使用基於Catalyst 4000/4500 IOS的管理引擎的QOS原則和標籤

目錄

簡介

策略功能確定流量級別是否在指定的配置檔案（合約）內。 策略功能允許丟棄超出設定檔的流量，或將流量標籤到不同的差分服務代碼點(DSCP)值，以強制執行約定服務等級。DSCP是封包的服務品質(QoS)等級的量度。除了DSCP，IP優先順序和服務類別(CoS)還用於傳送資料包的QoS級別。

不應將管制與流量調節混淆，儘管二者都確保流量保持在配置檔案（合約）內。 管制不會緩沖流量，因此傳輸延遲不會受到影響。策略不會緩衝超出配置檔案的資料包，而是會丟棄這些資料包，或使用不同的QoS級別（DSCP降級）對其進行標籤。 流量整形會緩衝超出配置檔案的流量並平滑流量爆發，但會影響延遲和延遲變化。整形只能應用於傳出介面，而策略可在傳入和傳出介面上應用。

搭載Supervisor Engine 3、4和2+（本檔案從現在起SE3、SE4、SE2+）的Catalyst 4000/4500支援傳入和傳出方向的管制。流量整形也受支援，但本文檔將僅處理策略和標籤。標籤是根據策略更改資料包QoS級別的過程。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

QoS管制和標籤引數

策略設定是通過定義QoS策略對映並將其應用於埠（基於埠的QoS）或VLAN（基於VLAN的QoS）來設定的。 監察器由速率和突發引數定義，以及針對配置檔案內和配置檔案外流量的操作。

支援兩種型別的策略器：聚合和每個介面。每個監察器可應用於多個埠或VLAN。

聚合管制器對所有應用的埠/VLAN上的流量起作用。例如，我們應用聚合管制器將簡單式檔案傳輸通訊協定(TFTP)流量限製為VLAN 1和3上的1 Mbps。此類管制器將允許VLAN 1和3中的1 Mbps的TFTP流量。如果應用每個介面監控器，則會將VLAN 1和3上的TFTP流量限製為每台1 Mbps。

注意：如果對資料包同時應用入口和出口策略，則會做出最嚴厲的決定。也就是說，如果輸入策略器指定丟棄資料包，而輸出策略器指定將資料包標籤為關閉，則資料包將被丟棄。表1總結了當入口和出口策略都處理資料包時，對該資料包執行的QoS操作。

表 1：QoS操作取決於入口和出口策略

	Ingress policy			
Egress policy	**Transmit**	**Drop**	**Markdown$_i$**	**Mark$_i$**
Transmit	Transmit	Drop	Markdown$_i$	Mark$_i$
Drop	Drop	Drop	Drop	Drop
Markdown$_e$	Markdown$_e$	Drop	Markdown$_e$	Markdown$_e$
Mark$_e$	Mark$_e$	Drop	Mark$_e$	Mark$_e$

