執行Cisco IOS軟體的Catalyst 6500/6000系列交換器上的QoS分類和標籤

目錄

簡介

本檔案將檢視執行Cisco IOS®軟體的Cisco Catalyst 6500/6000機箱內各個階段封包標籤和分類時發生的情況。本文描述特殊情況和限制，並提供簡短案例研究。

本檔案未提供所有與QoS或標籤相關的Cisco IOS軟體命令的詳盡清單。有關Cisco IOS軟體命令列介面(CLI)的詳細資訊，請參閱配置PFC QoS。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據以下硬體版本：

- 執行Cisco IOS軟體並使用以下Supervisor引擎之一的Catalyst 6500/6000系列交換器：具有原則功能卡(PFC)和多層交換功能卡(MSFC)的Supervisor引擎1A具有PFC和MSFC2的Supervisor引擎1A搭載PFC2和MSFC2的Supervisor引擎2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

技術

此清單提供本檔案使用的術語：

- 區別服務代碼點(DSCP)- IP報頭中服務型別(ToS)位元組的前六位。DSCP僅存在於IP資料包中。**注意**：交換機還會為每個資料包（無論是IP資料包還是非IP資料包）分配一個內部DSCP。本文檔的內部DSCP的四種可能來源部分詳細介紹了此內部DSCP分配。
- IP優先順序 — IP報頭中ToS位元組的前三個位。
- 服務類別(CoS) — 可用於在第2層(L2)標籤資料包的唯一欄位。 CoS由以下三個位元中的任何一個組成：dot1q資料包的IEEE 802.1Q(dot1q)標籤中的三個IEEE 802.1p(dot1p)位。**注意**：預設情況下，思科交換機不標籤本地VLAN資料包。ISL封裝封包的交換器間連結(ISL)標頭中稱為「使用者欄位」的三位元。**註**：非dot1q或ISL資料包中不存在CoS。
- 分類 — 用於選擇要標籤的流量的流程。
- 標籤 — 在資料包中設定第3層(L3)DSCP值的過程。本文檔擴展了標籤的定義，以包括L2 CoS值的設定。

Catalyst 6500/6000系列交換器可以基於以下三個引數作出分類：

- DSCP
- IP優先順序
- CoS

Catalyst 6500/6000系列交換器在不同的階段執行分類和標籤。不同地方的情況如下：

- 輸入連線埠（輸入特定應用積體電路[ASIC]）
- 交換引擎(PFC)
- 輸出埠（輸出ASIC）

輸入連線埠處理

輸入連線埠的主要組態引數（關於分類）是連線埠的狀態。系統的每個埠都可以具有以下狀態之一

：

- trust-ip-precedence
- trust-dscp
- trust-cos
-

若要設定或更改連線埠狀態，請在Cisco IOS命令：

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

注意：預設情況下，啟用QoS時，所有都處於不可信狀態。要在執行Cisco IOS軟體的Catalyst 6500上啟用QoS，請在主組態模式下發出**mls qos**命令。

