瞭解Catalyst 6000系列交換機的QoS

目錄

簡介

本檔案將說明Catalyst 6000系列交換器提供的服務品質(QoS)功能。本文檔介紹QoS配置功能，並提供如何實施QoS的一些示例。

不應將本文作為配置指南。本文使用配置示例來幫助Catalyst 6000系列硬體和軟體的QoS功能說明。有關QoS命令結構的語法參考，請參閱Catalyst 6000系列的以下配置和命令指南：

- Catalyst 6500系列交換器

定義第2層QoS

雖然許多人可能認為第2層(L2)交換機中的QoS只是確定乙太網幀的優先順序，但很少有人意識到它包含更多內容。L2 QoS要求如下：

1. **輸入隊列排程**：當幀進入埠時，可以將其分配給多個基於埠的隊列之一，然後再排程到出口埠。通常，當不同的流量需要不同的服務級別，或者必須將交換機延遲保持在最低值時，會使用多個隊列。例如，基於IP的影片和語音資料要求低延遲，因此可能需要在交換其他資料(如檔案傳輸協定(FTP)、Web、電子郵件、Telnet等)之前交換此資料。

2. **分類**：分類過程包括檢查乙太網路L2標頭中的不同欄位，以及IP標頭(第3層(L3))和傳輸控制通訊協定/使用者資料包通訊協定(TCP/UDP)標頭(第4層(L4))中的欄位，以協助確定在訊框經過交換器時將套用的服務等級。
3. **管制**：管制是檢查乙太網路訊框以確認它在特定時間訊框中是否超過預設流量速率的程式（此時間訊框通常為交換器內部的固定編號）。 如果該幀過於概觀（即，它是資料流中超

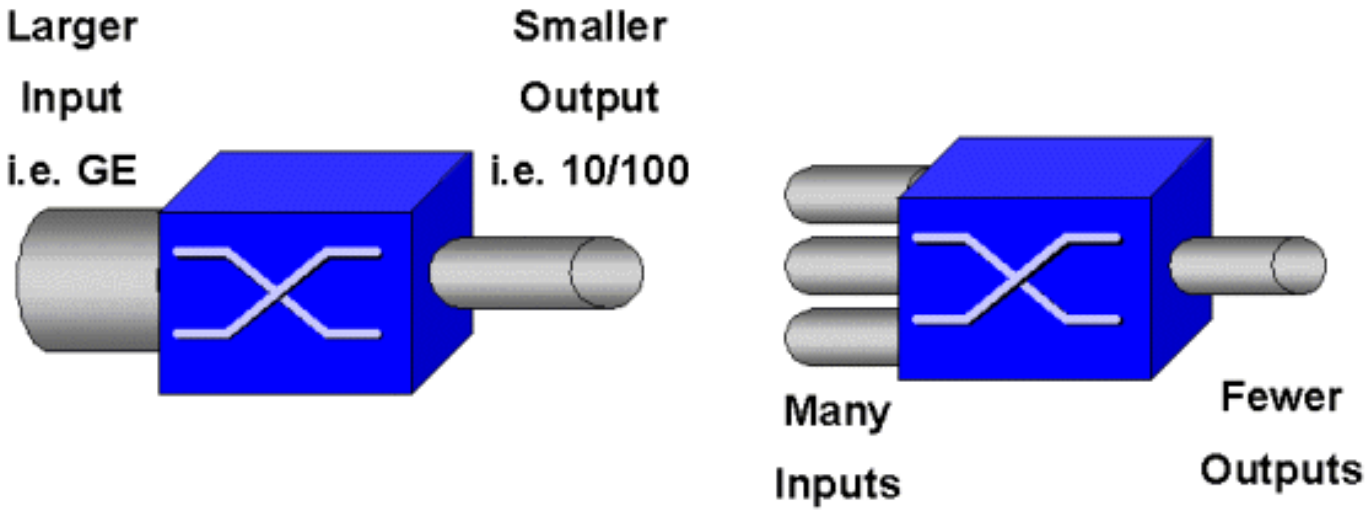
過預定速率限制部分），則可以丟棄該幀或者降級服務等級(CoS)值。

4. **重寫**：重寫過程是交換機修改乙太網報頭中的CoS或IPV4報頭中的服務型別(ToS)位的能力。
5. **輸出隊列排程**：重新寫入程式後，交換器會將乙太網路訊框放在適當的傳出（輸出）佇列中以進行交換。交換機將通過確保緩衝區不溢位對此隊列執行緩衝區管理。它通常通過使用隨機早期丟棄(RED)演算法來完成此操作，從而從隊列中移除（丟棄）隨機幀。Weighted RED(WRED)是RED的衍生物（用於Catalyst 6000系列中的某些模組），通過它可檢查CoS值以確定丟棄哪些幀。當緩衝區達到預定義的閾值時，通常丟棄優先順序較低的幀，從而使優先順序較高的幀保留在隊列中。

本檔案在後續各節中詳細介紹上述各項機制以及它們與Catalyst 6000系列的關係。

交換機對QoS的需求

巨大的背板、每秒數百萬的交換資料包以及無阻塞交換機都是當今許多交換機的同義詞。為什麼需要QoS?答案是因為擁塞。



交換機可能是世界上速度最快的交換機，但是如果您有上圖所示的兩種情況之一，則該交換機將會出現擁塞。在擁塞時，如果擁塞管理功能未就緒，資料包將被丟棄。丟棄資料包時，會發生重新傳輸。發生重新傳輸時，網路負載可能會增加。在已經擁塞的網路中，這會增加現有的效能問題，而且可能會進一步降低效能。

在融合網路中，擁塞管理甚至更為重要。如果發生延遲，語音和影片等延遲敏感流量可能會受到嚴重影響。簡單地為交換機新增更多緩衝區也不一定會緩解擁塞問題。延遲敏感型流量需要儘快交換。首先，您需要通過分類技術識別這一重要流量，然後實施緩衝區管理技術，以避免擁塞期間丟棄優先順序較高的流量。最後，您需要結合排程技術，儘快從隊列中切換重要資料包。正如您將在本文檔中閱讀的，Catalyst 6000系列實現了所有這些技術，從而使其QoS子系統成為當今業界最全面的子系統之一。

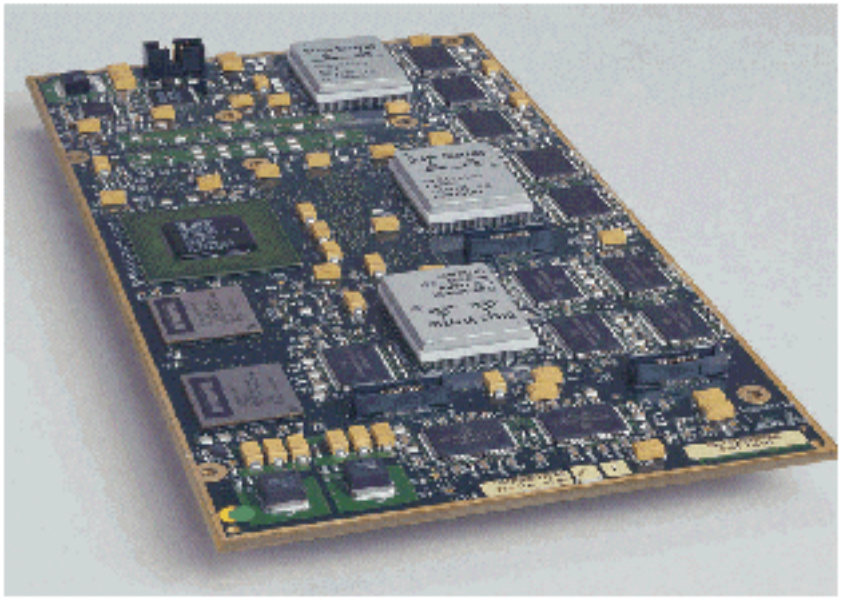
在本文檔中，將更詳細地探討上一節中介紹的所有QoS技術。

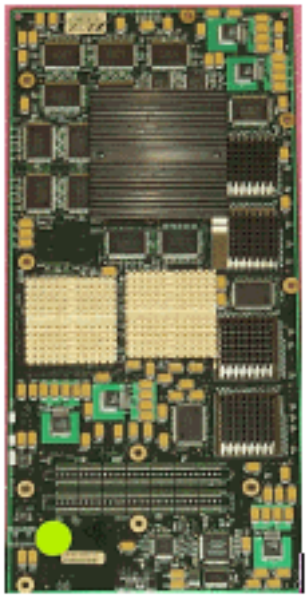
Catalyst 6000系列中的QoS硬體支援

要在Catalyst 6000系列中支援QoS，需要一些硬體支援。支援QoS的硬體包括線路卡本身上的多層次交換功能卡(MSFC)、原則功能卡(PFC)和連線埠應用程式特定積體電路(ASIC)。本文檔不探討MSFC的QoS功能，而是重點介紹PFC和線卡上的ASIC的QoS功能。

PFC

PFC版本1是位於Catalyst 6000系列的Supervisor I(SupI)和Supervisor IA(SupIA)上的子卡。PFC2是PFC1的翻版，隨附新的管理引擎II(SupII)和一些新的板載ASIC。雖然PFC1和PFC2主要以硬體加速L3交換而聞名，但QoS是它們的另一個目的。PFC如下所示。





雖然PFC 1和PFC2本質上相同，但QoS功能有一些差異。即，PFC2新增了以下內容：

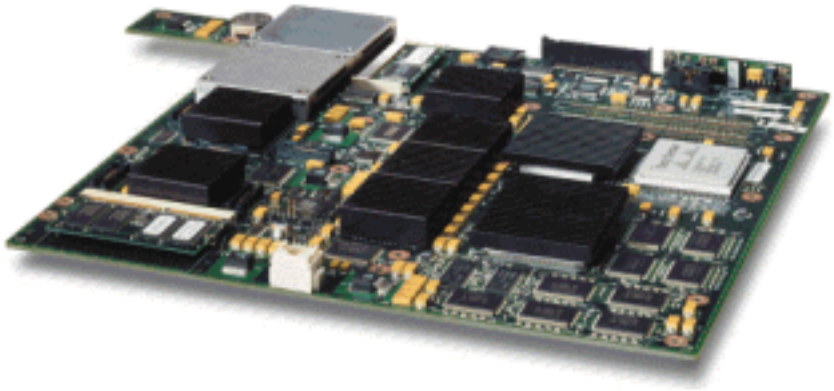
1. 將QoS策略向下推送到分散式轉發卡(DFC)的功能。
2. 警務決策略有不同。PFC1和PFC2都支援常規管制，從而當聚合或微流策略返回超出配置檔案範圍的決策時，丟棄或標籤幀。但是，PFC2增加了對超額速率的支援，這表示可以在第二個策略級別採取策略操作。

定義超額速率管制器時，當封包超出超額速率時，可以將其捨棄或降級。如果設定了超額警察級別，則使用超額DSCP對映將原始DSCP值替換為降級值。如果只設定了正常策略級別，則使用正常DSCP對映。當設定兩個警察級別時，多餘的警察級別將優先選擇對映規則。

必須注意的是，本文檔中描述的QoS功能由所述的ASIC執行，可產生高級別的效能。基本Catalyst 6000系列（無交換矩陣模組）中的QoS效能可產生15 MPPS。如果使用DFC，則可以獲得QoS的其他效能增益。

DFC

DFC可以作為選項連線到WS-X6516-GBIC。但它是WS-X6816-GBIC卡上的標準固定裝置。它也可以在其他未來交換矩陣線卡上支援，例如最近推出的交換矩陣10/100(WS-X6548-RJ45)線卡、交換矩陣RJ21線卡(WS-X6548-RJ21)和100FX線卡(WS-X6524-MM-FX)。 DFC如下所示。



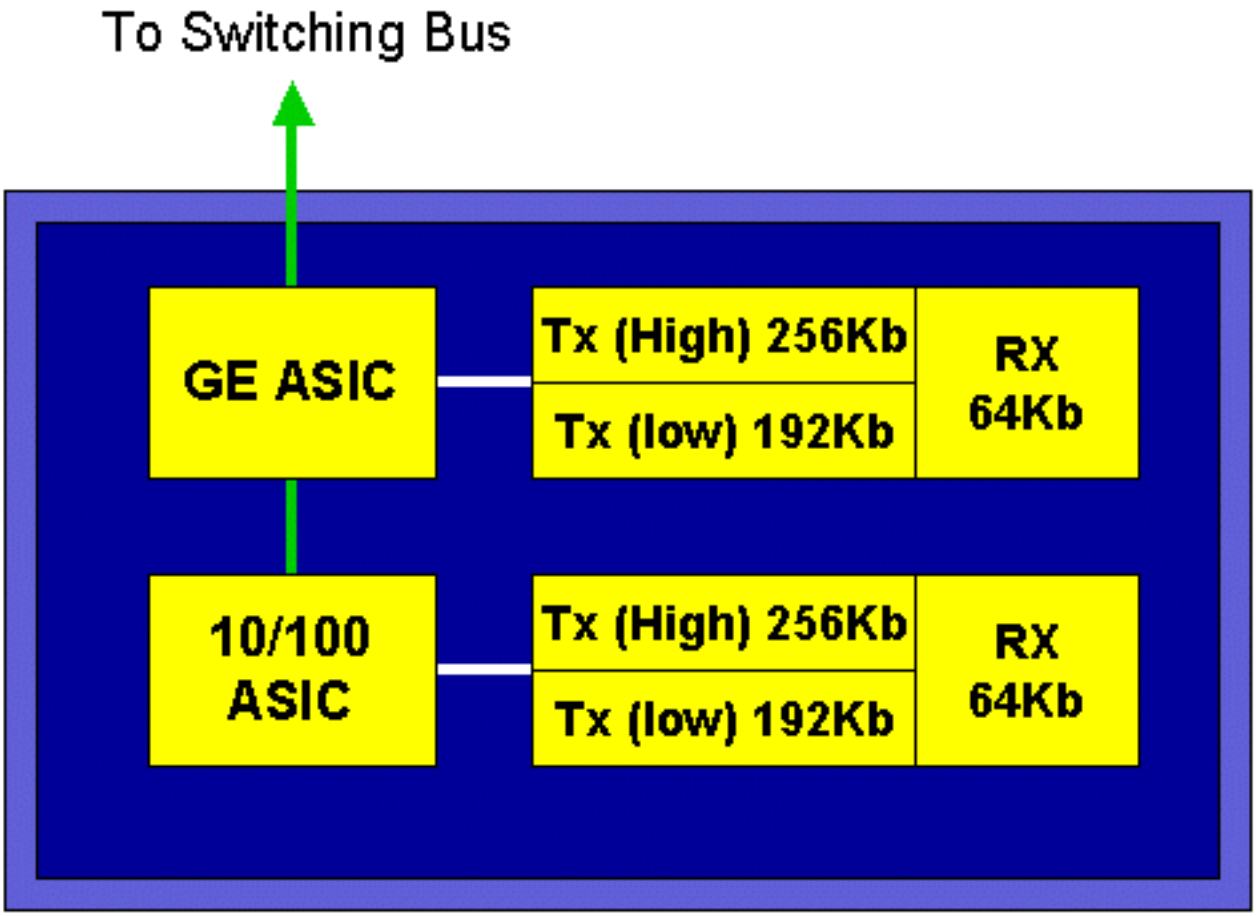
DFC允許交換矩陣（交叉開關連線）線卡執行本地交換。為此，它還必須支援為交換機定義的任何QoS策略。管理員無法直接配置DFC;相反，它處於主用管理引擎上的主MSFC/PFC的控制之下。主PFC將向下推送轉發資訊庫(FIB)表，為DFC提供其L2和L3轉發表。它還將向下推送一個QoS策略副本，以便它們也是線卡的本地策略。之後，本地交換決策可以參考任何QoS策略的本地複製，從而提供硬體QoS處理速度，並通過分散式交換提供更高的效能級別。

