Catalyst 4500交換器上的ACL和QoS TCAM耗盡避免

目錄

簡介

Cisco Catalyst 4500和Catalyst 4948系列交換器支援使用三重內容可定址記憶體(TCAM)的線速存取控制清單(ACL)和QoS功能。 只要ACL完全載入到TCAM中，啟用ACL和策略並不會降低交換機的交換或路由效能。如果TCAM耗盡，資料包可能會通過CPU路徑轉發，這會降低這些資料包的效能。本檔案提供以下各項的詳細資訊：

- Catalyst 4500和Catalyst 4948使用的不同型別的TCAM
- Catalyst 4500如何程式設計TCAM
- 如何在交換器上最佳設定ACL和TCAM，以避免TCAM耗盡

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Catalyst 4500 系列交換器
- Catalyst 4948 系列交換器

註：本檔案僅適用於基於Cisco IOS®軟體的交換器，而不適用於基於Catalyst OS(CatOS)的交換器。

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。

背景資訊

為了在硬體中實施各種型別的ACL和QoS策略，Catalyst 4500在Supervisor Engine中程式設計硬體查詢表(TCAM)和各種硬體暫存器。封包到達時，交換器會執行硬體表查詢（TCAM查詢），並決定允許或拒絕封包。

Catalyst 4500支援不同型別的ACL。表1概述了這些型別的ACL。

表1 - Catalyst 4500交換器支援的ACL型別

ACL型別	應用位置	受控流量	方向
RACL[1]	L3[2]埠、L3通道或SVI[3](VLAN)	路由IP流量	入站或出站
VACL[4]	VLAN(通過**vlan filter**命令)	路由入或出自VLAN或在VLAN內橋接的所有資料包	無方向
PACL[5]	L2[6]埠或L2通道	所有IP流量和非IPv4[7]流量（通過MAC ACL）	入站或出站

[1] RACL =路由器ACL

[2] L3 =第3層

[3] SVI =交換虛擬介面

[4] VACL = VLAN ACL

[5] PACL =埠ACL

[6] L2 =第2層

[7] IPv4 = IP版本4

Catalyst 4500 ACL和QoS硬體程式設計架構

Catalyst 4500 TCAM的條目數如下：

- 安全ACL（也稱為功能ACL）有32,000個條目
- 32,000個QoS ACL條目

對於安全ACL和QoS ACL，條目按以下方式專用：

- 輸入方向的16,000個條目
- 輸出方向的16,000個條目

圖3顯示TCAM條目專用性。有關TCAM的詳細資訊，請參閱TCAM的型別部分。

表2顯示可用於各種Catalyst 4500 Supervisor Engine和交換器的ACL資源。

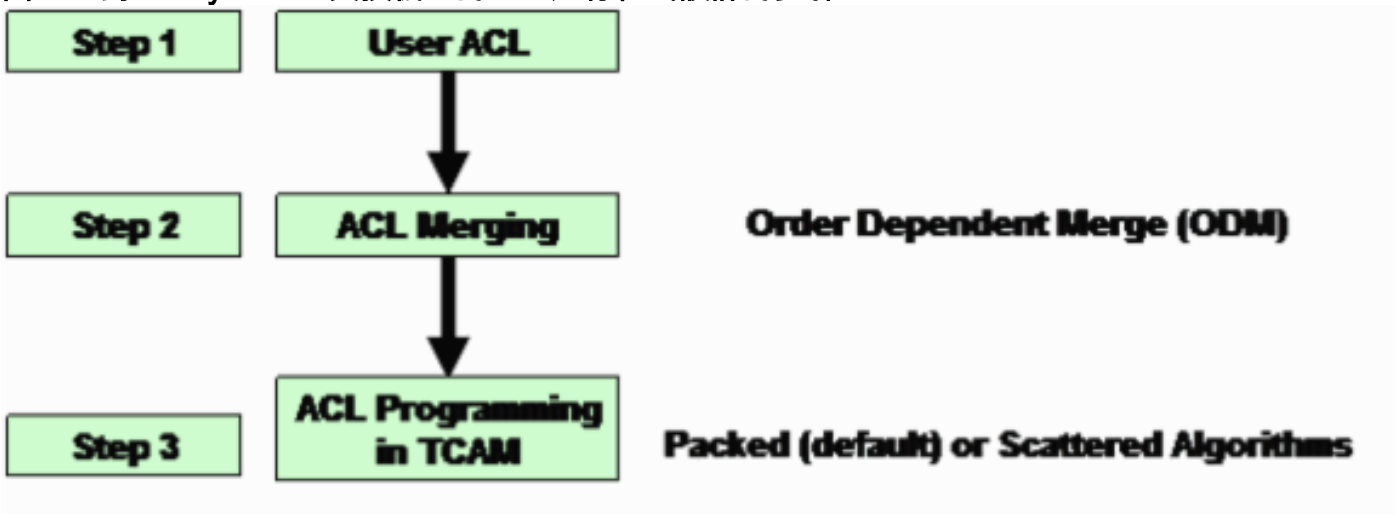
表2 — 各種Supervisor引擎和交換器上的Catalyst 4500 ACL資源

