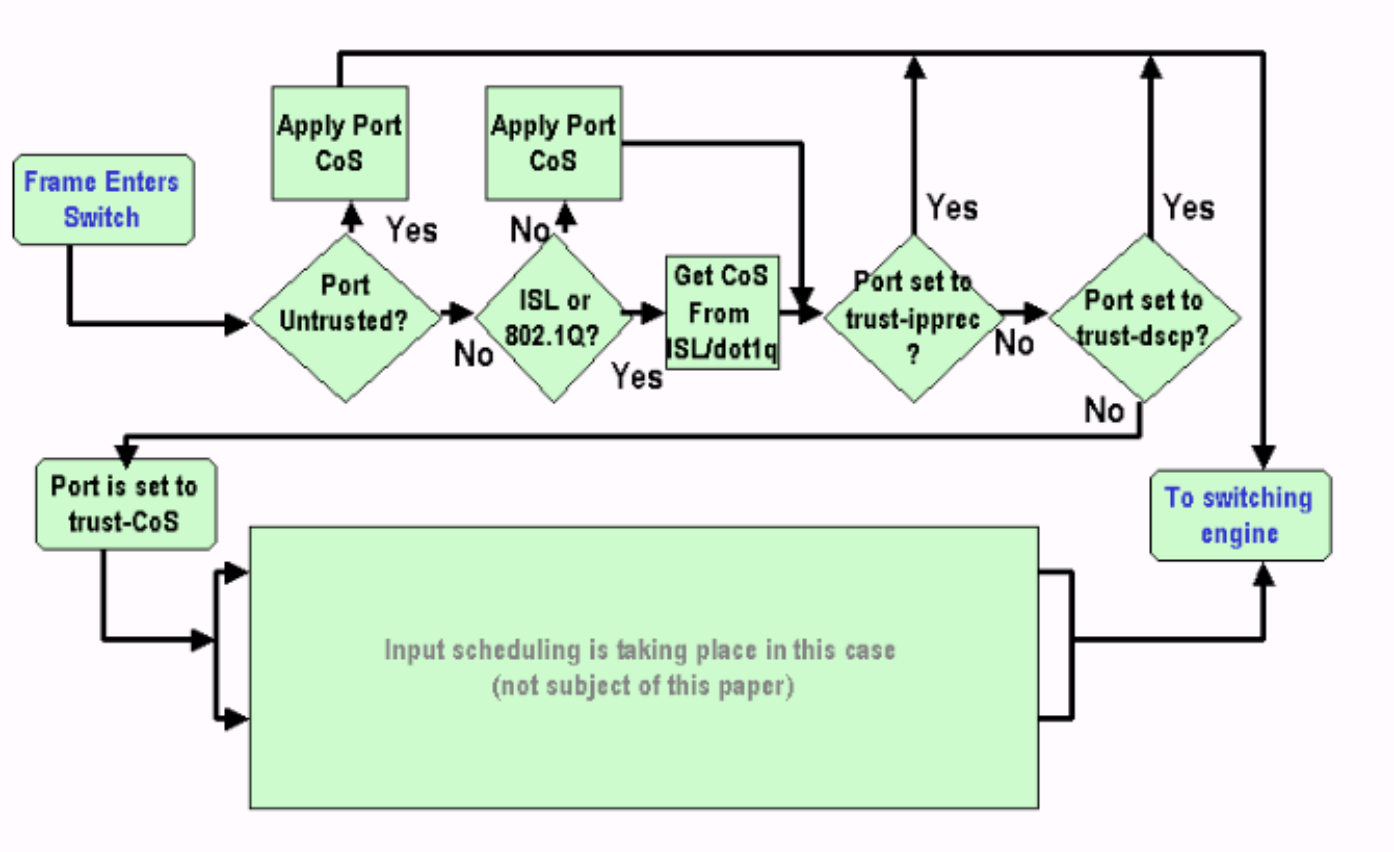
Einstellen von port qos *mod/port* trust {nicht vertrauenswürdig | Treuhandkosten | trust-ipprec | trust-dscp }

Hinweis: Standardmäßig befinden sich alle Ports im nicht vertrauenswürdigen Zustand, wenn QoS aktiviert ist.