基於埠的ASIC

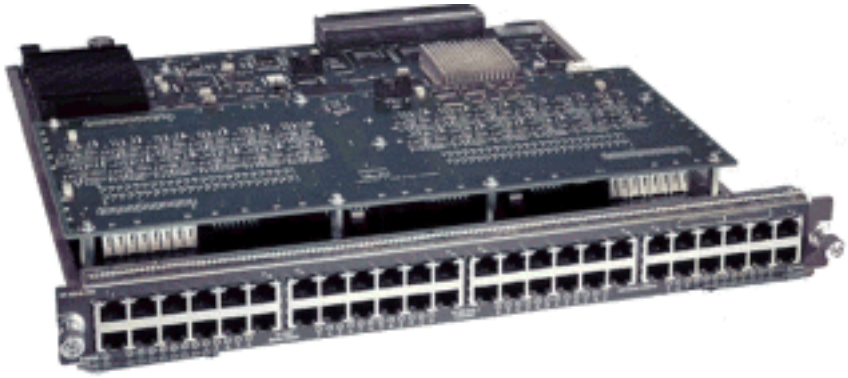
為了完成硬體配置，每個線卡都實施了多種ASIC。這些ASIC在傳輸交換機時實施用於臨時儲存幀的隊列、緩衝和閾值。在10/100卡上，ASIC的組合用於調配48個10/100埠。

原始10/100線卡(WS-X6348-RJ45)

10/100 ASIC為每個10/100連線埠提供一系列接收(Rx)和傳輸(TX)佇列。ASIC為每個10/100埠提供128 K緩衝。有關每個線卡上可用的每個埠緩衝的詳細資訊，請參閱發行說明。此線卡上的每個埠都支援一個Rx隊列和兩個TX隊列（分別表示高和低）。如下圖所示。



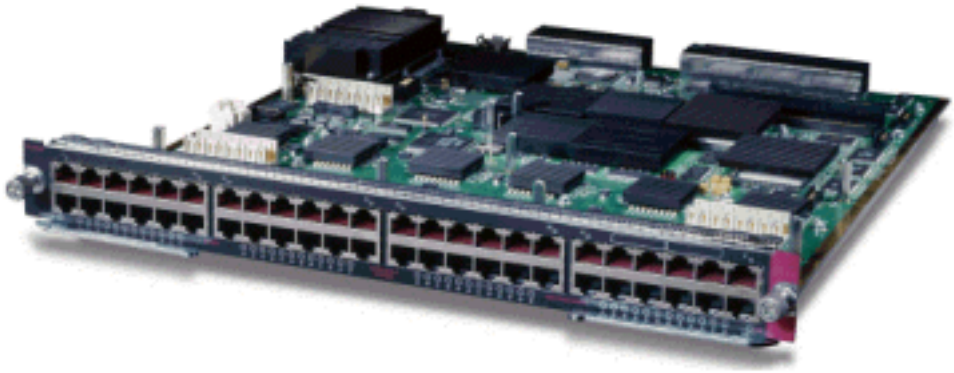
在上圖中，每個10/100 ASIC為12個10/100埠提供分支。每個10/100埠都提供128 K緩衝區。128 K緩衝區在三個隊列中的每一個隊列之間拆分。上面隊列中顯示的數字不是預設值，而是可以配置的表示形式。單個Rx隊列獲得16 K，而剩餘的記憶體(112 K)被分成兩個Tx隊列。預設情況下（在CatOS中），高隊列佔此空間的20%，低隊列佔80%。在Catalyst IOS中，預設為將高佇列指定為10%，將低佇列指定為90%。



雖然卡提供雙級緩衝，但在QoS配置期間，只能操作基於10/100 ASIC的緩衝。

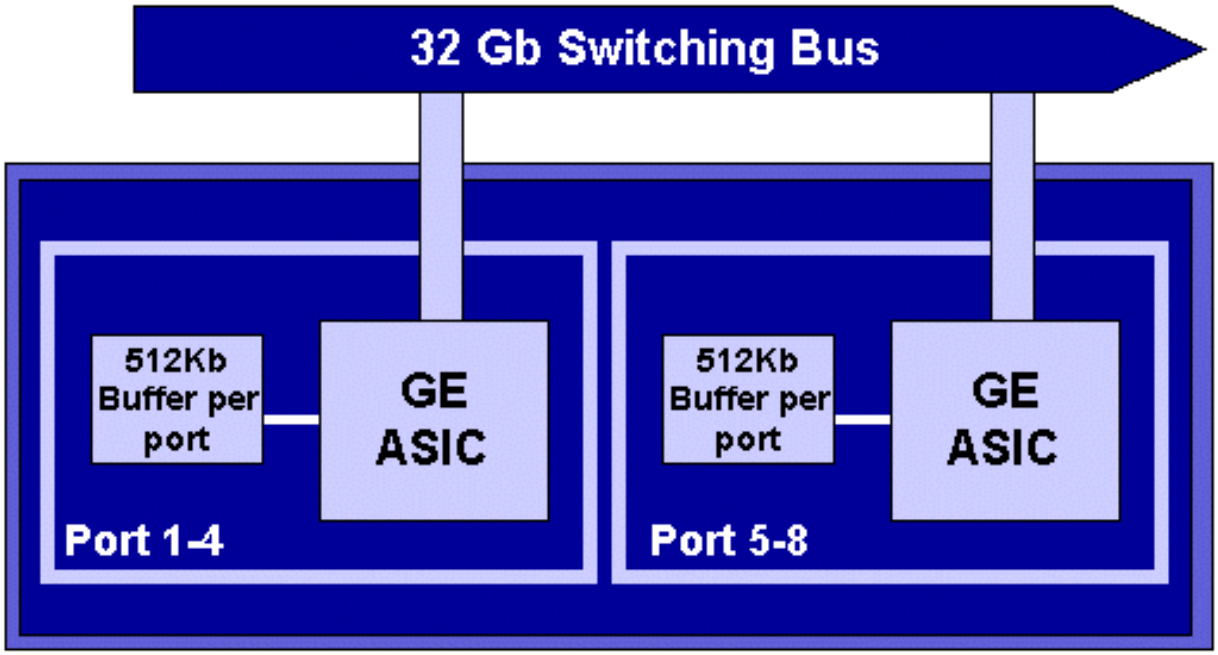
交換矩陣10/100線卡(WS-X6548-RJ45)

新的10/100 ASIC為每個10/100埠提供一系列的Rx和TX隊列。ASIC提供跨10/100埠可用的共用記憶體池。有關每個線卡上可用的每個埠緩衝的詳細資訊，請參閱發行說明。此線卡上的每個埠支援兩個Rx隊列和三個TX隊列。一個Rx隊列和一個TX隊列分別表示為絕對優先順序隊列。這相當於低延遲隊列，非常適合於延遲敏感型流量，例如IP語音(VoIP)流量。

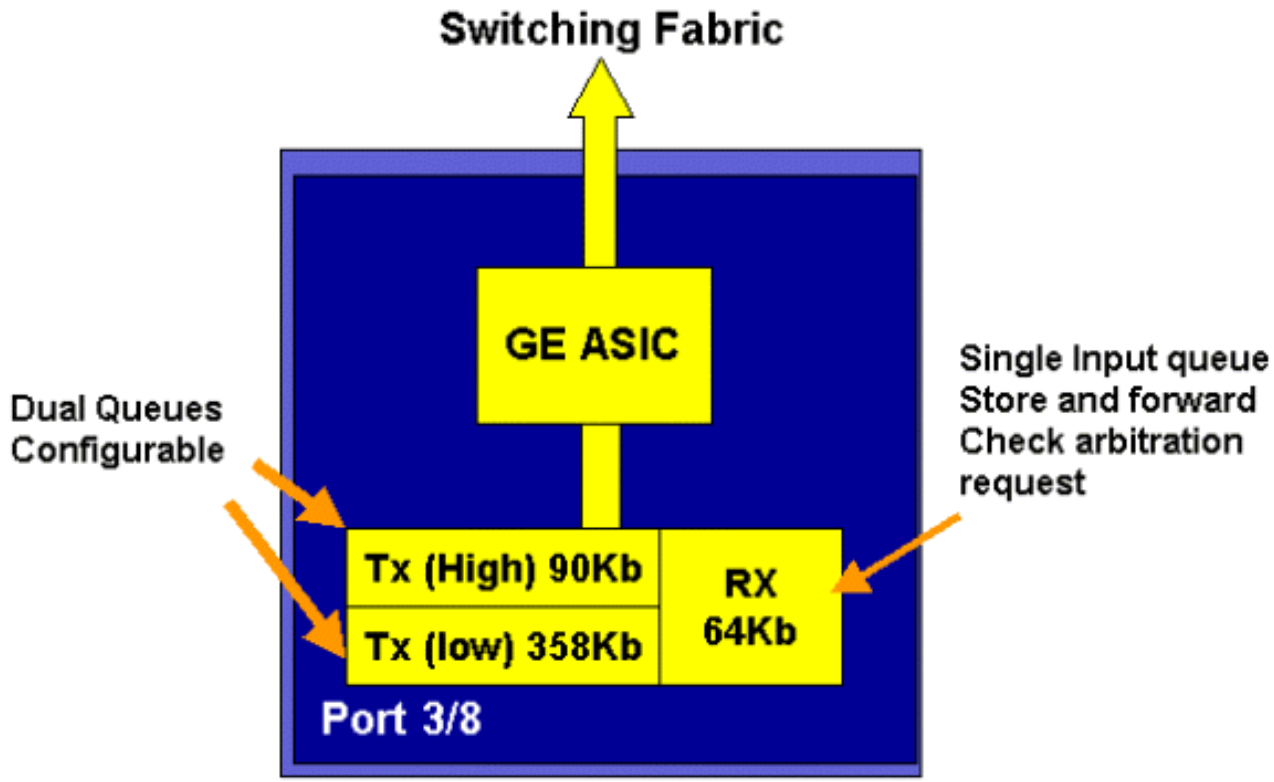


GE線卡(WS-X6408A、WS-X6516、WS-X6816)

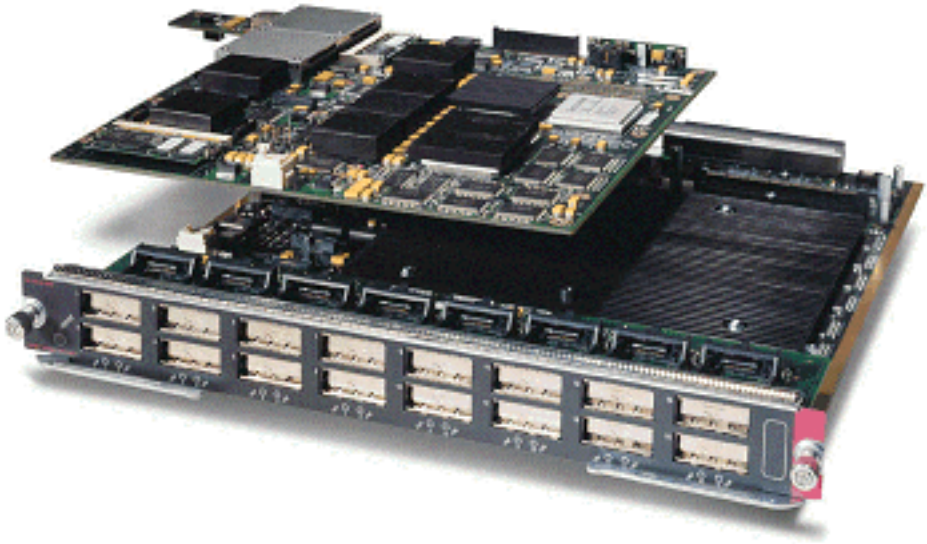
對於GE線卡，ASIC為每個埠提供512 K的緩衝。下圖顯示了八埠GE線卡的表示形式。



與10/100埠一樣，每個GE埠有三個隊列，一個Rx和兩個TX隊列。這是WS-X6408-GBIC線卡的預設設定，如下圖所示。

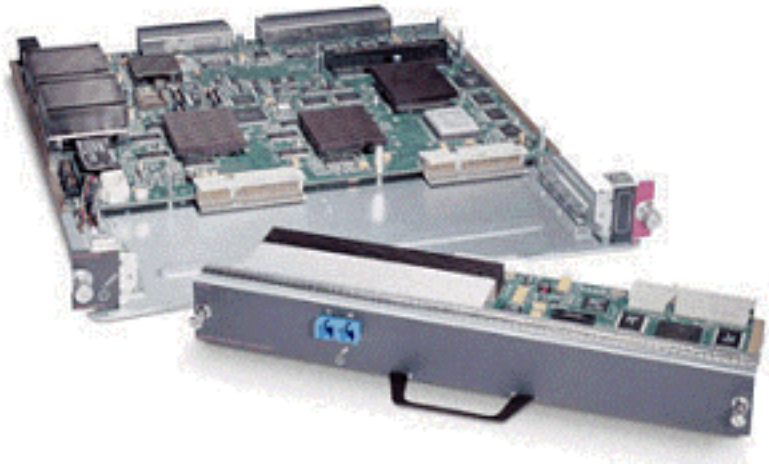


在更新的線路16埠GE卡、SupIA和SupII上的GBIC埠以及WS-X6408A-GBIC 8埠GE卡上，提供兩個額外的嚴格優先順序(SP)隊列。一個SP隊列被分配為Rx隊列，另一個隊列被分配為TX隊列。此SP隊列主要用於排隊延遲敏感流量（如語音）。使用SP隊列時，置於此隊列中的任何資料都將先於高隊列和低隊列中的資料進行處理。只有當SP隊列為空時，才會為高、低隊列提供服務。



10 GE線卡(WS-X6502-10GE)

2001年下半年，思科推出了一組10 GE線卡，每個線卡提供一個10 GE埠。此模組從6000機箱中抽出一個插槽。10 GE線卡支援QoS。對於10 GE埠，它提供兩個Rx隊列和三個TX隊列。一個Rx隊列和一個TX隊列分別指定為SP隊列。還為埠提供緩衝，提供總計256K的Rx緩衝和64MB的TX緩衝。此連線埠為Rx端實作1p1q8t佇列結構，為TX端實作1p2q1t佇列結構。稍後將詳細介紹隊列結構。



Catalyst 6000系列QoS硬體摘要

下表詳細列出了Catalyst 6000系列中執行上述QoS功能的硬體元件。

QoS Process	Catalyst 6500 Component that performs function
Input Scheduling	Performed by port ASIC's L2 only with or without the PFC
Classification	Performed by Supervisor or PFC L2 only is done by Supervisor L2/3 is done by PFC
Policing	Done by PFC via L3 forwarding Engine
Packet Re-write	Done by port ASIC's L2/L3 based on classification done in point 2 above
Output Scheduling	Done by port ASIC's L2/L3 based on classification done in point 2 above

適用於QoS的Catalyst 6000系列軟體支援

Catalyst 6000系列支援兩種作業系統。最初的軟體平台CatOS是從Catalyst 5000平台上使用的代碼庫衍生而來。最近，思科引入了整合式Cisco IOS ®（本機模式）（先前稱為本地IOS），它使用源自思科路由器IOS的代碼庫。兩個作業系統平台(CatOS和整合Cisco IOS（本地模式）)均實施軟體支援，以便使用前面部分中描述的硬體在Catalyst 6000交換機系列平台上啟用QoS。