產品	TCAM版本	功能TCAM（每個方向）	QoS TCAM（每個方向）
管理引擎II+	2	8000個條目，1000個掩碼	8000個條目，1000個掩碼
管理引擎II+TS/III/IV/V和WS-C4948	2	16,000個條目，2000個掩碼	16,000個條目，2000個掩碼
管理引擎V-10GE和WS-C4948-10GE	3	16,000個條目，16,000個掩碼	16,000個條目，16,000個掩碼

Catalyst 4500為IP單播和多播路由使用單獨的專用TCAM。Catalyst 4500最多可以有128,000個單播和多播路由共用的路由條目。但是這些詳細資訊超出本檔案的範圍。本文檔僅討論安全性和QoS TCAM耗盡問題。

圖1顯示了對Catalyst 4500上硬體表中的ACL進行程式設計的步驟。

圖1 — 對Catalyst 4500交換機上的ACL進行程式設計的步驟



步驟1

此步驟涉及以下操作之一：

- 將ACL或QoS策略配置和應用到介面或VLANACL建立可以動態進行。IP來源防護(IPSG)功能就是一個例子。通過此功能，交換機自動為與埠關聯的IP地址建立PACL。
- 修改已經存在的ACL

注意：僅配置ACL不會導致TCAM程式設計。必須將ACL（QoS策略）應用於介面，才能在TCAM中對ACL進行程式設計。

步驟2

必須先合併ACL，然後才能在硬體表(TCAM)中進行程式設計。 合併以組合方式在硬體中編排多個ACL（PACL、VACL或RACL）。透過這種方式，只需進行一次硬體查詢，即可檢查資料包邏輯轉發路徑中的所有適用ACL。

例如，在圖2中，從PC-A路由到PC-C的資料包可能具有以下ACL:

- PC-A埠上的輸入PACL
- VLAN 1上的VACL
- VLAN 1介面上輸入方向的輸入RACL

將合併這三個ACL，以便在輸入TCAM中進行一次查詢就足以作出允許或拒絕的轉發決策。同樣地，由於對TCAM進行程式設計時使用了以下三個ACL的合併結果，因此只需要一次輸出查詢：