Auf der Eingangsport-Ebene können Sie auch eine standardmäßige CoS pro Port anwenden, wie im folgenden Beispiel gezeigt:

Einstellen von port qos *mod/port* cos *cos value*

Wenn der Port auf den nicht vertrauenswürdigen Status festgelegt ist, markieren Sie einfach den Frame mit dem Port-Standard-CoS, und geben Sie den Header an die Switching Engine (PFC) weiter. Wenn der Port auf einen der Vertrauensstatus festgelegt ist, wenden Sie die Standard-Port-CoS an (wenn der Frame kein empfangenes CoS (dot1q oder ISL) hat), oder belassen Sie die CoS so, wie sie ist (bei dot1q- und ISL-Frames), und übergeben Sie den Frame an die Switching-Engine. Die Eingangsklassifizierung wird im folgenden Flussdiagramm veranschaulicht:



Hinweis: Wie im obigen Flussdiagramm gezeigt, wird jedem Frame eine interne CoS zugewiesen (entweder das empfangene CoS oder das Standard-Port-CoS), einschließlich nicht getaggte Frames, die keine echte CoS tragen. Diese interne CoS und das empfangene DSCP werden in einem speziellen Paket-Header (einem so genannten Data Bus-Header) geschrieben und über den Data Bus an die Switching-Engine gesendet. Dies geschieht an der Eingangs-Linecard, und es ist noch nicht bekannt, ob diese interne CoS in den ausgehenden ASIC übertragen und in den ausgehenden Frame eingefügt wird. Dies hängt davon ab, was die PFC tut und wird im nächsten Abschnitt genauer beschrieben.

Switching Engine (PFC)

Sobald der Header die Switching-Engine erreicht hat, weist die Switching-Engine Encoded Address Recognition Logic (EARL) jedem Frame ein internes DSCP zu. Dieses interne DSCP ist eine interne Priorität, die dem Frame vom PFC beim Transit durch den Switch zugewiesen wird. Dies ist nicht der DSCP im IPv4-Header. Sie basiert auf einer bestehenden CoS- oder ToS-Einstellung und wird zum Zurücksetzen des CoS oder ToS verwendet, wenn der Frame den Switch verlässt. Dieses interne DSCP wird allen Frames zugewiesen, die von der PFC (auch Nicht-IP-Frames) geswitcht (oder geroutet) werden.

Vier mögliche Quellen für internes DSCP

Das interne DSCP wird aus einem der folgenden Komponenten abgeleitet:

1. Ein vorhandener DSCP-Wert, der vor der Eingabe des Frames in den Switch festgelegt wird.
2. Die empfangenen IP-Prioritätsbits sind bereits im IPv4-Header festgelegt. Da 64 DSCP-Werte und nur acht IP-Rangfolgewerte vorhanden sind, konfiguriert der Administrator eine vom Switch verwendete Zuordnung, um das DSCP abzuleiten. Es sind Standard-Zuordnungen vorhanden, sollte der Administrator die Zuordnungen nicht konfigurieren.
3. Die empfangenen CoS-Bits wurden bereits vor der Eingabe des Frames in den Switch festgelegt, oder von der standardmäßigen CoS des eingehenden Ports, wenn kein CoS im eingehenden Frame vorhanden war. Wie bei der IP-Rangfolge gibt es maximal acht CoS-Werte, die jeweils einem der 64 DSCP-Werte zugeordnet werden müssen. Diese Zuordnung kann konfiguriert werden, oder der Switch kann die bereits vorhandene Standardzuordnung verwenden.
4. Das DSCP kann für den Frame mithilfe eines DSCP-Standardwerts festgelegt werden, der normalerweise über einen ACL-Eintrag (Access Control List) zugewiesen wird.

Für Nr. 2 und 3 in der obigen Liste wird die statische Zuordnung standardmäßig wie folgt verwendet:

- Die abgeleitete DSCP entspricht dem achtfachen CoS für die CoS-DSCP-Zuordnung.
- Die abgeleitete DSCP entspricht der achtfachen IP-Priorität für die IP-Rangfolge der DSCP-Zuordnung.

Diese statische Zuordnung kann vom Benutzer mithilfe der folgenden Befehle überschrieben werden:

set qos ipprec-dscp-map <dscp1> <dscp2>..<dscp8>

set qos cos-dscp-map <dscp1> <dscp2>..<dscp8>

Der erste Wert des DSCP, der der Zuordnung für die CoS (oder IP-Rangfolge) entspricht, ist "0", der zweite für die CoS (oder IP-Rangfolge) "1", und wird in diesem Muster fortgesetzt.

Welche der vier möglichen Quellen für internes DSCP werden verwendet?

