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系列交换机使用三态内容可寻址存储器(TCAM)支持线速访问控制列表(ACL)和QoS功能。 只要ACL在TCAM中完全加载，启用ACL和策略不会降低交换机的交换或路由性能。如果TCAM耗尽，则数据包可通过CPU路径转发，这会降低这些数据包的性能。本文档提供有关以下内容的详细信息：

- Catalyst 4500和Catalyst 4948使用的不同类型的TCAM
- Catalyst 4500如何编程TCAM。
- 如何在交换机上优化配置ACL和TCAM以避免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：本文档仅适用于基于Cisco IOS®软件的交换机，不适用于基于Catalyst OS(CatOS)的交换机。

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

为了在硬件中实施各种类型的ACL和QoS策略，Catalyst 4500在Supervisor引擎中编程硬件查找表(TCAM)和各种硬件寄存器。当数据包到达时，交换机执行硬件表查找（TCAM查找），并决定允许或拒绝该数据包。

Catalyst 4500支持不同类型的ACL。表1列出了这些类型的ACL。

表1 - Catalyst 4500交换机支持的ACL类型

ACL类型	应用位置	受控流量	方向
RACL[1]	L3[2]端口、L3通道或SVI[3](VLAN)	路由IP流量	入站或出站
VACL[4]	VLAN(通过vlan filter命令)	路由到VLAN或从VLAN路由到VLAN或桥接到VLAN的所有数据包	无方向
PACL[5]	L2[6]端口或L2通道	所有IP流量和非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] PACL =端口ACL