- VLAN 2介面上的輸出RACL
- VLAN 2 VACL
- PC-C埠上的輸出PACL

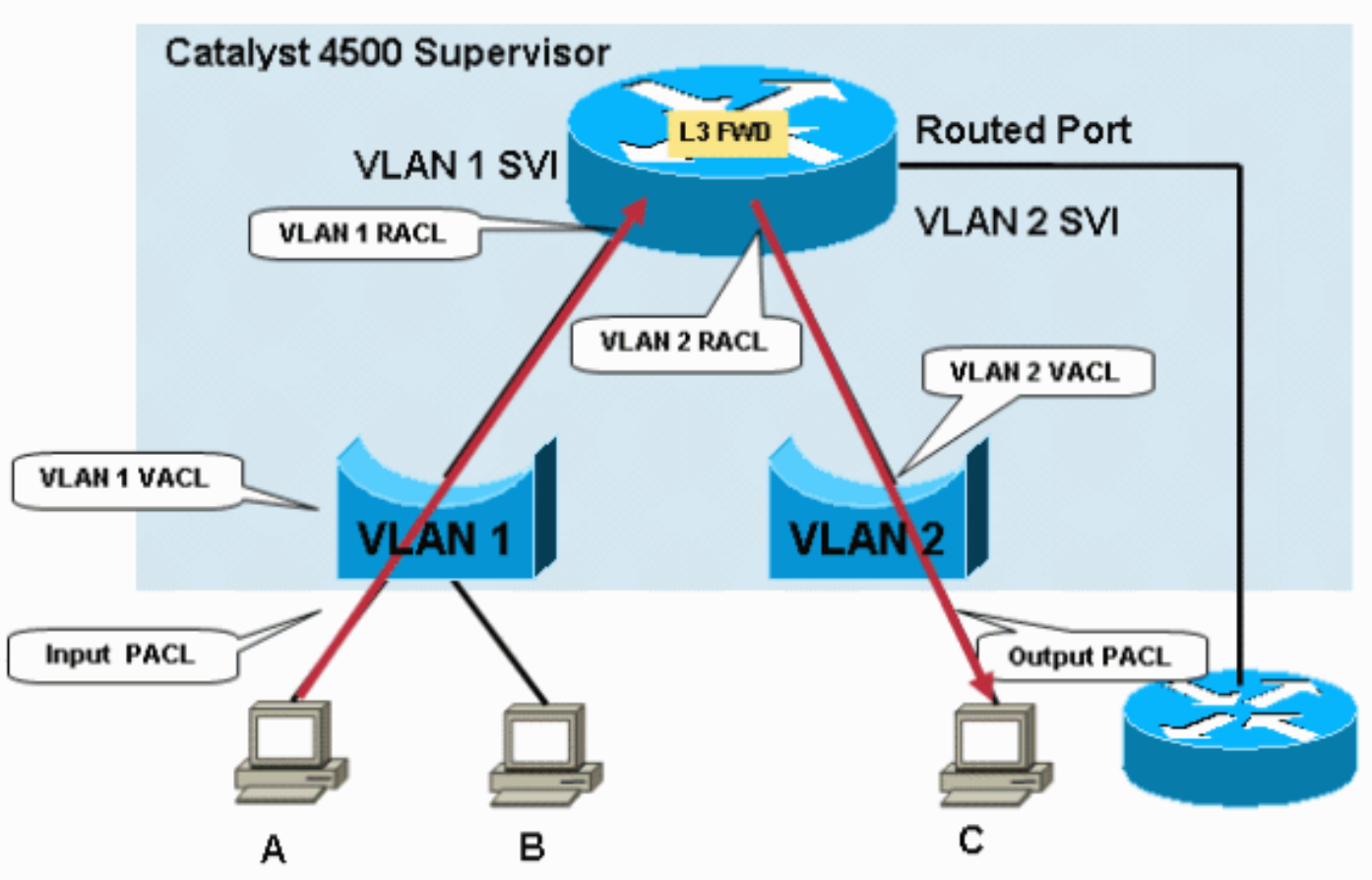
如果對輸入和輸出分別執行一次查詢，則當任何或所有ACL位於資料包轉發路徑中時，資料包的硬體轉發不會受到處罰。

註：輸入和輸出TCAM查詢在硬體中同時進行。一個常見的誤解是，輸出TCAM查詢在輸入TCAM查詢之後發生，如邏輯資料包流所示。瞭解此資訊很重要，因為Catalyst 4500輸出策略無法與輸入策略修改的QoS引數匹配。對於安全ACL，最嚴重的操作發生。在以下任何一種情況下，封包都會遭捨棄：

- 如果輸入查詢結果為丟棄且輸出查詢結果為允許
- 如果輸入查詢結果為允許且輸出查詢結果為丟棄

注意：如果輸入和輸出查詢結果都允許，則允許該資料包。

圖2 — 通過Catalyst 4500交換機上的安全ACL進行過濾



Catalyst 4500上的ACL合併取決於順序。此過程也稱為順序相關合併(ODM)。 使用ODM時，ACL條目將按照它們在ACL中的顯示順序進行程式設計。例如，如果ACL包含兩個訪問控制條目(ACE)，則交換機首先對ACE 1進行程式設計，然後對ACE 2進行程式設計。但是，順序相關性僅存在於特定ACL中的ACE之間。例如，ACL 120中的ACE可以先於TCAM中ACL 100中的ACE啟動。

步驟3

合併的ACL在TCAM中進行程式設計。ACL或QoS的輸入或輸出TCAM進一步分為兩個區域：PortAndVlan和PortOrVlan。如果組態在同一封包路徑中同時具有這些*ACL*，則合併的ACL會設定在TCAM的PortAndVlan區域：