In diesem Abschnitt werden die Regeln beschrieben, die festlegen, welche der vier oben beschriebenen möglichen Quellen für jedes Paket verwendet werden. Dies hängt von den folgenden Parametern ab:

1. Welche QoS-ACL wird auf das Paket angewendet? Dies wird durch die folgenden Regeln bestimmt:**Hinweis:** Jedes Paket durchläuft einen ACL-Eintrag.Wenn keine ACL an den eingehenden Port oder das VLAN angeschlossen ist, wenden Sie die Standard-ACL an.Wenn eine ACL mit dem eingehenden Port oder VLAN verbunden ist und der Datenverkehr mit einem der Einträge in der ACL übereinstimmt, verwenden Sie diesen Eintrag.Wenn eine ACL an den eingehenden Port oder das VLAN angeschlossen ist und der Datenverkehr *nicht* mit einem der Einträge in der ACL übereinstimmt, verwenden Sie die Standard-ACL.
2. Jeder Eintrag enthält ein Klassifizierungsschlüsselwort. Im Folgenden finden Sie eine Liste möglicher Schlüsselwörter und deren Beschreibungen:trust-ipprec: Das interne DSCP wird von der empfangenen IP-Rangfolge gemäß der statischen Zuordnung abgeleitet, unabhängig davon, welcher Port-Vertrauensstatus vorliegt.trust-dscp: Das interne DSCP wird

vom empfangenen DSCP abgeleitet, unabhängig davon, welcher Port-Vertrauensstatus vorliegt.Vertrauenskosten: Das interne DSCP wird von der empfangenen CoS entsprechend der statischen Zuordnung abgeleitet, wenn der Port-Vertrauensstatus vertrauenswürdig ist (trust-cos, trust-dscp, trust-ipprec). Wenn der Port-Vertrauensstatus trust-xx lautet, wird das DSCP vom Standard-Port-CoS entsprechend derselben statischen Zuordnung abgeleitet.dscp *xx*: Das interne DSCP hängt von den folgenden Status der eingehenden Port-Vertrauenswürdigkeit ab:Wenn der Port nicht vertrauenswürdig ist, wird das interne DSCP auf *xx* festgelegt.Wenn der Port trust-dscp ist, ist das interne DSCP das im eingehenden Paket empfangene DSCP.Wenn der Port trust-CoS ist, wird das interne DSCP von der CoS des empfangenen Pakets abgeleitet.Wenn der Port trust-ipprec ist, wird das interne DSCP von der IP-Rangfolge des empfangenen Pakets abgeleitet.

3. Jede QoS-ACL kann entweder auf einen Port oder auf ein VLAN angewendet werden, es ist jedoch ein zusätzlicher Konfigurationsparameter zu berücksichtigen. den ACL-Port-Typ. Ein Port kann für VLAN-basierte oder Port-basierte Verbindungen konfiguriert werden. Im Folgenden werden die beiden Konfigurationsarten beschrieben:Ein Port, der für VLAN-basiert konfiguriert ist, bezieht sich nur auf die ACL, die auf das VLAN angewendet wird, zu dem der Port gehört. Wenn eine ACL an den Port angeschlossen ist, wird die ACL für das Paket ignoriert, das an diesem Port eingeht.Wenn ein Port, der zu einem VLAN gehört, als Port-basiert konfiguriert ist, selbst wenn eine ACL mit diesem VLAN verbunden ist, wird er für den von diesem Port eingehenden Datenverkehr nicht berücksichtigt.

Es folgt eine Syntax zum Erstellen einer QoS-ACL zum Markieren von IP-Datenverkehr:

set qos acl ip ***acl_name*** **[dscp xx | Treuhandkosten | trust-dscp | trust-ipprec]** ***acl entry regel***

Die folgende ACL markiert den gesamten an Host 1.1.1.1 gerichteten IP-Datenverkehr mit dem DSCP "40" und Trust-DSCP für den gesamten anderen IP-Datenverkehr:

set qos acl TEST_ACL dscp 40 ip any host 1.1.1.1

qos acl TEST_ACL trust-dscp ip any

Nachdem die ACL erstellt wurde, müssen Sie sie einem Port oder einem VLAN zuordnen. Verwenden Sie hierzu den folgenden Befehl:

set qos acl map ***acl_name*** **[module/port] | VLAN]**

Standardmäßig ist jeder Port für die ACL portbasiert. Wenn Sie also eine ACL mit einem VLAN verbinden möchten, müssen Sie die Ports dieses VLAN als VLAN-basiert konfigurieren. Dazu muss der folgende Befehl eingegeben werden:

Einstellen von Port QoS-*Modul/Port* VLAN-basiert

Sie kann auch mithilfe des folgenden Befehls in den Port-basierten Modus zurückgesetzt werden:

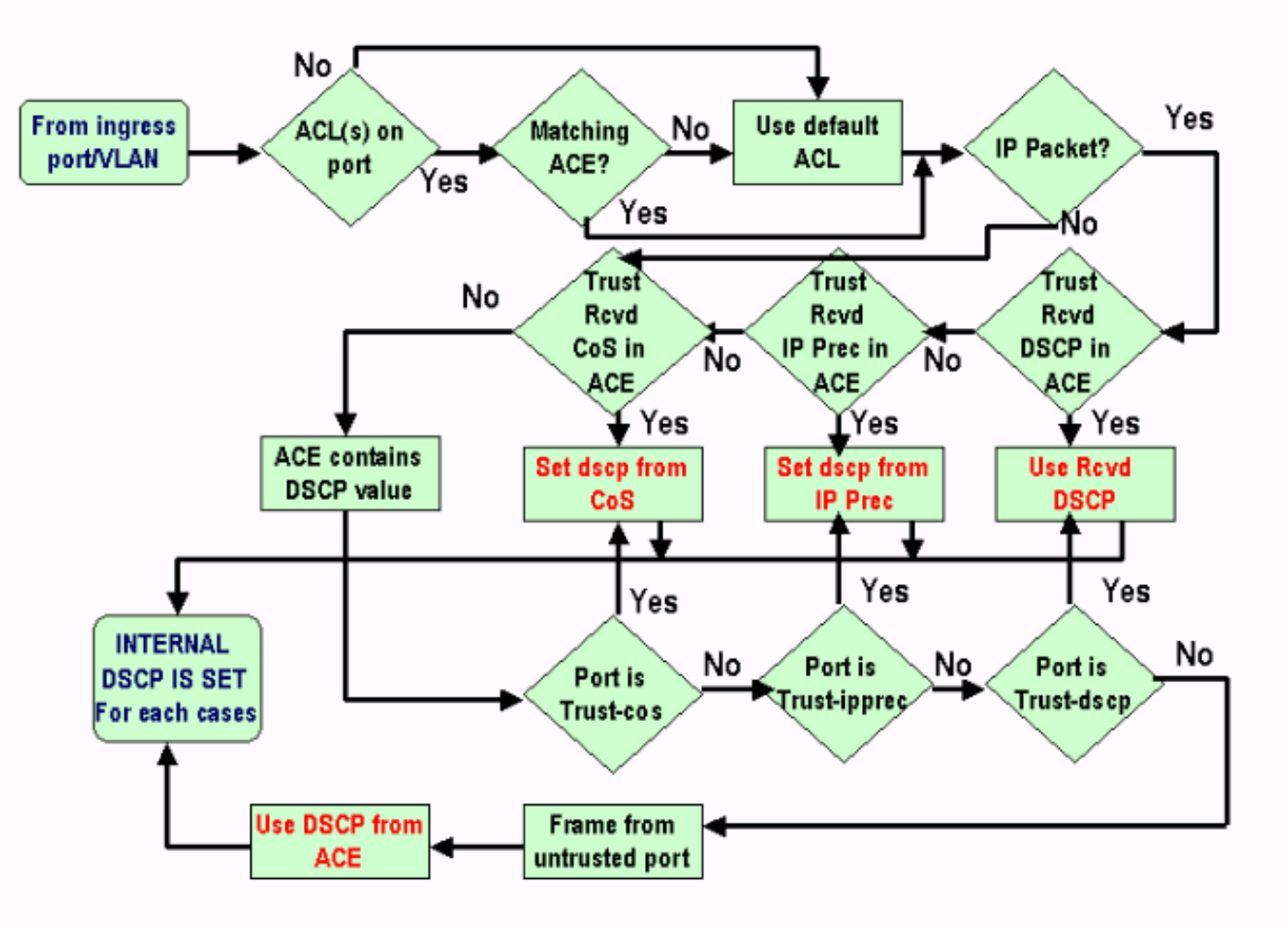
Port QoS-*Modul/Port*-basiert

Zusammenfassung: Wie wird das interne DSCP gewählt?

Das interne DSCP hängt von den folgenden Faktoren ab:

- Port Trust State
- Mit Port verbundene ACL
- Standard-ACL
- VLAN-basiert oder Port-basiert in Bezug auf die ACL