在輸入埠級別，您還可以為每個埠應用預設CoS。以下是範例：

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

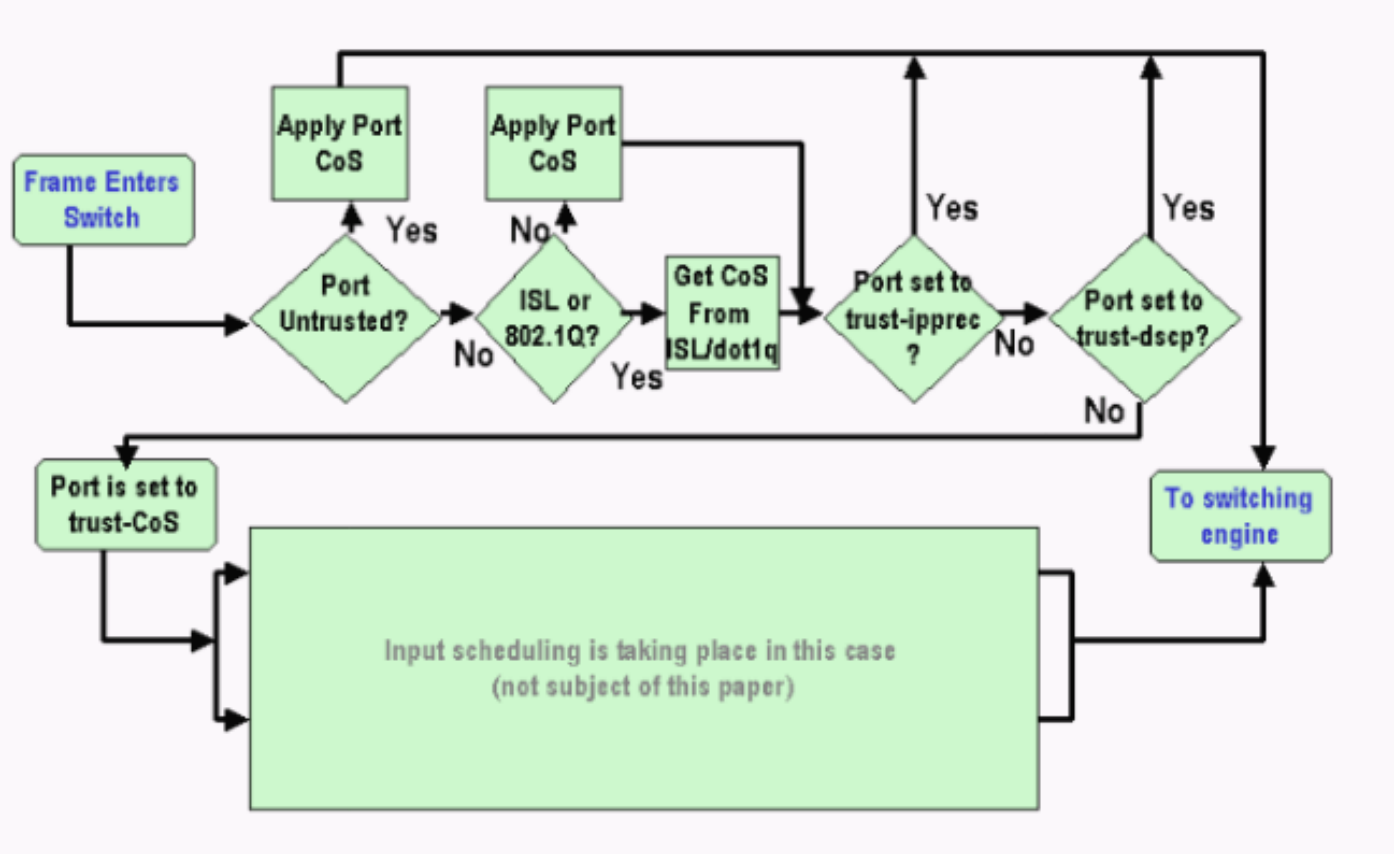
此預設CoS適用於所有封包，例如IP和網際網路封包交換(IPX)。 您可以將預設CoS應用於任何物理埠。

如果埠處於untrusted狀態，請使用埠預設CoS標籤幀，並將報頭傳遞給交換引擎(PFC)。 如果連線埠設定為狀態之一，請執行以下兩個選項之一：

- 如果幀沒有收到的CoS（dot1q或ISL），則應用預設埠CoS。
- 對於dot1q和ISL幀，保持CoS不變。

然後，將幀傳遞到交換引擎。

此示例說明輸入分類和標籤。此示例說明如何為每個幀分配內部CoS:



注意：如以下示例所示，每個幀都分配了一個內部CoS。分配基於接收的CoS或預設埠CoS。內部CoS包括不帶任何實際CoS的無標籤幀。內部CoS被寫入稱為資料匯流排報頭的特殊資料包報頭，並通過資料匯流排傳送到交換引擎。

交換引擎(PFC)

當報頭到達交換引擎時，交換引擎增強地址識別邏輯(EARL)會為每個幀分配一個內部DSCP。此內部DSCP是PFC在幀經過交換機時分配給幀的內部優先順序。這不是IP第4版(IPv4)標頭中的DSCP。內部DSCP從現有的CoS或ToS設定中匯出，用於在幀退出交換機時重置CoS或ToS。此內部DSCP分配給由PFC交換或路由的所有幀，甚至是非IP幀。

本節討論如何向介面分配服務策略以進行標籤。本節還討論內部DSCP的最終設定，具體取決於埠信任狀態和應用的服務策略。

在Cisco IOS軟體版本12.1(12c)E及更高版本中配置服務策略以分類或標籤資料包

完成以下步驟以配置服務策略：

1. 設定存取控制清單(ACL)，以定義您要考慮的流量。ACL可以是編號或命名，Catalyst 6500/6000支援擴展ACL。發出**access-list *xxx*** Cisco IOS軟體命令，如以下範例所示：
```
(config)#access-list 101 permit ip any host 10.1.1.1
```

2. 根據您定義的ACL或收到的DSCP配置流量類（類對映），以匹配流量。發出**class-map** Cisco IOS Software命令。PFC QoS不支援每個類對映多條match語句。此外，PFC QoS僅支援以下匹配語句：**match ip access-groupmatch ip dscpmatch ip precedencematch protocol注意：match protocol命令允許使用基於網路的應用識別(NBAR)來匹配流量。注意：**在這些選項中，僅支援**match ip dscp**和**match ip precedence語句**，並且這些語句有效。但是，這些語句在資料包的標籤或分類中不起作用。例如，可以使用這些語句對匹配特定DSCP的所有資料包進