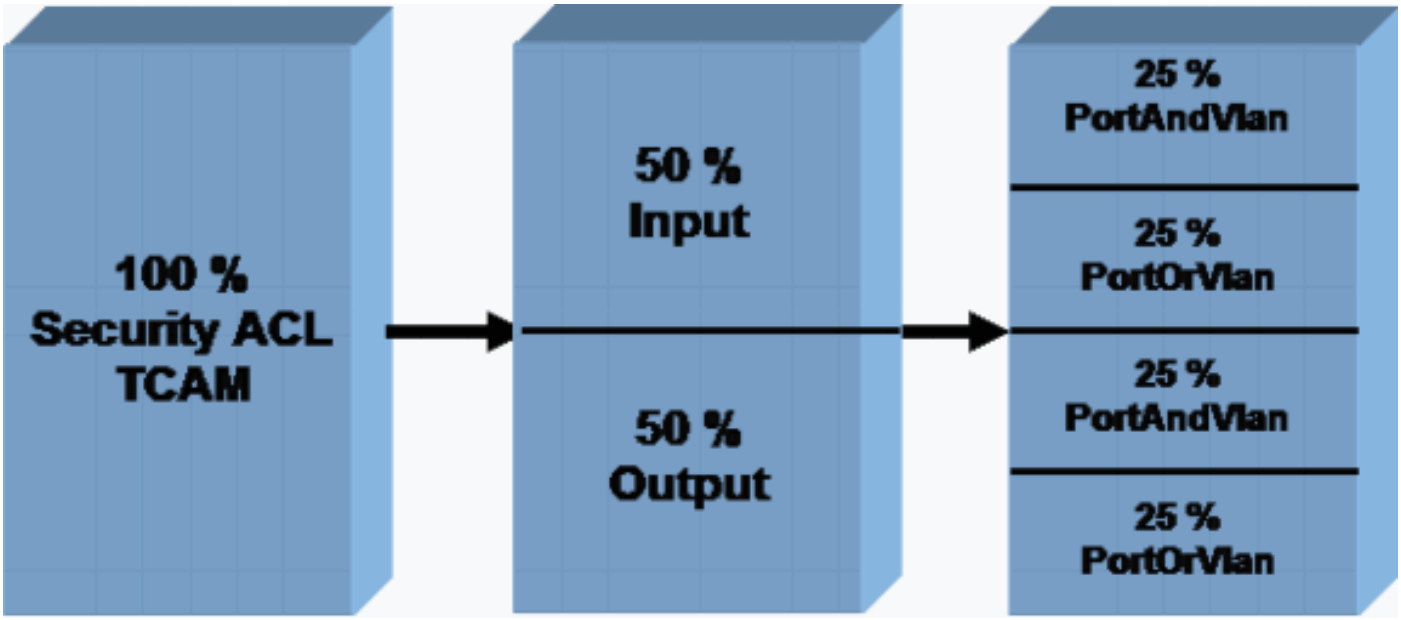
- A PACL**注意**：PACL是普通過濾ACL或IPSG建立的動態ACL。
- VACL或RACL

如果封包的特定路徑只有PACL、VACL或RACL，則會在TCAM的PortOrVlan區域中設定ACL。圖3顯示了各種型別ACL的安全ACL TCAM雕刻。QoS具有類似的分割、獨立的專用TCAM。

目前，您無法修改TCAM預設分配。但是，計畫在未來軟體版本中提供更改PortAndVlan和PortOrVlan區域可用的TCAM分配的功能。此更改將允許您增加或減少輸入或輸出TCAM中PortAndVlan和PortOrVlan的空間。

注意：PortAndVlan區域的任何分配增加都會導致輸入或輸出TCAM中PortOrVlan區域的相應減少。

圖3 - Catalyst 4500交換機上的安全ACL TCAM結構



show platform hardware ACL statistics utilization brief命令顯示ACL和QoS TCAM每個區域的此TCAM利用率。命令輸出會顯示可用的遮罩和專案，並將其按區域劃分，如圖3。此輸出範例來自Catalyst 4500 Supervisor Engine II+:

註：有關遮罩和條目的詳細資訊，請參閱本文檔的TCAM型別部分。

```
Switch#show platform hardware acl statistics utilization brief
                                    Entries/Total(%)  Masks/Total(%)
                                   ------------------  ---------------
            Input  Acl(PortAndVlan)  2016 / 4096 ( 49)   252 /  512 ( 49)
            Input  Acl(PortOrVlan)      6 / 4096 (  0)     5 /  512 (  0)
            Input  Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
            Input  Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
            Output Acl(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
            Output Acl(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
            Output Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
            Output Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
            L4Ops: used 2 out of 64
```

TCAM的型別

Catalyst 4500使用兩種型別的TCAM，如表2所示。本節介紹兩個TCAM版本之間的差異，以便您可以為您的網路和配置選擇適當的產品。

TCAM 2使用一種結構，其中八個條目共用一個掩碼。例如ACE中的八個IP地址。條目必須與它們共用的掩碼具有相同掩碼。如果ACE具有不同的掩碼，則條目必須根據需要使用單獨的掩碼。使用單獨的掩碼可能導致掩碼耗盡。在TCAM中，掩模耗盡是TCAM耗盡的常見原因之一。