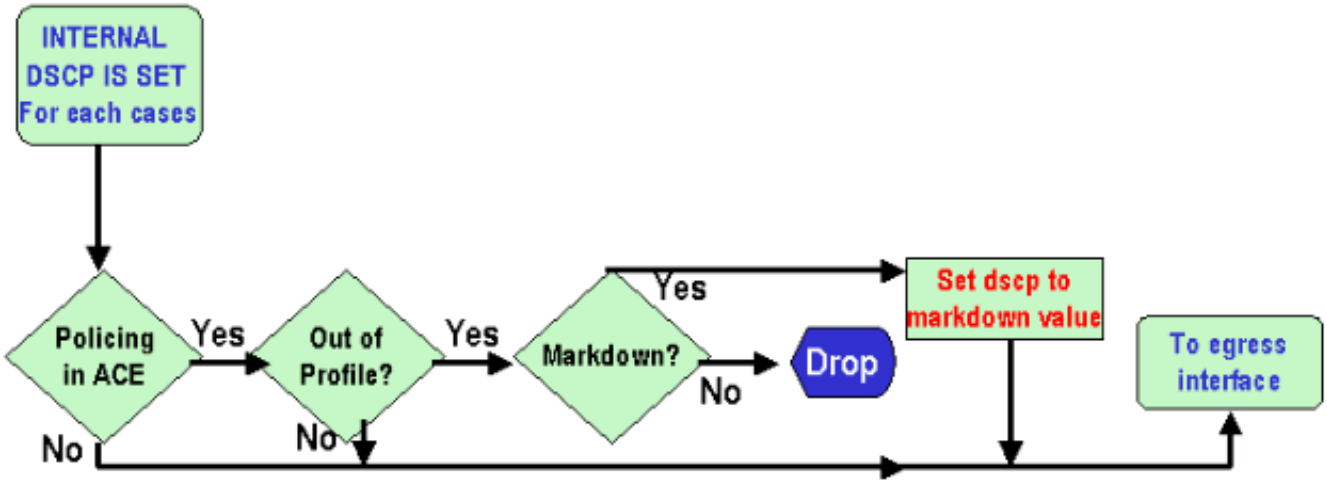
Das folgende Flussdiagramm fasst die Auswahl des internen DSCP je nach Konfiguration zusammen:



Die PFC kann auch Richtlinien erstellen. Dies kann letztendlich zu einer Aufschlüsselung des internen DSCP führen. Weitere Informationen zur Richtlinienvergabe finden Sie im folgenden Dokument:

- QoS-Richtlinienvergabe für Catalyst 6000

Das folgende Flussdiagramm zeigt, wie die Richtlinie angewendet wird:



Verarbeitung von Ausgabeports

Auf der Ausgangsport-Ebene können Sie die Klassifizierung nicht ändern. In diesem Abschnitt markieren Sie das Paket jedoch gemäß den folgenden Regeln:

- Wenn es sich bei dem Paket um ein IPv4-Paket handelt, kopieren Sie das vom Switching-Modul zugewiesene interne DSCP in das ToS-Byte des IPv4-Headers.
- Wenn der Ausgangsport für eine ISL- oder dot1q-Kapselung konfiguriert ist, verwenden Sie eine vom internen DSCP abgeleitete CoS, und kopieren Sie diese in den ISL- oder dot1q-Frame.

Hinweis: Die CoS wird vom internen DSCP abgeleitet, und zwar entsprechend einer statischen Konfiguration, die der Benutzer mit dem folgenden Befehl konfiguriert hat:

Hinweis: **set qos dscp-cos-map** ***dscp_list:cos_value***

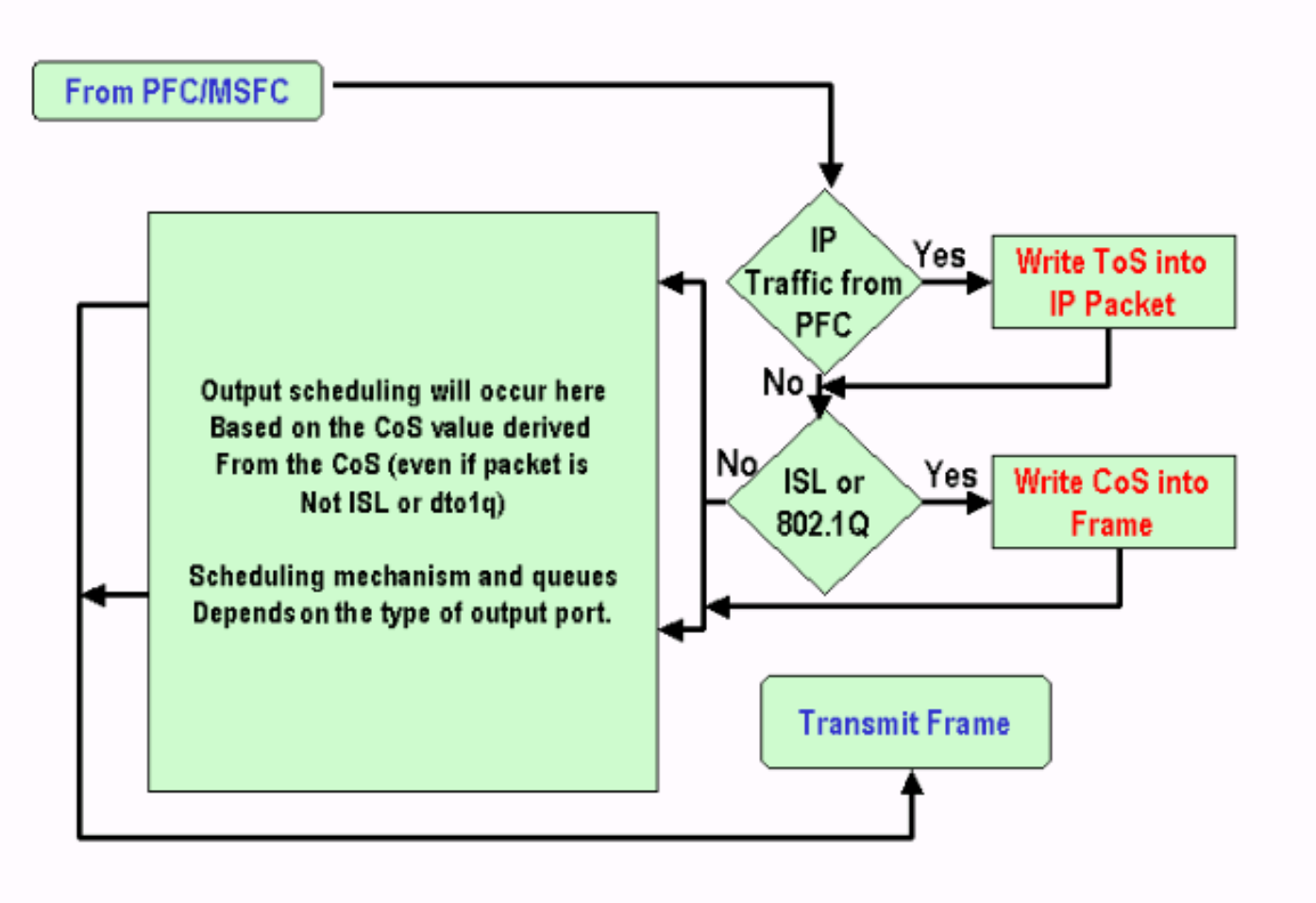
Hinweis: Die Standardkonfigurationen sind wie folgt: Standardmäßig ist CoS der ganze Teil des DSCP, geteilt durch acht:

```
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
```

Sobald das DSCP in den IP-Header geschrieben und die CoS vom DSCP abgeleitet wurde, wird das Paket zur Erstellung der Ausgabe-Scheduling-Daten basierend auf seiner CoS an eine der Ausgabewarteschlangen gesendet (auch wenn es sich nicht um ein dot1q oder eine ISL handelt). Weitere Informationen zur Planung von Ausgabewarteschlangen finden Sie im folgenden Dokument:

- QoS für Catalyst Switches der Serie 6000: Ausgabeplanung auf dem Catalyst 6000 mit PFC oder PFC 2 mit CatOS-Software

Das folgende Flussdiagramm fasst die Verarbeitung des Pakets hinsichtlich der Markierung im Ausgangsport zusammen:



Hinweise und Einschränkungen

Die Standard-ACL

Standardmäßig verwendet die Standard-ACL "dscp 0" als Klassifizierungsschlüsselwort. Das bedeutet, dass der gesamte Datenverkehr, der über einen nicht vertrauenswürdigen Port in den Switch gelangt, mit dem DSCP "0" markiert wird, wenn QoS aktiviert ist. Sie können die Standard-ACL für die IP überprüfen, indem Sie den folgenden Befehl eingeben:

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

Die standardmäßige ACL kann auch geändert werden, indem der folgende Befehl ausgegeben wird:

set qos acl default-action ip [dscp xx | trust-CoS | trust-dscp | trust-ipprec]

Vertrauenskosten bei Zugriffsbeschränkungen für Zugriffskontrolllisten

Wenn Sie das trust-CoS-Schlüsselwort innerhalb eines Eintrags verwenden, wird eine zusätzliche Einschränkung angezeigt. CoS kann in einem Eintrag nur dann vertrauenswürdig sein, wenn der

Treuhandzustand des Empfängers nicht nicht nicht vertrauenswürdig ist. Beim Konfigurieren eines Eintrags mit trust-CoS wird folgende Warnung angezeigt:

```
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.
```

Diese Einschränkung ist eine Folge dessen, was zuvor im Abschnitt "Handhabung von Eingangsports" beobachtet wurde. Wie im Flussdiagramm dieses Abschnitts gezeigt, wird dem Frame sofort die Standard-Port-CoS zugewiesen, wenn der Port nicht vertrauenswürdig ist. Daher wird die eingehende CoS nicht beibehalten und nicht an die Switching-Engine gesendet, was dazu führt, dass die CoS selbst mit einer bestimmten ACL nicht vertrauenswürdig ist.