附註：本文檔使用來自兩個作業系統平台的配置示例。

IP和乙太網路中的優先順序機制

對於要應用到資料的任何QoS服務，必須有一種方法對IP資料包或乙太網幀進行標籤或確定優先順序。ToS和CoS欄位用於實現此目的。

ToS

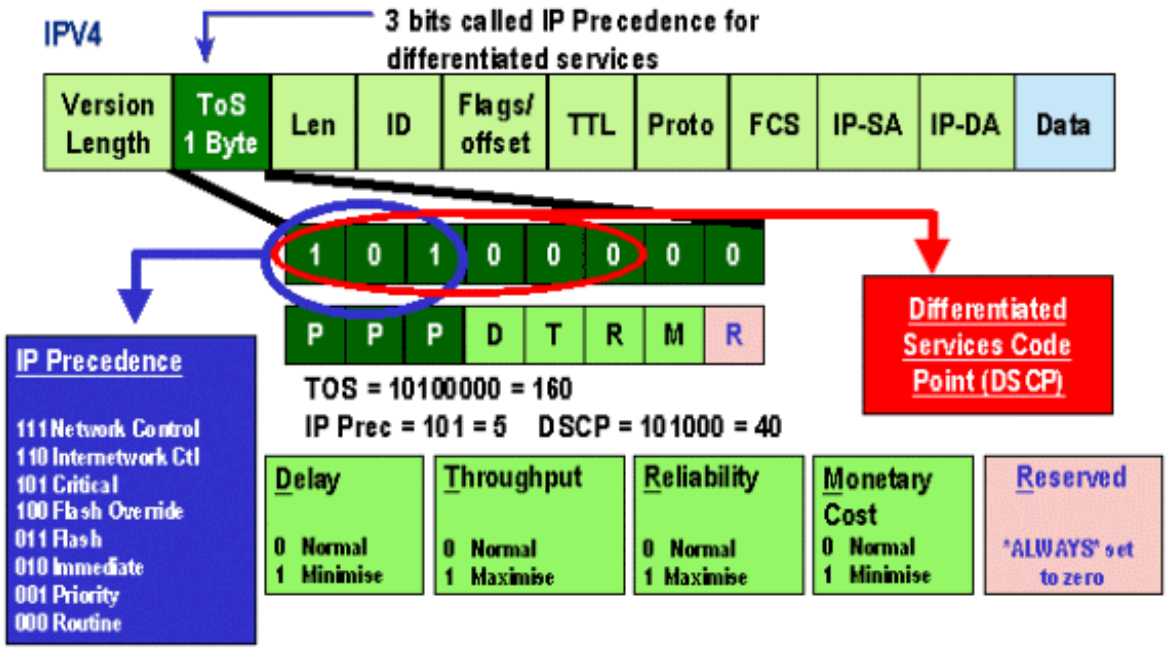
ToS是IPV4標頭中存在的一個單位元組欄位。ToS欄位由八位組成，其中前三位用於表示IP資料包的優先順序。前三個位稱為IP優先位元。這些位可以從0設定為7，其中0表示最低優先順序，7表示

最高優先順序。多年來一直支援在IOS中設定IP優先順序。MSFC或PFC（獨立於MSFC）可以支援重置IP優先順序。不可信的信任設定還可以清除傳入幀上的任何IP優先順序設定。

可以為IP優先順序設定的值如下：

IP Precedence bits	IP Precedence Value
000	Routine
001	Priority
010	Intermediate
011	Flash
100	Flash Override
101	Critical
110	Internetwork Control
111	Network Control

下圖顯示ToS報頭中的IP優先順序位。三個最高有效位元(MSB)將解釋為IP優先位元。



最近，ToS欄位的使用已經擴展為包括六個MSB（稱為DSCP）。DSCP產生可分配給IP資料包的64個優先順序值（二為六的冪）。

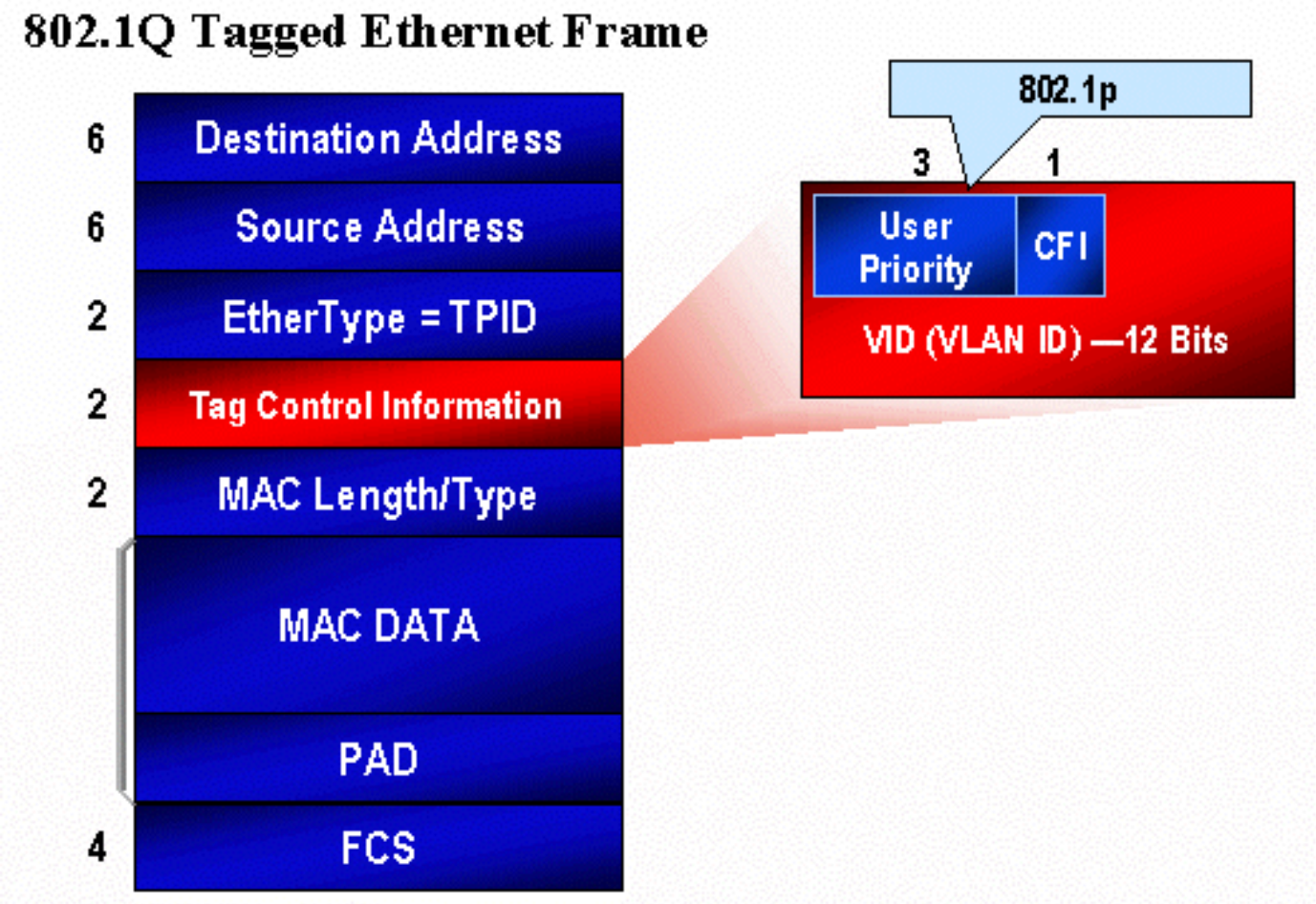
Catalyst 6000系列可以操縱ToS。這可以同時使用PFC和/或MSFC來實現。當幀進入交換機時，將為其分配DSCP值。此DSCP值在交換機內部使用，用於分配由管理員定義的服務級別（QoS策略）。DSCP可以存在於幀中並且可以使用，或者DSCP可以從幀中的現有CoS、IP優先順序或DSCP中匯出（如果埠受信任）。在交換機內部使用對映來匯出DSCP。使用八個可能的CoS/IP優先順序值和64個可能的DSCP值，預設對映將將CoS/IPrec 0對映到DSCP 0，將CoS/IPrec 1對映到DSCP 7，將CoS/IPrec 2對映到DSCP 15，依此類推。管理員可以覆蓋這些預設對映。當幀被排程到出站埠時，可以重寫CoS，並使用DSCP值來派生新的CoS。

CoS

CoS是指ISL標頭或802.1Q標頭中的三個位元，用來表示乙太網幀通過交換網路時的優先順序。就

本文檔而言，我們僅提及使用802.1Q報頭。802.1Q報頭中的CoS位通常稱為802.1p位。毫不奇怪，有三個CoS位元，它們匹配用於IP優先順序的位數。在許多網路中，為了保持端到端的QoS，資料包可能會同時經過第2層和第3層域。為了維護QoS，ToS可以對映到CoS，CoS可以對映到ToS。

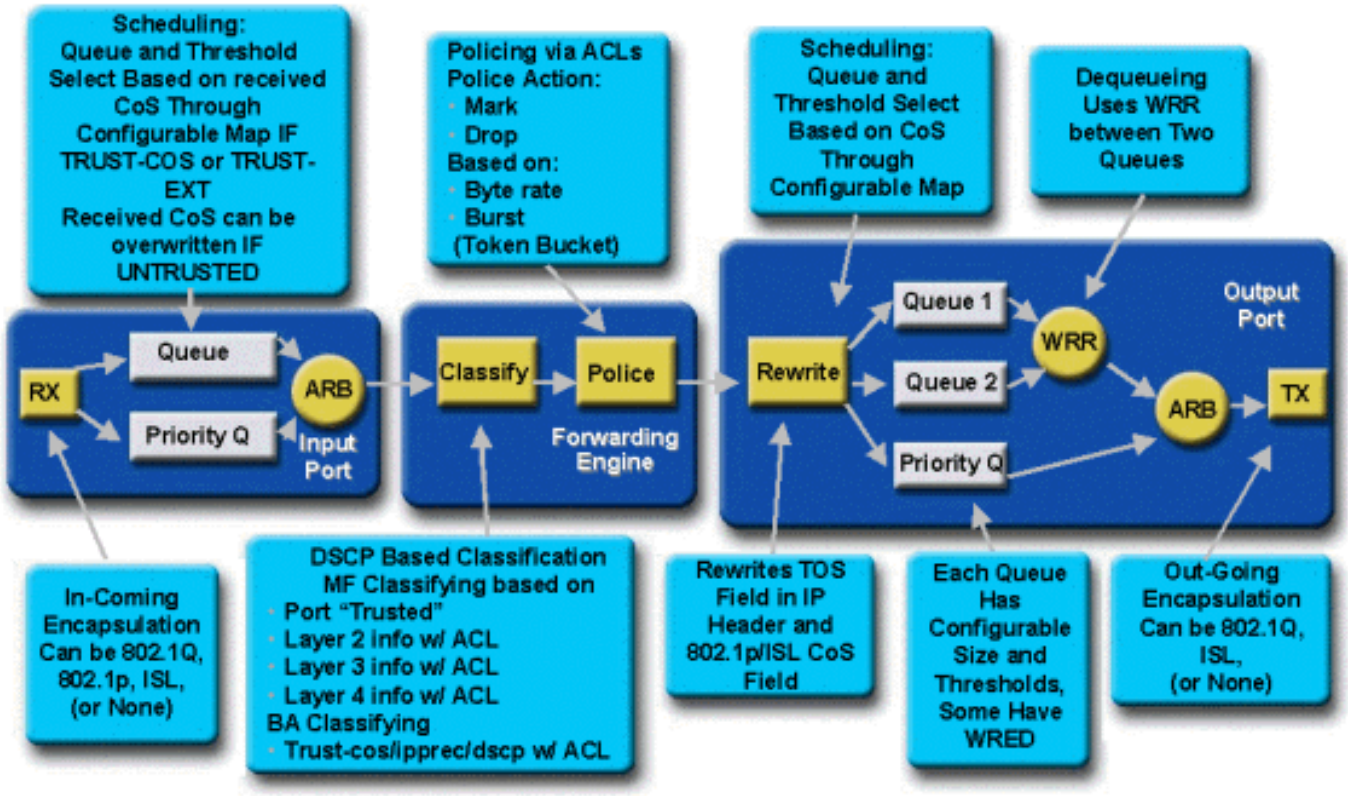
下圖為使用802.1Q欄位標籤的乙太網幀，該欄位由兩位元組Ethertype和兩位元組標籤組成。在兩個位元組標籤內是使用者優先順序位（稱為802.1p）。



Catalyst 6000系列中的QoS流

Catalyst 6000系列中的QoS是當前所有Cisco Catalyst交換機中最全面的QoS實施。以下各節介紹在幀經過交換機時如何對其應用各種QoS進程。

在本文檔的前面部分，我們注意到許多L2和L3交換機可以提供許多QOS元素。這些元素包括分類、輸入隊列排程、管制、重寫和輸出隊列排程。與Catalyst 6000系列的不同之處在於，這些QoS元素由第2層引擎應用，該引擎可深入瞭解第3層和第4層詳細資訊，以及僅瞭解L2報頭資訊。下圖總結了Catalyst 6000系列如何實施這些元素。



幀進入交換機，最初由接收該幀的埠ASIC處理。它將將該幀置於Rx隊列中。根據Catalyst 6000系列線卡，將有一個或兩個Rx隊列。

埠ASIC將使用CoS位指示將幀放入哪個隊列（如果存在多個輸入隊列）。 如果埠被歸類為不可信，則埠ASIC可以根據預定義的值覆蓋現有的CoS位。

然後將幀傳遞到L2/L3轉發引擎(PFC),PFC將對幀進行分類並選擇性地控制（速率限制）。分類是指為幀分配一個DSCP值的過程，交換機內部使用該值來處理幀。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. 接收的IP優先順序位已經在IPV4報頭中設定。由於DSCP值有64個，而只有8個IP優先順序值，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。與IP優先順序類似，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預設對映。
4. 使用通常通過訪問控制清單(ACL)條目分配的DSCP預設值設定幀。

將DSCP值分配給幀後，如果存在策略配置，則應用策略（速率限制）。策略將通過丟棄或標籤超出配置檔案的流量來限制通過PFC的資料流。Out-of-profile是一個術語，用於指示流量已超過管理員定義的限制，即PFC將每秒傳送的位數。超出設定檔的流量可能遭捨棄，也可能被降級CoS值。PFC1和PFC2目前僅支援輸入管制（速率限制）。 發佈新的PFC後，將對輸入和輸出策略提供支援。

然後，PFC會將幀傳遞到輸出埠進行處理。此時，會呼叫重寫過程來修改幀中的CoS值和IPV4報頭中的ToS值。這是從內部DSCP派生的。然後，該幀將基於其CoS值放入傳輸隊列中，準備傳輸。當幀在隊列中時，埠ASIC將監控緩衝區並實施WRED以避免緩衝區溢位。然後使用WRR排程演算法來排程並傳輸來自輸出埠的幀

下面的每個部分將更詳細地探討此流程，並給出上述每個步驟的配置示例。

隊列、緩衝區、閾值和對映

在詳細描述QoS配置之前，必須進一步解釋某些術語，以確保您完全瞭解交換機的QoS配置功能。

隊列

交換機上的每個埠都有一系列輸入和輸出隊列，這些隊列用作資料的臨時儲存區域。Catalyst 6000系列線卡為每個埠實現不同的隊列數。隊列通常在每個埠的硬體ASIC中實施。在第一代Catalyst 6000系列線卡上，典型配置是一個輸入隊列和兩個輸出隊列。在較新的線卡（10/100和GE）上，ASIC實施一組額外的2個隊列（1個輸入和1個輸出），從而產生2個輸入隊列和3個輸出隊列。這兩個額外隊列是用於延遲敏感流量（例如VoIP）的特殊SP隊列。它們以SP方式提供服務。也就是說，如果幀到達SP隊列，則停止排程來自較低隊列的幀以處理SP隊列中的幀。只有當SP隊列為空時，才會重新安排來自較低隊列的資料包。

當幀在擁塞時到達埠（用於輸入或輸出）時，它將被置於隊列中。通常根據傳入幀的乙太網報頭中的CoS值來決定幀位於哪個隊列後面。

在輸出時，將採用排程演算法清空TX（輸出）隊列。WRR是實現這一點的技術。對於每個隊列，加權用於指定在移至下一個隊列之前將從隊列中清空多少資料。管理員指定的權重是一個介於1和255之間的數字，該權重分配給每個TX隊列。

緩衝區

為每個隊列分配一定量的緩衝空間以儲存傳輸資料。位於埠ASIC上的是記憶體，它按埠進行拆分和分配。對於每個GE埠，GE ASIC分配512K的緩衝空間。對於10/100埠，埠ASIC為每個埠緩衝保留64 K或128 K（取決於線卡）。然後，此緩衝區空間在Rx（輸入）隊列和TX（輸出）隊列之間劃分。

閾值

一般資料傳輸的一個方面是，如果封包遭捨棄，將導致該封包被重新傳輸（TCP資料流）。 在擁塞時，這會增加網路的負載，並可能導致緩衝區過載更多。為了確保緩衝區不溢位，Catalyst 6000系列交換機採用多種技術來避免發生這種情況。

閾值是由交換機（或管理員）分配的假想級別，它定義了擁塞管理演算法可以從隊列中開始丟棄資料的利用率點。在Catalyst 6000系列埠上，通常有四個與輸入隊列關聯的閾值。通常有兩個閾值與輸出隊列相關聯。

在QoS環境中還部署這些閾值，作為為這些閾值分配具有不同優先順序的幀的方法。當緩衝區開始填充且超出閾值時，管理員可以將不同的優先順序對映到不同的閾值，以指示交換機在超出閾值時應丟棄哪些幀。