TCAM 3沒有任何此類限制。在TCAM中，每個條目都可以有自己的唯一掩碼。可以充分利用硬體中可用的所有條目，無論這些條目的掩碼如何。

為了演示此硬體體系結構，本節中的示例顯示了TCAM 2和TCAM 3如何在硬體中對ACL進行程式設計。

```
access-list 101 permit ip host 8.1.1.1 any
access-list 101 deny ip 8.1.1.0 0.0.0.255 any
```

此範例ACL有兩個包含兩個不同遮罩的專案。ACE 1是主機條目，因此它具有/32掩碼。ACE 2是子

網條目，掩碼為/24。由於第二個條目具有不同的掩碼，因此不能使用掩碼1中的空條目，在TCAM 2的情況下使用單獨的掩碼。

下表說明此ACL如何在TCAM 2中程式設計：

遮罩	**專案**
遮罩1 Match:源IP地址的所有32位「不比對」：所有剩餘位	源IP = 8.1.1.1
	空條目2
	空條目3
	空條目4
	空條目5
	空條目6
	空條目7
	空條目8
遮罩2 Match:源IP地址的最重要的24位「不比對」：所有剩餘位	源IP = 8.1.1.0
	空條目2
	空條目3
	空條目4
	空條目5
	空條目6
	空條目7
	空條目8

即使有作為掩碼1一部分的可用條目，TCAM 2結構仍會阻止掩碼1的空條目2中填充ACE 2。由於ACE 2的掩碼與ACE 1的/32掩碼不匹配，因此不允許使用此掩碼。TCAM 2必須使用單獨的掩碼（/24掩碼）對ACE 2進行程式設計。

如表2所示，使用單獨的掩碼可以更快地耗儘可用資源。其他ACL仍然可以使用掩碼1中的其餘條目。但是，在大多數情況下，TCAM 2的效率很高，但不是百分百的。效率因配置方案而異。

下表顯示的是TCAM 3中程式化的ACL。TCAM 3會為每個專案分配遮罩：

遮罩	專案
IP地址1的掩碼32位	源IP = 8.1.1.1
IP地址2的掩碼24位	源IP = 8.1.1.0
空掩碼3	空條目3
空掩碼4	空條目4
空掩碼5	空條目5
空掩碼6	空條目6
空掩碼7	空條目7
空掩碼8	空條目8
空掩碼9	空條目9
空掩碼10	空條目10
空掩碼11	空條目11
空掩碼12	空條目12
空掩碼13	空條目13
空掩碼14	空條目14
空掩碼15	空條目15
空掩碼16	空條目16

在本例中，其餘的14個條目可以各有具有不同掩碼的條目，沒有任何限制。因此，TCAM 3比TCAM 2更有效率。此示例被過度簡化，以說明TCAM版本之間的差異。Catalyst 4500軟體已進行多項最佳化，可提高TCAM 2中實際設定情景的程式設計效率。本文的TCAM 2的次優TCAM程式設計演算法部分討論了這些最佳化。

對於Catalyst 4500上的TCAM 2和TCAM 3，如果在不同介面上應用相同的ACL，則會共用TCAM條目。此最佳化可以節省TCAM空間。

排除TCAM耗盡故障

在安全ACL的程式設計過程中，Catalyst 4500交換器上發生TCAM用盡時，ACL會透過軟體路徑進行部分應用。與TCAM中未應用的ACE匹配的資料包將在軟體中處理。軟體中的這種處理會導致CPU使用率高。由於Catalyst 4500 ACL的程式設計是依序進行的，因此ACL的程式設計總是從上到下。如果特定ACL不能完全插入TCAM，則很可能不會在TCAM中對ACL底部的ACE進行程式設計。

發生TCAM溢位時，將顯示警告消息。以下是範例：

```
%C4K_HWACLMAN-4-ACLHWPROGERRREASON: (Suppressed 1times) Input(null, 12/Normal)
Security: 140 - insufficient hardware TCAM masks.
%C4K_HWACLMAN-4-ACLHWPROGERR: (Suppressed 4 times) Input Security: 140 - hardware TCAM
limit, some packet processing will be software switched.
```

如果您已啟用syslog，則還可以在**show logging**命令輸出中看到此錯誤消息。出現此消息明確表示將進行某些軟體處理。因此，CPU使用率可能較高。如果在應用新ACL期間耗盡TCAM容量，則已在TCAM中程式設計的ACL將保留在TCAM中。與已程式設計的ACL匹配的資料包將繼續在硬體中進行處理和轉發。

