Catalyst 4500交换机中ACL和QoS TCAM的耗尽避免

目录

简介

Cisco Catalyst 4500和Catalyst 4948系列交换机支持有线速率访问控制表(ACL)和QoS功能与使用三重内容可编址存储器。只要ACL在TCAM，充分地装载ACL和策略的启动不降低交换机的交换或路由性能。如果TCAM用尽，数据包可能通过CPU路径转发，能降低那些数据包的性能。本文提供细节：

- 不同种类的TCAM Catalyst 4500和Catalyst 4948使用
- Catalyst 4500如何编程TCAMs
- 如何最佳地配置ACL和TCAM在交换机为了避免TCAM耗尽

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Catalyst 4500 系列交换机
- Catalyst 4948 系列交换机

注意： 本文仅适用于基于Cisco IOS软件的交换机，并且不适用于Catalyst OS (CatOS) -基本交换机。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

为了实现ACL的多种在硬件、Catalyst 4500程序硬件查询表(TCAM)和多种硬件寄存器的类型和QoS策略在Supervisor引擎。当数据包到达时，交换机执行硬件表查找(TCAM查找)并且决定对permit或丢弃数据包。

Catalyst 4500支持不同种类的ACL。表1概述ACL的这些类型。

表1 – Catalyst 4500交换机支持ACL的类型

ACL类型	那里它应用	控制流量	方向
RACL[1]	L3[2]端口、L3信道或者SVI[3] (VLAN)	路由的IP流量	入站或出站
VACL[4]	VLAN (通过**vlan filter命令**)	路由或在VLAN外面或在VLAN内桥接的所有信息包	无方向
PACL[5个]	L2[6]端口或L2信道	所有IP数据流和non-IPv4[7]流量(通过MAC ACL)	入站或出站

[1] RACL =路由器ACL

[2] L3 =第3层

[3] SVI =交换虚拟接口

[4] VACL = VLAN ACL

[5个]PACL =端口ACL

[6] L2 = Layer2

[7个]IPv4 = IP版本4

Catalyst 4500 ACL和QoS硬件编程的体系结构

Catalyst 4500 TCAM有条目以下数量：

- 安全ACL的32,000个条目，亦称是功能ACL
- QoS ACL的32,000个条目

对于两安全ACL和QoS ACL，条目接下来投入：

- 输入方向的16,000个条目
- 输出方向的16,000个条目

图3显示TCAM条目致力。请参阅TCAM部分种类关于TCAMs的更多信息。

表2显示为多种Catalyst 4500 Supervisor引擎和交换机是可用的ACL资源。

表2 – Catalyst 4500在多种Supervisor引擎和交换机的ACL资源

产品	TCAM版本	功能TCAM（每个方向）	QoS TCAM（每个方向）
Supervisor引擎II+	2	8000个条目，1000个掩码	8000个条目，1000个掩码
Supervisor引擎II+TS/III/IV/V和WS-C4948	2	16,000个条目，2000个掩码	16,000个条目，2000个掩码
Supervisor引擎V-10GE和WS-C4948-10GE	3	16,000个条目，16,000个掩码	16,000个条目，16,000个掩码

Catalyst 4500用途分离，投入IP单播和组播路由的TCAMs。Catalyst 4500能有单播和组播路由共享的128,000路由条目。然而，在本文的范围之外，这些详细信息是。本文只讨论安全和QoS TCAM耗尽问题。

图1在Catalyst 4500的硬件表里显示步骤编程ACL。

图1 -编程在Catalyst 4500交换机的ACL的步骤

步骤 1

此步骤介入这些操作之一：

- ACL或QoS策略的配置和应用程序对接口或VLANACL创建能动态地发生。示例是IP源防护(IPSG)功能的事例。使用此功能，交换机自动地创建用端口关联的IP地址的一PACL。
- 已经存在ACL的修改