行管制。但是，此操作不在本檔案的範圍之內。

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

注意：此示例僅顯示match命令的**三個**選項。但是您可以在此命令提示符下配置更多選項。**注意：**此match命令中的任何一個選項均用於匹配條件，而其它選項則根據傳入資料包被省略。以下是範例：

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

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

3. 配置策略對映，將策略應用到您先前定義的類。策略對映包含：名稱一組類語句對於每個類語句，需要為該類執行的操作PFC1和PFC2 QoS中支援的操作包括：**信任dscp信任ip優先順序信任cos**Cisco **IOS軟體**版本12.1(12c)E1和更新版本中的set ip dscp**在**Cisco **IOS軟體**版本12.1(12c)E1和更新版本中設定ip優先順序**警察注意：**此操作不屬於本文檔的範圍。

```
(config)#policy-map policy-name
(config-pmap)#class class-name
(config-pmap-c)#{police | set ip dscp}
```

注意：此示例只顯示兩個選項，但是您可以在此(config-pmap-c)#的選項。以下是範例：

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

4. 配置服務策略輸入，將先前定義的策略對映應用於一個或多個介面。**注意：**您可以將服務策略連線到物理介面、交換虛擬介面(SVI)或VLAN介面。如果將服務策略連線到VLAN介面，則使用此服務策略的埠只有屬於該VLAN且配置為基於VLAN的QoS的埠。如果埠未設定為基於VLAN的QoS，則該埠仍使用預設基於埠的QoS，並且只檢視附加到物理介面的服務策略。此範例將服務原則test_policy套用到連線埠Gigabit Ethernet 1/1:

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

此範例將服務原則test_policy套用到VLAN 10中從QoS角度具有基於VLAN組態的所有連線埠：

```
(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
```

注意：如果跳過類的特定定義並在策略對映的定義中直接附加ACL，則可以合併此過程中的步驟2和步驟3。在本示例中，如果在配置策略對映之前尚未定義TEST police類，則會在策略對映內定義該類：

```
(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
```

在低於Cisco IOS軟體版本12.1(12c)E的Cisco IOS軟體版本中配置服務策略以分類或標籤資料包

在低於Cisco IOS軟體版本12.1(12c)E1的Cisco IOS軟體版本中，不能在策略對映中使用**set ip dscp**或**set ip precedence**操作。因此，對類定義的特定流量進行標籤的唯一方法是使用非常高的速率配置監察器。例如，此速率應至少是埠的線路速率，或足夠高以允許所有流量到達該管制器。然後，使用**set-dscp-transmit *xx*** 作為conform操作。請依照以下步驟操作，以設定此組態：

1. 配置ACL以定義要考慮的流量。ACL可以是編號或命名，Catalyst 6500/6000支援擴展ACL。發出**access-list *xxx*** Cisco IOS軟體命令，如以下範例所示：
   ```
   (config)#access-list 101 permit ip any host 10.1.1.1
   ```

2. 根據您定義的ACL或收到的DSCP配置流量類（類對映），以匹配流量。發出**class-map** Cisco IOS Software命令。PFC QoS不支援每個類對映多條match語句。此外，PFC QoS僅支援以下匹配語句：**match ip access-groupmatch ip dscpmatch ip precedencematch protocol注意：match protocol命令允許使用NBAR來匹配流量。注意：**在這些語句中，僅支援**match ip dscp**和**match ip precedence語句，這些語句可**以正常工作。但是，這些語句在標籤資料包或對其進行分類時沒有用處。例如，可以使用這些語句對匹配特定DSCP的所有資料包進行管制。但是，此操作不在本檔案的範圍之內。
   ```
   (config)#class-map  class-name
   (config-cmap)#match {access-group | input-interface | ip dscp}
   ```

   注意：此示例僅顯示**match**命令的**三個**選項。但是您可以在此命令提示符下配置更多選項。以下是範例：

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

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

3. 配置策略對映，將策略應用到您先前定義的類。策略對映包含：名稱一組類語句對於每個類語句，需要為該類執行的操作PFC1或PFC2 QoS中支援的操作包括：**信任dscp信任ip優先順序信任cos警察**因為不支援**set ip dscp**和**set ip precedence**操作，所以必須使用**police**語句。因為您實際上並不想管制流量，而只是想標籤流量，所以請使用定義為允許所有流量的管制器。因此，請為監察器配置較大的速率和突發量。例如，可以使用允許的最大速率和突發配置監察器。以下是範例：