Einschränkungen der Linecards WS-X6248-xx, WS-X6224-xx und WS-X6348-xx

Dieser Abschnitt betrifft nur die folgenden Linecards:

- WS-X6224-100FX-MT: CATALYST 6000 MULTIMODE MIT 24 100 FX-PORTS
- WS-X6248-RJ-45 : CATALYST 6000-MODUL MIT 48 10/100-RJ-45-PORTS
- WS-X6248-TEL: CATALYST 6000 TELCO-MODUL MIT 48 10/100-PORTS
- WS-X6248A-RJ-45 : CATALYST 6000, 48 10/100-PORTS, ERWEITERTE QOS
- WS-X6248A-TEL: CATALYST 6000, 48 10/100-PORTS, ERWEITERTE QOS
- WS-X6324-100FX-MM : CATALYST 6000, 24 PORTS, 100FX, ENH QOS, MT
- WS-X6324-100FX-SM : CATALYST 6000, 24 PORTS, 100FX, ENH QOS, MT
- WS-X6348-RJ-45 : CATALYST 6000, 48 10/100-PORTS, ERWEITERTE QO
- WS-X6348-RJ21V : CATALYST 6000, 48 10/100-PORTS, INLINE-LEISTUNG
- WS-X6348-RJ45V : CATALYST 6000 MIT 48 10/100-PORTS, ENH QOS, INLI NE POWER

Diese Linecards unterliegen jedoch einigen zusätzlichen Beschränkungen:

- Auf Portebene können Sie trust-dscp oder trust-ipprec nicht durchführen.
- Wenn auf Portebene der Port-Vertrauensstatus trust-CoS ist, gelten die folgenden Anweisungen:Der Empfangs-Grenzwert für die Eingabeplanung ist aktiviert. Darüber hinaus dient die CoS im Empfangspaket zur Priorisierung von Paketen für den Zugriff auf den Bus.Die CoS ist nicht vertrauenswürdig und wird nicht zur Ableitung des internen DSCP verwendet, es sei denn, Sie haben auch die ACL für diesen Datenverkehr in Trust-cos konfiguriert. Darüber hinaus reicht es nicht aus, dass die Linecards auf dem Port Vertrauensgebühren anbieten, sondern es ist auch eine Zugriffskontrollliste mit Vertrauenslisten für diesen Datenverkehr erforderlich.
- Wenn der Port-Vertrauensstatus nicht vertrauenswürdig ist, erfolgt eine normale Markierung (wie im Standardfall). Dies hängt von der ACL ab, die auf den Datenverkehr angewendet wird.

Bei jedem Versuch, einen Vertrauensstatus auf einem dieser Ports zu konfigurieren, wird eine der folgenden Warnmeldungen angezeigt:

```
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.
```

Zusammenfassung der Klassifizierung

Die nachfolgende Tabelle zeigt das resultierende DSCP, das wie folgt klassifiziert ist:

- Der eingehende Port-Vertrauensstatus.
- Das Klassifizierungsschlüsselwort in der angewendeten ACL.

Zusammenfassung der allgemeinen Tabelle für alle Ports außer WS-X62*xx* und WS-X63*xx*

ACL-Schlüsselwort Port Trust-Status	dscp xx	trust-dscp	Trust-Ipprec	trust-CoS
Nicht vertrauenswürdig	xx (1)	Rx dscp	abgeleitet von Rx ipprec	0
trust-dscp	Rx-dscp	Rx dscp	abgeleitet von Rx ipprec	abgeleitet von Rx CoS oder Port CoS
Trust-Ipprec	abgeleitet von Rx ipprec	Rx dscp	abgeleitet von Rx ipprec	abgeleitet von Rx CoS oder Port CoS
trust-CoS	abgeleitet von Rx COS oder Port CoS	Rx dscp	abgeleitet von Rx ipprec	abgeleitet von Rx CoS oder Port CoS

(1) Nur so kann ein Rahmen neu gekennzeichnet werden.