注意： 单独配置ACL不导致TCAM编程。ACL (QoS策略)在TCAM必须对已应用对接口为了编程ACL。

步骤 2

必须合并ACL，在硬件表前(TCAM)里可以被编程。归并程序多个ACL (PACL、VACL或者RACL)在

硬件里在一个复合方式。这样，仅单个硬件查找是必要检查所有可适用的ACL在数据包逻辑转发路径。

例如，在表2，从PC-A潜在路由到PCC的数据包能有这些ACL ：

- 在PC-A端口的一输入PACL
- 在VLAN1的VACL
- 在VLAN1接口的一个输入RACL在输入方向

这三个ACL合并，以便在输入TCAM的单个查找是做出转发决策的足够允许或拒绝。同样地，因为TCAM编程与这三个ACL，合并的结果仅独立输出集成查找是必要的：

- 在VLAN 2接口的输出RACL
- VLAN 2 VACL
- 在PCC端口的输出PACL

使用输入的单个查找和一个，当任一或所有这些ACL在信息包转发路径时，输出的，没有数据包的补偿硬件转发。

注意： 输入和输出TCAM查找在硬件方面同时发生。常见的误解是输出TCAM查找在输入TCAM查找以后发生，因为逻辑数据包流建议。因为Catalyst 4500输出策略在输入策略被修改的QoS参数，不能配比此信息是重要了解。一旦安全ACL，最严重的操作发生。数据包在这些情况之一丢弃：

- 如果输入查找结果是丢弃和输出查找结果是permit
- 如果输入查找结果是permit和输出查找结果是丢弃

注意： 如果两个输入和输出查找结果是permit，数据包允许。

图2 –过滤通过在Catalyst 4500交换机的安全ACL

在Catalyst 4500的ACL合并根据顺序的。亦称进程是Order Dependent Merge (ODM)。使用ODM，ACL条目按他们在ACL出现的顺序被编程。 例如，如果ACL包含两访问控制条目(ACE)，交换机首先编程ACE 1然后编程ACE 2。然而，命令依赖因素仅在特定ACL内的ACE之间。例如，在ACL 120的ACE能在ACL 100的ACE前开始在TCAM。

步骤 3

合并的ACL在TCAM被编程。ACL或QoS的输入或输出TCAM是进一步已分解到两地区、PortAndVlan和PortOrVlan。如果配置有*这两个*ACL在同一个信息包路径，合并的ACL在TCAM的PortAndVlan区域被编程：

- 一PACL**注意：** PACL是过滤ACL或IPSG-created动态ACL的正常。
- VACL或RACL

如果数据包的特定路径有一PACL或VACL或者仅RACL， ACL在TCAM的PortOrVlan区域被编程。图3显示雕刻为ACL的多种类型的安全ACL TCAM。QoS有一类似被雕刻的，分开，专用的TCAM。

目前，您不能修改TCAM默认分配。然而，有规划提供能力更改为PortAndVlan和PortOrVlan区域是可用的在将来软件版本的TCAM分配。此更改将允许您增加或减少PortAndVlan和PortOrVlan的空间在输入或输出TCAMs中。

注意： 在分配的所有增加PortAndVlan区域将导致PortOrVlan区域的一等同的降低输入或输出TCAM的。

图3 –安全ACL在Catalyst 4500交换机的TCAM结构

show platform hardware ACL statistics utilization brief命令显示此TCAM利用率每个ACL和QoS的TCAMs区域。命令输出显示可用的掩码和条目并且以地域分开他们，正如在图3。此输出示例:是从Catalyst 4500 Supervisor引擎II+ ：

注意： 请参阅本文的TCAM部分种类关于掩码和条目的更多信息。

```
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的类型

因为表2显示， Catalyst 4500使用TCAM的两种类型。此部分提交两个TCAM版本之间的差异，以便您能选择您的网络和配置的适当的产品。

TCAM 2使用八条目共享一掩码的一个结构。示例是在ACE的八个IP地址。条目必须有掩码和他们共享的掩码一样。如果ACE有不同的掩码，条目必须如所需要使用独立的掩码。此使用独立的掩码可以导致屏蔽耗尽。在TCAM的掩码耗尽是其中一TCAM耗尽的常见原因。

TCAM3没有任何如此限制。每个条目能有其在TCAM的自己的唯一掩码。是可用的在硬件方面所有条目的充分的利用是可能的，不管那些条目掩码。

为了展示此硬件体系结构，在此部分的示例如何在硬件方面显示TCAM 2和TCAM3程序ACL。