[6] L2 =第2层

[7] IPv4 = IP版本4

Catalyst 4500 ACL和QoS硬件编程架构

Catalyst 4500 TCAM具有以下条目数：

- 32,000个安全ACL条目，也称为功能ACL
- 32,000个QoS ACL条目

对于安全ACL和QoS ACL，条目都以以下方式专用：

- 输入方向16,000个条目
- 输出方向有16,000个条目

图3显示了TCAM条目题注。有关TCAM的详细信息，请参阅TCAM类型部分。

表2显示了可用于各种Catalyst 4500 Supervisor引擎和交换机的ACL资源。

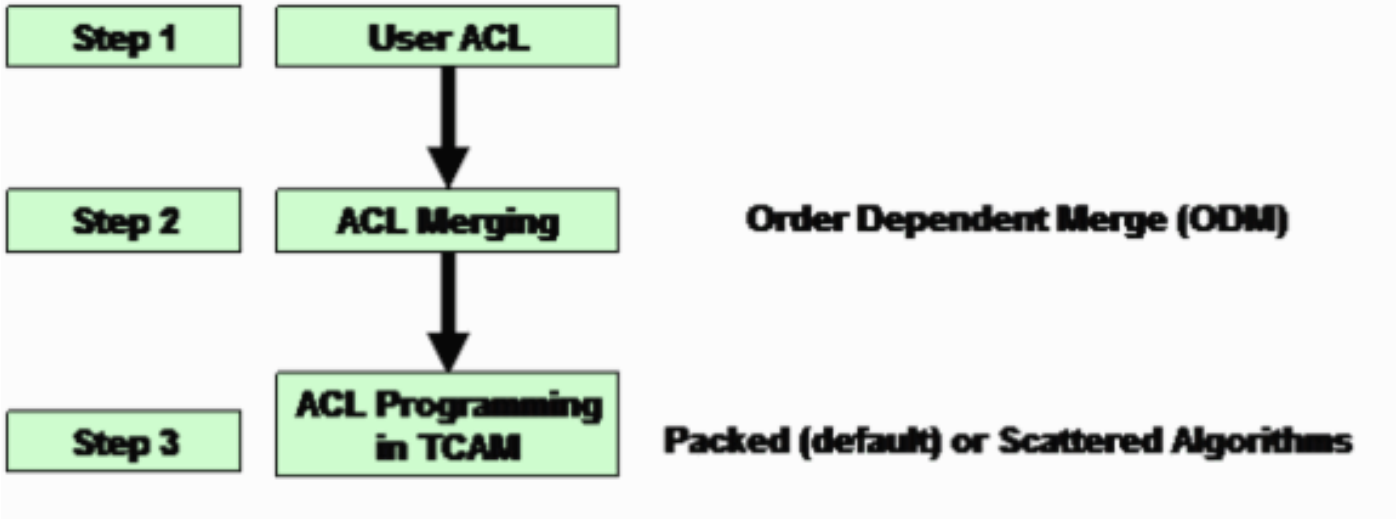
表2 — 各种管理引擎和交换机上的Catalyst 4500 ACL资源

产品	TCAM版本	功能TCAM（每个方向）	QoS TCAM（每个方向）
管理引擎II+	2	8000个条目、1000个掩码	8000个条目、1000个掩码
管理引擎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
管理引擎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使用单独的专用TCAM进行IP单播和组播路由。Catalyst 4500最多可以有128,000个单播和组播路由共享的路由条目。但是，这些详细信息不在本文档的范围内。本文档仅讨论安全和QoS TCAM耗尽问题。

图1显示了在Catalyst 4500的硬件表中编程ACL的步骤。

图1 — 在Catalyst 4500交换机上编程ACL的步骤



第 1 步

此步骤涉及以下操作之一：

- ACL或QoS策略在接口或VLAN上的配置和应用ACL的创建可以动态进行。IP源防护(IPSG)功能的示例。通过此功能，交换机自动为与端口关联的IP地址创建PACL。
- 修改已存在的ACL

注意：仅ACL的配置不会导致TCAM编程。ACL（QoS策略）必须应用于接口，才能在TCAM中对ACL进行编程。

步骤 2

ACL必须合并，才能在硬件表(TCAM)中进行编程。 合并以组合方式在硬件中编程多个ACL（PACL、VACL或RACL）。这样，只需进行一次硬件查找即可检查数据包逻辑转发路径中的所有适用ACL。

例如，在图2中，从PC-A路由到PC-C的数据包可能具有以下ACL:

- PC-A端口上的输入PACL
- VLAN 1上的VACL
- VLAN 1接口上输入方向的RACL

这三个ACL将合并，以便在输入TCAM中进行一次查找就足以做出允许或拒绝的转发决策。同样，只需执行一次输出查找，因为TCAM是使用以下三个ACL的合并结果进行编程的：

