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

Inhalt

Einführung

In diesem Dokument wird untersucht, was in Bezug auf die Kennzeichnung und Klassifizierung eines Pakets in den verschiedenen Phasen des Chassis des Cisco Catalyst 6500/6000, in dem die Cisco IOS® Software ausgeführt wird, geschieht. Dieses Dokument beschreibt Sonderfälle und Einschränkungen und enthält kurze Fallstudien.

Dieses Dokument enthält keine vollständige Liste aller Cisco IOS Software-Befehle, die sich auf QoS oder Marking beziehen. Weitere Informationen zur Cisco IOS Software Command-Line Interface (CLI) finden Sie unter Konfigurieren der PFC-QoS.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Hardwareversionen:

- Catalyst Switches der Serien 6500/6000 mit Cisco IOS Software und einer der folgenden Supervisor Engines:Eine Supervisor Engine 1A mit Policy Feature Card (PFC) und einer Multilayer Switch Feature Card (MSFC)Eine Supervisor Engine 1A mit PFC und MSFC2Eine Supervisor Engine 2 mit PFC2 und MSFC2

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Terminologie

Die Liste enthält Terminologie, die in diesem Dokument verwendet wird:

- Differentiated Services Code Point (DSCP) - Die ersten sechs Bit des ToS-Byte (Type of Service) im IP-Header. DSCP ist nur im IP-Paket vorhanden.**Hinweis:** Der Switch weist jedem Paket, ob IP oder Nicht-IP, ein internes DSCP zu. Im Abschnitt "Vier mögliche Quellen für internes DSCP" dieses Dokuments wird diese interne DSCP-Zuweisung beschrieben.
- IP Precedence (IP-Rangfolge): Die ersten drei Bit des ToS-Byte im IP-Header.
- Class of Service (CoS) - Das einzige Feld, das verwendet werden kann, um ein Paket auf Layer 2 (L2) zu kennzeichnen. CoS besteht aus einer der folgenden drei Bits:Die drei IEEE 802.1p-Bits (dot1p) im IEEE 802.1Q-Tag (dot1q) für das dot1q-Paket.**Hinweis:** Cisco Switches kennzeichnen standardmäßig keine nativen VLAN-Pakete.Die drei Bits mit der Bezeichnung "User Field" (Benutzerfeld) im Inter-Switch Link (ISL)-Header für ein ISL-gekapseltes Paket.**Hinweis:** CoS ist in einem nicht dot1q- oder ISL-Paket nicht vorhanden.
- Klassifizierung - Der Prozess zur Auswahl des zu markierenden Datenverkehrs.
- Marking (Markierung) - Der Prozess, der einen Layer 3 (L3)-DSCP-Wert in einem Paket festlegt. In diesem Dokument wird die Definition von Markierungen erweitert, sodass auch L2-CoS-Werte festgelegt werden.

Catalyst Switches der Serien 6500/6000 können Klassifizierungen anhand der folgenden drei

Parameter vornehmen:

- DSCP
- IP-Rangfolge
- CoS

Die Catalyst Switches der Serien 6500/6000 führen Klassifizierungen und Markierungen in verschiedenen Phasen durch. Dies geschieht an verschiedenen Orten:

- Eingangsport (ASIC (Ingress Application-Specific Integrated Circuit))
- Switching Engine (PFC)
- Ausgangsport (Ausgangs-ASIC)

Verarbeitung der Eingangsports

Der Hauptkonfigurationsparameter für den Eingangsport in Bezug auf die Klassifizierung ist der `Vertrauensstatus` des Ports. Jeder Port des Systems kann einen der folgenden `Trust`-Zustände aufweisen:

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

Führen Sie den folgenden Befehl der Cisco IOS Software im `Schnittstellenmodus aus`, um den Status "port `trust`" festzulegen oder zu ändern:

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

Hinweis: Standardmäßig befinden sich alle Ports im `nicht vertrauenswürdigen` Zustand, wenn QoS aktiviert ist. Um QoS auf dem Catalyst 6500 zu aktivieren, auf dem die Cisco IOS-Software ausgeführt wird, führen Sie den Befehl **mls qos** im Hauptkonfigurationsmodus aus.

Auf der Eingangsport-Ebene können Sie auch eine Standard-CoS pro Port anwenden. Hier ein Beispiel:

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

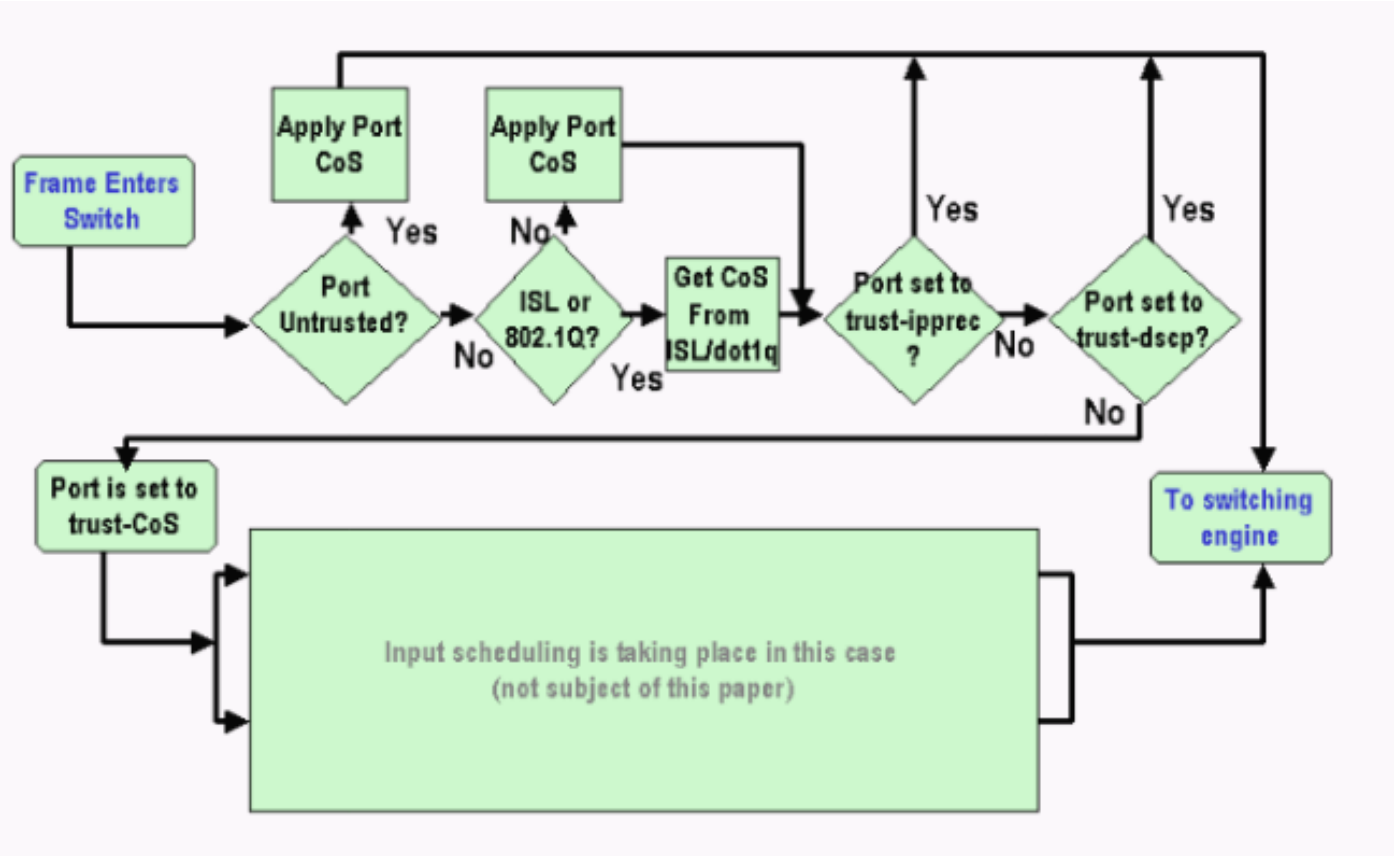
Diese Standard-CoS gilt für alle Pakete, z. B. IP und Internetwork Packet Exchange (IPX). Sie können die Standard-CoS auf jeden physischen Port anwenden.

Wenn sich der Port im `nicht vertrauenswürdigen` Zustand befindet, markieren Sie den Frame mit dem standardmäßigen CoS für den Port, und übergeben Sie den Header an die Switching Engine (PFC). Wenn der Port auf einen der `Vertrauensstatus` festgelegt ist, führen Sie eine der beiden folgenden Optionen aus:

- Wenn der Frame kein empfangenes CoS (dot1q oder ISL) hat, wenden Sie das Standard-Port-CoS an.
- Bei dot1q- und ISL-Frames behalten Sie die CoS so bei, wie sie ist.

Übergeben Sie dann den Frame an die Switching-Engine.

Dieses Beispiel veranschaulicht die Eingabeklassifizierung und -markierung. Das Beispiel zeigt, wie jedem Frame eine interne CoS zugewiesen wird:



Hinweis: Wie dieses Beispiel zeigt, wird jedem Frame eine interne CoS zugewiesen. Die Zuweisung basiert entweder auf dem empfangenen CoS oder dem Standard-Port-CoS. Die interne CoS enthält nicht getaggte Frames, die keine echte CoS tragen. Die interne CoS wird in einem speziellen Paket-Header geschrieben, der Datenbus-Header genannt wird, und wird über den Datenbus an die Switching-Engine gesendet.

Switching Engine (PFC)

Wenn der Header die Switching-Engine erreicht, weist die Switching Engine Enhanced Address Recognition Logic (EARL) jedem Frame ein internes DSCP zu. Dieses interne DSCP ist eine interne Priorität, die dem Frame vom PFC zugewiesen wird, während der Frame den Switch durchläuft. Dies ist nicht das DSCP im IP-Header Version 4 (IPv4). Das interne DSCP wird aus einer bestehenden CoS- oder ToS-Einstellung abgeleitet 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 geschaltet oder geroutet werden, auch Nicht-IP-Frames.

In diesem Abschnitt wird erläutert, wie Sie der Schnittstelle eine Dienstrichtlinie zuweisen können, um eine Markierung vorzunehmen. In diesem Abschnitt wird auch die endgültige Einstellung des internen DSCP beschrieben, die vom Port-`Vertrauensstatus` und der angewendeten Service-Richtlinie abhängt.

Konfigurieren der Service-Richtlinie zur Klassifizierung oder Markierung eines Pakets in Cisco IOS Software, Version 12.1(12c)E oder höher

Gehen Sie wie folgt vor, um die Service-Richtlinie zu konfigurieren:

1. Konfigurieren Sie eine Zugriffskontrollliste (ACL), um den zu berücksichtigenden Datenverkehr zu definieren.Die ACL kann nummeriert oder benannt werden, und der Catalyst 6500/6000 unterstützt eine erweiterte ACL. Geben Sie den Befehl **access-list *xxx*** Cisco IOS Software ein, wie im folgenden Beispiel gezeigt:
   ```
   (config)#access-list 101 permit ip any host 10.1.1.1
   ```

2. Konfigurieren Sie eine Datenverkehrsklasse (Klassenzuordnung) so, dass sie dem Datenverkehr auf der Grundlage der von Ihnen definierten oder auf der Grundlage des empfangenen DSCP entspricht.Geben Sie den Befehl **class-map** Cisco IOS Software ein. PFC QoS unterstützt nicht mehr als eine Übereinstimmungsanweisung pro Klassenzuordnung. Darüber hinaus unterstützt PFC QoS nur folgende Übereinstimmungsanweisungen:**match ip access-groupmatch ip dscpÜbereinstimmung IP-RangfolgeÜbereinstimmungsprotokollHinweis:** Der Befehl **match protocol** ermöglicht die Verwendung von Network Based Application Recognition (NBAR) zur Anpassung des Datenverkehrs.**Hinweis:** Von diesen Optionen werden nur die Anweisungen **match ip dscp** und **match ip priority** unterstützt und ausgeführt. Diese Aussagen sind jedoch für die Kennzeichnung oder Klassifizierung der Pakete nicht hilfreich. Mit diesen Anweisungen können Sie beispielsweise Richtlinien für alle Pakete festlegen, die einem bestimmten DSCP entsprechen. Diese Aktion geht jedoch über den Rahmen dieses Dokuments hinaus.
   ```
   (config)#class-map class-name
   (config-cmap)#match {access-group | input-interface | ip dscp}
   ```
   Hinweis: Dieses Beispiel zeigt nur drei Optionen für den Befehl **match**. Sie können jedoch an dieser Eingabeaufforderung viele weitere Optionen konfigurieren.**Hinweis:** Jede der Optionen in diesem **Match-**Befehl wird für die Anpassungskriterien übernommen, und die anderen Optionen werden je nach den eingehenden Paketen ausgelassen.Hier ein Beispiel:

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

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

3. Konfigurieren einer Richtlinienzuordnung zum Anwenden einer Richtlinie auf eine zuvor definierte KlasseDie Richtlinienzuordnung enthält:Ein NameEine Gruppe von KlassenanweisungenFür jede Klassenanweisung muss die für diese Klasse erforderliche Aktion ausgeführt werdenFolgende Aktionen werden in PFC1 und PFC2 QoS unterstützt:**dscp vertrauenTrust-IP-RangfolgeTreuhandkostenip dscp** in Cisco IOS Softwareversion 12.1(12c)E1 und höher **einstellenip priority** in Cisco IOS Software Release 12.1(12c)E1 und höher**PolizeiHinweis:** Diese Aktion wird in diesem Dokument nicht behandelt.
   ```
   (config)#policy-map policy-name
   (config-pmap)#class class-name
   (config-pmap-c)#{police | set ip dscp}
   ```

   Hinweis: Dieses Beispiel zeigt nur zwei Optionen, Sie können jedoch an dieser `(config-pmap-c)#`-Eingabeaufforderung viele weitere Optionen konfigurieren.Hier ein Beispiel:

   ```
   policy-map test_policy
    class TEST
      trust ip precedence
   ```

```
 class TEST2
   set ip dscp 16
```

4. Konfigurieren Sie eine Dienstrichtlinieneingabe, um eine Richtlinienzuordnung anzuwenden, die Sie zuvor auf eine oder mehrere Schnittstellen definiert haben.**Hinweis:** Sie können eine Service-Richtlinie entweder an die physische Schnittstelle oder an die Switch Virtual Interface (SVI)- oder VLAN-Schnittstelle anhängen. Wenn Sie eine Service-Richtlinie an eine VLAN-Schnittstelle anhängen, sind die einzigen Ports, die diese Service-Richtlinie verwenden, Ports, die zu diesem VLAN gehören und für VLAN-basierte QoS konfiguriert sind. Wenn der Port nicht für VLAN-basierte QoS festgelegt ist, verwendet der Port weiterhin die standardmäßige Port-basierte QoS und überprüft nur die Service-Richtlinie, die an die physische Schnittstelle angeschlossen ist.In diesem Beispiel wird die Service Policy `test_policy` auf den Gigabit Ethernet 1/1-Port angewendet:

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

   In diesem Beispiel wird die Service Policy `test_policy` auf alle Ports in VLAN 10 angewendet, die eine VLAN-basierte Konfiguration aus QoS-Sicht aufweisen:

```
(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
```

   Hinweis: Sie können die Schritte 2 und 3 dieses Verfahrens kombinieren, wenn Sie die spezifische Definition der Klasse überspringen und die ACL direkt in die Definition der Richtlinienzuordnung einfügen. Wenn in diesem Beispiel die `TEST-Klassenrichtlinie` vor der Konfiguration der Richtlinienzuordnung nicht definiert wurde, wird die Klasse in der Richtlinienzuordnung definiert:

```
(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
```

Konfigurieren der Service-Richtlinie zur Klassifizierung oder Markierung eines Pakets in Cisco IOS-Softwareversionen vor der Cisco IOS-Softwareversion 12.1(12c)E

In Cisco IOS Software-Versionen vor der Cisco IOS-Softwareversion 12.1(12c)E1 können Sie die **set ip dscp** nicht verwenden oder in einer Richtlinienzuordnung **ip priority** Action festlegen. Daher besteht die einzige Möglichkeit, eine Markierung für bestimmten Datenverkehr zu erstellen, die von einer Klasse definiert wird, in der Konfiguration eines Policers mit einer sehr hohen Rate. Diese Rate sollte z. B. mindestens die Leitungsrate des Ports oder etwas Hoch genug sein, um den gesamten Datenverkehr auf diese Policer zu übertragen. Verwenden Sie dann **set-dscp-send *xx*** **als** konforme Aktion. Führen Sie die folgenden Schritte aus, um diese Konfiguration einzurichten:

1. Konfigurieren Sie eine ACL, um den zu berücksichtigenden Datenverkehr zu definieren.Die ACL kann nummeriert oder benannt werden, und der Catalyst 6500/6000 unterstützt eine erweiterte ACL. Geben Sie den Befehl **access-list *xxx*** Cisco IOS Software ein, wie im folgenden Beispiel gezeigt:
   ```
   (config)#access-list 101 permit ip any host 10.1.1.1
   ```

2. Konfigurieren Sie eine Datenverkehrsklasse (Klassenzuordnung) so, dass sie mit dem Datenverkehr übereinstimmt, entweder anhand der von Ihnen definierten ACL oder anhand des empfangenen DSCP.Geben Sie den Befehl **class-map** Cisco IOS Software ein. PFC QoS unterstützt nicht mehr als eine Übereinstimmungsanweisung pro Klassenzuordnung. Darüber hinaus unterstützt PFC QoS nur folgende Übereinstimmungsanweisungen:**match ip access-groupmatch ip dscpÜbereinstimmung IP-RangfolgeÜbereinstimmungsprotokollHinweis:** Der Befehl **match protocol** ermöglicht die Verwendung von NBAR zur Anpassung des Datenverkehrs.**Hinweis:** Von diesen Anweisungen werden nur die Anweisungen **match ip dscp** und **match ip priority** unterstützt und ausgeführt. Diese Aussagen sind jedoch für die Kennzeichnung oder Klassifizierung der Pakete nicht hilfreich. Mit diesen Anweisungen können Sie beispielsweise Richtlinien für alle Pakete festlegen, die einem bestimmten DSCP entsprechen. Diese Aktion geht jedoch über den Rahmen dieses Dokuments hinaus.
   ```
   (config)#class-map  class-name
   (config-cmap)#match {access-group | input-interface | ip dscp}
   ```