對映

在上述隊列和閾值部分中，有人提到，乙太網幀中的CoS值用於確定將幀放入哪個隊列，以及在緩衝區填充的哪個點是符合丟棄條件的幀。這就是對映的目的。

在Catalyst 6000系列上配置QoS時，會啟用定義以下內容的預設對映：

- 具有特定CoS值的幀符合丟棄的條件
- 將幀放入哪個隊列（基於其CoS值）

如果存在預設對映，管理員可以覆蓋這些預設對映。存在以下專案的對映：

- 傳入幀上的CoS值變為DSCP值

- 傳入幀的IP優先順序值變為DSCP值
- DSCP值為傳出幀的CoS值
- 用於在接收隊列上丟棄閾值的CoS值
- CoS值，用於在傳輸隊列上丟棄閾值
- 超出管制語句的幀的DSCP降級值
- 具有特定目的MAC地址的幀的CoS值

WRED和WRR

WRED和WRR是Catalyst 6000系列上存在的兩個功能非常強大的演算法。WRED和WRR都使用乙太網幀內的優先順序標籤(CoS)來提供增強的緩衝區管理和出站排程。B

WRED

WRED是Catalyst 6000系列使用的緩衝區管理演算法，用於最小化在擁塞時丟棄高優先順序流量的影響。WRED基於RED演算法。

為了瞭解RED和WRED，請重新訪問TCP流量管理的概念。流量管理可確保TCP傳送方不會淹沒網路。TCP慢啟動演算法是解決此問題的解決方案的一部分。它指示流量開始時，在等待確認之前傳送單個資料包。然後，在接收一個ACK之前傳送兩個資料包，逐漸增加接收每個ACK之前傳送的資料包數量。這將繼續進行，直到流量達到網路可以處理的傳輸層級(即，傳送*x*封包數量)，而不會造成負載擁塞。如果發生擁塞，慢啟動演算法將限制視窗大小（即等待確認之前傳送的資料包數量），從而降低該TCP會話（流）的總體效能。

RED將在隊列開始填充時監視該隊列。超過某個閾值後，資料包將開始隨機丟棄。沒有考慮具體資金流動；而是丟棄隨機資料包。這些資料包可能來自高優先順序流或低優先順序流。丟棄的資料包可以是單個資料流或多個TCP資料流的一部分。如果如上所述多個流受到影響，則可能會對每個流視窗大小產生相當大的影響。

與RED不同的是，WRED在丟棄幀時並不是隨機的。WRED會考慮訊框的優先順序（在Catalyst 6000系列的情況中，它使用CoS值）。 使用WRED時，管理員會為具有特定CoS值的幀分配特定閾值。一旦超過這些閾值，具有對映到這些閾值的CoS值的幀就有資格被丟棄。CoS值指定給更高閾值的其他幀將保留在隊列中。此程式可讓較高優先順序的流量保持不變，而保留其較大的視窗大小，並將從傳送者傳送到接收者的封包所涉及的延遲降至最低。

如何知道您的線卡是否支援WRED?發出以下命令。在輸出中，檢查指示該埠支援WRED的部分。

```
Console> show qos info config 2/1
QoS setting in NVRAM:
QoS is enabled
Port 2/1 has 2 transmit queue with 2 drop thresholds (2q2t).
Port 2/1 has 1 receive queue with 4 drop thresholds (1q4t).
Interface type:vlan-based
ACL attached:
The qos trust type is set to untrusted.
Default CoS = 0
Queue and Threshold Mapping:
Queue Threshold CoS
----- --------- ---------------
1     1         0 1
1     2         2 3
```

```
2     1         4 5
2     2         6 7
Rx drop thresholds:
Rx drop thresholds are disabled for untrusted ports.
Queue #  Thresholds - percentage (abs values)
-------  ---------------------------------
1        50% 60% 80% 100%
TX drop thresholds:
Queue #  Thresholds - percentage (abs values)
-------  ---------------------------------
1        40% 100%
2        40% 100%
TX WRED thresholds:
WRED feature is not supported for this port_type.
!-- Look for this. Queue Sizes: Queue # Sizes - percentage (abs values) ------- ----------------
-------------------- 1 80% 2 20% WRR Configuration of ports with speed 1000MBPS: Queue # Ratios
(abs values) ------- ----------------------------------- 1 100 2 255 Console> (enable)
```

如果WRED在埠上不可用，則該埠將使用緩衝區管理的尾部丟棄方法。尾部丟棄（顧名思義）只是一旦緩衝區已完全使用後丟棄傳入幀。

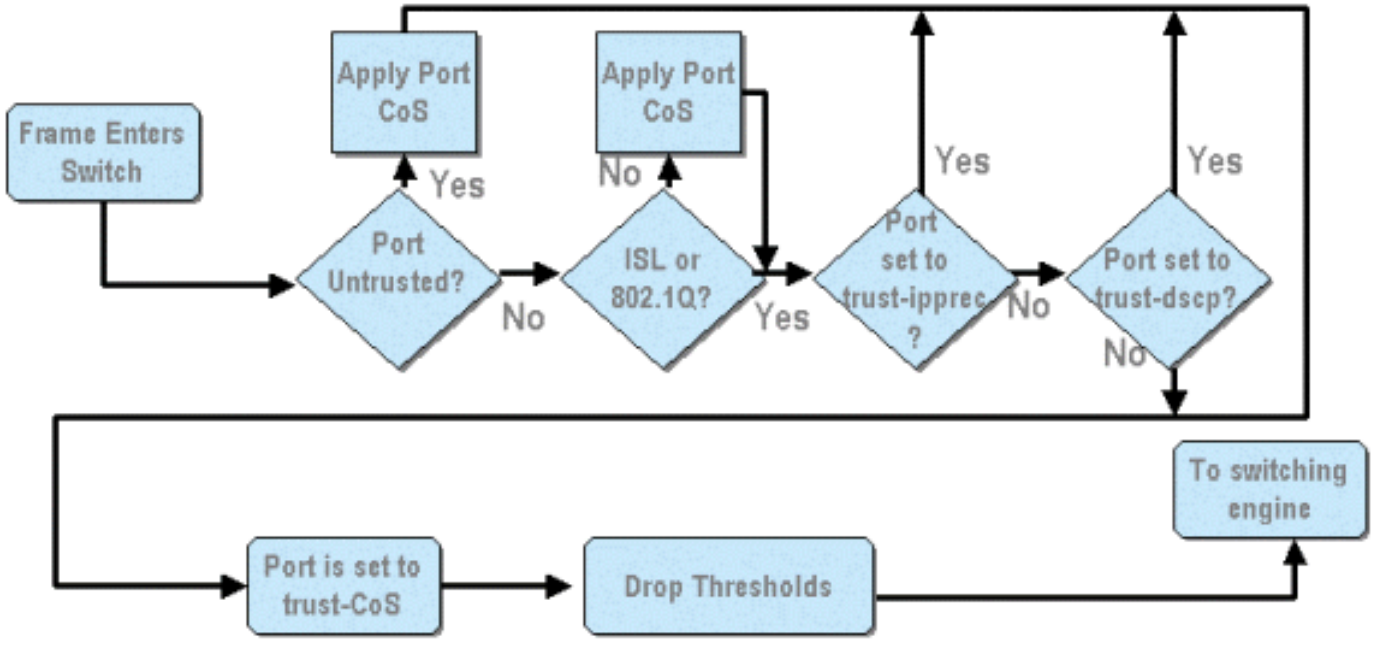
WRR

WRR用於計畫來自TX隊列的輸出流量。在移至下一個隊列之前，常規輪詢演算法將在TX隊列之間交替傳送，從每個隊列傳送相同數量的資料包。WRR的加權特性允許排程演算法檢查已分配給隊列的加權。這允許定義的隊列訪問更多的頻寬。與其他隊列相比，WRR排程演算法將清空標識隊列中的更多資料，從而為指定隊列提供偏差。

WRR的配置以及上述內容的其他方面將在以下章節中說明。

在Catalyst 6000系列上配置基於ASIC的埠QoS

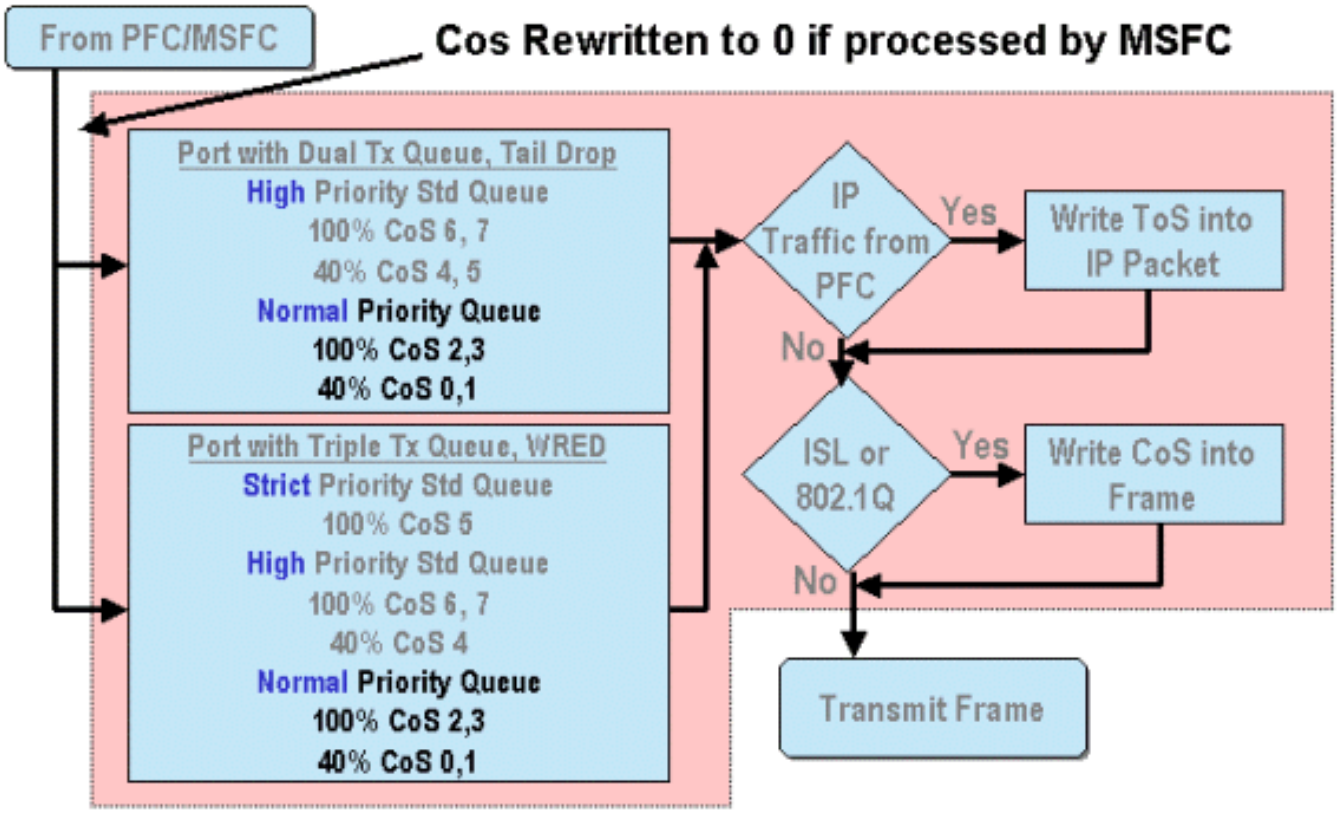
QoS配置指示埠ASIC或PFC執行QoS操作。以下各節將介紹這兩個進程的QoS配置。在埠ASIC上，QoS配置會影響入站和出站通訊流。



從上圖可以看出，應用以下QoS配置過程：

1. 信任埠狀態

2. 應用基於埠的CoS
3. Rx丟棄閾值分配
4 CoS到Rx丟棄閾值對映



當幀由MSFC或PFC處理時，會將其傳遞到出站埠ASIC以進行進一步處理。MSFC處理的任何幀的CoS值都將重置為零。出站埠上的QoS處理需要考慮這一點。

上圖顯示埠ASIC對出站流量執行的QoS處理。對出站QoS處理呼叫的一些進程包括：

1. TX尾部丟棄和WRED閾值分配

2. CoS到TX尾部丟棄和WRED對映

此外，在上圖中未顯示的是使用DSCP到CoS對映將CoS重新分配到出站幀的過程。

以下各節將詳細分析基於埠的ASIC的QoS配置功能。

附註：需要強調的重要一點是，使用CatOS呼叫QoS命令時，它們通常適用於具有指定隊列型別的所有埠。例如，如果將WRED丟棄閾值應用於隊列型別為1p2q2t的埠，則此WRED丟棄閾值應用於支援此隊列型別的所有線卡上的所有埠。使用Cat IOS時，QoS命令通常應用於介面級別。

啟用QoS

在Catalyst 6000系列上執行任何QOS配置之前，必須先在交換機上啟用QoS。這可以通過發出以下命令來實現：

CatOS

```
Console> (enable) set qos enable
!-- QoS is enabled. Console> (enable)
```

整合Cisco IOS（本機模式）

```
Cat6500(config)# mls qos
```

在Catalyst 6000系列中啟用QoS時，交換機將為交換機設定一系列QoS預設值。這些預設值包括以下設定：

QoS Feature	Default setting
Trust state of each port	Un-trusted
Receive Queue drop threshold percentages	Threshold 1 – 50% Threshold 2 – 60% Threshold 3 – 80% Threshold 4 – 100%
Transmit Queue drop threshold percentages	Low priority queue threshold 1 – 80% Low priority queue threshold 2 – 100% High priority queue threshold 1 – 80% High priority queue threshold 2 – 100%
CoS value to Drop threshold mapping	Receive queue 1/drop threshold 1: CoS 0 and 1 Transmit queue 1/drop threshold 1: CoS 0 and 1 Receive queue 1/drop threshold 2: CoS 2 and 3 Transmit queue 1/drop threshold 2: CoS 2 and 3 Receive queue 1/drop threshold 3: CoS 4 and 5 Transmit queue 2/drop threshold 1: CoS 4 and 5 Receive queue 1/drop threshold 4: CoS 6 and 7

	Transmit queue 2/drop threshold 2: CoS 6 and 7
CoS to DSCP Mapping (DSCP set from CoS value)	CoS 0 = DSCP 0 CoS 1 = DSCP 8 CoS 2 = DSCP 16 CoS 3 = DSCP 24 CoS 4 = DSCP 32 CoS 5 = DSCP 40 CoS 6 = DSCP 48 CoS 7 = DSCP 56
IP Precedence to DSCP Map (DSCP set from IP Precedence value)	IP precedence 0 = DSCP 0 IP precedence 1 = DSCP 8 IP precedence 2 = DSCP 16 IP precedence 3 = DSCP 24 IP precedence 4 = DSCP 32 IP precedence 5 = DSCP 40 IP precedence 6 = DSCP 48 IP precedence 7 = DSCP 56
DSCP to CoS map (CoS set from DSCP values)	DSCP 0-7 = CoS 0 DSCP 8-15 = CoS 1 DSCP 16-23 = CoS 2 DSCP 24-31 = CoS 3 DSCP 32-39 = CoS 4 DSCP 40-47 = CoS 5 DSCP 48-55 = CoS 6 DSCP 56-63 = CoS 7

受信任和不受信任的埠

Catalyst 6000系列上的任何給定埠都可以配置為受信任或不受信任埠的受信任狀態決定了它在傳輸交換機時標籤、分類和排程幀的方式。預設情況下，所有埠都處於不可信狀態。

不可信埠（埠的預設設定）

如果埠配置為不受信任的埠，則最初進入埠的幀的CoS和ToS值將由埠ASIC重置為零。這表示訊框將通過交換器的路徑會獲得最低優先順序的服務。

或者，管理員可以將進入不可信埠的任何乙太網幀的CoS值重置為預先確定的值。稍後部分將討論配置此功能。

將埠設定為不可信將指示交換機不執行任何擁塞規避。擁塞迴避是一種方法，用於在幀超過為該隊列定義的閾值時，根據幀的CoS值丟棄幀。一旦緩衝區達到100%，進入此埠的所有幀同樣有資格被丟棄。

在CatOS中，可通過發出以下命令將10/100或GE埠配置為不可信：

CatOS

```
Console> (enable) set port qos 3/16 trust untrusted
!-- Port 3/16 qos set to untrusted. Console> (enable)
```

