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

目錄

簡介

本檔案將檢視在Catalyst 6000機箱內傳輸過程中有關在不同位置對封包進行標籤和分類的情況。其中提到了特殊案例、限制，並提供了簡短的案例研究。

不應將本文詳盡列出所有與服務品質(QoS)或標籤相關的Catalyst OS(CatOS)命令。有關CatOS命令列介面(CLI)的詳細資訊，請參閱以下文檔：

- 配置QoS

注意：本檔案僅考慮IP流量。

開始之前

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

必要條件

本文件沒有特定先決條件。

採用元件

本檔案適用於執行CatOS軟體並使用下列其中一個Supervisor Engine的Catalyst 6000系列交換器：

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

但是所有範例命令都已在執行6.3版軟體的SUP1A/PFC的Catalyst 6506上嘗試。

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。如果您在即時網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

技術

以下是本文檔中使用的術語清單：

- 區別服務代碼點(DSCP):IP標頭中服務型別(ToS)位元組的前六位。DSCP僅存在於IP資料包中。**注意：**您還要為每個資料包（IP或非IP）分配一個內部DSCP，本文檔稍後將對此內部DSCP分配進行詳細說明。
- IP優先順序：IP報頭中ToS位元組的前三個位。
- 服務類別(CoS):唯一可用於在第2層(L2)標籤資料包的欄位。 它由以下三個位中的任一個組成：IEEE dot1q資料包的dot1q標籤中的三個dot1p位。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。非dot1q或ISL資料包中沒有CoS。
- 分類：用於選擇要標籤的流量的過程。
- 標籤：在資料包中設定第3層(L3)DSCP值的過程。在本文檔中，對標籤的定義進行了擴展，包括設定L2 CoS值。