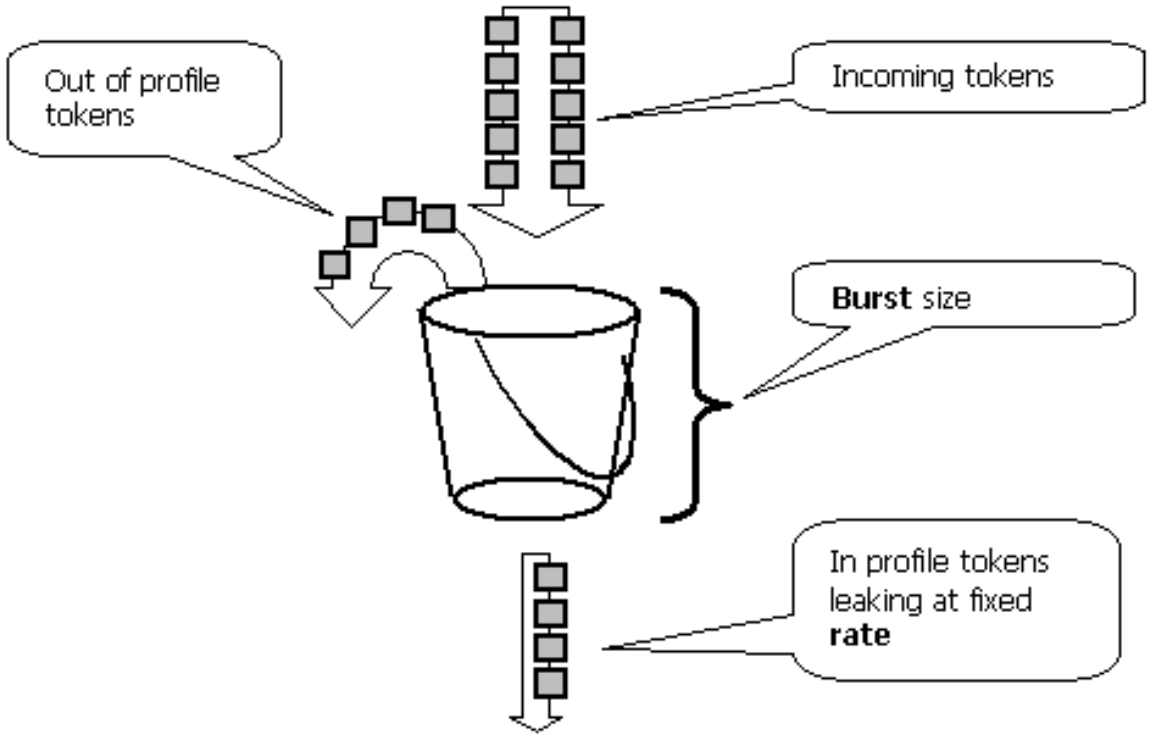
Catalyst 4000 SE3、SE4、SE2+ QoS硬體的實施方式使得在輸出管制器之後對封包進行實際標籤。這表示即使輸入策略對資料包進行註釋（通過策略器標籤為關閉或正常標籤），輸出策略仍會看到以原始QoS級別標籤的資料包。輸出策略將看到資料包，就像它們未被輸入策略標籤一樣。這意味著以下內容：

- 輸出標籤覆蓋輸入標籤。
- 輸出策略無法匹配通過輸入標籤更改的新QoS級別。

其他重要影響如下：

- 在同一策略中的同一流量類內無法執行標籤和標籤操作。
- 聚合策略器是按方向的。也就是說，如果聚合管制器同時應用於輸入和輸出，則有兩個聚合管制器，一個在輸入上，一個在輸出上。
- 當策略內將聚合管制器應用於VLAN和物理介面時，實際上將有兩個聚合管制器，一個用於VLAN介面，另一個用於物理介面。目前，在聚合時無法同時監管VLAN介面和物理介面。

Catalyst 4000 SE3、SE4、SE2+中的策略遵循漏桶概念，如下面的型號所示。將對應於傳入流量資料包的令牌放入桶中（令牌的編號=資料包的大小）。 定期從儲存桶中移除已定義的令牌數（從配置的速率派生）。如果儲存桶中沒有位置容納傳入資料包，則會根據配置的策略操作將資料包視為超出配置檔案並丟棄或降級。



應該注意的是，流量不會緩衝在桶中，因為流量可能會出現在上述模型中。實際流量完全不通過儲存桶。儲存段僅用於決定資料包是位於配置檔案中還是位於配置外。

請注意，策略的具體硬體實施可能不同，在功能上它符合上述模型。

以下引數控制策略的操作：

- Rate定義在每個間隔刪除的令牌數。這有效地設定了管制速率。低於該速率的所有流量都視為配置內。
- 間隔定義令牌從桶中移除的頻率。間隔固定為16納秒（16秒*10-9）。 不能更改間隔。
- 突發數定義儲存桶可隨時容納的最大令牌數。