此命令將模組3上的埠16設定為不可信狀態。

附註：對於整合Cisco IOS（本機模式），軟體當前僅支援為GE埠設定信任。

整合Cisco IOS（本機模式）

```
Cat6500(config)# interface gigabitethernet 1/1
Cat6500(config-if)# no mls qos trust
```

在上方範例中，我們輸入介面組態，並套用命令的**no**形式，將連線埠設定為不受信任，因為這是IOS。

可信埠

有時，進入交換機的乙太網幀會具有CoS或ToS設定，管理員希望交換機在幀經過交換機時對其進行維護。對於此流量，管理員可將進入交換機的流量的埠的信任狀態設定為受信任。

如前所述，交換機在內部使用DSCP值為該幀分配預定級別的服務。當幀進入受信任埠時，管理員可以配置該埠以檢視現有的CoS、IP優先順序或DSCP值以設定內部DSCP值。或者，管理員可以為進入埠的每個資料包設定預定義的DSCP。

可通過發出以下命令將埠的信任狀態設定為可信：

CatOS

```
Console> (enable) set port qos 3/16 trust trust-cos
!-- Port 3/16 qos set to trust-COs Console> (enable)
```

此命令適用於WS-X6548-RJ45線卡，並將埠3/16的信任狀態設定為可信。交換機將使用傳入幀中設定的CoS值來設定內部DSCP。DSCP是從在交換機上啟用QoS時建立的預設對映派生的，也可以是從管理員定義的對映派生的。管理員還可以使用trust-dscp或trust-ipprec關鍵字代替trust-COs關鍵字。

在先前的10/100線卡（WS-X6348-RJ45和WS-X6248-RJ45）上，需要發出**set qos acl**命令來設定埠信任。在此命令中，可以使用**set qos acl**命令的子引數指定信任狀態。不支援在這些線卡上的埠上設定信任CoS，如下所示。

```
Console> (enable) set port qos 4/1 trust trust-COs
Trust type trust-COs not supported on this port.
!-- Trust-COs not supported, use acl instead. Rx thresholds are enabled on port 4/1. !-- Need to
turn on input queue scheduling. Port 4/1 qos set to untrusted. !-- Trust-COs not supported, so
port is set to untrusted.
```

上面的命令表明需要啟用輸入隊列排程。因此，對於WS-X6248-RJ45和WS-X6348-RJ45線卡上的10/100埠，仍然必須配置**set port qos x/y trust-COs**命令，儘管要設定信任狀態，必須使用ACL。

使用整合Cisco IOS（本地模式），可以在新的WS-X6548-RJ45線卡的GE介面和10/100埠上執行信任設定。

整合Cisco IOS（本機模式）

```
Cat6500(config)# interface gigabitethernet 5/4
```

```
Cat6500(config-if)# mls qos trust ip-precedence
Cat6500(config-if)#
```

此示例將GE埠5/4的信任狀態設定為可信。幀的IP優先順序值將用於匯出DSCP值。

基於輸入分類和設定埠的CoS

在向交換機埠輸入時，如果乙太網幀滿足以下兩個條件之一，則可以更改其CoS:

1. 埠配置為不可信，或
2. 乙太網幀未設定現有的CoS值

如果要重新配置傳入乙太網幀的CoS，應發出以下命令：

CatOS

```
Console> (enable) set port qos 3/16 cos 3
!-- Port 3/16 qos set to 3. Console> (enable)
```

當未標籤的幀到達時，或者如果埠設定為不可信，此命令將模組3上的埠16上的傳入乙太網幀的CO值設定為3。

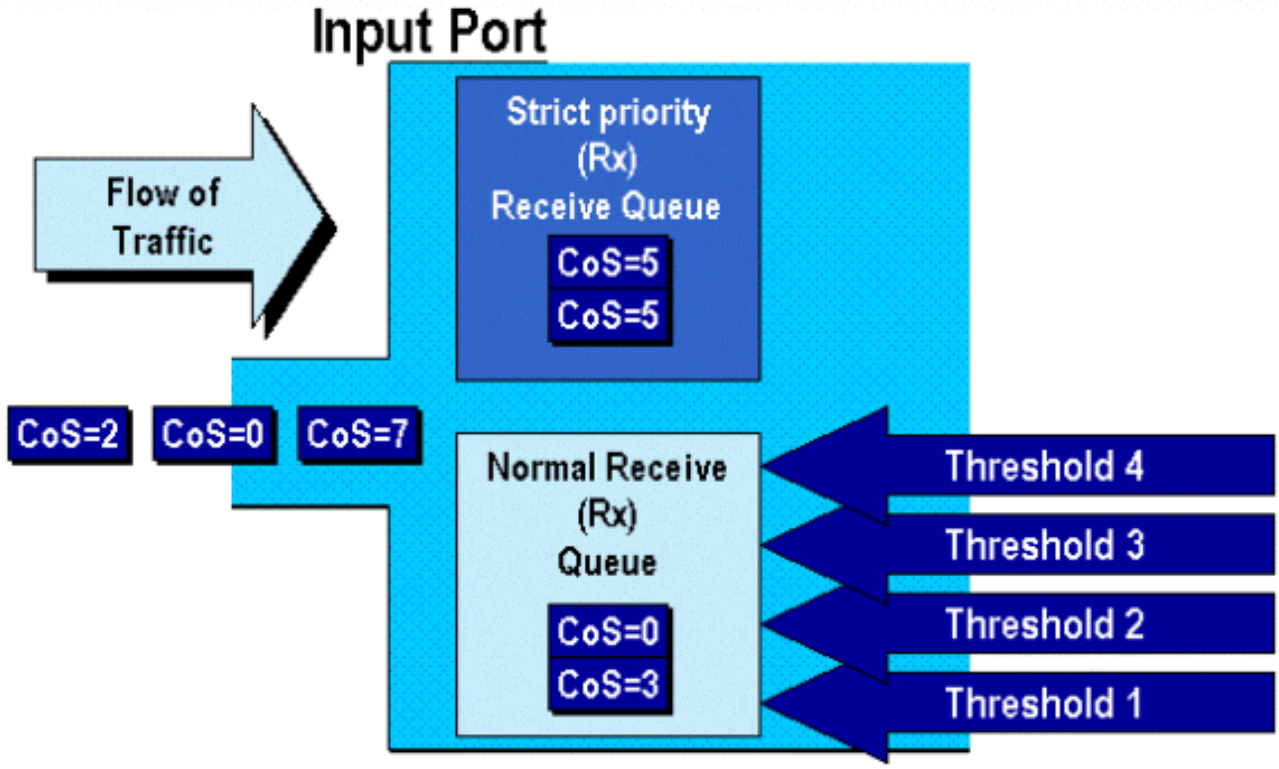
整合Cisco IOS（本機模式）

```
Cat6500(config)# interface fastethernet 5/13
Cat6500(config-if)# mls qos COs 4
Cat6500(config-if)#
```

當未標籤的幀到達時，或者如果埠設定為不可信，此命令將模組5上的埠13上的傳入乙太網幀的CO值設定為4。

配置Rx丟棄閾值

在輸入交換機埠時，該幀將被置於Rx隊列中。為避免緩衝區溢位，埠ASIC對每個Rx隊列實施四個閾值，並使用這些閾值來識別超出這些閾值後可丟棄的幀。埠ASIC將使用幀設定COs值來識別超過閾值時可以丟棄的幀。當發生擁塞時，此功能允許更高優先順序的幀在緩衝區中保留更長時間。



如上圖所示，幀到達並放置在隊列中。當隊列開始填充時，埠ASIC會監控閾值。超過閾值時，會從隊列中隨機丟棄具有管理員識別的CO值的幀。1q4t隊列（在WS-X6248-RJ45和WS-X6348-RJ45線卡上找到）的預設閾值對映如下：

- 閾值1設定為50%，且CO值0和1對映到此閾值
- 閾值2設定為60%，且CO值2和3對映到此閾值
- 閾值3設定為80%，且COs值4和5對映到此閾值
- 閾值4設定為100%，且COs值6和7對映到此閾值

對於1P1q4t（在GE埠上找到）隊列，預設對映如下所示：

- 閾值1設定為50%，且CO值0和1對映到此閾值
- 閾值2設定為60%，且CO值2和3對映到此閾值
- 閾值3設定為80%，且COs值4對映到此閾值
- 閾值4設定為100%，且COs值6和7對映到此閾值
- COs值5對映到嚴格優先順序隊列

對於1p1q0t（在WS-X6548-RJ45線卡的10/100埠上找到），預設對映如下：

- 具有CO 5的幀將進入SP Rx隊列（隊列2），在此隊列中，交換機僅當SP接收隊列緩衝區已滿100%時才丟棄傳入幀。
- CO為0、1、2、3、4、6或7的幀將進入標準Rx隊列。當Rx隊列緩衝區已滿100%時，交換機將丟棄傳入的幀。

管理員可以更改這些丟棄閾值。此外，還可以更改對映到每個閾值的預設CO值。不同的線卡實施不同的Rx隊列實施。隊列型別的概要如下所示。

CatOS

```
Console> (enable) set qos drop-threshold 1q4t rx queue 1 20 40 75 100
!-- Rx drop thresholds for queue 1 set at 20%, 40%, 75%, and 100%. Console> (enable)
```

此命令將具有一個隊列和四個閾值（表示1q4t）的所有輸入埠的接收丟棄閾值設定為20%、40%、75%和100%。

在整合Cisco IOS（本機模式）中發出的命令如下所示。

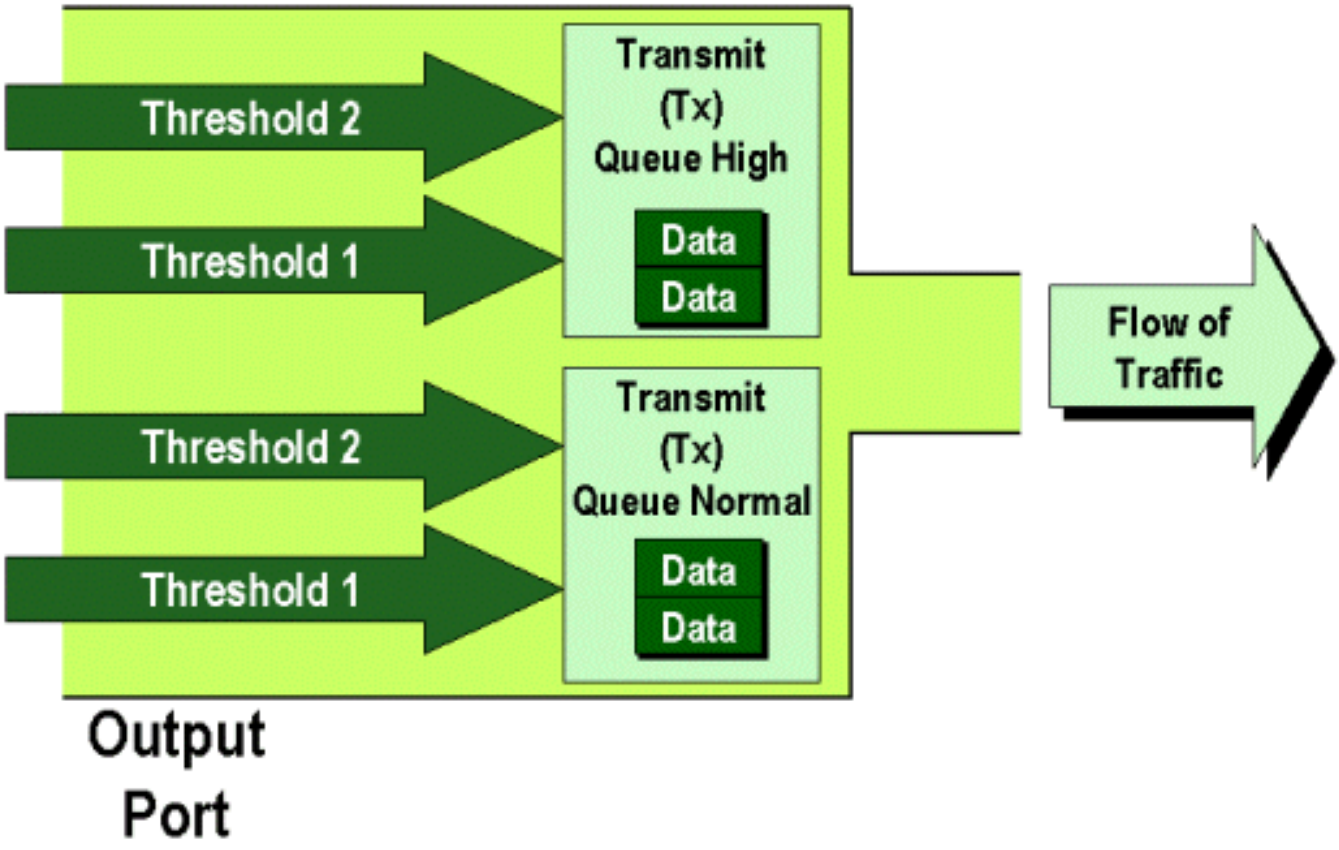
整合Cisco IOS（本機模式）

```
Cat6500(config-if)# wrr-queue threshold 1 40 50
Cat6500(config-if)# wrr-queue threshold 2 60 100

!-- Configures the 4 thresholds for a 1q4t rx queue and. Cat6500(config-if)# rcv-queue threshold
1 60 75 85 100

!-- Configures for a 1p1q4t rx queue, which applies to !-- the new WS-X6548-RJ45 10/100 line
card.
```

Rx丟棄閾值必須由管理員啟用。目前，應該使用**set port qos x/y trust-COs**命令來啟用Rx丟棄閾值(其中*x*是模組編號，*y*是該模組上的埠)。

配置TX丟棄閾值

在輸出埠上，埠將具有兩個TX閾值，它們用作擁塞迴避機制的一部分：隊列1和隊列2。隊列1表示為標準低優先順序隊列，隊列2表示為標準高優先順序隊列。根據使用的線卡，它們將採用尾部丟棄或WRED閾值管理演算法。這兩種演算法都為每個TX隊列使用兩個閾值。



管理員可以按如下方式手動設定這些閾值：

CatOS

```
Console> (enable) set qos drop-threshold 2q2t TX queue 1 40 100
!-- TX drop thresholds for queue 1 set at 40% and 100%. Console> (enable)
```

此命令將具有兩個隊列和兩個閾值（表示2q2t）的所有輸出埠的隊列1的TX丟棄閾值設定為40%和100%。

```
Console> (enable) set qos wred 1p2q2t TX queue 1  60 100
!-- WRED thresholds for queue 1 set at 60% 100% on all WRED-capable 1p2q2t ports. Console>
(enable)
```

此命令將具有一個SP隊列、兩個正常隊列和兩個閾值（表示1p2q2t）的所有輸出埠的隊列1的WRED丟棄閾值設定為60%和100%。隊列1被定義為普通低優先順序隊列，具有最低優先順序。隊列2是高優先順序的普通隊列，其優先順序高於隊列1。隊列3是SP隊列，在該埠上的所有其他隊列之前提供服務。

在整合Cisco IOS（本機模式）中發出的等效命令如下所示。

整合Cisco IOS（本機模式）

```
Cat6500(config-if)# wrr-queue random-detect max-threshold  1 40 100
Cat6500(config-if)#
```

這會將1p2q2t埠的WRED丟棄閾值設定為將閾值1(TX)的WRED丟棄閾值設定為40% ，將閾值2(TX)的WRED丟棄閾值設定為100%。

如果需要，在整合Cisco IOS（本機模式）中也可以禁用WRED。 用於執行此操作的方法是使用命令的**n**"形式。禁用WRED的示例如下所示：

整合Cisco IOS（本機模式）

```
Cat6500(config-if)# no wrr-queue random-detect queue_id
```

將MAC地址對映到COs值

除了根據全域性埠定義設定COs外，交換機還允許管理員根據目標MAC地址和VLAN ID設定COs值。這樣，目的地為特定目標的幀便可以使用預定COs值進行標籤。可通過發出以下命令實現此配置：