注意：如果對大型ACL進行更改，可能會顯示超過TCAM的消息。交換器會嘗試在TCAM中重新程式設計ACL。在大多數情況下，修改後的新ACL可以在硬體中完全重新程式設計。如果交換器成功

將整個ACL重新程式設計到TCAM中，系統會顯示以下訊息：

```
*Apr 12 08:50:21: %C4K_COMMONHWACLMAN-4-ALLACLINHW: All configured ACLs
now fully loaded in hardware TCAM - hardware switching / QoS restored
```

使用**show platform software acl input summary interface *interface-id*** 命令以驗證ACL是否已在硬體中完全程式設計。

此輸出顯示ACL 101到VLAN 1的配置，並驗證ACL是否已在硬體中完全程式設計：

註：如果ACL未完全程式設計，可能會顯示TCAM耗盡錯誤消息。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip access-group 101 in
Switch(config-if)#end
Switch#
Switch#show platform software acl input summary interface vlan 1
Interface Name                 : Vl1
  Path(dir:port, vlan)         : (in :null, 1)
    Current TagPair(port, vlan) : (null, 0/Normal)
    Current Signature          : {FeatureCam:(Security: 101)}
  Type                         : Current
    Direction                  : In
    TagPair(port, vlan)        : (null, 0/Normal)
    FeatureFlatAclId(state)    : 0(FullyLoadedWithToCpuAces)
    QosFlatAclId(state)        : (null)
    Flags                      : L3DenyToCpu
```

Flags欄位(L3DenyToCpu)表示如果封包因為ACL而遭到拒絕，則封包會被傳送到CPU。交換器然後發出網際網路控制訊息通訊協定(ICMP) — 無法連線訊息。此行為是預設行為。當封包湧入CPU時，交換器上可能會發生CPU使用率較高的情況。但是在Cisco IOS軟體版本12.1(13)EW和更新版本中，這些封包是限速到CPU。在大多數情況下，思科建議您關閉傳送ICMP無法到達訊息的功能。

此輸出會顯示交換器設定為不傳送ICMP無法到達訊息，以及變更後驗證TCAM程式。命令輸出顯示，ACL 101的狀態現在為FullyLoaded。遭到拒絕的流量不會進入CPU。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#no ip unreachables
Switch(config-if)#end

Switch#show platform software acl input summary interface vlan 1
Interface Name                 : Vl1
  Path(dir:port, vlan)         : (in :null, 1)
    Current TagPair(port, vlan) : (null, 1/Normal)
    Current Signature          : {FeatureCam:(Security: 101)}
  Type                         : Current
    Direction                  : In
    TagPair(port, vlan)        : (null, 1/Normal)
    FeatureFlatAclId(state)    : 0(FullyLoaded)
    QosFlatAclId(state)        : (null)
    Flags                      : None
```

注意：如果在應用某個QoS策略期間超過QoS TCAM，則不會將該特定策略應用到介面或VLAN。Catalyst 4500不會在軟體路徑中實作QoS原則。因此，在超過QoS TCAM時，CPU利用率不會激增

。

```
*May 13 08:01:28: %C4K_HWACLMAN-4-ACLHWPROGERR: Input Policy Map: 10Mbps - hardware TCAM
limit, qos being disabled on relevant interface.

*May 13 08:01:28: %C4K_HWACLMAN-4-ACLHWPROGERRREASON: Input Policy Map: 10Mbps - no
available hardware TCAM entries.
```

發出**show platform cpu packet statistics**命令。確定ACL sw processing隊列是否收到大量資料包。大量資料包表示安全TCAM已用盡。此TCAM耗盡會導致資料包傳送到CPU進行軟體轉發。

```
Switch#show platform cpu packet statistics
!--- Output suppressed. Packets Received by Packet Queue  Queue                  Total
5 sec avg 1 min avg 5 min avg 1 hour avg ---------------------- -------------- --------- ------
--- --------- ---------- Control                        57902635        22        16
12          3 Host Learning                   464678         0         0         0          0 L3
Fwd Low                       623229         0         0         0          0 L2 Fwd
Low                     11267182         7         4         6          1 L3 Rx
High                          508         0         0         0          0 L3 Rx
Low                       1275695        10         1         0          0 ACL
fwd(snooping)               2645752         0         0         0          0 ACL log,
unreach               51443268         9         4         5          5 ACL sw
processing             842889240      1453      1532      1267       1179

Packets Dropped by Packet Queue

Queue                   Total           5 sec avg 1 min avg 5 min avg 1 hour avg
---------------------- -------------- --------- --------- --------- ----------
L2 Fwd Low                          3270         0         0         0          0
ACL sw processing                  12636         0         0         0          0
```