```
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
```

此示例ACL有有两个不同的掩码的两个条目。ACE 1是主机条目和，因此有一/32掩码。ACE 2是与/24掩码的一个子网条目。由于第二个条目有一不同的掩码，不可能使用在掩码1的空条目，并且一分开的掩码使用一旦TCAM 2。

此表显示此ACL如何在TCAM 2被编程：

掩码	条目
掩码1匹配：源IP地址"do not care"的全部32个位：所有剩余位	来源IP = 8.1.1.1
	空entry2
	空entry3
	空条目4
	空条目5
	空条目6
	空条目7
	空条目8
掩码2匹配：源IP地址"do not care"的多数重大的24个位：所有剩余位	来源IP = 8.1.1.0
	空entry2
	空entry3
	空条目4
	空条目5

	空条目6
	空条目7
	空条目8

即使有自由输入可用作为掩码1一部分， TCAM 2结构防止ACE 2的人口在空entry2的掩码的1。因为掩码ACE 2不匹配/32掩码ACE 1. TCAM 2必须编程与使用的ACE 2一分开的掩码， /24掩码，使用此掩码不是可允许的。

因为表2显示，此使用一分开的掩码能导致可用资源的更加快速的耗尽。其他ACL在掩码1.能仍然使用剩余的条目。然而，在大多数情况下，效率TCAM 2高，但是不是100百分比。效率变化以每个配置情形。

此表显示在TCAM 3. TCAM3编程的同样ACL分配每个条目的一掩码：

掩码	**条目**
掩码IP地址的1 32个位	来源IP = 8.1.1.1
掩码IP地址的2 24个位	来源IP = 8.1.1.0
倒空掩码3	倒空entry3
倒空掩码4	倒空条目4
倒空掩码5	倒空条目5
倒空掩码6	倒空条目6
倒空掩码7	倒空条目7
倒空掩码8	倒空条目8
倒空掩码9	倒空条目9
倒空掩码10	倒空条目10
倒空掩码11	倒空条目11
倒空掩码12	倒空条目12
倒空掩码13	倒空条目13
倒空掩码14	倒空条目14
倒空掩码15	倒空条目15
倒空掩码16	倒空条目16

在本例中， 14个剩余的条目能中的每一个有用不同的掩码的条目，没有限制。所以， TCAM3比TCAM 2.是更有效的。此示例过度地简化为了说明TCAM版本之间的差异。Catalyst 4500软件有增加许多的优化效率编程在一个实用的配置情形的TCAM 2。编程本文的TCAM 2部分的不最理想的TCAM算法讨论这些优化。

对于在Catalyst 4500的TCAM 2和TCAM3，如果同样ACL在不同的接口，应用， TCAM条目共享。此优化节省TCAM空间。

排除故障TCAM耗尽

在编程安全ACL期间时，当TCAM耗尽在Catalyst 4500交换机发生， ACL的一部分应用程序通过软件路径发生。匹配ACE在TCAM没有应用的数据包在软件方面处理。处理在软件方面的这导致高CPU利用率。由于Catalyst 4500 ACL编程根据顺序的， ACL从上到下总是被编程。如果特定ACL不完全地适合到TCAM，在ACL的底下部分的ACE在TCAM很可能没有被编程。

当TCAM溢出发生，警告消息出现。示例如下：

```
%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.
```

如果启用Syslog，您在**show logging命令**输出中能也看到此错误消息。此消息出现确实地表明若干软件处理将发生。结果，可以有高CPU利用率。在TCAM已经被编程了的ACL在TCAM保持编程，如果TCAM产能的耗尽在新的ACL的应用程序时发生。匹配ACL已经被编程了的数据包在硬件方面继续处理和转发。

注意： 如果做对大ACL的变动， TCAM-exceeded消息可能显示。交换机设法重编程序在TCAM的ACL。在大多数情况下，新，已修改ACL在硬件方面可以充分地被重编程序。如果交换机能顺利地重编程序在整体的ACL到TCAM，此消息出现：

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

请使用**show platform software acl input summary interface interface-id命令**为了验证ACL在硬件方面充分地被编程。

此输出显示ACL 101的配置对VLAN1和验证ACL在硬件方面充分地被编程：

注意： 如果ACL不充分地被编程， TCAM-exhaustion错误消息可能显示。