CatOS

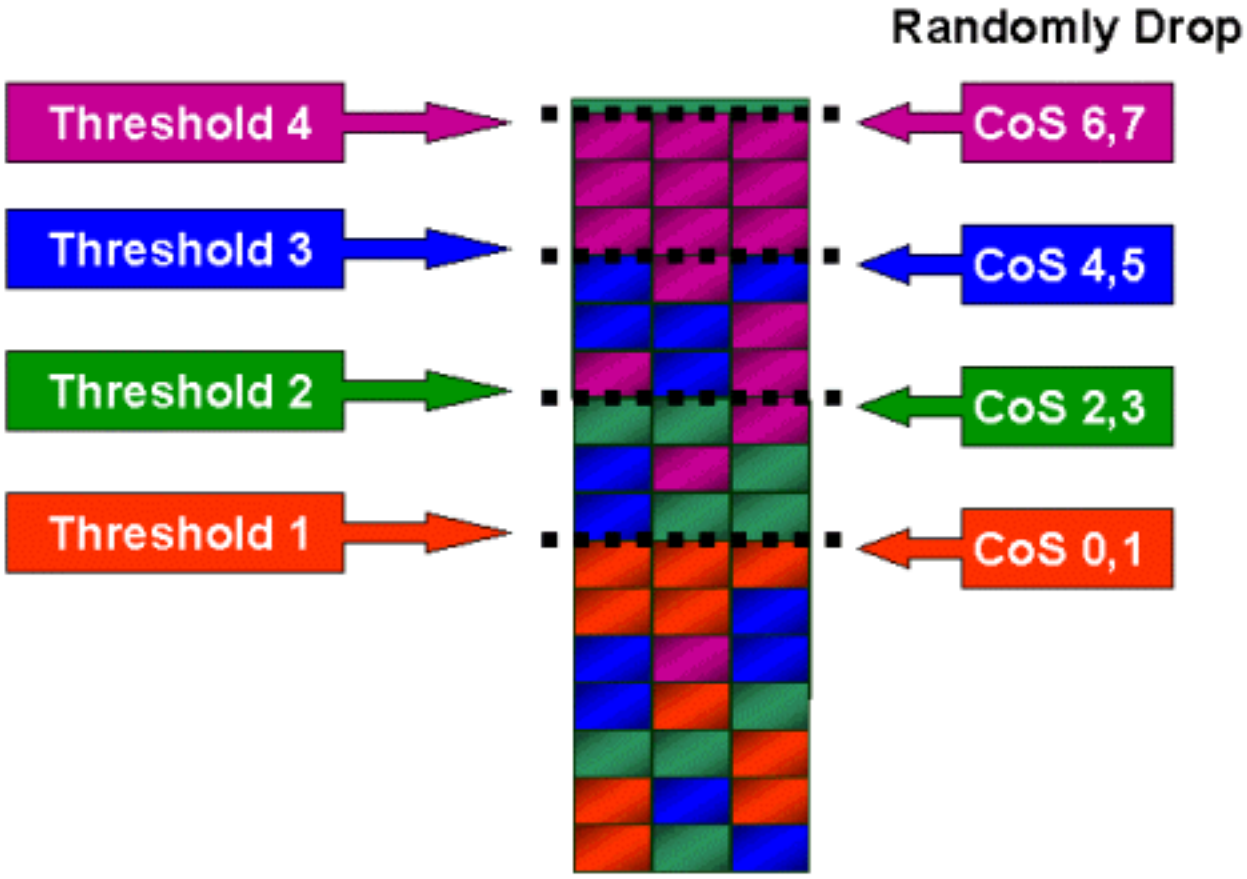
```
Console> (enable) set qos Mac-COs 00-00-0c-33-2a-4e 200 5
!-- COs 5 is assigned to 00-00-0c-33-2a-4e VLAN 200. Console> (enable)
```

此命令將目的MAC地址為00-00-0c-33-2a-4e且來自VLAN 200的任何幀的CO值設定為5。

在整合Cisco IOS（本機模式）中沒有等效命令。 這是因為僅當沒有PFC且整合Cisco IOS（本地模式）需要PFC才能正常工作時，才支援此命令。

將COs對映到閾值

在配置了閾值後，管理員可以將COs值分配給這些閾值，這樣，在超過閾值時，具有特定COs值的幀將被丟棄。通常，管理員會將優先順序較低的幀分配給較低的閾值，從而在發生擁塞時維持隊列中優先順序較高的流量。



上圖顯示了具有四個閾值的輸入隊列，以及如何將CO值分配給每個閾值。

以下輸出顯示了如何將COs值對映到閾值：

CatOS

```
Console> (enable) set qos map 2q2t 1 1 COs 0 1
!-- QoS TX priority queue and threshold mapped to COs successfully. Console> (enable)
```

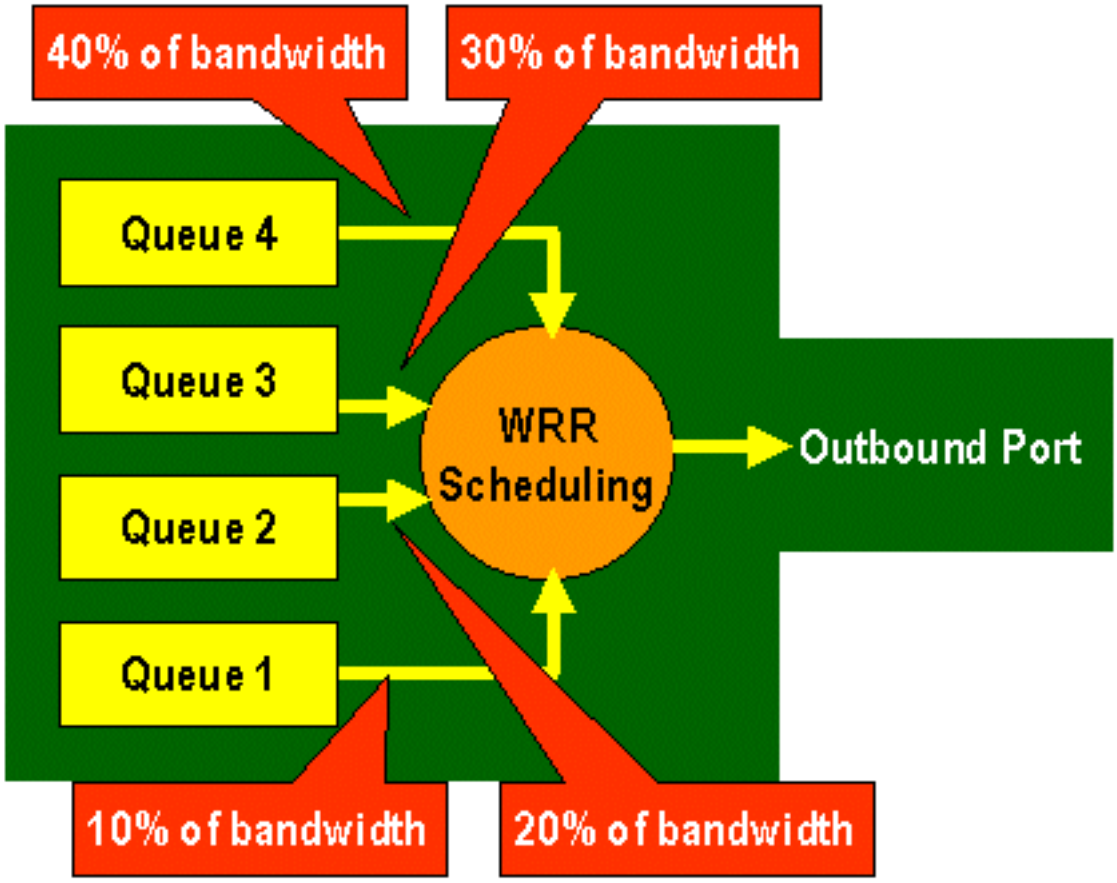
此命令將0和1的CO值分配給隊列1，閾值1。下面顯示了整合Cisco IOS（本地模式）中的等效命令。

整合Cisco IOS（本機模式）

```
Cat6500(config-if)# wrr-queue COs-map  1  1  0  1
Cat6500(config-if)#
```

在TX隊列上配置頻寬

當幀被置於輸出隊列中時，將使用輸出排程演算法傳輸該幀。輸出排程程式進程使用WRR從輸出隊列傳輸幀。根據使用的線卡硬體，每個埠有兩個、三個或四個傳輸隊列。



在WS-X6248和WS-X6348線卡（具有2q2t隊列結構）上，WRR機制使用兩個TX隊列進行排程。在WS-X6548線卡（具有1p3q1t隊列結構）上有四個TX隊列。在這四個TX隊列中，三個TX隊列通過WRR演算法提供服務（最後一個TX隊列是SP隊列）。 在GE線卡上，有三個TX隊列（使用1p2q2t隊列結構）；其中一個隊列是SP隊列，因此WRR演算法只為兩個TX隊列提供服務。

通常，管理員會為TX隊列分配權重。WRR的工作原理是檢視分配給埠隊列的權重，該權重由交換機在內部使用，用於確定在移動到下一個隊列之前要傳輸多少流量。可為每個埠隊列分配介於1和255之間的加權值。

CatOS

```
Console> (enable) set qos wrr 2q2t 40 80
!-- QoS wrr ratio set successfully. Console> (enable)
```

此命令將權重40分配給隊列1，將權重80分配給隊列2。這實際上意味著在兩個隊列之間分配的頻寬是二比一（80到40 = 2到1）。此命令對所有埠有效，埠上有兩個隊列和兩個閾值。

在整合Cisco IOS（本機模式）中發出的等效命令如下所示。

整合Cisco IOS（本機模式）

```
Cat6500(config-if)# wrr-queue bandwidth 1 3
Cat6500(config-if)#
```

以上表示兩個隊列之間的比例為3比1。您會注意到此命令的Cat IOS版本僅適用於特定介面。

DSCP到COs對映

當幀被放入出口埠時，埠ASIC將使用分配的CO執行擁塞規避（即WRED），同時使用CO來確定幀的排程（即，傳輸幀）。 此時，交換機將使用預設對映獲取分配的DSCP並將其對映回COs值。此表格中顯示此默認對映。

或者，管理員可以建立一個對映，交換機使用該對映獲取分配的內部DSCP值，並為幀建立一個新的COs值。下面舉例說明如何使用CatOS和整合Cisco IOS（本機模式）來實現此功能。

CatOS

```
Console> (enable) set qos dscp-cos--map 20-30:5 10-15:3 45-52:7
!-- QoS dscp-cos-map set successfully. Console> (enable)
```

上面的命令將DSCP值20到30對映到COs值5,DSCP值10到15對映到COs值3,DSCP值45到52對映到COs值7。所有其他DSCP值都使用交換機上啟用QoS時建立的預設對映。

在整合Cisco IOS（本機模式）中發出的等效命令如下所示。

整合Cisco IOS（本機模式）

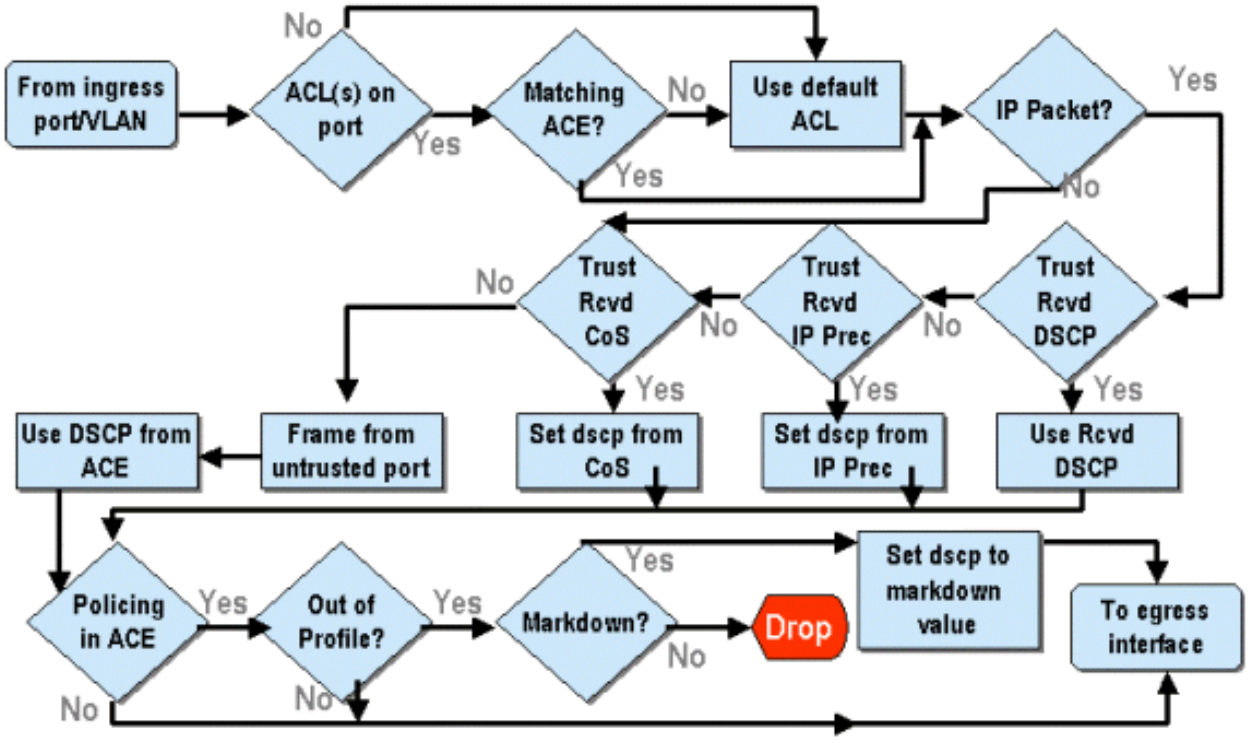
```
Cat6500(config)# mls qos map dscp-cos 20 30 40 50 52 10 1 to 3
Cat6500(config)#
```

這會將DSCP值20、30、40、50、52、10和1設定為CO值3。

使用PFC的分類和管制

PFC支援幀的分類和管制。分類可以使用ACL來分配（標籤）具有優先順序(DSCP)的傳入幀。 管制允許流量流被限制到一定頻寬量。

以下各節將從CatOS和整合Cisco IOS（本機模式）OS平台的角度介紹PFC上的這些功能。PFC應用的進程如下圖所示：



使用CatOS在Catalyst 6000系列上配置管制

管制功能分為兩個部分，一個用於CatOS，另一個用於整合Cisco IOS（本機模式）。 兩者都達到相同的最終結果，但配置和實施方式不同。

管制

PFC支援對傳入到交換機的流量進行速率限制（或管制）的功能，並可將流量減少到預定義限制。超過此限制的流量可能會被丟棄，或者將幀中的DSCP值降為較低值。

PFC1或PFC2目前都不支援輸出（輸出）速率限制。這將會新增到計畫於2002年下半年推出的支援輸出（或輸出）策略的PFC新修訂版中。

CatOS和新的整合Cisco IOS（本機模式）都支援管制，不過這些功能的配置非常不同。以下各節將介紹這兩種作業系統平台中的策略配置。

聚合與微流(CatOS)

聚合和微流是用於定義PFC執行的策略範圍的術語。

微流定義單個流的管制。流由具有唯一SA/DA MAC地址、SA/DA IP地址和TCP/UDP埠號的會話定義。對於通過VLAN埠發起的每個新流，可以使用微流來限制交換機接收到的該流的資料量。在微流定義中，超過規定速率限制的資料包可能被丟棄，或者被降級DSCP值。

類似於微流，聚合可用於對限制流量進行評級。但是，聚合速率適用於與指定QoS ACL匹配的埠或VLAN上的所有入站流量。您可以將聚合視為與訪問控制條目(ACE)中的配置檔案相匹配的累積流量的策略。

聚合和微流都會定義交換機可以接受的流量量。可將聚合和微流同時分配給埠或VLAN。

在定義微流時，最多可以定義63個微流，最多可以定義1023個聚集。

存取控制專案和QoS ACL(CatOS)

QoS ACL由定義一組QoS規則的ACE清單組成，PFC使用這些規則處理傳入幀。Ace類似於路由器訪問控制清單(RACL)。 ACE為傳入幀定義分類、標籤和管制標準。如果傳入幀與ACE中設定的條件匹配，則QoS引擎將處理該幀（如ACE認為的那樣）。