   Hinweis: Dieses Beispiel zeigt nur drei Optionen für den Befehl **match**. Sie können jedoch an dieser Eingabeaufforderung viele weitere Optionen konfigurieren.Hier ein Beispiel:

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

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

3. Konfigurieren einer Richtlinienzuordnung zum Anwenden einer Richtlinie auf eine zuvor definierte KlasseDie Richtlinienzuordnung enthält:Ein NameEine Gruppe von KlassenanweisungenFür jede Klassenanweisung muss die für diese Klasse erforderliche Aktion ausgeführt werdenFolgende Aktionen werden in PFC1 oder PFC2 QoS unterstützt:**dscp vertrauenTrust-IP-RangfolgeTreuhandkostenPolizei**Sie müssen die **polizeiliche** Anweisung verwenden, da die Aktionen **set ip dscp** und **set ip priority** nicht unterstützt werden. Da Sie den Datenverkehr nicht wirklich überwachen, sondern nur markieren möchten, verwenden Sie eine Richtlinie, die definiert ist, um den gesamten Datenverkehr zuzulassen. Konfigurieren Sie daher die Policer mit einer hohen Rate und Burst. Sie können beispielsweise die Policer mit der maximal zulässigen Rate und Burst konfigurieren. Hier ein Beispiel:

   ```
   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. Konfigurieren Sie eine Dienstrichtlinieneingabe, um eine Richtlinienzuordnung anzuwenden, die Sie zuvor auf eine oder mehrere Schnittstellen definiert haben.**Hinweis:** Die Service-

Richtlinie kann entweder an eine physische Schnittstelle oder an die SVI- oder VLAN-Schnittstelle angeschlossen werden. Wenn eine Service-Richtlinie an eine VLAN-Schnittstelle angeschlossen ist, verwenden nur Ports, die zu diesem VLAN gehören und für VLAN-basierte QoS konfiguriert sind, diese Service-Richtlinie. Wenn der Port nicht für VLAN-basierte QoS festgelegt ist, verwendet der Port weiterhin die standardmäßige Port-basierte QoS und überprüft nur eine Service-Richtlinie, die an die physische Schnittstelle angeschlossen ist.In diesem Beispiel wird die Service Policy `test_policy` auf den Gigabit Ethernet 1/1-Port angewendet:

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

In diesem Beispiel wird die Service Policy `test_policy` auf alle Ports in VLAN 10 angewendet, die eine VLAN-basierte Konfiguration aus QoS-Sicht aufweisen:

```
(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 mögliche Quellen für internes DSCP

Das interne DSCP basiert auf einem der folgenden Elemente:

1. Ein bestehender empfangener DSCP-Wert, der festgelegt wird, bevor der Frame in den Switch gelangt.Ein Beispiel ist **trust dscp**.
2. Die empfangenen IP-Prioritätsbits, die bereits im IPv4-Header festgelegt sindDa es 64 DSCP-Werte und nur acht IP-Rangfolgewerte gibt, konfiguriert der Administrator eine Zuordnung, die der Switch zum Ableiten des DSCP verwendet. Für den Fall, dass der Administrator die Karten nicht konfiguriert, sind Standardzuordnungen vorhanden. Ein Beispiel hierfür ist die **Trust-IP-Rangfolge**.
3. Die empfangenen CoS-Bits, die bereits festgelegt wurden, bevor der Frame in den Switch eintritt, und die im Datenbus-Header gespeichert werden, oder, wenn im eingehenden Frame kein CoS vorhanden ist, vom Standard-CoS des eingehenden PortsWie bei der IP-Rangfolge gibt es maximal acht CoS-Werte, die jeweils einem der 64 DSCP-Werte zugeordnet werden müssen. Der Administrator kann diese Zuordnung konfigurieren, oder der Switch kann die bereits vorhandene Standardzuordnung verwenden.
4. Die Service-Richtlinie kann für das interne DSCP einen bestimmten Wert festlegen.

Für die Nummern 2 und 3 in dieser Liste ist die statische Zuordnung standardmäßig auf diese Weise:

- Für die CoS-zu-DSCP-Zuordnung entspricht das abgeleitete DSCP dem Achtfachen der CoS.
- Für die Zuordnung von IP-Rangfolge zu DSCP entspricht das abgeleitete DSCP dem Achtfachen der IP-Rangfolge.

Sie können diese Befehle ausgeben, um diese statische Zuordnung zu überschreiben und zu überprüfen:

- **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*

Der erste Wert des DSCP, der der Zuordnung für die CoS (oder IP-Rangfolge) entspricht, ist 0. Der zweite Wert für die CoS (oder die IP-Rangfolge) ist 1, und das Muster wird auf diese Weise fortgesetzt. Mit diesem Befehl wird z. B. die Zuordnung so geändert, dass der CoS 0 dem DSCP 0 und der CoS von 1 dem DSCP von 8 zugeordnet wird usw.:

```
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
```

Wie wird das interne DSCP gewählt?