   ```
   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. 配置服務策略輸入，將先前定義的策略對映應用於一個或多個介面。**注意：**服務策略可以附加到物理介面或SVI或VLAN介面。如果服務策略連線到VLAN介面，則只有屬於該VLAN且配置為基於VLAN的QoS的埠才使用此服務策略。如果埠未設定為基於VLAN的QoS，則該埠仍使用預設基於埠的QoS，並且只檢視附加到物理介面的服務策略。此範例將服務原則`test_policy`套

用到連線埠Gigabit Ethernet 1/1:

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

此範例將服務原則test_policy套用到VLAN 10中從QoS角度具有基於VLAN組態的所有連線埠：

```
(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
```

內部DSCP的四種可能來源

內部DSCP源於以下其中一項：

1. 在幀進入交換機之前設定的現有已接收DSCP值例如**trust dscp**。
2. 收到的IPv4報頭中已設定的IP優先順序位因為有64個DSCP值而只有8個IP優先順序值，所以管理員配置一個對映，交換機使用該對映匯出DSCP。如果管理員未配置對映，則預設對映就位。例如**trust ip precedence**。
3. 接收的CoS位，在幀進入交換機之前已設定，儲存在資料匯流排報頭中，或者如果傳入幀中沒有來自傳入埠的預設CoS的CoS與IP優先順序一樣，最多有八個CoS值，每個值必須對映到64個DSCP值之一。管理員可以配置此對映，或者交換機可以使用預設對映。
4. 服務策略可以將內部DSCP設定為特定值。

對於此清單中的數字2和3，預設情況下靜態對映為：

- 對於CoS到DSCP對映，匯出的DSCP等於CoS的八倍。
- 對於IP優先順序到DSCP對映，派生的DSCP等於IP優先順序的八倍。

您可以發出以下命令以覆寫和驗證此靜態對應：

- **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*

與CoS（或IP優先順序）的對映對應的DSCP的第一個值為0。CoS（或IP優先順序）的第二個值為1，模式以這種方式繼續。例如，此命令更改對映，以便將CoS 0對映到DSCP 0，並將CoS的1對映到DSCP 8，等等：