Tabellenübersicht für WS-X62*xx* oder WS-X63*xx*

ACL-Schlüsselwort Port Trust-Status	dscp xx	trust-dscp	Trust-Ipprec	trust-CoS
Nicht vertrauenswürdig	xx	Rx dscp	abgeleitet von Rx ipprec	0
trust-dscp	Nicht unterstüt	Nicht unterstüt	Nicht unterstütz	Nicht unterstü

	zt	zt	t	tzt
Trust-Ipprec	Nicht unterstützt zt	Nicht unterstützt zt	Nicht unterstützt t	Nicht unterstützt tzt
trust-CoS	xx	Rx dscp	abgeleitet von Rx ipprec	abgeleitet von Rx CoS oder Port CoS (2)

(2) Nur so kann die eingehende CoS für Datenverkehr beibehalten werden, der von einer 62*xx*- oder 63*xx*-Linecard stammt.

Überwachen und Überprüfen einer Konfiguration

Überprüfen der Portkonfiguration

Die Porteinstellungen und -konfigurationen können mithilfe des folgenden Befehls überprüft werden:

Port QoS-*Modul/Port* anzeigen

Mit diesem Befehl können Sie unter anderem die folgenden Klassifizierungsparameter überprüfen:

- Port- oder VLAN-basiert
- Treuhandport-Typ
- Mit Port verbundene ACL

Im Folgenden sehen Sie ein Beispiel für diese Befehlsausgabe, in dem die wichtigen Felder zur Klassifizierung hervorgehoben sind:

```
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
```

Hinweis: Für jedes Feld gibt es den konfigurierten Parameter und den Runtime-Parameter. Der Parameter, der auf das Paket angewendet wird, ist der Laufzeitparameter.

Überprüfen der ACL

Mithilfe des folgenden Befehls können Sie die angewendete und in früheren Befehlen angezeigte Zugriffskontrollliste überprüfen:

show qos acl info runtime *acl_name*

```
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
```

Fallstudien

Die folgenden Beispiele sind Beispielkonfigurationen für häufig auftretende Fälle, die in einem Netzwerk auftreten können.

Fall 1: Markierung am Edge

Nehmen Sie an, Sie konfigurieren einen Catalyst 6000, der als Access Switch verwendet wird und an den zahlreiche Benutzer mit Steckplatz 2 verbunden sind. Dies ist eine WS-X6348 Line Card (10/100M). Die Benutzer können Folgendes senden:

- Normaler Datenverkehr: Dies gilt immer für VLAN 100 und muss einen DSCP von "0" erhalten.
- Sprachdatenverkehr von einem IP-Telefon: Dies gilt immer für das Sprach-Hilfs-VLAN 101 und muss ein DSCP von "40" erhalten.
- Geschäftskritischer Anwendungsdatenverkehr: Dies ist auch in VLAN 100 enthalten und wird an den Server 10.10.10.20 weitergeleitet. Dieser Datenverkehr muss ein DSCP von "32" erhalten.

Da dieser Datenverkehr von der Anwendung nicht gekennzeichnet wird, lassen Sie den Port als nicht vertrauenswürdig und konfigurieren eine bestimmte ACL zur Klassifizierung des Datenverkehrs. Für VLAN 100 wird eine ACL und für VLAN 101 eine ACL angewendet. Sie müssen außerdem alle Ports als VLAN-basiert konfigurieren. Das folgende Beispiel zeigt die resultierende Konfiguration:

```
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
```

Fall 2: Trusting im Core mit nur einer Gigabit-Schnittstelle

Nehmen Sie an, Sie konfigurieren einen Catalyst 6000-Core mit nur einer Gigabit-Schnittstelle in Steckplatz 1 und Steckplatz 2 (keine 62xx- oder 63xx-Linecard im Chassis). Der Datenverkehr wurde zuvor korrekt von den Access Switches gekennzeichnet. Sie müssen daher keine erneute Markierung vornehmen, aber sicherstellen, dass Sie dem eingehenden DSCP vertrauen. Dies ist der einfachste Fall, da alle Ports als trust-dscp markiert werden und dies ausreichend sein sollte:

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

Fall 3: Trusting im Core mit einem 62xx- oder 63xx-Port im Chassis

Angenommen, Sie konfigurieren ein Core-/Distribution-Gerät mit einer Gigabit-Verbindung auf einer WS-X6416-GBIC-Linecard (in Steckplatz 2) und einer 10/100-Verbindung auf einer WS-X6348-Linecard (in Steckplatz 3). Sie müssen außerdem allen eingehenden Datenverkehr vertrauen, da dieser zuvor auf Access Switch-Ebene markiert wurde. Da Sie auf der 6348-Linecard kein trust-dscp ausführen können, ist es in diesem Fall am einfachsten, alle Ports als nicht vertrauenswürdig zu belassen und die Standard-ACL wie im folgenden Beispiel in trust-dscp zu ändern:

```
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
```

Zugehörige Informationen

- LAN-Produktunterstützung
- Unterstützung der LAN Switching-Technologie
- Technischer Support - Cisco Systems