- VLAN 2接口上的输出RACL
- VLAN 2 VACL
- PC-C端口上的输出PACL

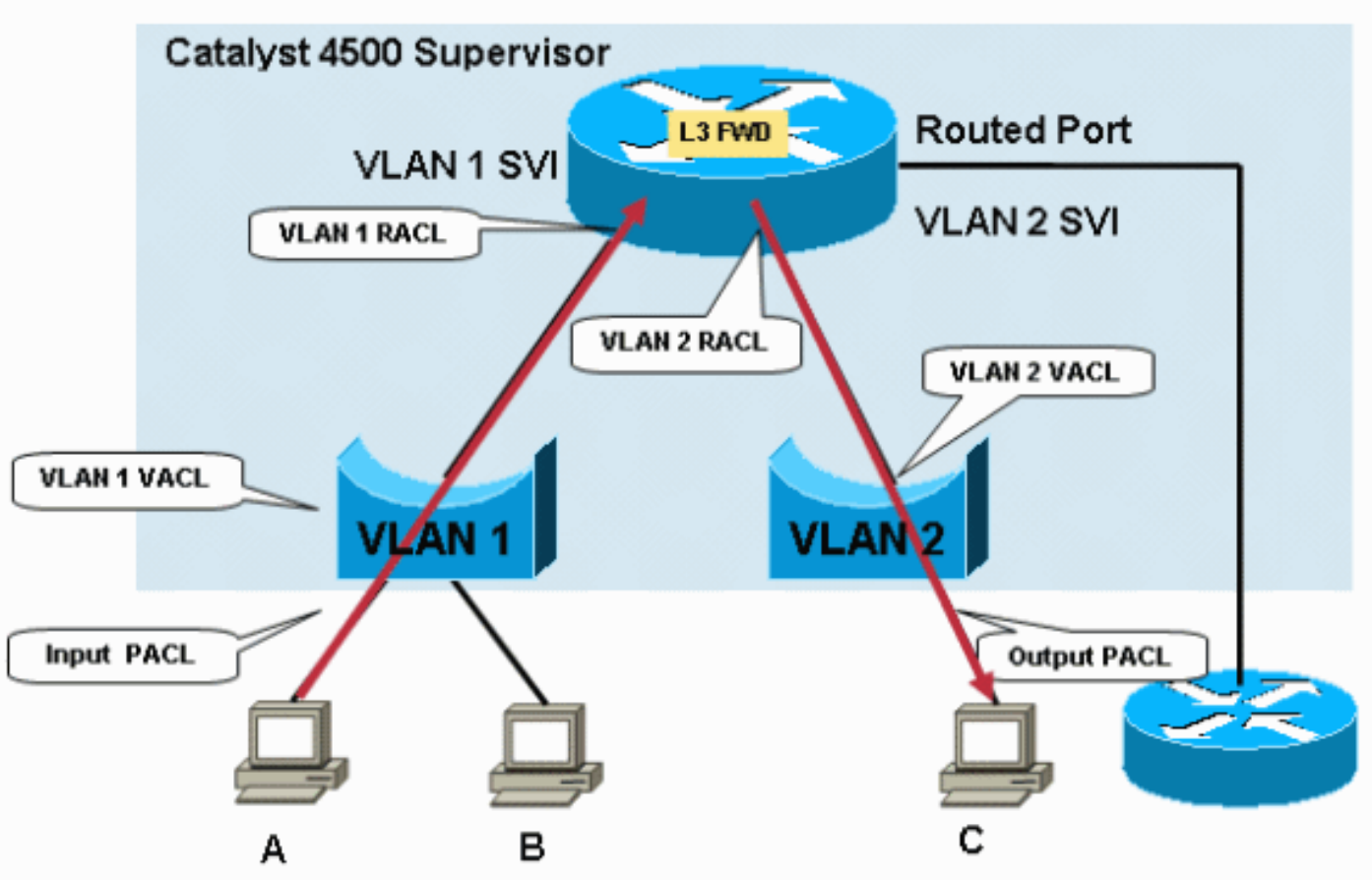
使用单次输入查找和一次输出查找，当任何或所有ACL都在数据包转发路径中时，不会对数据包进行惩罚性硬件转发。

注：输入和输出TCAM查找在硬件中同时进行。一个常见的误解是输出TCAM查找在输入TCAM查找之后发生，如逻辑数据包流所示。此信息非常重要，因为Catalyst 4500输出策略无法匹配输入策略修改的QoS参数。在安全ACL中，最严重的操作发生。在以下任一情况下，数据包都会被丢弃：

- 如果输入查找结果为drop，而输出查找结果为permit
- 如果输入查找结果为permit，而输出查找结果为drop

注意：如果输入和输出查找结果都允许，则允许数据包。

图2 — 在Catalyst 4500交换机上通过安全ACL过滤



Catalyst 4500上的ACL合并取决于顺序。该过程也称为顺序相关合并(ODM)。 使用ODM时，ACL条目按照它们在ACL中显示的顺序进行编程。例如，如果ACL包含两个访问控制条目(ACE)，则交换机首先编程ACE 1，然后编程ACE 2。但是，顺序依赖仅在特定ACL中ACE之间。例如，ACL 120中的ACE可以先于TCAM中ACL 100中的ACE启动。