所有QoS處理均在硬體中完成，因此啟用QoS管制不會影響交換機的效能。

PFC2目前最多支援500個ACL，這些ACL最多可以包含32000個ACE（總計）。 實際ACE編號將取決於PFC中定義的其他服務和可用記憶體。

可以定義三種型別的Ace。它們是IP、IPX和MAC。IP和IPX Ace都檢查L3報頭資訊，而基於MAC的Ace只檢查L2報頭資訊。還應注意，MAC Ace只能應用於非IP和非IPX流量。

建立策略規則

建立策略規則的過程需要建立聚合（或微流），然後將該聚合（或微流）對映到ACE。

例如，如果要求將埠5/3上的所有傳入IP流量限制在最大為20 MB，則必須配置上述兩個步驟。

首先，該示例請求限制所有傳入的IP流量。這意味著必須定義聚合監察器。例如：

```
Console> (enable) set qos policer aggregate test-flow rate 20000 burst 13 policed-dscp
!-- Hardware programming in progress !-- QoS policer for aggregate test-flow created
successfully. Console> (enable)
```

我們建立了名為test-flow的聚合。它定義速率20000 KBPS(20MBPS)和突發13。 policed-dscp關鍵字指示任何超過此策略的資料都將按照DSCP降級對映中的指定將其DSCP值降級（預設的DSCP值存在，或者可由管理員修改）。 使用policed-dscp關鍵字的另一種方法是使用drop關鍵字。drop關鍵字只會丟棄所有配置檔案外流量（超出分配的突發值範圍的流量）。

策略機制在漏洞令牌桶方案上運行，其中定義一個突發(即在一定（固定）時間間隔內您接受的以位每秒為單位的資料量)，然後定義速率（定義為在一秒鐘內清空該令牌桶的資料量）。 溢位此儲存桶的任何資料要麼已丟棄，要麼已標籤其DSCP。上面提到的給定時間段（或時間間隔）是0.00025秒（或秒的1/4000），而且是固定的（也就是說，不能使用任何配置命令更改此數字）。

上面的示例中的數字13表示一個儲存桶，它最多會接受每1/4000秒的13,000位資料。這與52 MB/秒(13K *(1 / 0.00025)或13K * 4000有關。 您必須始終確保拆分配置為等於或高於要傳送資料的速率。換句話說，突發量應大於或等於給定時間段內要傳輸的最小資料量。如果突發產生的數字低於您指定的速率，則速率限制將等於突發。換句話說，如果定義20 MBPS的速率和計算為15MBPS的突發量，則您的速率只能達到15MBPS。你可能會問下一個問題，為什麼是13歲？請記住，突發定義令牌桶的深度，或者換句話說，用於每1/4000秒接收傳入資料的桶的深度。因此，突發可以是大於或等於20 MB秒的到達資料速率上支援的任意數字。對於20MB的速率限制，可以使用的最小突發量為20000/4000 = 5。

處理策略器時，策略演算法首先向令牌桶填充完整的令牌補數。令牌數等於突發值。因此，如果突發值為13，則桶中的令牌數等於13,000。對於每1/4000秒，策略演算法將發出等於定義的速率除以4000的資料量。對於傳送的每位（二進位制數字）資料，它都會使用桶中的一個令牌。在間隔結束時，它將向桶中補充一組新的令牌。替換的令牌數由rate / 4000定義。請考慮上面的示例，以理解這一點：

```
Console> (enable) set qos policer aggregate test-flow rate 20000 burst 13
```

假設這是一個100 MBPS埠，我們向埠傳送100 MBPS的恆定流。我們知道，這相當於每秒傳入速率100,000,000位。此處的引數是速率20000和突發13。在時間間隔t0處，令牌桶中有一個完整的補碼（即13,000）。 在時間間隔t0處，第一組資料將到達埠。對於此時間間隔，到達率將為

100,000,000 / 4000 = 25,000位/秒。由於我們的令牌桶深度只有13,000個令牌，因此在此間隔內到達埠的25,000個位中，只有13,000個位符合傳送條件，12,000個位被丟棄。

指定的速率定義了20,000,000位/秒的轉發速率，等於每1/4000間隔傳送5,000位。每傳送5,000個位元，就消耗5,000個令牌。在時間間隔T1處，又有25,000位資料到達，但桶會丟棄12,000位。用速率/4000（相當於5,000個新令牌）定義的令牌來補充該桶。 然後演算法會發出下一個資料補丁，每個區間等於另一個5,000位資料（這將消耗另一個5,000個令牌）等等。

實質上，任何超過桶深度（定義的突發量）的資料都會被丟棄。在傳送資料後剩餘的資料（與所宣告的速率匹配）也會被丟棄，從而為下一組到達的資料鋪平道路。不完整資料包是指在時間間隔內沒有完全接收的資料包，它不會被丟棄，但會一直保留，直到將其完全接收到埠為止。

此突發數假定流量是恆定的。然而，在真實的網路中，資料不是恆定的，其流量由TCP視窗大小決定，TCP視窗大小在傳輸序列中包含TCP確認。為了考慮TCP視窗大小的問題，建議將突發值加倍。在上方範例中，建議值13實際設定為26。

另外一點需要強調的重要一點是，在時間間隔0（即策略週期的開始），令牌桶中充滿了令牌。

現在，此聚合策略必須合併到QoS ACE中。在ACE中，將制定規範以將一組條件與傳入幀匹配。請考慮以下示例。您想將上面定義的聚合應用到所有IP流量，但特別適用於來自子網10.5.x.x且目的地為子網203.100.45.x的流量。ACE將如下所示：

```
Console> (enable) set qos acl ip test-acl trust-dscp aggregate test-flow tcp 10.5.0.0
203.100.45.0
!-- Test-acl editbuffer modified. Issue the commit command to apply changes.
Console> (enable)
```

上述命令已建立一個IP ACE(使用**set qos acl ip**命令表示)，現在它與名為test-acl的QoS ACL相關聯。建立並與ACL test-acl關聯的後續Ace附加在ACE清單的末尾。ACE條目具有與其關聯的聚合測試流。源子網為10.5.0.0且目標子網為203.100.45.0的任何TCP流都將應用此策略。

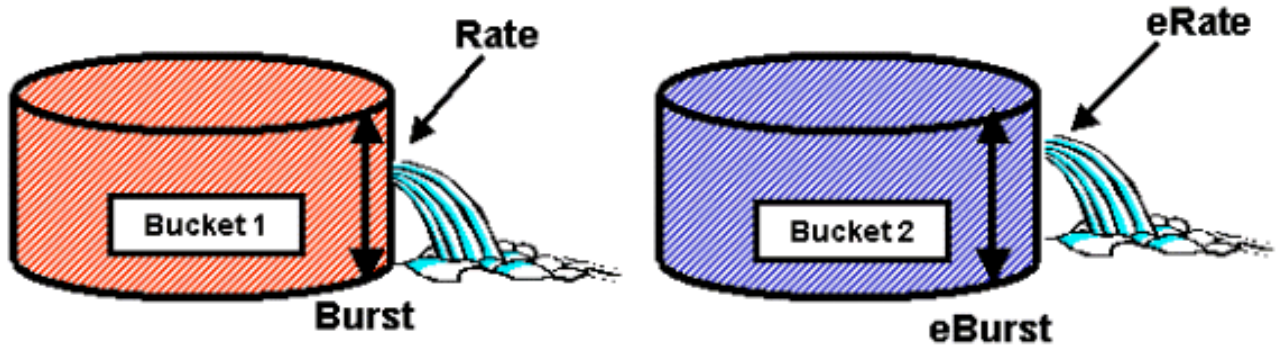
ACL（和關聯的Ace）提供了管理員可以使用的非常精細的配置靈活性。ACL可以包含一個或多個Ace，源和/或目標地址以及L4埠值可用於標識需要管制的特定流。

但是，在實際執行任何管制之前，必須將ACL對映到物理埠或VLAN。

PFC2策略決定

對於PFC2，在CatOS 7.1和CatOS 7.2中進行了更改，引入了雙洩漏桶演算法來進行管制。通過此新演算法，它增加了以下兩個新級別：

1. **正常策略級別：**這等同於第一個桶，並定義指定桶的深度（突發）和應該從桶傳送資料的速率（速率）的引數。
2. **超額策略級別：**這等同於第二桶，並且定義指定桶的深度(eburst)和應該從桶傳送資料的速率(erate)的引數。



此過程的工作方式是資料開始填充第一個儲存桶。PFC2接受小於或等於第一桶的深度（突發值）的傳入資料流。可以向下標籤從第一儲存段溢位的資料，並將其傳遞到第二儲存段。第二儲存桶可以接受從儲存桶1以小於或等於突發值的值流過的資料的傳入速率。來自第二桶的資料以由生成引數減去速率引數定義的速率傳送。從第二個儲存桶溢位的資料也可以降級或丟棄。

以下是雙漏桶管制器的示例：

```
Console> (enable) set qos policer aggregate AGG1 rate 10000 policed-dscp erate 12000 drop burst
13 eburst 13
```

此示例設定了一個名為AGG1的聚合，該聚合的流量速率超過10 MBPS，將根據管制的DSCP對映進行降級。根據drop關鍵字丟棄超過該速率（設定為12 MBPS）的流量。

將聚合管制器應用於啟用DFC的模組

請注意，由於6000使用集中轉發引擎(PFC)來轉發流量，因此可在非DFC線卡上應用聚合監察器。通過實施中央轉發引擎，可以跟蹤給定VLAN的流量統計資訊。此程式可用於將聚合管制器應用於VLAN。

但是，在啟用DFC的線卡上，轉發決策會分配給該線卡。DFC只知道其直接線卡上的埠，而不知道其他線卡上的流量移動。因此，如果將聚合管制器應用於成員埠跨越多個DFC模組的VLAN，則管制器可能會產生不一致的結果。原因是DFC只能跟蹤本地埠統計資訊，而不考慮其他線卡上的埠統計資訊。因此，對啟用DFC的線卡上具有成員埠的VLAN應用聚合管制器將導致DFC管制流量達到僅駐留在DFC線卡上的VLAN埠的額定限制。

DSCP降級對映(CatOS)

當策略器被定義為對超出配置檔案的流量進行降級而不是丟棄時，會使用DSCP降級對映。超出設定檔流量定義為超出所定義突發設定的流量。

啟用QoS時設定預設DSCP降級對映。此預設降級對映在文檔前面的此表中列出。命令列介面(CLI)允許管理員通過發出**set qos policed-dscp-map**命令修改預設降級對映。下面是一個示例。

```
Cat6500(config)# set qos policed-dscp-map 20-25:7 33-38:3
```

此示例修改管制的DSCP對映，以反映DSCP值20到25將被降級為DSCP值7，而DSCP值33到38將被降級為DSCP值3。

將原則對應到VLAN和連線埠(CatOS)

ACL構建完成後，必須對映到埠或VLAN才能生效。

有一個有趣命令會引起許多人的注意，那就是讓所有QoS埠都基於的預設QoS設定。如果將聚合（或微流）應用於VLAN，則它不會對埠生效，除非該埠已配置為基於VLAN的QoS。

```
Console> (enable) set port qos 2/5-10 vlan-based
!-- Hardware programming in progress  !-- QoS interface is set to vlan-based for ports 2/5-10.
Console> (enable)
```

將基於埠的QoS更改為基於VLAN的QoS會立即分離分配給該埠的所有ACL，並將任何基於VLAN的ACL分配給該埠。

通過發出以下命令將ACL對映到埠（或VLAN）：

```
Console> (enable) set qos acl map test-acl 3/5
!-- Hardware programming in progress  !-- ACL test-acl is attached to port 3/5. Console>
(enable) Console> (enable) set qos acl map test-acl 18
!-- Hardware programming in progress  !-- ACL test-acl is attached to VLAN 18. Console> (enable)
```

即使將ACL對應到連線埠（或VLAN）後，ACL仍不會生效，直到將ACL提交到硬體。下一節將對此進行說明。此時，ACL駐留在記憶體中的臨時編輯緩衝區中。在此緩衝區中，可以修改ACL。

如果要刪除位於編輯緩衝區中的任何未提交ACL，請發出**rollback**命令。此命令實際上會從編輯緩衝區中刪除ACL。

```
Console> (enable) rollback qos acl test-acl
!-- Rollback for QoS ACL test-acl is successful. Console> (enable)
```

提交ACL(CatOS)

要應用您定義（上述）的QoS ACL，必須將ACL提交到硬體。將ACL從臨時緩衝區提交到PFC硬體的過程。一旦駐留在PFC記憶體中，QoS ACL中定義的策略即可應用於與Ace匹配的所有流量

為便於配置，大多數管理員發出**commit all**命令。但是，您可以提交目前可能駐留在編輯緩衝區中的特定ACL（其中一個）。commit命令的示例如下所示。

```
Console> (enable) commit qos acl test-acl
!-- Hardware programming in progress  !-- ACL test-acl is committed to hardware. Console>
(enable)
```

如果要從連線埠（或VLAN）中移除ACL，需要發出以下命令來清除將該ACL與該連線埠（或VLAN）相關聯的映像：

```
Console> (enable) clear qos acl map test-acl 3/5
!-- Hardware programming in progress  !-- ACL test-acl is detached from port 3/5.
Console>(enable)
```

使用整合Cisco IOS（本機模式）在Catalyst 6000系列上配置管制

整合Cisco IOS（本機模式）支援管制。 但是，使用策略對映實現策略功能的配置和實施。每個策略對映使用多個策略類組成策略對映，並且可以為不同型別的流量定義這些策略類。

在過濾時，策略對映類使用基於IOS的ACL和類匹配語句來標識要被監管的流量。識別流量後，策略類可以使用聚合和微流策略器將策略應用到匹配的流量。

以下各節詳細說明了整合Cisco IOS（本地模式）的策略配置。

聚合和微流(整合Cisco IOS（本機模式））

聚合和微流是用於定義PFC執行的策略範圍的術語。與CatOS類似，聚合和微流也用於整合Cisco IOS（本機模式）。

微流定義單個流的管制。流由具有唯一SA/DA MAC地址、SA/DA IP地址和TCP/UDP埠號的會話定義。對於通過VLAN埠發起的每個新流，可以使用微流來限制交換機接收到的該流的資料量。在微流定義中，超過規定速率限制的資料包可能被丟棄，或者被降級DSCP值。使用構成策略對映類一部分的police flow命令應用微流。

要在整合Cisco IOS（本機模式）中啟用微流管制，必須在交換機上全域性啟用微流管制。這可以通過發出以下命令來實現：

```
Cat6500(config)# mls qos flow-policing
```

微流管制還可以應用於橋接流量，即非L3交換的流量。若要使交換器支援橋接流量上的微流量管制，請發出以下命令：

```
Cat6500(config)# mls qos bridged
```

此命令還啟用組播流量的微流管制。如果組播流量需要應用微流管制器，則必須啟用此命令(**mls qos bridged**)。

類似於微流，聚合可用於對限制流量進行評級。但是，聚合速率適用於與指定QoS ACL匹配的埠或VLAN上的所有入站流量。您可以將聚合視為與定義的流量配置檔案匹配的累積流量的策略。

在整合Cisco IOS（本機模式）中可以定義兩種形式的聚合，如下所示：

- 每個介面聚合監察器
- 命名的聚合策略器

通過在策略對映類內發出**police**命令，將每個介面聚合應用到單個介面。這些對映類可以應用於多個介面，但監察器會單獨控制每個介面。命名聚合會累積應用於所有介面的一組埠和策略流量。通過發出**mls qos aggregate policer**命令應用命名聚合。

在定義微流時，最多可以定義63個微流，最多可以定義1023個聚集。

建立策略規則(整合Cisco IOS（本機模式））

建立策略規則的過程包括通過策略對映建立聚合（或微流），然後將該策略對映附加到介面。

考慮為CatOS建立的相同示例。要求將埠5/3上的所有傳入IP流量限制在最高20 MBPS。

首先，必須建立策略對映。建立名為limit-traffic的策略對映。具體如下：

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)#
```

您會立即注意到交換機提示符的變化，反映您處於建立對映類的配置模式。請記住，策略對映可以

包含多個類。每個類包含一組可應用於不同流量流的單獨策略操作。

我們將建立一個流量類，專門將傳入流量限製為20 MBPS。我們將此類限製為–20。如下所示。

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20
Cat6500(config-pmap-c)#
```