請參閱本文結尾的比較Catalyst 6000和Catalyst 4000/4500 IOS型Supervisor Engine上的管制和標籤一節，瞭解Catalyst 6000和Catalyst 4000 SE3、SE4、SE2+之間的突發差異。

如果檢查任何時間段（從零到無窮大），則策略器將不允許超過以下值

```
<rate> * <period> + <burst-bytes> + <1 packet> bytes
```

通過監察器的流量的大小。

Catalyst 4000 SE3、SE4、SE2+ QoS硬體具有一定策略粒度。根據配置的速率，與速率的最大偏差為速率的1.5%。

設定突發速率時，您需要考慮某些通訊協定（例如TCP）實作對封包遺失作出反應的流量控制機制。例如，TCP會將每個丟失封包的視窗減少一半。當管制到一定的速率時，有效鏈路利用率將低於配置的速率。可以增加突發量，以實現更好的利用率。對於此類流量，一個好的開始是設定突發量，使其等於來回時間(RTT)期間以所需速率傳送流量的兩倍。 出於同樣的原因，建議不要根據面向連線的流量來設定監察器操作的基準，因為它通常顯示的效能低於監察器所允許的效能。

注意：無連線流量也可能以不同的方式響應策略。例如，網路檔案系統(NFS)使用區塊，其中可能包含多個使用者資料包通訊協定(UDP)封包。丟棄一個資料包可能會觸發重新傳輸多個資料包（整個塊）。

例如，以下是TCP會話突發量的計算結果，策略速率是64 Kbps，TCP RTT是0.05秒：

```
<burst> = 2* <RTT> * <rate> = 2 * 0.05 [sec] * 64000/8 [bytes/sec] = 800 [bytes]
```

注意： <burst>適用於一個TCP作業階段，因此應將其縮放為通過監察器的預期作業階段的平均數。這只是一個示例，因此，在每種情況下，您需要對照可用資源評估流量/應用需求和行為，以便選擇策略引數。

策略操作是丟棄資料包（丟棄）或更改資料包的DSCP（標籤關閉）。 為了標籤資料包，必須修改策略的DSCP對映。預設管制的DSCP將資料包註釋到同一個DSCP，即不發生降級。

注意：當將配置檔案外的資料包標籤為DSCP時，資料包可能會無序傳送，使其傳送到與原始DSCP不同的輸出隊列。因此，如果資料包的順序非常重要，建議將配置檔案外的資料包標籤為DSCP，DSCP對映到與配置檔案內資料包相同的輸出隊列。

Catalyst 4000/4500基於IOS的管理引擎支援的管制和標籤功能

Catalyst 4000 SE3、SE4、SE2+同時支援輸入（傳入介面）和輸出（傳出介面）管制。交換機支援1024個入口策略器和1024個出口策略器。系統使用兩個入口策略和兩個出口策略器執行預設無策略行為。

請注意，在策略中將聚合策略器應用到VLAN和物理介面時，會使用其他硬體策略器條目。目前，在聚合時無法同時監管VLAN介面和物理介面。未來軟體版本可能會變更此項。

所有軟體版本均支援管制。Catalyst 4000最多支援每類8個有效match語句，每個策略對映最多支援8個類。有效的match語句如下：

- match access-group
- match ip dscp
- match ip precedence
- match any

注意：對於非IP V4資料包，如果資料包進入信任CoS的中繼埠，**match ip dscp**語句是唯一的分類方法。不要被命令**match ip dscp**中的關鍵字ip誤導，因為內部DSCP已匹配，這適用於所有資料包，而不僅僅是IP。當連線埠設定為信任CoS時，會從L2（802.1Q或ISL標籤）訊框擷取後者，並使用CoS到DSCP QoS的對應關係轉換為內部DSCP。然後可以使用**match ip dscp**在策略中匹配此內部DSCP值。