步骤 3

合并的ACL在TCAM中编程。ACL或QoS的输入或输出TCAM进一步分为两个区域：PortAndVlan和PortOrVlan。如果配置在同一数据包路径中同时包含这两个ACL，则合并的ACL会*在TCAM*的PortAndVlan区域中编程：

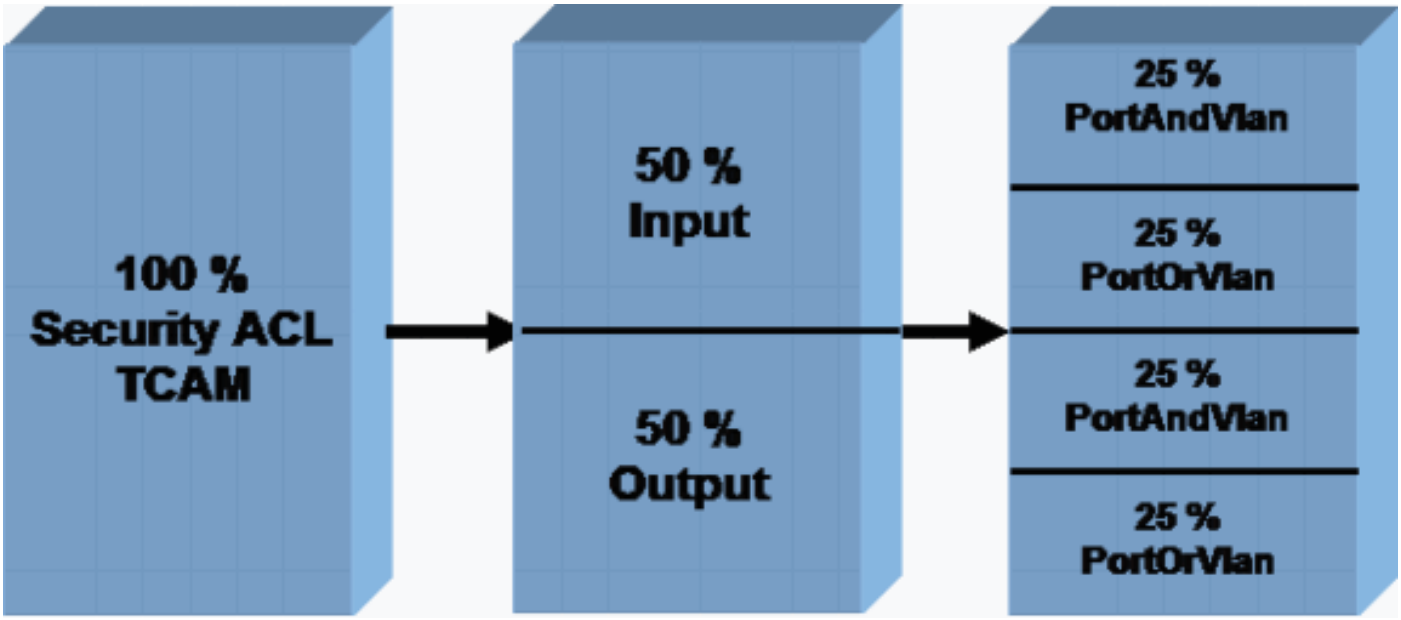
- PACL**注意**：PACL是正常过滤ACL或IPSG创建的动态ACL。
- VACL或RACL

如果数据包的特定路径只有PACL、VACL或RACL，则ACL会在TCAM的PortOrVlan区域中编程。图3显示了各种类型ACL的安全ACL TCAM划分。QoS具有类似的雕刻、独立的专用TCAM。

目前，您无法修改TCAM默认分配。但是，我们计划提供更改TCAM分配的功能，该TCAM分配在未来软件版本中可用于PortAndVlan和PortOrVlan区域。此更改将允许您增加或减少输入或输出TCAM中PortAndVlan和PortOrVlan的空间。