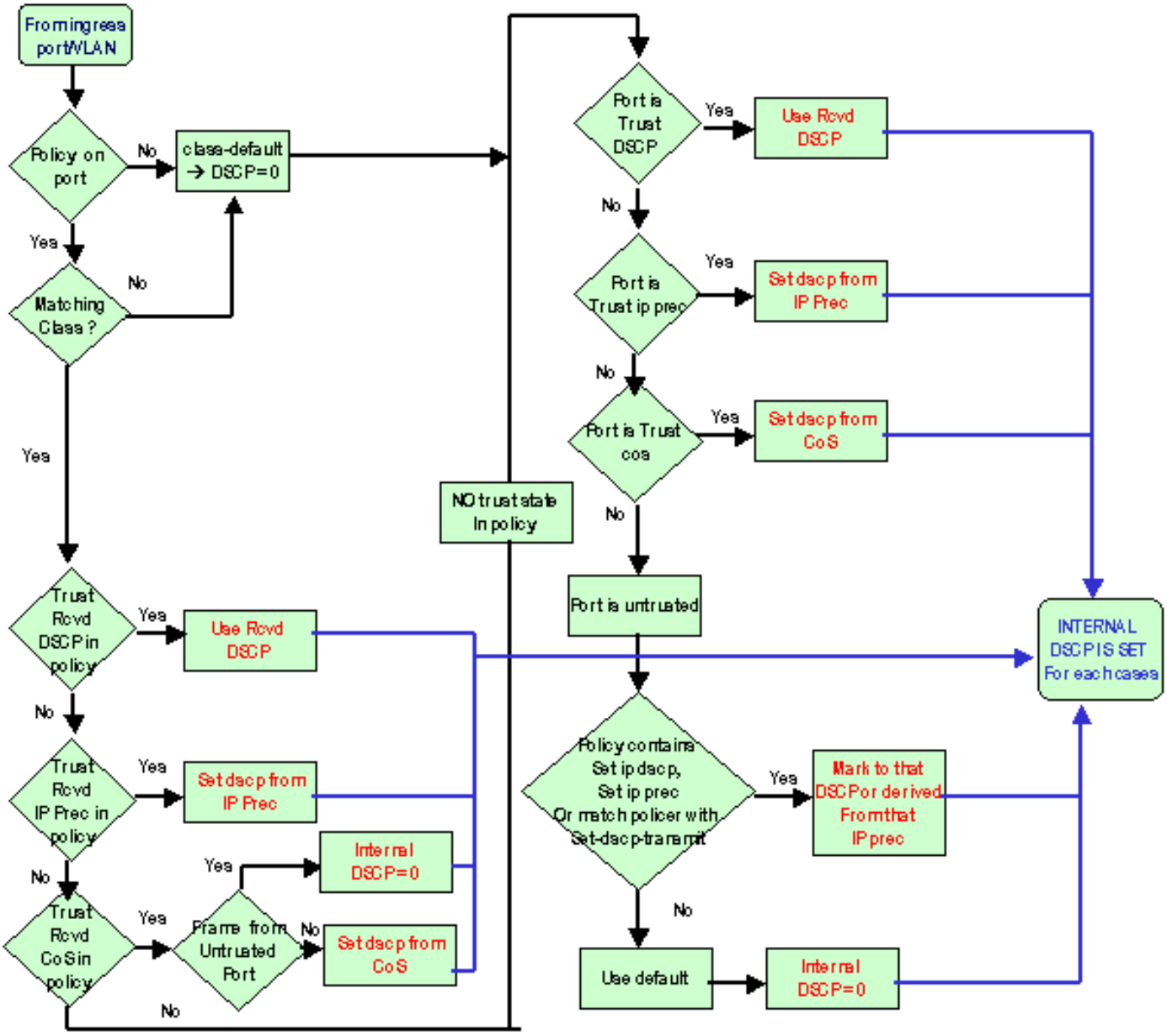
Das interne DSCP wird anhand der folgenden Parameter ausgewählt:

- Die auf das Paket angewendete QoS-RichtlinienzuordnungDie QoS-Richtlinienzuordnung wird durch folgende Regeln bestimmt:Wenn keine Service-Richtlinie an den eingehenden Port oder das VLAN angeschlossen ist, verwenden Sie die Standardeinstellung.**Hinweis:** Mit dieser Standardaktion wird das interne DSCP auf 0 festgelegt.Wenn eine Dienstrichtlinie an den eingehenden Port oder das eingehende VLAN angeschlossen ist und der Datenverkehr mit einer der Klassen übereinstimmt, die die Richtlinie definiert, verwenden Sie diesen Eintrag.Wenn eine Dienstrichtlinie an den eingehenden Port oder das eingehende VLAN angeschlossen ist und der Datenverkehr nicht mit einer der Klassen übereinstimmt, die die Richtlinie definiert, verwenden Sie die Standardeinstellung.
- Der `vertrauenswürdige` Zustand des Ports und die Aktion der RichtlinienzuordnungWenn der Port einen bestimmten `Vertrauenszustand` und eine Richtlinie mit einer bestimmten Markierung (gleichzeitiges vertrauenswürdiges Handeln) aufweist, gelten folgende Regeln:Der Befehl **set ip dscp** oder das in einer Richtlinienzuordnung per Richtlinie definierte DSCP wird nur angewendet, wenn der Port im `nicht vertrauenswürdigen` Zustand bleibt.Wenn der Port einen `vertrauenswürdigen` Zustand hat, wird dieser `vertrauenswürdige` Zustand zum Ableiten des internen DSCP verwendet. Der `vertrauenswürdige` Port-Status hat immer Vorrang vor dem Befehl **set ip dscp**.Der Befehl **trust** ***xx*** **in einer Richtlinienzuordnung hat Vorrang vor dem** `vertrauenswürdigen` Zustand des Ports.Wenn der Port und die Richtlinie einen anderen `Vertrauenszustand` enthalten, wird der `Vertrauenszustand` aus der Richtlinienzuordnung berücksichtigt.

Daher hängt das interne DSCP von folgenden Faktoren ab:

- Der Port `Trust`-Status
- Die Service-Richtlinie (mit Verwendung von ACL), die an den Port angeschlossen ist
- Die Standard-Richtlinienzuordnung**Hinweis:** DSCP wird standardmäßig auf 0 zurückgesetzt.
- Legt fest, ob VLAN-basiert oder Port-basiert in Bezug auf die ACL

In diesem Diagramm wird zusammengefasst, wie das interne DSCP anhand der Konfiguration ausgewählt wird:



Die PFC kann auch Richtlinien erstellen. Dies kann letztendlich zu einer Markierung des internen DSCP führen. Weitere Informationen zur Richtlinienvergabe finden Sie unter QoS Policing auf Catalyst Switches der Serien 6500 und 6000.