有效的策略操作如下：

- 警察
- set ip dscp
- set ip precedence
- 信任dscp
- 信任cos

標籤允許根據分類或策略更改資料包的QoS級別。分類根據定義的標準將流量劃分為不同的類別以進行QoS處理。為了匹配IP優先順序或DSCP，相應的傳入介面應設定為受信任模式。交換機支援信任的CoS、信任的DSCP和不受信任的介面。信任指定將從中匯出資料包的QoS級別的欄位。

信任CoS時，QoS級別將從ISL或802.1Q封裝資料包的L2報頭派生。當信任DSCP時，交換機將從資料包的DSCP欄位獲取QoS級別。信任CoS僅在中繼介面上有意義，而信任DSCP僅對IP V4資料包有效。

當介面不受信任時（這是啟用QoS時的預設狀態），內部DSCP將從對應介面的可配置預設CoS或DSCP中派生。如果未配置預設CoS或DSCP，則預設值為零(0)。 確定資料包的原始QoS級別後，將其對映到內部DSCP。內部DSCP可以通過標籤或策略進行保留或更改。

在對資料包進行QoS處理後，將從內部DSCP更新QoS級別欄位（在IP的IP DSCP欄位內和ISL/802.1Q報頭內，如果有）。

有特殊的對映用於將資料包的受信任QoS度量轉換為內部DSCP，反之亦然。這些地圖如下：

- DSCP到管制的DSCP;用於在標籤資料包時匯出管制的DSCP。
- DSCP到CoS:用於從內部DSCP匯出CoS級別，以更新傳出資料包ISL/802.1Q報頭。
- CoS到DSCP:用於在介面處於信任CoS模式時從傳入CoS（ISL/802.1Q報頭）派生內部DSCP。

請注意，當介面處於信任CoS模式時，傳出CoS將始終與傳入CoS相同。這特定於Catalyst 4000 SE3、SE4、SE2+中的QoS實施。

配置和監控管制

在IOS中配置策略涉及以下步驟：

1. 定義監察器。
2. 定義標準以選擇流量進行管制。
3. 使用類定義service-policy並將監察器應用於指定的類。
4. 將服務策略應用於埠或VLAN。

請考慮以下示例。連線到連線埠5/14的流量產生器會傳送約17 Mbps的UDP流量，目的地為連線埠111。我們希望將此流量管製為1 Mbps，且應捨棄多餘流量。

```
! enable qos
qos
! define policer, for rate and burst values, see 'policing parameters
qos aggregate-policer pol_1mbps 1mbps 1000 conform-action transmit
exceed-action
drop
! define ACL to select traffic
access-list 111 permit udp any any eq 111
! define traffic class to be policed
class-map match-all cl_test
match access-group 111
! define QoS policy, attach policer to traffic class
policy-map po_test
class cl_test
police aggregate pol_1mbps
! apply QoS policy to an interface
interface FastEthernet5/14
switchport access vlan 2
! switch qos to vlan-based mode on this port
qos vlan-based
! apply QoS policy to an interface
interface Vlan 2
service-policy output po_test
!
```

請注意，當連線埠處於基於VLAN的QoS模式，但沒有服務原則套用到對應的VLAN時，交換器會依照在實體連線埠上套用的服務原則（如有）。這樣在組合基於埠和基於VLAN的QoS時可以有更大的靈活性。

支援兩種型別的策略器：命名聚合和每個介面。命名的聚合管制器將管制從應用該管制器的所有介面合併的流量。上面的示例使用命名管制器。與命名管制器不同，每個介面管制器將分別管制應用它的每個介面上的流量。在策略對映配置中定義每個介面的策略器。請考慮以下帶有每個介面聚合監察器的示例：

```
! enable qos
qos
! define traffic class to be policed
class-map match-all cl_test2
match ip precedence 3 4
! define QoS policy, attach policer to traffic class
policy-map po_test2
class cl_test2
! per-interface policer is defined inside the policy map
police 512k 1000 conform-action transmit exceed-action drop
interface FastEthernet5/14
switchport
! set port to trust DSCP - need this to be able to match to incoming IP precedence
qos trust dscp
! switch to port-based qos mode
no qos vlan-based
! apply QoS policy to an interface
service-policy input po_test2
```