注意：PortAndVlan区域的分配增加将导致输入或输出TCAM中PortOrVlan区域的分配减少。

图3 - Catalyst 4500交换机上的安全ACL TCAM结构



show platform hardware ACL statistics utilization brief**命令显示ACL和QoS TCAM的每个区**域的此TCAM利用率。命令输出显示可用的掩码和条目，并按区域划分，如图3所示。此示例输出来自Catalyst 4500 Supervisor引擎II+:

注：有关蒙版和条目的详细信息，请参阅本文档的TCAM类型部分。

```
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的类型

如表2所示，Catalyst 4500使用两种类型的TCAM。本节介绍两个TCAM版本之间的区别，以便您为网络和配置选择适当的产品。

TCAM 2使用八个条目共享一个掩码的结构。例如，ACE中有八个IP地址。条目必须具有与它们共享的掩码相同的掩码。如果ACE具有不同的掩码，则条目必须根据需要使用单独的掩码。使用单独的掩码可能导致掩码耗尽。TCAM中的掩码耗尽是TCAM耗尽的常见原因之一。

TCAM 3没有任何此类限制。每个条目在TCAM中都可以有其自己的唯一掩码。无论这些条目的掩码如何，都可以充分利用硬件中可用的所有条目。

为了演示此硬件架构，本节中的示例展示了TCAM 2和TCAM 3程序ACL在硬件中的方式。

```
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有两个条目，它们有两个不同的掩码。ACE 1是主机条目，因此它具有/32掩码。ACE 2是掩码为/24的子网条目。由于第二个条目具有不同的掩码，因此不能使用掩码1中的空条目，在

TCAM 2的情况下使用单独的掩码。

下表显示了如何在TCAM 2中编程此ACL:

掩码	条目
掩码1匹配：源IP地址的32位全部为“不关心”：所有剩余位	源IP = 8.1.1.1
	空条目 2
	空条目 3
	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“不关心”的24位最重要：所有剩余位	源IP = 8.1.1.0
	空条目 2
	空条目 3
	空条目 4
	空条目 5
	空条目 6
	空条目 7
	空条目 8

即使掩码1中有可用的空闲条目，TCAM 2结构也会阻止掩码1的空条目2中填充ACE 2。由于ACE 2的掩码与ACE 1的/32掩码不匹配，因此不允许使用此掩码。TCAM 2必须使用单独的掩码/24掩码对ACE 2进行编程。

如表2所示，使用单独的掩码可加快可用资源的耗尽速度。其他ACL仍然可以使用掩码1中的其余条目。但是，在大多数情况下，TCAM 2的效率很高，但不是100%。效率因配置方案而异。

下表显示了TCAM 3中编程的相同ACL。TCAM 3为每个条目分配掩码：

掩码	条目

IP地址1的掩码32位	源IP = 8.1.1.1
IP地址2的掩码24位	源IP = 8.1.1.0
空掩码3	空条目3
空掩码4	空条目4
空掩码5	空条目5
空掩码6	空条目6
空掩码7	空条目7
空掩码8	空条目8
空掩码9	空条目9
空掩码10	空条目10
空掩码11	空条目11
空掩码12	空条目12
空掩码13	空条目13
空掩码14	空条目14
空掩码15	空条目15
空掩码16	空条目16

在本例中，其余14个条目可以具有不同掩码的条目，且无限制。因此，TCAM 3比TCAM 2效率更高。为了说明TCAM版本之间的差异，本示例过于简化。Catalyst 4500软件有许多优化，以提高TCAM 2中编程效率，以实现实际配置方案。本文的TCAM 2次优TCAM编程算法讨论了这些优化。

对于Catalyst 4500上的TCAM 2和TCAM 3，如果在不同接口上应用相同的ACL，则TCAM条目将共享。此优化可节省TCAM空间。

排除TCAM耗尽故障

当Catalyst 4500交换机在编程安全ACL时发生TCAM耗尽时，ACL的部分应用会通过软件路径进行。与ACE匹配且未应用于TCAM的数据包在软件中处理。软件中的此处理会导致CPU使用率较高。由于Catalyst 4500 ACL编程与顺序相关，因此ACL始终从上到下进行编程。如果特定ACL不完全适合TCAM，则ACL底部的ACE很可能未在TCAM中编程。