Catalyst 6000系列交換機能夠基於以下三個引數進行分類：

- DSCP
- IP優先順序
- CoS

Catalyst 6000系列交換機在不同的位置進行分類和標籤。下面將介紹這些不同位置發生的情況：

- 輸入連線埠(輸入特定應用積體電路(ASIC))
- 交換引擎(原則功能卡(PFC))
- 輸出埠（輸出ASIC）

啟用QoS

預設情況下，Catalyst 6000交換機上禁用QoS。可以通過發出CatOS命令**set qos enable**來啟用QoS。

當禁用QoS時，交換機不執行任何分類或標籤，因此，每個資料包在進入交換機時都以DSCP/IP優先順序離開交換機。

輸入連線埠處理

輸入連線埠的主要組態引數（關於分類）是連線埠的信任狀態。系統的每個埠可以具有以下信任狀態之一：

- trust-ip-precedence
- trust-dscp
- trust-cos
- 不可信

本節的其餘部分說明連線埠信任狀態如何影響封包的最終分類。可使用以下CatOS命令設定或更改埠信任狀態：

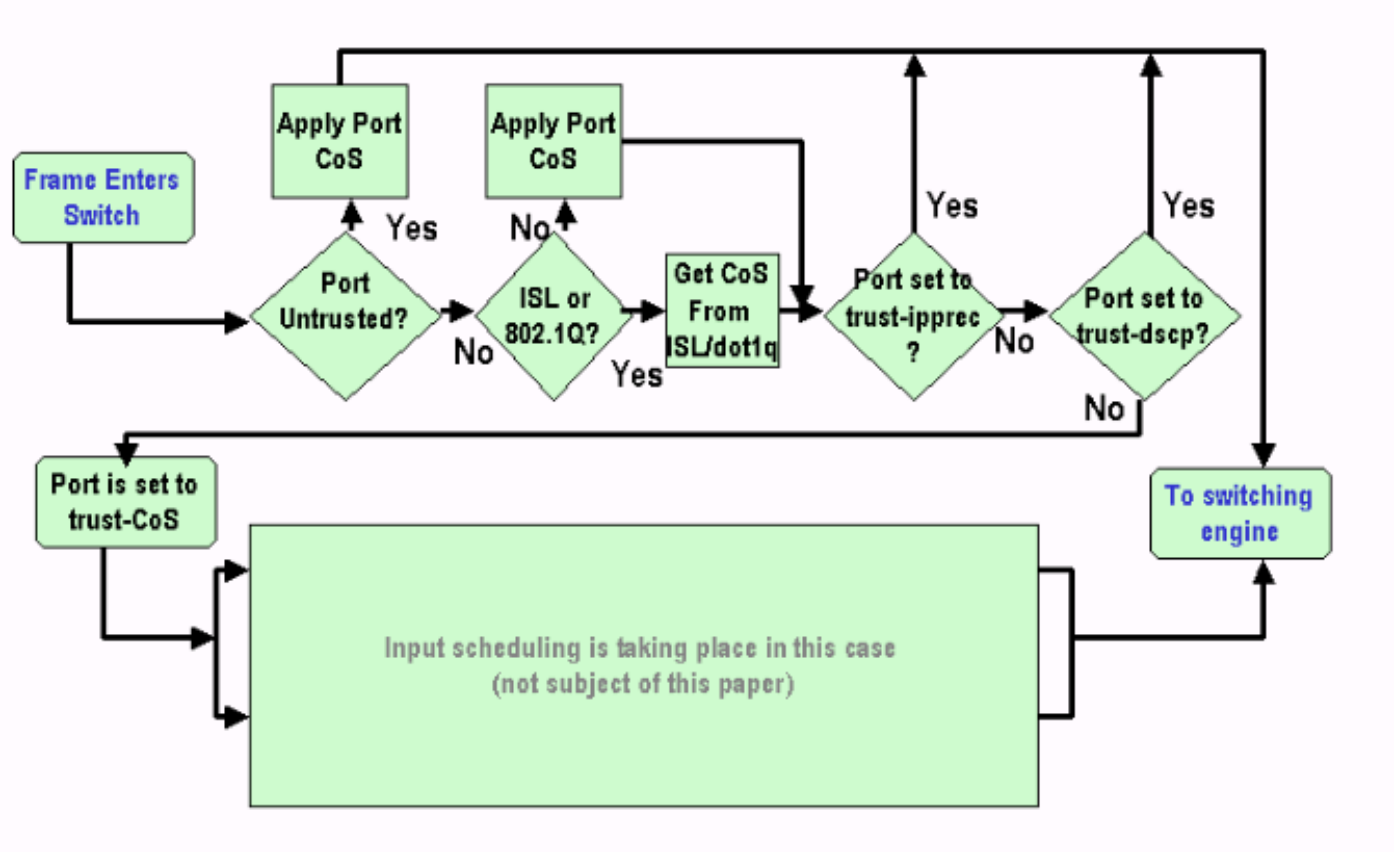
set port qos *mod/port* **trust {untrusted | trust-cos | trust-ipprec | trust-dscp }**

注意：預設情況下，啟用QoS時，所有埠都處於不可信狀態。

在輸入埠級別上，還可以為每個埠應用預設CoS，如下例所示：

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

如果埠設定為不受信任狀態，只需使用埠預設CoS標籤幀並將報頭傳遞給交換引擎(PFC)即可。 如果埠設定為信任狀態之一，請應用預設埠CoS(如果幀沒有收到的CoS（dot1q或ISL））,或保留CoS（對於dot1q和ISL幀）並將幀傳遞到交換引擎。以下流程圖說明了輸入分類：



註：如上面的流程圖所示，每個幀都將分配一個內部 CoS（可以是接收的CoS，也可以是預設埠CoS），包括不帶任何實際CoS的無標籤幀。此內部CoS和收到的DSCP寫入一個特殊的資料包報頭（稱為資料匯流排報頭），並通過資料匯流排傳送到交換引擎。這發生在入口線卡上，此時尚不知道此內部CoS是否會被攜帶到出口ASIC並插入傳出幀。這完全取決於PFC的作用，下一節將進一步介紹。

交換引擎(PFC)

報頭到達交換引擎後，交換引擎編碼地址識別邏輯(EARL)將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IPv4標頭中的DSCP。它源自現有的CoS或ToS設定，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。