提示符會再次更改，以反映您現在位於對映類配置中（提示符後帶有 — c顯示）。 如果要應用速率限制以匹配特定傳入流量，可以配置ACL並將其應用於類名。如果要對來自網路10.10.1.x的流量應用20 MBPS限制，請發出以下ACL:

```
Cat6500(config)# access-list 101 permit ip 10.10.1.0  0.0.0.255 any
```

您可以將此ACL新增到類名中，如下所示：

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20 access-group 101
Cat6500(config-pmap-c)#
```

一旦定義了類對映，您就可以為該類定義單個策略器。您可以建立聚合（使用police關鍵字）或microflows（使用police flow關鍵字）。 建立聚合，如下所示。

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20 access-group 101
Cat6500(config-pmap-c)# police 20000000 13000 confirm-action transmit exceed-action drop
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

上述class語句(police命令)將速率限制設定為20000 k(20 MBPS)，突發量為52 MBPS(13000 x 4000 = 52MB)。 如果流量與配置檔案匹配且處於額定限制內，則操作是通過confirm-action語句設定來傳輸配置檔案中的流量。如果流量超出設定檔（即，在我們的範例中超過20 MB限制），則exceed-action陳述式會設定為捨棄流量（即，在我們的範例中，所有超過20 MB的流量都會捨棄）。

配置微流時，會執行類似的操作。如果想要將所有流速率限制到與給定類對映匹配到200 K的埠，則該流的配置將類似於以下內容：

```
Cat6500(config)# mls qos flow-policing
Cat6500(config)# policy-map limit-each-flow
Cat6500(config-pmap)# class limit-to-200
Cat6500(config-pmap-c)# police flow 200000 13000 confirm-action transmit exceed-action drop
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
```

DSCP降級對映

當策略器被定義為對超出配置檔案的流量進行降級而不是丟棄時，會使用DSCP降級對映。超出設定檔流量定義為超出所定義突發設定的流量。

啟用QoS時，會建立預設DSCP降級對映。此表中列出了此預設降級對映。CLI允許管理員通過發出**set qos policed-dscp-map**命令修改預設降級對映。下面是一個示例。

```
Cat6500(config)#

mls qos map policed-dscp normal-burst 32 to 16
```

此示例定義對預設策略化dscp對映的修改，該DSCP值32將被降級為DSCP值16。對於已定義此策略器的埠，任何具有此DSCP值的傳入資料（屬於超出所述突發的資料塊）的DSCP值都將降級為16。

將策略對映到VLAN和埠(整合Cisco IOS（本機模式））

策略構建完成後，必須將其對映到埠或VLAN才能生效。與CatOS中的提交流程不同，在整合Cisco IOS（本機模式）中沒有等價的提交流程。 當策略對映到介面時，該策略生效。要將上述策略對映到介面，請發出以下命令：

```
Cat6500(config)# interface fastethernet 3/5
Cat6500(config-if)# service-policy input limit-traffic
```

如果策略對映到VLAN，則對於要應用VLAN策略的VLAN中的每個埠，必須通過發出**mls qos vlan-based**命令通知介面基於VLAN。

```
Cat6500(config)# interface fastethernet 3/5
Cat6500(config-if)# mls qos vlan-based
Cat6500(config-if)# exit
Cat6500(config)# interface vlan 100
Cat6500(config-if)# service-policy input limit-traffic
```

假設介面3/5是VLAN 100的一部分，則套用到VLAN 100的名為limit-traffic的原則也會套用到介面3/5。

使用CatOS在Catalyst 6000系列上配置分類

PFC引入了使用可檢視L2、L3和L4報頭資訊的ACL對資料進行分類的支援。對於SupI或IA（不帶PFC），分類僅限於在埠上使用信任關鍵字。

以下部分介紹PFC在CatOS中用於分類的QoS配置元件。

COs到DSCP對應(CatOS)

在輸入交換機時，幀將具有交換機設定的DSCP值。如果埠處於受信任狀態，並且管理員已使用trust-COs關鍵字，則幀中設定的CO值將用於確定為該幀設定的DSCP值。如前所述，交換機根據內部DSCP值傳輸交換機時，可以為幀分配服務級別。

不支援某些早期的10/100模組（WS-X6248和WS-X6348）上的此關鍵字。對於這些模組，建議使用ACL為傳入資料應用COs設定。

啟用QoS後，交換機將建立預設對映。此對映用於標識將基於COs值設定的DSCP值。這些圖會列在文檔前面的此表格中。或者，管理員可以設定唯一對映。下面是一個示例。

```
Console> (enable) set qos cos-dscp-map 20 30 1 43 63 12 13 8
!-- QoS cos-dscp-map set successfully. Console> (enable)
```
上面的命令設定以下對映：

COs	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

雖然上述地圖在現實生活網路中使用的可能性極小，但它有助於提供使用這個命令可以達到什麼的想法。

IP優先順序到DSCP對應(CatOS)

與COs到DSCP的對映類似，幀的DSCP值也可由傳入資料包IP優先順序設定確定。僅當管理員將埠設定為受信任且其已使用trust-ipprec關鍵字時，才會出現這種情況。

啟用QoS後，交換機將建立預設對映。此對映在本文件前面的表中被引用。此對映用於標識將基於IP優先順序值設定的DSCP值。或者，管理員可以設定唯一對映。下面是一個示例：

```
Console> (enable) set qos ipprec-dscp-map 20 30 1 43 63 12 13 8
!-- QoS ipprec-dscp-map set successfully. Console> (enable)
```
上面的命令設定以下對映：

IP優先順序	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

雖然上述地圖在現實生活網路中使用的可能性極小，但它有助於提供使用這個命令可以達到什麼的想法。

分類(CatOS)

當將幀傳遞到PFC進行處理時，對幀執行分類處理。PFC將使用預配置的ACL（或預設ACL）為幀分配DSCP。在ACE中，四個關鍵字之一用於分配DSCP值。它們如下：

1. TRUST-DSCP（僅限IP ACL）
2. TRUST-IPPREC（僅限IP ACL'=s）
3. TRUST-COS（除PFC2上的IPX和MAC以外的所有ACL）
4. DSCP

TRUST-DSCP關鍵字假定到達PFC的幀在進入交換機之前已設定DSCP值。交換機將保持此DSCP值。

使用TRUST-IPPREC時，PFC將從ToS欄位中駐留的現有IP優先順序值中獲取DSCP值。PFC將使用IP優先順序到DSCP對映來分配正確的DSCP。在交換機上啟用QoS時，將建立預設對映。或者，管理員建立的對映可用於匯出DSCP值。

與TRUST-IPPREC類似，TRUS-COS關鍵字會指示PFC從幀頭中的CO派生DSCP值。還將有一個CO到DSCP對映（管理員分配的CO的預設對映），以幫助PFC派生DSCP。

當幀從不受信任的埠到達時，使用DSCP關鍵字。這就為匯出DSCP提供了有趣的情況。此時，在set qos acl語句中配置的DSCP用於匯出DSCP。但是，在此階段，ACL可用於根據ACE中設定的分類標準為流量匯出DSCP。這表示在ACE中，可以使用分類標準(例如IP來源和目的地位址、

TCP/UDP連線埠號碼、ICMP代碼、IGMP型別、IPX網路和通訊協定編號、MAC來源和目的地位址，以及Ethertype（僅針對非IP和非IPX流量）來識別流量。這表示可以將ACE配置為分配特定DSCP值以表示通過FTP流量的HTTP流量。

請考慮以下示例：

```
Console> (enable) set port qos 3/5 trust untrusted
```

將埠設定為不受信任將指示PFC使用ACE來匯出幀的DSCP。如果ACE配置了分類標準，則來自該埠的單個流可以按不同的優先順序進行分類。以下Ace說明了這一點：

```
Console> (enable) set qos acl ip abc dscp 32 tcp any any eq http
Console> (enable) set qos acl ip ABC dscp 16 tcp any any eq ftp
```

在本例中，我們有兩個ACE語句。第一個標識將埠號為80(80 = HTTP)的任何TCP流（關鍵字any用於標識源和目標流量）分配的DSCP值為32。第二個ACE標識源自TCP埠號為21(FTP)的任何主機的流量，並將DSCP值分配為16。

使用整合Cisco IOS（本機模式）在Catalyst 6000系列上配置分類

以下部分介紹用於支援使用整合Cisco IOS（本機模式）在PFC上進行分類的QoS配置元件。

COs到DSCP對映(整合Cisco IOS（本機模式））

在輸入交換機時，幀將具有交換機設定的DSCP值。如果埠處於受信任狀態，並且管理員已使用mls qos trust-COs關鍵字（在GE埠上或在WS-X6548線卡上使用10/100埠），則將使用幀中設定的COs值來確定為該幀設定的DSCP值。如前所述，交換機根據內部DSCP值傳輸交換機時，可以為幀分配服務級別。

啟用QoS後，交換機將建立預設對映。有關預設設定，請參閱此表。此對映用於標識將基於COs值設定的DSCP值。或者，管理員可以設定唯一對映。下面是一個示例。

```
Cat6500(config)# mls qos map cos-dscp 20 30 1 43 63 12 13 8
Cat6500(config)#
```

上面的命令設定以下對映：

COs	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

雖然上述地圖在現實生活網路中使用的可能性極小，但它有助於提供使用這個命令可以達到什麼的想法。

IP優先順序到DSCP對映(整合Cisco IOS（本機模式））

與COs到DSCP的對映類似，幀的DSCP值也可由傳入資料包IP優先順序設定確定。僅當管理員將埠設定為受信任並且已使用mls qos trust-ipprec關鍵字時，才會出現這種情況。只有GE埠和WS-X6548線卡上的10/100埠支援此關鍵字。對於WS-X6348和WS-X6248線卡的10/100埠，應使用ACL為傳入資料分配ip優先順序信任。

啟用QoS後，交換機將建立預設對映。有關預設設定，請參閱此表。此對映用於標識將基於IP優先順序值設定的DSCP值。或者，管理員可以設定唯一對映。下面是一個示例。

```
Cat6500(config)# mls qos map ip-prec-dscp 20 30 1 43 63 12 13 8
Cat6500(config)#
```

上面的命令設定以下對映：

IP優先順序	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

雖然上述地圖在現實生活網路中使用的可能性極小，但它有助於提供使用這個命令可以達到什麼的想法。

分類(整合Cisco IOS（本機模式））

當幀傳遞到PFC時，可以執行分類過程來為傳入幀分配新的優先順序。這裡需要注意的是，僅當幀來自不受信任的埠，或者幀被歸類為不受信任時，才能執行此操作。

策略對映類操作可用於：

1. 信任CO
2. 信任IP優先順序
3. 信任DSCP
4. 無信任

TRUST DSCP關鍵字假定到達PFC的幀在進入交換機之前已設定了DSCP值。交換機將保持此DSCP值。

藉助TRUST IP-PRECEDENCE，PFC將從ToS欄位中駐留的現有IP優先順序值中獲取DSCP值。PFC將使用IP優先順序到DSCP對映來分配正確的DSCP。在交換機上啟用QoS時，將建立預設對映。或者，管理員建立的對映可用於匯出DSCP值。

與TRUST IP-PRECEDENCE類似，TRUST COs關鍵字會指示PFC從幀頭中的CO派生DSCP值。還將有一個CO到DSCP對映（管理員分配的CO的預設對映），以幫助PFC派生DSCP。

以下是一個從現有優先順序（DSCP、IP優先順序或CO）派生DSCP的示例。

```
Cat6500(config)# policy-map assign-dscp-value
Cat6500(config-pmap)# class test
Cat6500(config-pmap-c)# trust COs
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

上述類對映將從乙太網報頭中的CO匯出DSCP值。

當幀從不受信任的埠到達時，使用關鍵字的NO TRUST形式。這樣，在策略執行過程中可以為幀分配DSCP值。

請考慮以下示例，說明如何使用以下策略定義將新優先順序(DSCP)分配給進入PFC的不同流。

```
Cat6500(config)# access-list 102 permit tcp any any eq http
Cat6500(config)# policy-map new-dscp-for-flow
Cat6500(config-pmap)# class test access-group 102
Cat6500(config-pmap-c)# no trust
Cat6500(config-pmap-c)# police 1000 1 confirm-action set-dscp-transmit 24  Cat6500(config-pmap-
c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

上面的示例顯示以下內容：

1. 正在建立的ACL用於識別進入埠的http流。
2. 名為new-dscp-for-flow的策略對映。
3. 類對映（名稱測試），使用訪問清單102來標識該類對映將對其執行操作的流量。
4. 類對映測試會將傳入幀的信任狀態設定為不可信，並為該流分配24的DSCP。
5. 此類對映還將所有http流的聚合限製為最多1MB。

通用開放原則伺服器(COPS)

COPS是一種允許Catalyst 6000系列從遠端主機配置QoS的協定。目前，COPS僅支援使用CatOS，並且是QoS的intserv架構的一部分。使用整合Cisco IOS（原生模式）時，目前（截至本檔案日期）不支援COPS。 雖然COPS協定將QoS配置資訊傳送給交換機，但它不是QoS配置資訊的來源。使用COPS協定需要外部QoS管理器來託管交換機的QoS配置。外部QoS管理器將使用COPS協定啟動這些配置向交換機向下推送。Cisco QoS Policy Manager(QPM)是外部QoS Manager的一個示例。

本文檔的目的不是解釋QPM的工作原理，而是解釋使用QPM時支援外部QoS配置所需的交換機配置。

COPS配置

預設情況下，禁用COPS支援。若要在交換器上使用COPS，必須啟用它。這可以通過發出以下命令來實現：

```
Console> (enable) set qos policy-source cops
!-- QoS policy source for the switch set to COPS. Console> (enable)
```

啟動此命令時，某些預設QoS配置值將源自COPS伺服器。其中包括：

1. CO到隊列的對映
2. 輸入和輸出隊列閾值分配
3. WRR頻寬分配
4. 任何聚合和微流策略
5. 出口流量的DSCP到CO對映
6. ACL
7. 預設埠CO分配

使用COPS執行QoS配置時，必須瞭解這些配置的應用是以不同的方式應用的。COPS用於配置埠ASIC，而不是直接配置埠。埠ASIC通常控制一組埠，因此COPS配置同時應用於多個埠。

配置的埠ASIC是GE ASIC。在GE線卡上，每個GE有四個埠（埠1-4、5-8、9-12、13-16）。 在這些線卡上，COPS配置會影響每組埠。在10/100線卡上（如本文前面所述），有兩組ASIC，GE和

10/100 ASIC。一個GE ASIC可用於四個10/100 ASIC。每個10/100 ASIC支援12個10/100埠。COPS配置GE ASIC。因此，當通過COPS將QoS配置應用於10/100線卡時，該配置將應用於所有48個10/100埠。

通過發出**set qos policy-source cops**命令啟用COPS支援時，通過COPS的QoS配置將應用於交換機機箱中的所有ASIC。可以將COPS配置應用到特定ASIC。可以使用以下命令實現這一點：

```
Console> (enable) set port qos 5/4 policy-source cops
!-- QoS policy source set to COPS for port (s) 5/1-4. Console> (enable)
```

從應用上述命令可以看出，此命令是在GE模組上發出的，因為有四個埠受到該命令的影響。

策略決策點伺服器和域名

策略決策點伺服器(PDPS)是外部策略管理器，用於儲存向下推送到交換機的QoS配置詳細資訊。如果交換機上啟用了COPS，則必須使用外部管理器的IP地址配置交換機，該外部管理器將為交換機提供QoS配置詳細資訊。這類似於啟用SNMP並定義SNMP管理器IP地址的情況。

標識外部PDPS的命令使用以下命令完成：

```
Console> (enable) set cops server 192.168.1.1 primary
!-- 192.168.1.1 is added to the COPS diff-serv server table as primary server. !-- 192.168.1.1
is added to the COPS rsvp server table as primary server. Console> (enable)
```

上面的命令將裝置192.168.1.1識別為主決策點伺服器。

當交換機與PDPS通訊時，它需要是PDPS上定義的域的一部分。PDPS只與構成其定義域一部分的交換機通訊，因此必須配置交換機以標識它所屬的COPS域。這可以通過發出以下命令來完成：

```
Console> (enable) set cops domain name remote-cat6k
!-- Domain name set to remote-cat6k. Console> (enable)
```

上面的命令顯示交換機已配置為名為remote-cat6k的域的一部分。此域應在QPM中定義，交換機應新增到該域。

相關資訊

- 交換器產品支援
- LAN 交換技術支援
- 技術支援與文件 - Cisco Systems