```
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
```

标志字段(L3DenyToCpu)表明，如果数据包拒绝由于ACL，数据包被踢对CPU。交换机然后派出网际控制信息规约(ICMP)无法得到的信息。此行为是默认。当数据包被踢对CPU时，高CPU利用率在交换机能发生。然而，在Cisco IOS软件版本12.1(13)EW和以后，这些数据包是速率限制对CPU。在大多数情况下，思科建议您关闭传送ICMP不可达信息的功能。

此输出显示交换机的配置不发送ICMP不可达信息和编程在更改以后的TCAM的验证。因为命令输出显示， ACL 101的状态当前是FullyLoaded。拒绝的数据流不去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QoS TCAM在有些QoS策略的应用程序时被超出，该特定策略没有应用对接口或VLAN。Catalyst 4500不在软件路径实现QoS策略。所以，当QoS TCAM被超出时， CPU利用率不阻止。

```
*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.
```

发出 **show platform cpu packet statistics** 命令。确定队列的ACL sw是否收到数据包大量。数据包大量指示安全TCAM的耗尽。此TCAM耗尽造成数据包被发送到软件转发的CPU。

```
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
```

如果发现队列的ACL sw收到过量的流量，参考在基于Cisco IOS软件的Catalyst 4500交换机的高CPU利用率其他可能的原因的。本文提供信息关于怎样排除故障其他高CPU利用率方案。

Catalyst 4500 TCAM能溢出对于这些原因：

- 编程TCAM的2的一不最理想的TCAM算法
- 额外的使用Layer4操作(L4Ops)在ACL
- Supervisor引擎或交换机类型的额外的ACL

编程TCAM的2的不最理想的TCAM算法

因为TCAM的部分类型讨论， TCAM 2效率更低归结于事实八条目共享一掩码。Catalyst 4500软件允许编程改进效率TCAM 2 TCAM的2的TCAM的两种类型的算法：

- 包装—适用于多数安全ACL方案**注意：** 这是默认设置。
- 分散—使用在IPSG方案

您能更改算法到一种分散的算法，但是这不典型地帮助，如果配置仅安全ACL，例如RACL。分散的算法只是有效在同样或相似，小ACL在许多端口被重复的方案。此方案是在多个接口启用有IPSG的实际情形。在IPSG方案中，每个动态ACL ：

- 有很小数量的条目这包括允许IP地址的许可证和拒绝在末端为了由未授权的IP地址防止端口的访问。
- 为所有配置的访问存取端被重复ACL为Catalyst 4507R的240个端口被重复。

注意： TCAM3使用默认被包装的算法。由于TCAM结构是每个条目一掩码，被包装的算法是最好算法。所以，分散的算法选项在这些交换机没有启用。

为IPSG功能配置的此示例在Supervisor引擎II+。输出显示，虽然仅使用条目的49百分比，掩码的89百分比被消耗：

```
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
```

在这种情况下，在编程的算法上的一个变化从默认包装了算法对分散的算法帮助。分散的算法减少从89百分比的总掩码使用情况到49百分比。

```
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
```

关于安全功能的最佳实践的信息在Catalyst 4500交换机，参考Catalyst 4500 Supervisor的安全功能最佳实践。

额外的使用在ACL的L4Ops

期限L4Ops是指使用**gt**、**Lt**、**neq**和**范围**关键字在ACL配置。Catalyst 4500有在您在单个ACL能使用这些关键字的数量的限额。限制，由Supervisor引擎和交换机变化，是每个ACL六或八L4Ops。表3显示限制每Supervisor引擎和每个ACL。

表3 – L4Op限制每个在不同的Catalyst 4500 Supervisor引擎和交换机的ACL

产品	L4Op
Supervisor 引擎 II+/II+TS	32 (6每个ACL)
Supervisor引擎III/IV/V和WS-C4948	32 (6每个ACL)
Supervisor引擎V-10GE和WS-C4948-10GE	64 (8每个ACL)

如果L4Op限制每个ACL超过，警告消息在控制台显示。消息类似于此：