內部DSCP的四種可能來源

內部DSCP將從以下其中一項匯出：

1. 在幀進入交換機之前設定的現有DSCP值。
2. 收到的IP優先位已經在IPv4標頭中設定。由於DSCP值有64個，而只有8個IP優先順序值，因此管理員將配置交換機用來派生DSCP的對映。如果管理員未配置對映，則預設對映就位。
3. 收到的CoS位在幀進入交換機之前已設定，或者如果傳入幀中沒有CoS，則從傳入埠的預設CoS設定。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。可以配置此對映，或者交換機可以使用已經存在的預設對映。
4. 可以使用通常通過訪問控制清單(ACL)條目分配的DSCP預設值為幀設定DSCP。

對於Nos。在上述清單中，預設情況下使用的靜態對映如下：

- 對於CoS到DSCP的對映，匯出的DSCP等於CoS的八倍。

- 對於IP優先順序到DSCP的對映，匯出的DSCP等於IP優先順序的八倍。

使用者可通過發出以下命令來覆蓋此靜態對映：

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

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

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」，並繼續該模式。

將使用內部DSCP的四個可能來源中的哪一個？

本節介紹決定上述四種可能來源中哪一種將用於每個資料包的規則。這取決於以下引數：

1. 對資料包應用什麼QoS ACL?這由以下規則確定：**注意：**每個資料包都經過一個ACL條目。如果沒有將ACL附加到傳入埠或VLAN，請應用預設ACL。如果傳入連線埠或VLAN連線有ACL，且流量與ACL中的其中一個專案相符，請使用以下專案。如果傳入連線埠或VLAN連線有ACL，且流量與ACL中的其中一個專案不相*符，則使用預*設ACL。
2. 每個條目都包含一個分類關鍵字。以下是可能的關鍵字及其說明的清單：trust-ipprec:無論埠信任狀態如何，內部DSCP都將根據靜態對映從接收到的IP優先順序派生。trust-dscp:內部DSCP將從收到的DSCP派生，無論埠信任狀態為何。trust-cos:如果埠信任狀態是受信任的(trust-cos、trust-dscp、trust-ipprec)，則根據靜態對映從接收到的CoS派生內部DSCP。 如果埠信任狀態為trust-xx，將根據相同的靜態對映從預設埠CoS中匯出DSCP。dscp *xx*:內部DSCP將取決於以下傳入埠信任狀態：如果埠不受信任，則內部DSCP將設定為*xx*。如果埠為trust-dscp，則內部DSCP將是傳入資料包中接收的DSCP。如果埠為trust-CoS，則內部DSCP將從接收資料包的CoS中匯出。如果埠為trust-ipprec，則內部DSCP將從接收資料包的IP優先順序派生。
3. 每個QoS ACL可以應用到埠或VLAN，但還需要考慮其他配置引數；acl埠型別。埠可以配置為基於VLAN或基於埠。以下是對兩種配置型別的說明：設定為基於VLAN的連線埠只會檢視應用於連線埠所屬的VLAN的ACL。如果連線埠連線有ACL，則傳入該連線埠的封包將略過ACL。如果屬於VLAN的連線埠設定為連線埠型，即使該VLAN連線有ACL，系統也不會考慮來自該連線埠的流量。

以下是用於建立用於標籤IP流量的QoS ACL的語法：

set qos acl ip ***acl_name*** **[dscp xx | trust-cos | trust-dscp | trust-ipprec] acl*條目規則***

以下ACL將使用DSCP "40"標籤定向到主機1.1.1.1的所有IP流量，並將為所有其他IP流量使用trust-dscp:

set qos acl TEST_ACL dscp 40 ip any host 1.1.1.1

set qos acl TEST_ACL trust-dscp ip any any

建立ACL後，您需要將其對映到埠或VLAN，這可以通過發出以下命令來完成：

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

預設情況下，ACL的每個埠都基於埠，因此，如果要將ACL附加到VLAN中，需要將此VLAN的埠配置為基於VLAN。可通過發出以下命令完成此操作：

set port qos *module/port* vlan-based

您也可以發出以下命令將其回覆為基於埠的模式：

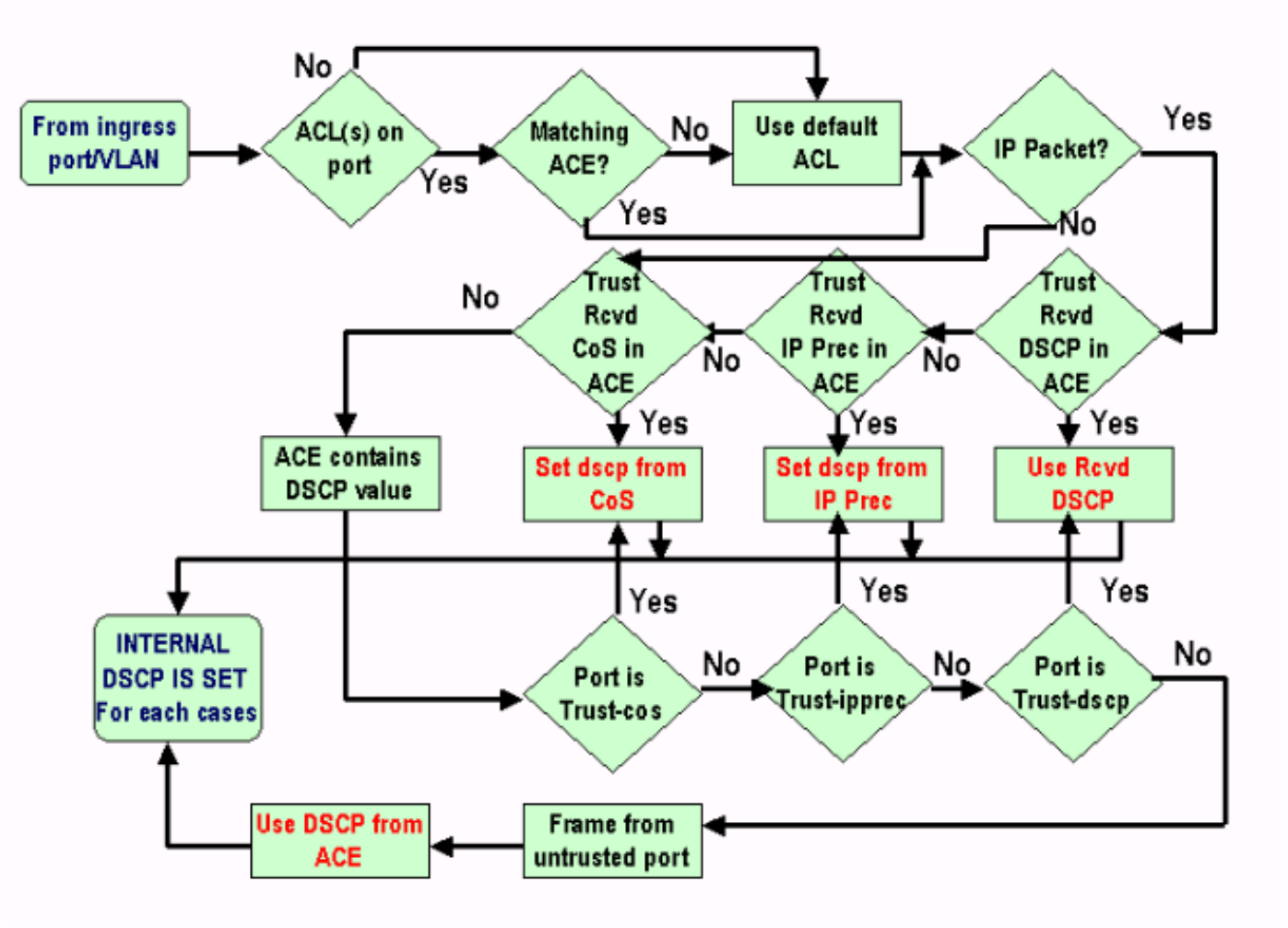
set port qos *module/port* port-based

摘要:如何選擇內部DSCP?