Verarbeitung von Ausgabeports

Sie können auf Ausgangsport-Ebene keine Änderungen an der Klassifizierung vornehmen. Kennzeichnen Sie das Paket jedoch anhand der folgenden Regeln:

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

Hinweis: Die CoS wird vom internen DSCP ausgehend von einem statischen Wert abgeleitet. Geben Sie diesen Befehl ein, um die statische Konfiguration durchzuführen:

```
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.
```

Die Standardkonfigurationen werden hier angezeigt. Standardmäßig ist CoS der ganze Teil des DSCP, geteilt durch acht. Geben Sie diesen Befehl ein, um die Zuordnung anzuzeigen und zu überprüfen:

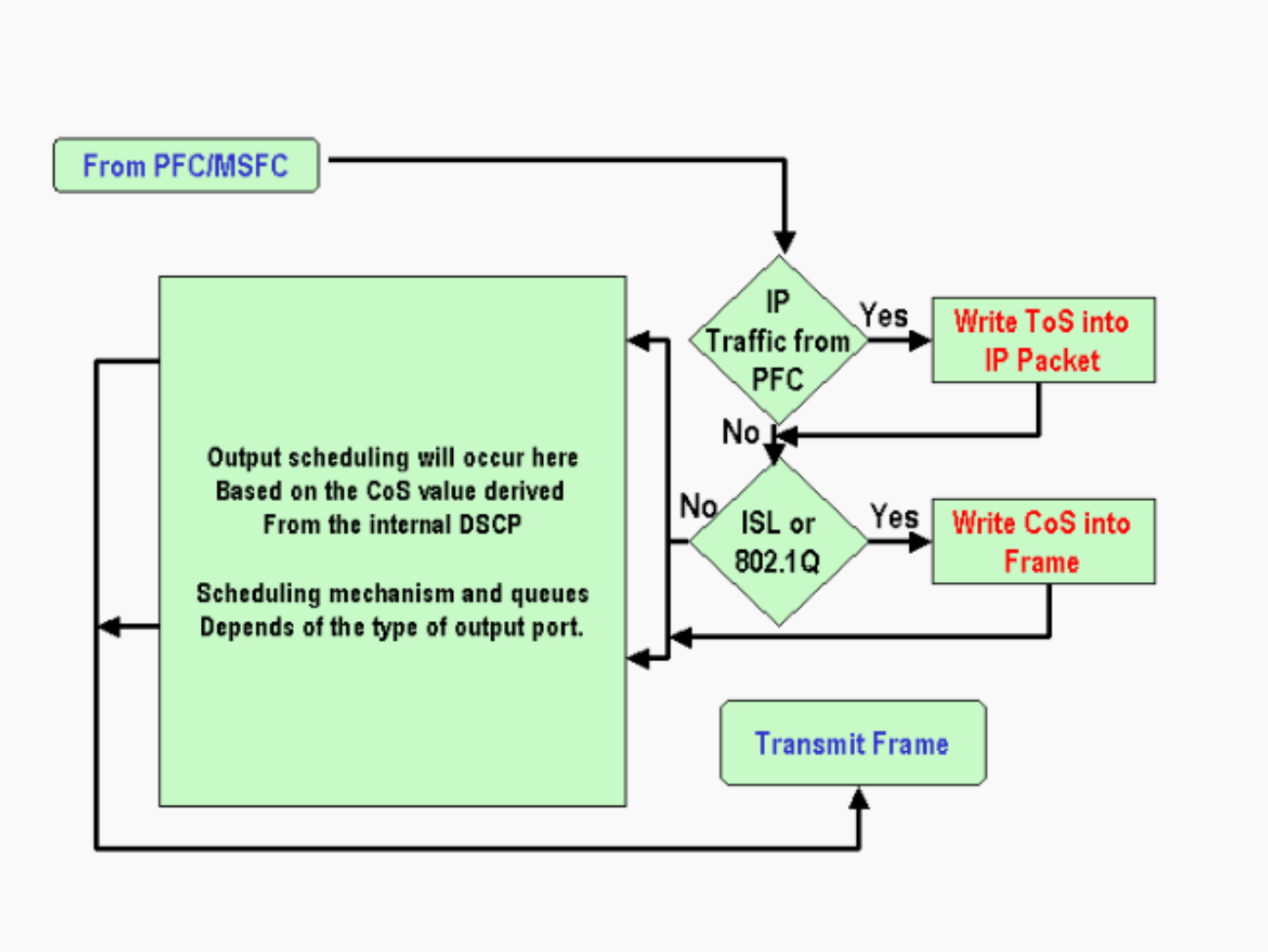
```
cat6k#show mls qos maps
...
  Dscp-cos map:                                     (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ------------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 02 02 02 02
      2 :    02 02 02 02 03 03 03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

Führen Sie zum Ändern dieser Zuordnung den folgenden Konfigurationsbefehl im normalen Konfigurationsmodus aus:

```
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
...
```

Nachdem das DSCP in den IP-Header geschrieben und die CoS vom DSCP abgeleitet wurde, wird das Paket zur Ausgabeplanung auf der Grundlage des CoS an eine der Ausgabewarteschlangen gesendet. Dies tritt auch dann auf, wenn es sich bei dem Paket nicht um einen dot1q oder eine ISL handelt. Weitere Informationen zur Planung von Ausgabewarteschlangen finden Sie unter QoS-Ausgabeplanung für Catalyst Switches der Serien 6500 und 6000 mit Cisco IOS-Systemsoftware.

Dieses Diagramm fasst die Verarbeitung des Pakets hinsichtlich der Kennzeichnung im Ausgabeport zusammen:



Hinweise und Einschränkungen

Die Standard-ACL

Die Standard-ACL verwendet "dscp 0" als Klassifizierungsschlüsselwort. Der gesamte Datenverkehr, der über einen nicht vertrauenswürdigen Port in den Switch gelangt und keinen Service-Richtlinieneintrag erfasst, wird mit dem DSCP 0 markiert, wenn QoS aktiviert ist. Derzeit können Sie die Standard-ACL in der Cisco IOS-Software nicht ändern.

Hinweis: In der Catalyst OS (CatOS)-Software können Sie dieses Standardverhalten konfigurieren und ändern. Weitere Informationen finden Sie im Abschnitt *Default ACL (Standard-ACL)* der QoS-Klassifizierung und -Kennzeichnung auf Catalyst Switches der Serien 6500/6000 mit CatOS-Software.

Einschränkungen der Linecards WS-X61xx, WS-X6248-xx, WS-X6224-xx und WS-X6348-xx

Dieser Abschnitt betrifft nur die folgenden Linecards:

- WS-X6224-100FX-MT: Catalyst 6000 24-Port 100 FX Multimode
- WS-X6248-RJ-45: Catalyst 6000 RJ-45-Modul mit 48 10/100-Ports
- WS-X6248-TEL: Catalyst 6000 10/100-Telco-Modul mit 48 Ports

- WS-X6248A-RJ-45: Catalyst 6000 mit 48 10/100-Ports, Enhanced QoS
- WS-X6248A-TEL: Catalyst 6000 mit 48 10/100-Ports, Enhanced QoS
- WS-X6324-100FX-MM: Catalyst 6000, 24 Ports, 100 FX, erweiterte QoS, MT
- WS-X6324-100FX-SM: Catalyst 6000, 24 Ports, 100 FX, erweiterte QoS, MT
- WS-X6348-RJ-45: Catalyst 6000 mit 48 10/100-Ports, Enhanced QoS
- WS-X6348-RJ21V: Catalyst 6000, 48 10/100-Ports, Inline-Stromversorgung
- WS-X6348-RJ45V: Catalyst 6000 mit 48 10/100-Ports, Enhanced QoS, Inline-Stromversorgung
- WS-X6148-RJ21V: Catalyst 6500, 48 10/100-Ports, Inline-Stromversorgung
- WS-X6148-RJ45V: Catalyst 6500, 48 10/100-Ports, Inline-Stromversorgung

Diese Line Cards haben eine Einschränkung. Auf Portebene können Sie den `Vertrauenszustand` nicht mithilfe eines der folgenden Schlüsselwörter konfigurieren:

- `trust-dscp`
- `Trust-Ipprec`
- `Treuhandkosten`

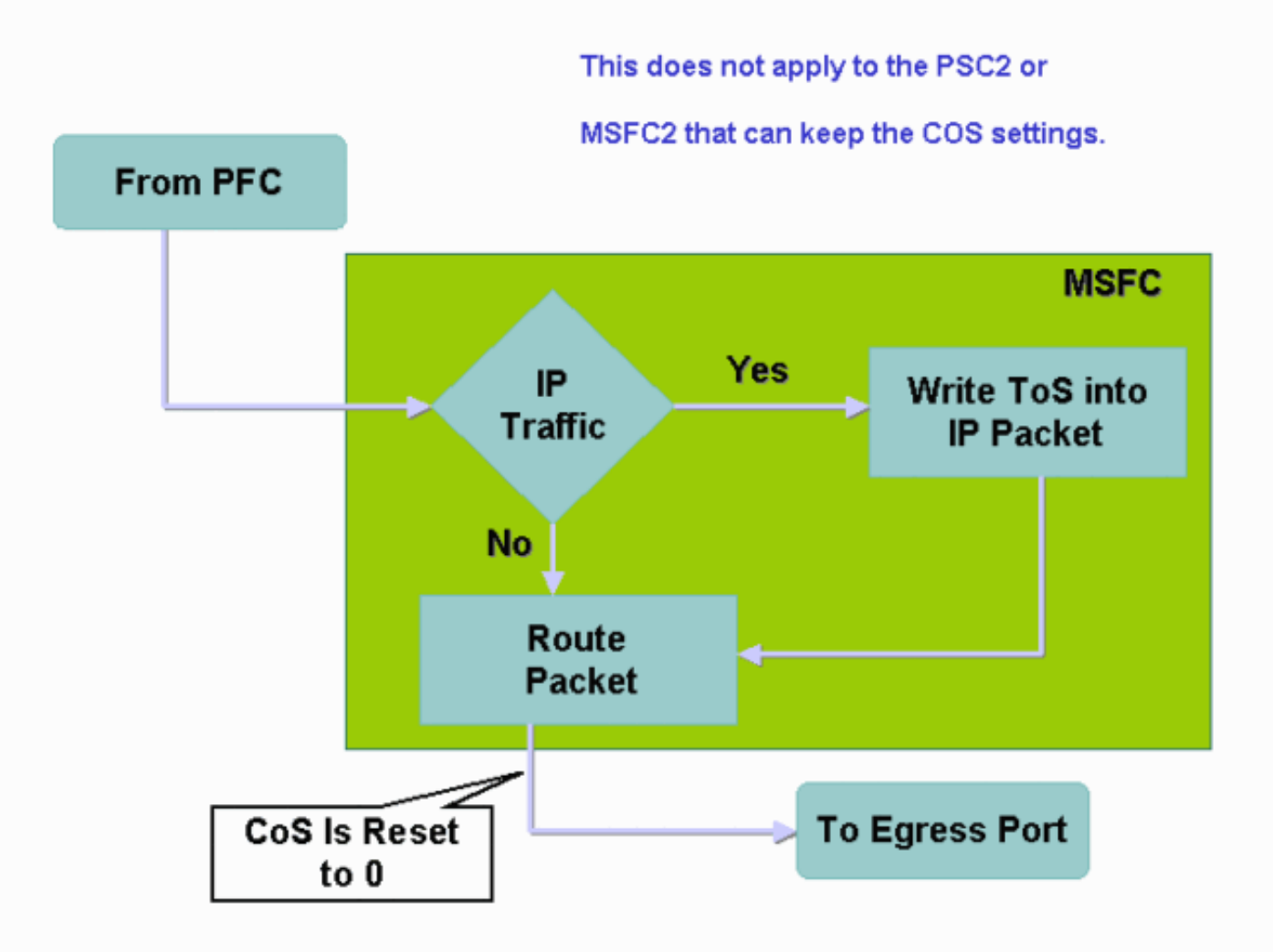
Sie können nur den `nicht vertrauenswürdigen` Zustand verwenden. Bei jedem Versuch, einen `vertrauenswürdigen` Zustand auf einem dieser Ports zu konfigurieren, wird eine der folgenden Warnmeldungen angezeigt:

```
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.
```

Wenn ein vertrauenswürdiger Frame auf einer solchen Linecard eingehen soll, müssen Sie eine Service-Richtlinie an den Port oder das VLAN anhängen. Verwenden Sie die Methode in Fall 1: Markieren im Abschnitt Edge dieses Dokuments

Pakete, die von MSFC1 oder MSFC2 auf der Supervisor Engine 1A/PFC stammen

Alle Pakete, die von MSFC1 oder MSFC2 stammen, haben eine CoS von 0. Beim Paket kann es sich entweder um ein softwaregeroutetes Paket oder um ein Paket handeln, das von der MSFC ausgegeben wird. Dies ist eine Einschränkung der PFC, da die CoS aller Pakete aus der MSFC zurückgesetzt wird. Die DSCP- und die IP-Rangfolge werden weiterhin beibehalten. PFC2 hat diese Einschränkung nicht. Die vorhandene CoS des PFC2 entspricht der IP-Priorität des Pakets.



Zusammenfassung der Klassifizierung

Die Tabellen in diesem Abschnitt zeigen das DSCP, das auf der Grundlage der folgenden Klassifizierungen ermittelt:

- Der `Vertrauensstatus` des eingehenden Ports
- Das Klassifizierungsschlüsselwort in der angewendeten ACL

Diese Tabelle enthält eine allgemeine Zusammenfassung für alle Ports mit Ausnahme von WS-X62xx und WS-X63xx:

Policy Map-Schlüsselwort Port Trust-Status	set-ip-dscp xx oder set-dscp-send xx	trust-dscp	Trust-Ipprec	Treuhandkosten
nicht vertrauenswürdig	xx[1]	Rx[2] 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
Treuhandkosten	Abgeleitet von Rx CoS oder Port CoS	Rx DSCP	Abgeleitet von Rx ipprec	Abgeleitet von Rx CoS oder Port CoS

[1] Nur so kann eine neue Markierung eines Frames erstellt werden.

[2] x = empfangen

Diese Tabelle enthält eine Zusammenfassung der Ports WS-X61xx, WS-X62xx und WS-X63xx:

Policy Map-Schlüsselwort **Port Trust-Status**	**set-ip-dscp xx oder set-dscp-send xx**	**trust-dscp**	**Trust-Ipprec**	**Treuhandkosten**
nicht vertrauenswürdig	xx	Rx DSCP	Abgeleitet von Rx ipprec	0
trust-dscp	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Trust-Ipprec	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Treuhandkosten	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

Überwachen und Überprüfen einer Konfiguration

Überprüfen der Portkonfiguration

Führen Sie den Befehl **show queuing interface *interface-id* aus, um die Porteinstellungen und -konfigurationen zu überprüfen.**

Wenn Sie diesen Befehl ausgeben, können Sie unter anderem folgende Klassifizierungsparameter überprüfen:

- Ob Port- oder VLAN-basiert
- Der `vertrauenswürdige` Porttyp
- Die ACL, die an den Port angeschlossen ist

Hier ein Beispiel für diese Befehlsausgabe. Die wichtigen Felder für die Klassifizierung werden in Fettschrift angezeigt:

```
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]:
```

Die Ausgabe zeigt, dass die Konfiguration dieses bestimmten Ports mit `Vertrauenscodes` auf Portebene erfolgt. Außerdem ist der Standard-Port CoS 0.

Definierte Klassen überprüfen

Geben Sie den Befehl **show class-map** aus, um die definierten Klassen zu überprüfen. Hier ein Beispiel:

```
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)
```

Überprüfen der Richtlinienzuordnung, die auf eine Schnittstelle angewendet wird

Führen Sie die folgenden Befehle aus, um die Richtlinienzuordnung zu überprüfen, die in den vorherigen Befehlen angewendet und angezeigt wird:

- **show mls qos ip interface** *interface-id*
- **show policy-map interface** *interface-id*

Hier einige Beispiele für die Ausgabe der folgenden Befehle:

```
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
```

Hinweis: Sie können sich die folgenden Felder zur Klassifizierung ansehen:

- `Class-map`: Gibt an, welche Klasse an die Dienstrichtlinie angefügt ist, die an diese Schnittstelle angehängt ist.
- `Trust` (`Vertrauen`): Gibt an, ob die Polizeiaktion in dieser Klasse einen **Trust**-Befehl enthält und was in der Klasse vertrauenswürdig ist.
- `DSCP`: Gibt das DSCP an, das für die Pakete übertragen wird, die diese Klasse erreichen.

```
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
```

Fallstudien

Dieser Abschnitt enthält Beispielkonfigurationen für häufige Fälle, die in einem Netzwerk angezeigt werden können.

Fall 1: Markierung am Edge

Angenommen, Sie konfigurieren einen Catalyst 6000, der als Access Switch verwendet wird. Viele Benutzer stellen eine Verbindung zum Switch-Steckplatz 2 her, bei dem es sich um eine WS-X6348 Line Card (10/100 Mbit/s) handelt. Die Benutzer können Folgendes senden:

- Normal Data Traffic (Normaler Datenverkehr): Dieser Datenverkehr läuft immer im VLAN 100 und muss einen DSCP von 0 erhalten.
- Sprachdatenverkehr von einem IP-Telefon - Dieser Datenverkehr befindet sich immer im Sprach-AUX-VLAN 101 und benötigt ein DSCP von 46.
- Geschäftskritischer Anwendungsdatenverkehr - Dieser Datenverkehr kommt ebenfalls in VLAN 100 und wird an den Server 10.10.10.20 weitergeleitet. Dieser Datenverkehr muss ein DSCP von 32 erhalten.

Die Anwendung kennzeichnet keinen dieser Datenverkehr. Lassen Sie den Port daher als `nicht vertrauenswürdig`, und konfigurieren Sie eine spezifische ACL zur Klassifizierung des Datenverkehrs. Eine ACL wird auf VLAN 100 und eine ACL auf VLAN 101 angewendet. Sie müssen außerdem alle Ports als VLAN-basiert konfigurieren. Im Folgenden finden Sie ein Beispiel für eine Konfiguration, die Folgendes bewirkt:

```
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
```

Fall 2: Vertrauen in den Core mit nur Gigabit Ethernet-Schnittstellen

Nehmen Sie an, Sie konfigurieren einen Catalyst 6000-Core nur mit einer Gigabit Ethernet-Schnittstelle in Steckplatz 1 und Steckplatz 2. Die Access Switches haben den Datenverkehr zuvor korrekt markiert. Daher müssen Sie keine weiteren Markierungen vornehmen. Sie müssen jedoch sicherstellen, dass der Core-Switch dem eingehenden DSCP vertrauenswürdig ist. Dies ist der einfachere Fall, da alle Ports als `trust-dscp` gekennzeichnet sind, was ausreichend sein sollte:

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

Zugehörige Informationen

- Quality of Service auf Catalyst Switches der Serie 6000
- QoS-Klassifizierung und -Kennzeichnung für Catalyst Switches der Serien 6500 und 6000 mit CatOS-Software
- LAN-Produktunterstützung
- Unterstützung der LAN Switching-Technologie
- Technischer Support und Dokumentation - Cisco Systems