```
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
```

如何選擇內部DSCP?

內部DSCP是根據以下引數選擇的：

- 應用於資料包的QoS策略對映QoS策略對映由以下規則確定：如果未將任何服務策略附加到傳入埠或VLAN，則使用預設值。**注意**：此預設操作是將內部DSCP設定為0。如果服務策略連線

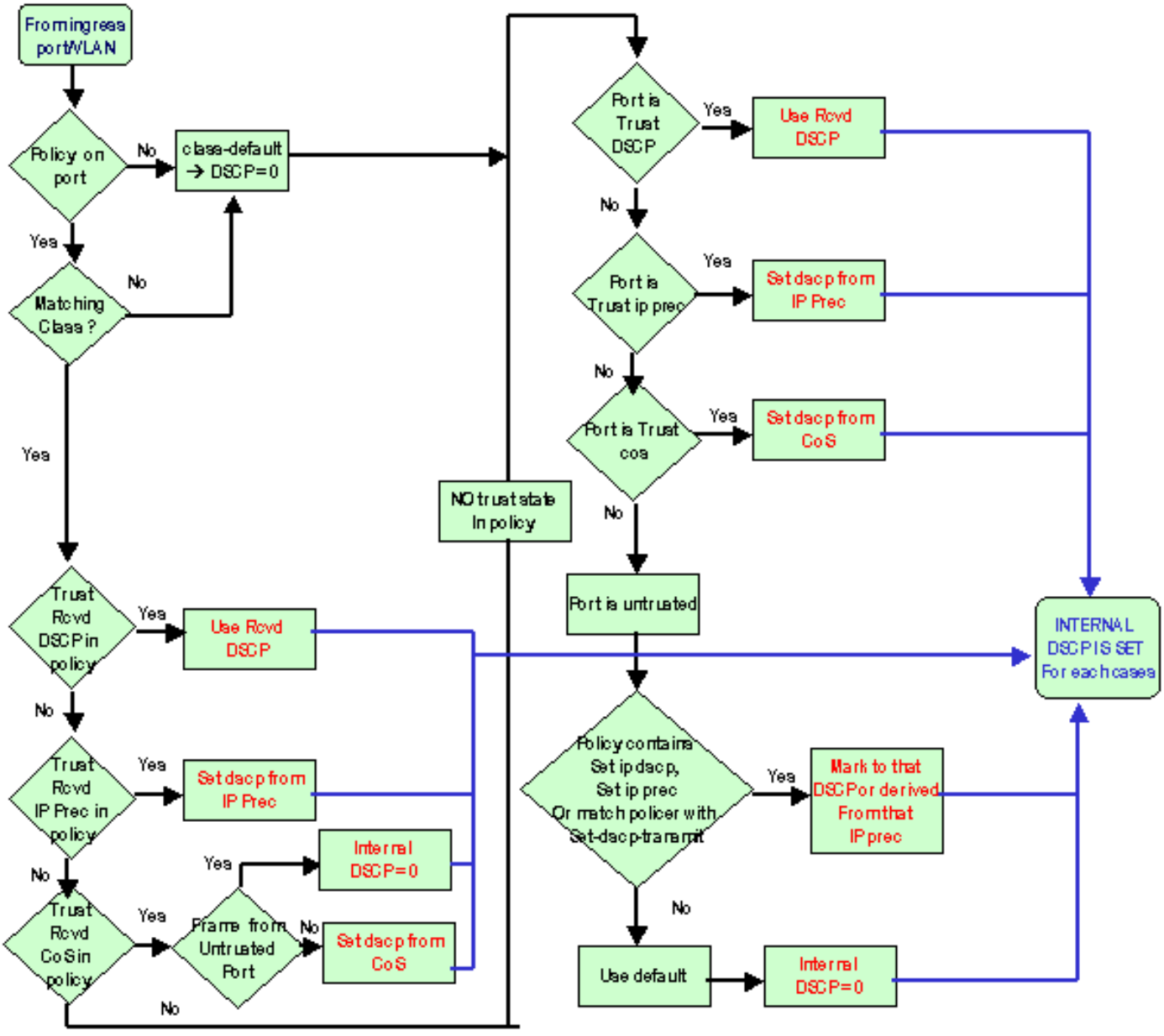
到傳入埠或VLAN，且流量與策略定義的某個類匹配，則使用此條目。如果服務策略連線到傳入埠或VLAN，且流量與策略定義的某個類不匹配，則使用預設值。

- 埠的trust狀態和策略對映的操作當埠具有特定的狀態和具有特定標籤（同時信任操作）的策略時，將應用以下規則：僅當埠處於不可信狀態時，才應用策略對映中每個策略器定義的**set ip dscp**命令或DSCP。如果埠具有狀態，則此狀態用於派生內部DSCP。port trust狀態一律優先於**set ip dscp**命令。策略對映中的**trust *xx***命令優先於埠信態。如果埠和策略包含不同的狀態，則會考慮來自策略對映的

因此，內部DSCP取決於以下因素：

- 埠信態
- 附加到埠的服務策略（使用ACL）
- 預設策略對映**注意**：預設設定會將DSCP重置為0。
- 針對ACL是基於VLAN還是基於埠

此圖總結了如何根據配置選擇內部DSCP:



PFC還可以執行策略管理。這最終可能導致內部DSCP降級。如需更多有關原則制定的資訊，請參閱Catalyst 6500/6000系列交換器上的QoS原則制定。

輸出埠處理

不能在輸出連線埠層級執行任何操作來變更分類。但是，根據以下規則標籤資料包：

- 如果該資料包是IPv4資料包，請將交換引擎分配的內部DSCP複製到IPv4報頭的ToS位元組中。
- 如果輸出埠配置為ISL或dot1q封裝，請使用從內部DSCP派生的CoS。複製ISL或dot1q幀中的CoS。

註：CoS根據靜態從內部DSCP匯出。發出以下命令以設定靜態：