內部DSCP取決於以下因素：

- 埠信任狀態
- 連線到埠的ACL
- 預設ACL
- ACL方面的基於VLAN或基於埠

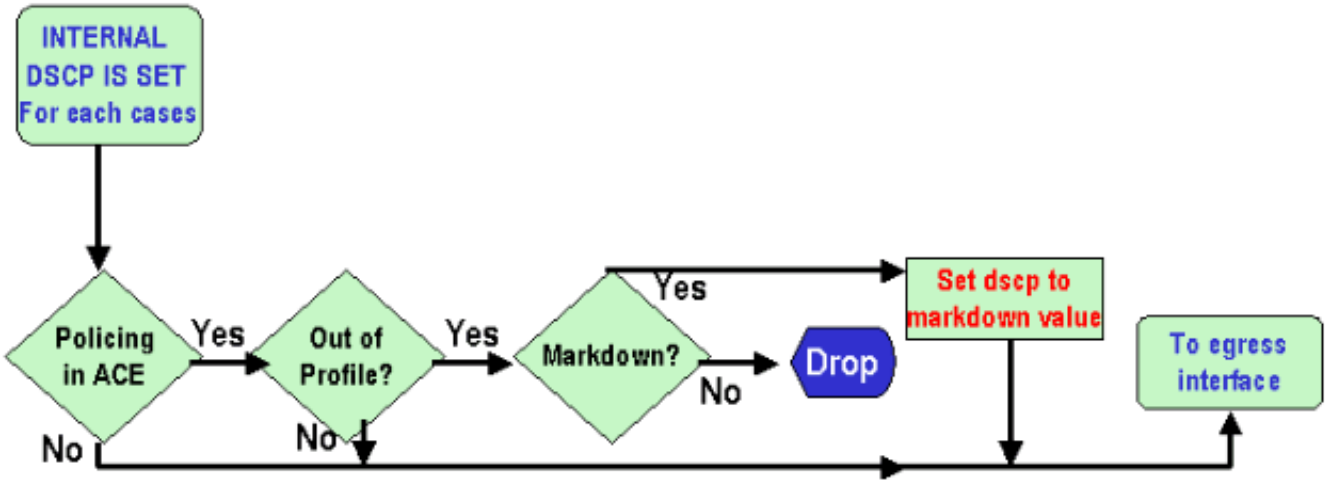
以下流程圖總結了如何根據配置選擇內部DSCP:



PFC還可以執行策略管理。這最終可能會導致內部DSCP的降級。有關管制的詳細資訊，請參閱以下文檔：

- Catalyst 6000上的QoS管制

以下流程圖顯示了如何應用監察器：



輸出埠處理

在出口埠級別無法更改分類，但在本部分中，您將根據以下規則標籤資料包：

- 如果該封包是IPv4封包，請將交換引擎指派的內部DSCP複製到IPv4標頭的ToS位元組。
- 如果輸出埠配置為ISL或dot1q封裝，請使用從內部DSCP派生的CoS，然後將其複製到ISL或dot1q幀中。