如果您發現ACL swCisco IOS軟體型Catalyst 4500交換器上的CPU使用率高以瞭解其他可能的原因。本文提供有關如何對其它高CPU使用率情況進行故障排除的資訊。

Catalyst 4500 TCAM可能因以下原因而溢位：

- TCAM 2的一種次優規划演算法
- ACL中過度使用第4層操作(L4Ops)
- Supervisor Engine或交換器型別的ACL過多

TCAM 2的次優TCAM程式設計演算法

如TCAM的型別一節所述，由於八個條目共用一個掩碼，TCAM 2的效率較低。Catalyst 4500軟體支援兩種型別的TCAM程式設計演算法，用於提高TCAM 2的效率：

- 壓縮 — 適用於大多數安全ACL場景**注意：**這是預設設定。
- 分散 — 用於IPSG方案

您可以將該演算法更改為散亂演算法，但如果您只配置了安全ACL（如RACL），通常這樣做沒有幫助。只有在多個埠上重複相同或相似的小型ACL的情況下，分散演算法才有效。在多個介面上啟用了IPSG的情況就是如此。在IPSG的情況中，每個動態ACL:

- 只有少量條目這包括允許允許允許的IP地址，並在末端執行拒絕操作，以防止未經授權的IP地址訪問埠。
- 對所有已配置的接入埠重複Catalyst 4507R上最多240個埠重複該ACL。

注意：TCAM 3使用預設打包演算法。由於TCAM結構是每個條目一個掩碼，因此壓縮演算法是最好

的可能演算法。因此，這些交換器上未啟用分散式演演算法選項。

此範例位於針對IPSG功能設定的Supervisor引擎II+上。輸出顯示，儘管只使用了49%的條目，但使用了89%的掩碼：

```
Switch#show platform hardware acl statistics utilization brief

                                    Entries/Total(%)  Masks/Total(%)
                                   ----------------  --------------
          Input  Acl(PortAndVlan)  2016 / 4096 ( 49)   460 /  512 ( 89)
          Input  Acl(PortOrVlan)      6 / 4096 (  0)     4 /  512 (  0)
          Input  Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
          Input  Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
          Output Acl(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
          Output Acl(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
          Output Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
          Output Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
          L4Ops: used 2 out of 64
```

在這種情況下，將程式設計演算法從預設打包演算法更改為散亂演算法會有所幫助。散亂演算法將總掩碼使用率從89%降低到49%。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#access-list hardware entries scattered
Switch(config)#end
Switch#show platform hardware acl statistics utilization brief
                                    Entries/Total(%)  Masks/Total(%)
                                   ----------------  --------------
          Input  Acl(PortAndVlan)  2016 / 4096 ( 49)   252 /  512 ( 49)
          Input  Acl(PortOrVlan)      6 / 4096 (  0)     5 /  512 (  0)
          Input  Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
          Input  Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
          Output Acl(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
          Output Acl(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
          Output Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
          Output Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
          L4Ops: used 2 out of 64
```

有關Catalyst 4500交換機上的安全功能的最佳實踐的資訊，請參閱Catalyst 4500安全功能管理引擎的最佳實踐。

ACL中過度使用L4Ops

術語L4Ops是指ACL設定中使用**gt**、**lt**、**neq**和**range**關鍵字。Catalyst 4500對可在單個ACL中使用的這些關鍵字的數量進行了限制。限制因管理引擎和交換機而異，為每個ACL六或八個L4Op。表3顯示每個Supervisor Engine和每個ACL的限制。

表3 — 不同Catalyst 4500 Supervisor引擎和交換器上的每個ACL的L4Op限制

產品	L4Op
管理引擎II+/ II+TS	32個（每個ACL 6個）
管理引擎III/IV/V和WS-C4948	32個（每個ACL 6個）
管理引擎V-10GE和WS-C4948-10GE	64個（每個ACL 8個）

如果超過每個ACL的L4Op限制，則控制檯上會顯示一條警告消息。訊息與以下類似：

```
%C4K_HWACLMAN-4-ACLHWPROGERR: Input Security: severn - hardware TCAM limit, some
packet processing will be software switched.
19:55:55: %C4K_HWACLMAN-4-ACLHWPROGERRREASON: Input Security: severn - hardware TCAM L4
operators/TCP flags usage capability exceeded.
```

此外，如果超過L4Op限制，則在TCAM中擴展特定ACE。其他TCAM利用率結果。此ACE用作示例：