```
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.
```

預設配置將顯示在此處。預設情況下，CoS是DSCP的整數部分，除以八。核發此命令，以便檢視和驗證對應：

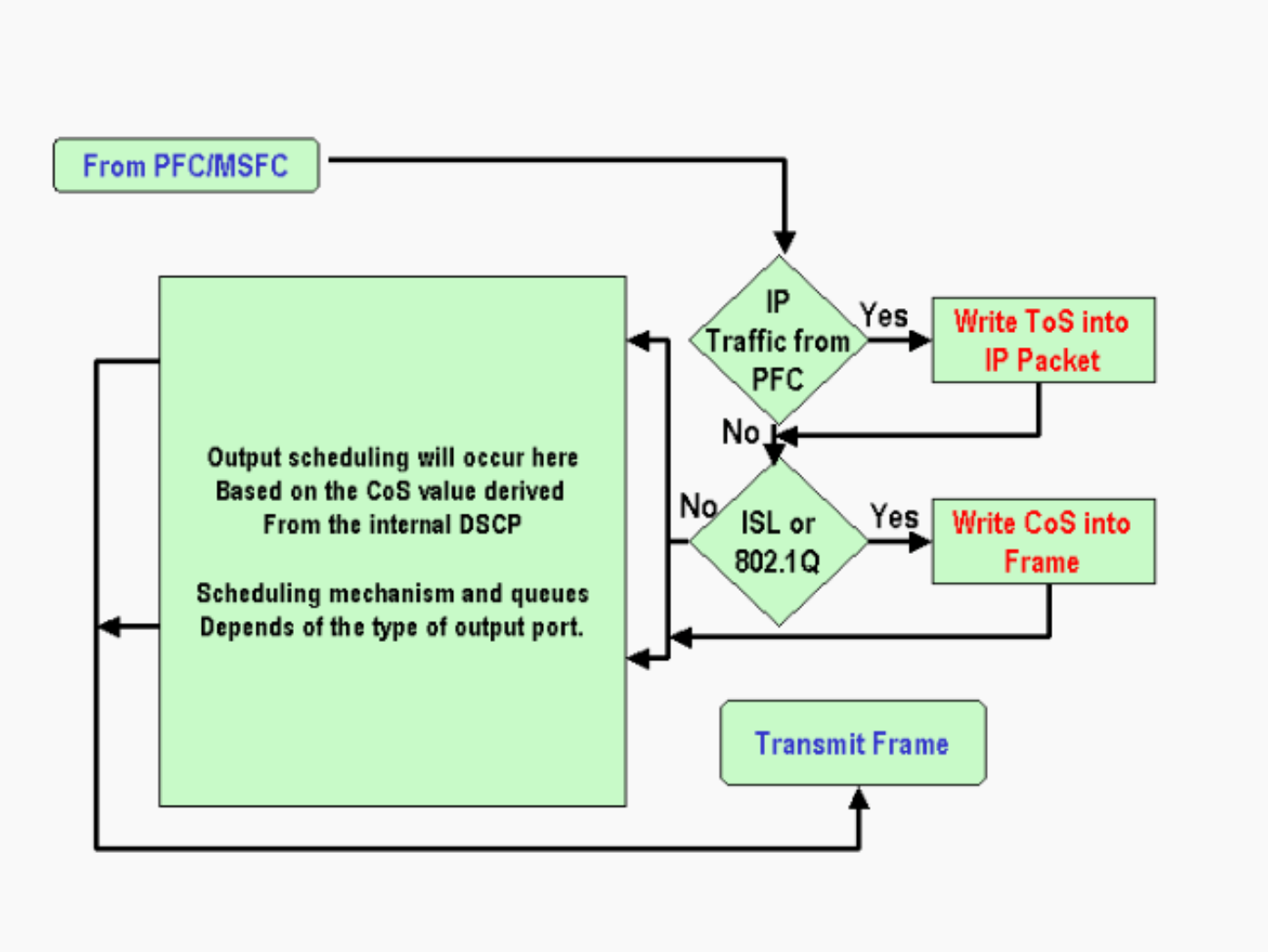
```
cat6k#show mls qos maps
...
  Dscp-cos map:                                     (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ------------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 02 02 02 02
      2 :    02 02 02 02 03 03 03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

若要變更此對應，請在正常組態模式下發出以下組態命令：

```
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
...
```

在將DSCP寫入IP報頭並且從DSCP匯出CoS之後，根據CoS將分組傳送到輸出隊列中的一個用於輸出排程。即使封包不是dot1q或ISL，也會發生這種情況。如需輸出佇列排程的詳細資訊，請參閱執行Cisco IOS系統軟體的Catalyst 6500/6000系列交換器上的QoS輸出排程。

此圖總結了輸出連線埠中標籤相關的封包處理：



註釋和限制

預設ACL

預設ACL使用「dscp 0」作為分類關鍵字。如果啟用QoS，所有通過不可信埠進入交換機並且未命中服務策略條目的流量都會標籤為DSCP 0。目前，您無法在Cisco IOS軟體中變更預設ACL。

注意：在Catalyst OS(CatOS)軟體中，您可以設定和變更此預設行為。如需詳細資訊，請參閱執行CatOS軟體的Catalyst 6500/6000系列交換器上的QoS分類和標籤的*預設ACL*一節。

WS-X61xx、WS-X6248-xx、WS-X6224-xx和WS-X6348-xx線卡的限制

本節僅涉及以下線卡：

- WS-X6224-100FX-MT:Catalyst 6000 24埠100 FX多模式
- X6248-RJ-45:Catalyst 6000 48埠10/100 RJ-45模組
- WS-X6248 — 電話：Catalyst 6000 48埠10/100 Telco模組
- X6248A-RJ-45:Catalyst 6000 48埠10/100，增強型QoS
- WS-X6248A — 電話：Catalyst 6000 48埠10/100，增強型QoS
- WS-X6324-100FX-MM:Catalyst 6000 24埠100 FX、增強型QoS、MT
- WS-X6324-100FX-SM:Catalyst 6000 24埠100 FX、增強型QoS、MT
- X6348-RJ-45:Catalyst 6000 48埠10/100，增強型QoS