注意：CoS根據發出以下命令的使用者配置的靜態從內部DSCP匯出：

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

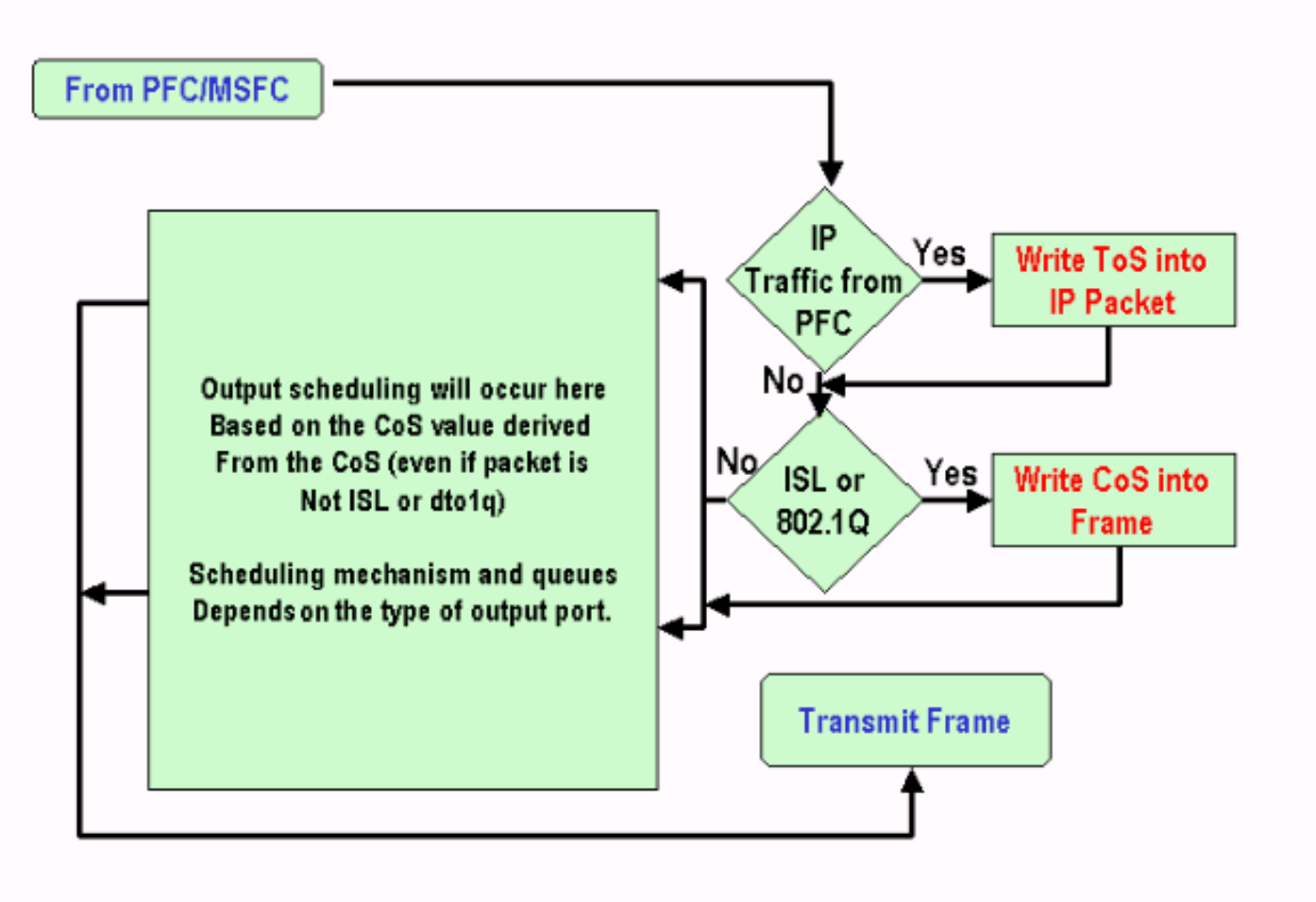
注意：以下是預設配置。預設情況下，CoS將是DSCP的整數部分，除以八：

```
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
```

一旦DSCP寫入IP報頭，並且從DSCP匯出CoS，資料包將傳送到輸出隊列之一以基於其CoS進行輸出排程（即使資料包不是dot1q或ISL）。 有關輸出隊列排程的詳細資訊，請參閱以下文檔：

- Catalyst 6000系列交換器上的QoS:使用CatOS軟體在搭載PFC或PFC 2的Catalyst 6000上進行輸出排程

以下流程圖總結了輸出埠中標籤相關的資料包的處理：



註釋和限制

預設ACL

預設情況下，預設ACL使用「dscp 0」作為分類關鍵字。這表示如果啟用QoS，所有通過不可信埠進入交換機的流量都將標籤為DSCP「0」。您可以發出以下命令來驗證IP的預設ACL:

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

也可發出以下命令來更改預設ACL:

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

acl條目限制中的trust-cos

在條目中使用trust-CoS關鍵字時會出現其他限制。僅當接收的信任狀態不是不可信時，才能在條目中信任CoS。嘗試使用trust-CoS配置條目將顯示以下警告：

```
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.
```

此限制是先前在「輸入埠處理」部分中看到的內容的結果。如該節的流程圖所示，如果埠不受信任，幀將立即分配預設埠CoS。因此，傳入CoS不會保留，也不會傳送到交換引擎，導致即使使用特定ACL也無法信任CoS。

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-TEL:CATALYST 6000 48埠10/100 TELCO模組
- X6248A-RJ-45:CATALYST 6000 48埠10/100，增強型QOS
- X6248A — 電話：CATALYST 6000 48埠10/100，增強型QOS
- WS-X6324-100FX-MM:CATALYST 6000 24埠100FX、增強型QOS、MT
- WS-X6324-100FX-SM:CATALYST 6000 24埠100FX、增強型QOS、MT
- X6348-RJ-45:CATALYST 6000 48埠10/100，增強型QO
- 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，INLI NE電源