```
%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.
```

并且，如果L4Op限制超过，特定ACE在TCAM展开。另外的TCAM利用率结果。此ACE服务得为例：

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

使用在ACL的此ACE，交换机只使用一个条目和一L4Op。然而，如果六L4Ops已经用于此ACL，此ACE在硬件里展开对10个条目。这样扩展在TCAM能潜在用完很多条目。仔细使用这些L4Ops防止TCAM溢出。

注意： 如果此案件介入Supervisor引擎V-10GE和WS-C4948-10GE，在ACL的八以前使用的L4Ops导致ACE扩展。

当您使用在Catalyst 4500交换机时的L4Op请记住这些项目：

- 如果操作员或操作数有所不同， L4操作被认为不同的。例如，因为**gt 10**和**gt 11**认为两不同的

L4操作，此ACL包含三不同的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`

- 如果同一对操作员/操作数夫妇一次适用到源端口和一次于目的地端口， L4操作被认为不同的。示例如下：`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交换机共享L4Ops，当可能。在本例中，线路以***黑体斜体字***展示此方案：ACL 101的L4Op使用情况= 5ACL 102的L4Op使用情况= 4 **注意： eq**关键字不消耗其中任一种L4Op硬件资源。总L4Op使用情况= **8注意：** ACL 101和102共享一L4Op。**注意：** L4Op共享，即使协议，例如TCP或用户数据报协议(UDP)，不配比或permit/拒绝操作不匹配。

Supervisor引擎或交换机类型的额外的ACL

因为表2显示， TCAM是有限资源。如果配置额外的ACL或功能类似IPSG用IPSG条目，大量您可以超出所有Supervisor引擎TCAM资源。

如果超出您的Supervisor引擎的TCAM空间，请采取这些步骤：

- 如果有一Supervisor引擎II+，并且运行早于Cisco IOS软件版本12.2(18)EW的Cisco IOS软件版本，请升级到最新的Cisco IOS软件版本12.2(25)EWA维护版。TCAM产能在最新版本增加。
- 如果使用DHCP监听，并且IPSG和您开始用尽TCAM，使用最新的Cisco IOS软件版本12.2(25)EWA维护版和使用分散的算法一旦TCAM 2产品。**注意：** 分散的算法是可用的在Cisco IOS软件版本12.2(20)EW和以后。新版本也有更加好的TCAM利用率的增强与DCHP监听和动态地址解析服务(ARP)检查(戴)功能。
- 如果开始用尽TCAM，因为L4Op限制超过，请设法减少在ACL的L4Op使用情况为了防止TCAM溢出。
- 如果在同样VLAN使用许多相似的ACL或策略在多种端口，请聚集他们到单个ACL或策略在VLAN接口。此聚合节省若干TCAM空间。例如，当您运用基于语音的策略时，默认基于端口的QoS使用分类。此默认QoS能导致TCAM能力被超出。如果换成QoS基于vlan的，您减少TCAM使用情况。
- 如果仍然有与TCAM的问题间隔，考虑一高端Supervisor引擎，例如Supervisor引擎V-10GE或Catalyst 4948-10GE。这些产品使用最高效的TCAM3硬件。

摘要

Catalyst 4500编程与使用的已配置的ACL TCAM。TCAM允许ACL的应用程序在硬件转发路径没有在交换机的性能的影响。不管 ACL 的大小如何，性能都不变，因为 ACL 查找的性能在于线路速率。但是，TCAM 是一种有限的资源。因此，如果配置了过量的 ACL 条目，则会超出 TCAM 容量。Catalyst 4500实现许多优化和，假设命令变化TCAM编程的算法为了达到最大效率。TCAM3产品例如Supervisor引擎V-10GE和Catalyst 4948-10GE提供安全ACL和QoS策略的多数TCAM资源。

相关信息

- LAN 产品支持页
- LAN 交换技术支持页
- 技术支持和文档 - Cisco Systems