- WS-X6348-RJ21V:Catalyst 6000 48埠10/100，線上供電
- WS-X6348-RJ45V:Catalyst 6000 48埠10/100，增強型QoS，內嵌供電
- WS-X6148-RJ21V:Catalyst 6500 48埠10/100線上供電
- WS-X6148-RJ45V:Catalyst 6500 48埠10/100線上供電

這些線卡有侷限性。在埠級別，您無法使用下列任一關鍵字配置trust狀態：

- trust-dscp
- trust-ipprec
- trust-cos

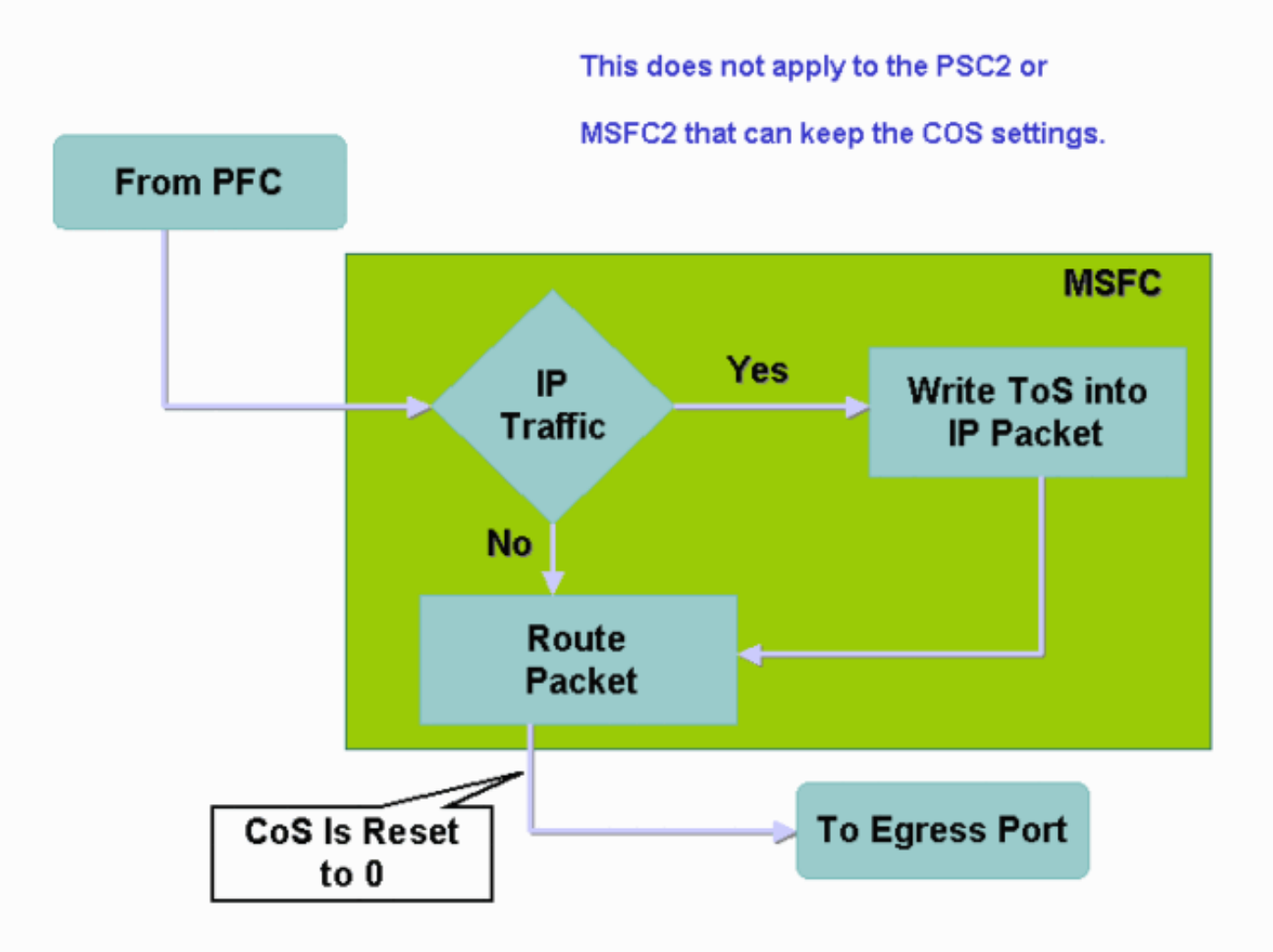
只能使用untrusted狀態。嘗試在這些埠之一上配置trust狀態時將顯示以下警告消息之一：

```
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.
```