但是，這些線卡有一些其他限制：

- 在埠級別，不能信任dscp或trust-ipprec。
- 在埠級別，如果埠信任狀態為trust-CoS，則適用以下語句：已啟用輸入排程的接收閾值。此外，接收分組中的CoS用於優先化分組以訪問匯流排。CoS不會被信任，並且不會用於派生內部DSCP，除非您還將該流量的ACL配置為trust-cos。此外，線卡在連線埠上僅具有信任cos是不夠的，您還需要具有適用於該流量的trust-cos的ACL。
- 如果埠信任狀態為不可信，則會發生正常標籤（與標準情況一樣）。 這取決於應用於流量的ACL。

在其中一個埠上配置信任狀態的任何嘗試將顯示以下警告消息之一：

```
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.
```

分類摘要

下表顯示了按以下方式分類的結果DSCP:

- 傳入埠信任狀態。
- 所應用ACL中的classification關鍵字。

除WS-X62xx和WS-X63xx以外的所有端口的通用表摘要

ACL關鍵字	dscp xx	trust-dscp	trust-ipprec	trust-CoS

埠信任狀態				
不受信任	xx(1)	Rx 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)這是對幀進行新標籤的唯一方法。

WS-X62xx或*WS*-X63xx表摘要

ACL關鍵字 埠信任狀態	dscp xx	trust-dscp	trust-ipprec	trust-CoS
不受信任	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	xx	Rx dscp	源自Rx ipprec	源自Rx CoS或埠CoS(2)

(2)這是為來自62xx或63xx線卡的流量保留傳入CoS的*唯*一方法。

監控和驗證配置

檢查埠配置

可通過發出以下命令驗證埠設定和配置：

show port qos *module/port*

通過發出此命令，您可以驗證以下分類引數以及其他引數：

- 基於埠或基於VLAN
- 信任埠型別
- 連線到埠的ACL

以下是該命令輸出的示例，其中突出顯示了關於分類的重要欄位：

```
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
```

注意：對於每個欄位，都存在已配置的引數和運行時引數。將應用於資料包的引數是運行時引數。

檢查ACL

通過發出以下命令，可以檢查在先前命令中應用和看到的ACL:

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
```

示例案例研究

以下示例是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

假設您正在將Catalyst 6000配置為接入交換機，其中許多使用者連線到插槽2，該插槽是WS-X6348線卡(10/100M)。 使用者可以傳送以下內容：

- 正常資料流量：此值始終位於VLAN 100中，需要取得「0」的DSCP。
- 來自IP電話的語音流量：它始終位於語音輔助VLAN 101中，需要獲取「40」的DSCP。
- 關鍵任務應用流量：此流量也來自VLAN 100，並定向到伺服器10.10.10.20。此流量需要獲取DSCP「32」。

所有此類流量都不會被應用標籤，因此您會將埠保留為不可信狀態，並將配置特定ACL來對流量進行分類。一個ACL將應用於VLAN 100，一個ACL將應用於VLAN 101。您還需要將所有埠配置為基於VLAN。以下是結果配置的示例：

```
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
```

案例2:信任僅具有Gigabit介面的核心

假設您在插槽1和插槽2中僅配置千兆位介面的核心Catalyst 6000（機箱中沒有62xx或63xx線卡）。流量之前已被接入交換機正確標籤，因此您不需要進行任何重新標籤，但是您需要確保信任傳入的DSCP。這是最簡單的情況，因為所有連線埠均會標籤為trust-dscp，而且應該足夠：

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

案例3:通過機箱中的62xx或63xx埠信任核心

假設您要在WS-X6416-GBIC線卡（在插槽2中）上配置千兆鏈路，在WS-X6348線卡（在插槽3中）上配置一個10/100鏈路。 您還需要信任所有傳入流量，因為之前已在接入交換機級別進行了標籤。由於您無法在6348線卡上信任DSCP，因此在這種情況下，最簡單的方法是將所有埠都保留為不受信任狀態，並將預設ACL更改為trust-dscp，如以下示例所示：

```
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
```

相關資訊

- LAN 產品支援
- LAN 交換技術支援
- 技術支援 - Cisco Systems