```
access-list 101 permit tcp host 8.1.1.1 range 10 20 any
```

若此ACE位於ACL中，交換器僅使用一項和L4Op。但是，如果此ACL中已使用六個L4Op，則此ACE將擴展到硬體中的10個條目。這樣的擴展可能會耗盡TCAM中的大量條目。仔細使用這些L4Ops可以防止TCAM溢位。

注意：如果此案例涉及Supervisor Engine V-10GE和WS-C4948-10GE，則之前在ACL中使用的8個L4Op會導致ACE擴展。

在Catalyst 4500交換器上使用L4Op時，請記住以下專案：

- 如果運算子或運算元不同，則L4運算被視為不同。例如，此ACL包含三個不同的L4操作，因為**gt 10**和**gt 11**被視為兩個不同的L4操作：
  ```
  access-list 101 permit tcp host 8.1.1.1 any gt 10
  access-list 101 deny tcp host 8.1.1.2 any lt 9
  access-list 101 deny tcp host 8.1.1.3 any gt 11
  ```

- 如果同一個運算子/運算元耦合對源埠應用一次，對目標埠應用一次，則認為L4操作是不同的。以下是範例：
  ```
  access-list 101 permit tcp host 8.1.1.1 gt 10 any
  access-list 101 permit tcp host 8.1.1.2 any gt 10
  ```

- Catalyst 4500交換器儘可能共用L4Ops。在本例中，粗體***斜體***中的行演示了以下情況：ACL 101的L4Op使用率= 5ACL 102的L4Op使用率= 4 **注意：eq關鍵字不會佔用任何L4Op硬體資源**。L4Op總使用率= **8注意：**ACL 101和102共用一個L4Op。**注意：即使**TCP或使用者資料包通訊協定(UDP)等通訊協定不相符或permit/deny作業不相符，也會共用第4層通訊協定。

Supervisor Engine或交換器型別的ACL過多

如表2所示，TCAM是有限的資源。如果使用大量IPSG條目配置過多的ACL或功能（如IPSG），則您可以超過任何Supervisor Engine的TCAM資源。

如果您超出了Supervisor Engine的TCAM空間，請執行以下步驟：

- 如果您搭載Supervisor Engine II+，且執行低於*Cisco IOS軟體版*本12.2(18)EW的Cisco IOS軟體版本，請升級至最新的Cisco IOS軟體版本12.2(25)EWA維護版本。TCAM容量在後續版本中已增加。
- 如果您使用DHCP監聽和IPSG，並且開始用完TCAM，請使用最新的Cisco IOS軟體版本12.2(25)EWA維護版本，並在TCAM 2產品的情況下使用分散演算法。**註：**Cisco IOS軟體版本12.2(20)EW及更新版本提供分散式演演算法。最新版本還增強了DCHP監聽和動態地址解析協定(ARP)檢測(DAI)功能，以提高TCAM利用率。
- 如果因為超出了L4Op限制而開始用盡TCAM，請嘗試減少ACL中的L4Op使用量以防止TCAM溢

位。

- 如果您在同一個VLAN中的不同連線埠上使用許多類似ACL或原則，請將其聚合到VLAN介面上的單個ACL或原則中。此聚合可節省一些TCAM空間。例如，當您應用基於語音的策略時，預設基於埠的QoS用於分類。此預設QoS可能導致超過TCAM容量。如果將QoS切換為基於VLAN，則可以減少TCAM使用。
- 如果TCAM空間仍有問題，請考慮高端Supervisor引擎，例如Supervisor引擎V-10GE或Catalyst 4948-10GE。這些產品使用最高效的TCAM 3硬體。

摘要

Catalyst 4500使用TCAM對配置的ACL進行程式設計。TCAM允許在硬體轉發路徑中應用ACL，而不會影響交換機的效能。無論ACL的大小如何，效能都是恆定的，因為ACL查詢的效能是以線速執行的。但是，TCAM資源有限。因此，如果您配置的ACL條目數量過多，將超過TCAM容量。Catalyst 4500已執行許多最佳化並提供命令來改變TCAM的程式設計演算法以達到最大的效率。TCAM 3產品（如管理引擎V-10GE和Catalyst 4948-10GE）為安全ACL和QoS策略提供了最多的TCAM資源。

相關資訊

- LAN 產品支援頁面
- LAN 交換支援頁面
- 技術支援與文件 - Cisco Systems