以下命令用於監控策略操作：

```
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400026 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166067574 bytes Exceed: 5268602114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400138 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166088574 bytes Exceed: 5268693114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
```

counter near class-map正在計算與相應類匹配的資料包數。

請注意以下實施的具體注意事項：

- 每類資料包計數器不是每個介面。也就是說，它在服務策略中應用了該類的所有介面中計算與該類匹配的所有資料包。

- 策略器不維護資料包計數器，只支援位元組計數器。
- 沒有特定命令可驗證每個監察器的已提供或傳出流量速率。
- 計數器定期更新。如果快速連續重複執行上述命令，計數器可能仍會在某個時間出現。

配置和監控標籤

配置標籤涉及以下步驟：

1. 定義流量分類標準 — 訪問清單、DSCP、IP優先順序等。
2. 使用之前定義的標準定義要分類的流量類。
3. 建立將標籤操作和/或策略操作附加到已定義類的策略對映。
4. 在相應的介面上配置信任模式。
5. 將策略對映應用於介面。

考慮以下示例，我們希望將IP優先順序3的傳入流量對映到主機192.168.196.3 UDP埠777以對映到IP優先順序6。所有其他IP優先順序3流量都將被管製為1 Mbps，多餘流量應被標籤為IP優先順序2。

```
! enable QoS globally
qos
! define ACL to select UDP traffic to 192.168.196.3 port 777
ip access-list extended acl_test4
permit udp any host 192.168.196.3 eq 777
! define class of traffic using ACL and ip precedence matching
class-map match-all cl_test10
match ip precedence 3
match access-group name acl_test4
! all the remaining ip precedence 3 traffic will match this class
class-map match-all cl_test11
match ip precedence 3
! define policy with above classes
policy-map po_test10
class cl_test10
! mark traffic belonging to class with ip precedence 6
set ip precedence 6
class cl_test11
! police and mark down all other ip precedence 3 traffic
police 1 mbps 1000 exceed-action policed-dscp-transmit
!
! adjust DSCP to policed DSCP map so to map DSCP 24 to DSCP 16
qos map dscp policed 24 to dscp 16
!
interface FastEthernet5/14
! set interface to trust IP DSCP
qos trust dscp
! apply policy to interface
service-policy input po_test10
!
```

sh policy interface命令用於監視標籤。示例輸出和影響記錄在以上策略配置中。

比較基於Catalyst 6000和Catalyst 4000/4500 IOS的管理引擎上的策略和標籤

Feature	Catalyst6000	Catalyst4000 SE3
Egress QoS policies	Not supported by Supervisor 1A and Superviso r2 hardware.	Supported.
Burst policing parameter calculation	Burst should be at least the same size as maximum frame supposed to pass via policer and no less then rate/interval, with the interval being 250 microseconds	No such restriction.
QoS policing L2 & L3	By default, microflow policing is only enabled for L3 on the sup1a and is not enabled at all for Supervisor 2. A CLI command is available to enable it for L2 on sup1a and L2 & L3 for sup2. Aggregate policing for sup1a & Supervisor 2 is enabled by default for L2 & L3.	Always.
Egress CoS	Always derived from internal DSCP using DSCP to CoS QoS map.	If the ingress port is in trust CoS mode, the egress CoS will be the same as the ingress CoS. Otherwise, it will be derived from the internal DSCP.
Microflow policing	Supported.	Not supported.
QoS behavior when port is in VLAN-based QoS mode, but no policy is applied to the VLAN.	No policy applied.	Fallback to port-based QoS. Will apply policy attached to port.

相關資訊

- 瞭解和配置QoS
- 技術支援 - Cisco Systems