如果希望此類線卡上傳入信任幀，則必須將服務策略附加到埠或VLAN。使用案例1中的方法：在本文檔的邊緣部分標籤。

來自Supervisor引擎1A/PFC上MSFC1或MSFC2的資料包

來自MSFC1或MSFC2的所有封包的CoS都為0。該封包可以是軟體路由封包或MSFC發出的封包。這是PFC的限制，因為它重置來自MSFC的所有資料包的CoS。DSCP和IP優先順序仍然保留。PFC2沒有此限制。PFC2的現有CoS等於資料包的IP優先順序。



分類摘要

本節中的表格顯示了基於以下分類得出的DSCP:

- 傳入埠信態
- 所應用ACL中的classification關鍵字

下表是除WS-X62xx和WS-X63xx以外的所有埠的通用摘要：

策略對映關鍵字 埠信任狀態	set-ip-dscp xx或set-dscp-transmit xx	trust-dscp	trust-ipprec	trust-cos
不可信	xx[1]	Rx[2] DSCP	源自Rx ipprec	0
trust-dscp	Rx DSCP	Rx DSCP	源自Rx ipprec	源自Rx CoS或埠CoS
trust-ipprec	源自Rx ipprec	Rx DSCP	源自Rx ipprec	源自Rx CoS或埠CoS
trust-cos	源自Rx CoS或埠CoS	Rx DSCP	源自Rx ipprec	源自Rx CoS或埠CoS

[1]這是製作幀的新標籤的唯一方法。

[2] Rx =接收

下表提供了WS-X61xx、WS-X62xx和WS-X63xx埠的摘要：

策略對映關鍵字 埠信任狀態	set-ip-dscp xx或set-dscp-transmit xx	trust-dscp	trust-ipprec	trust-cos
不可信	xx	Rx DSCP	源自Rx ipprec	0
trust-dscp	不支援	不支援	不支援	不支援
trust-ipprec	不支援	不支援	不支援	不支援
trust-cos	不支援	不支援	不支援	不支援

監控和驗證配置

檢查埠配置

發出**show queuing interface** *interface-id* 命令以驗證連線埠設定和設定。

發出此命令時，可以驗證這些分類引數以及其他引數：

- 是基於埠還是基於VLAN
- `trust`連線埠型別
- 連線到連線埠的ACL

以下是此指令輸出的範例。有關分類的重要欄位以粗體顯示：

```
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]:
```

輸出顯示，此特定連線埠的組態在連線埠層級具有`trust cos`。此外，預設埠CoS為0。

檢查定義的類

發出**show class-map**命令以檢查定義的類。以下是範例：

```
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)
```

檢查應用於介面的策略對映

發出以下命令，以檢查已應用並在前面命令中看到的策略對映：

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

以下是發出以下命令的輸出的示例：

```
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
```

注意：您可以檢視與分類相關的以下欄位：

- `Class-map` — 告訴您哪個類連線到連線到此介面的服務策略。
- `Trust` — 告訴您該類中的策略操作是否包含**trust**命令以及該類中受信任的內容。
- `DSCP` — 通知您為到達該類的包傳輸的DSCP。

```
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
```

示例案例研究

本節提供網路中可能出現的常見情況的配置示例。

案例1:在邊緣進行標籤

假設您配置了一個用作接入交換機的Catalyst 6000。許多使用者連線到交換機插槽2，該插槽是WS-X6348線卡(10/100 Mbps)。 使用者可以傳送：

- 正常資料流量 — 此流量始終在VLAN 100中，需要獲取DSCP 0。
- 來自IP電話的語音流量 — 此流量始終位於語音輔助VLAN 101中，需要獲取46的DSCP。
- 任務關鍵型應用流量 — 此流量也來自VLAN 100，並定向到伺服器10.10.10.20。此流量需要獲得32的DSCP。

應用程式不會標籤任何此類流量。因此，將連線埠保留為，並設定特定ACL以分類流量。一個

ACL應用於VLAN 100，一個ACL應用於VLAN 101。您還需要將所有埠配置為基於VLAN。以下是得出的組態範例：

```
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
```

案例2:信任僅具有千兆乙太網介面的核心

假設您在插槽1和插槽2中僅配置千兆乙太網介面的核心Catalyst 6000。接入交換機以前正確標籤了流量。因此，您無需進行任何重新標籤。但是，您需要確保核心交換機信任傳入的DSCP。此案例比較簡單，因為所有連線埠都標籤為`trust-dscp`，這應該就足夠了：

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

相關資訊

- 瞭解Catalyst 6000系列交換器上的服務品質
- 執行CatOS軟體的Catalyst 6500/6000系列交換器上的QoS分類和標籤
- LAN 產品支援
- LAN 交換技術支援
- 技術支援與文件 - Cisco Systems