当TCAM溢出时，会显示警告消息。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.
```

如果已启用系统日志，则还可以在**show logging**命令输出中看到此错误消息。此消息的出现最终表明将进行一些软件处理。因此，CPU利用率可能很高。如果在应用新ACL期间TCAM容量耗尽，则已在TCAM中编程的ACL仍在TCAM中编程。与已编程的ACL匹配的数据包将继续在硬件中处理和转发。

注意：如果对大型ACL进行更改，则可能会显示TCAM-exceeded消息。交换机尝试在TCAM中重新编程ACL。在大多数情况下，可在硬件中完全重新编程新的修改ACL。如果交换机能成功将ACL完全重新编程到TCAM中，将显示以下消息：

```
*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**令以验证ACL是否已在硬件中完全编程。

此输出显示了ACL 101到VLAN 1的配置，并验证ACL已在硬件中完全编程：

注意：如果ACL未完全编程，则可能显示TCAM耗尽错误消息。

```
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字段(L3DenyToCpu)表示，如果数据包因ACL而被拒绝，则数据包会被传送到CPU。然后，交换机会发出Internet控制消息协议(ICMP)不可达消息。此行为是默认行为。当数据包被传送到CPU时，交换机上可能会出现高CPU利用率。但是，在Cisco IOS软件版本12.1(13)EW及更高版本中，这些数据包的速率限制在CPU。在大多数情况下，思科建议您关闭发送ICMP不可达消息的功能。

此输出显示交换机配置为不发送ICMP不可达消息，以及更改后TCAM编程的验证。ACL 101的状态现在为FullyLoaded，如命令输出所示。拒绝的流量不会进入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：如果在应用某些QoS策略期间超出QoS TCAM，则该特定策略不会应用到接口或VLAN。Catalyst 4500不在软件路径中实施QoS策略。因此，当QoS TCAM超出时，CPU利用率不会激增。

```
*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.
```

发出 **show platform cpu packet statistics 命令。**确定ACL软列是否收到大量数据包。大量数据包表示安全TCAM耗尽。此TCAM耗尽会导致数据包发送到CPU以进行软件转发。

```
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ACL理队列未收到过多流量，请参阅Cisco IOS基于软件的Catalyst 4500交换机上的CPU使用率高以了解其他可能原因。本文档提供了有关如何排除其他高CPU使用率情况的故障的信息。

Catalyst 4500 TCAM可能因以下原因溢出：

- TCAM 2次优TCAM规划算法
- ACL中过度使用第4层操作(L4Ops)
- 管理引擎或交换机类型的ACL过多

TCAM 2次优TCAM规划算法

正如“TCAM的类型”一节所讨论的，TCAM 2效率较低，因为八个条目共享一个掩码。Catalyst 4500软件支持两种TCAM 2的TCAM编程算法，可提高TCAM 2的效率：

- 打包 — 适用于大多数安全ACL场景**注意：**这是默认值。
- 散乱 — 用于IPSG场景

可以将算法更改为分散的算法，但是，如果仅配置了安全ACL（如RACL），这通常不会有帮助。散乱的算法仅在许多端口上重复相同或相似的小型ACL的情况下才有效。这种情况是在多个接口上启用的IPSG。在IPSG场景中，每个动态ACL:

- 条目数很少这包括允许允许的IP地址和在末尾的拒绝，以防止未经授权的IP地址访问端口。
- 对所有已配置的接入端口重复在Catalyst 4507R上，ACL最多可重复240个端口。

注意：TCAM 3使用默认的打包算法。由于TCAM结构是每个条目一个掩码，因此打包算法是最佳的算法。因此，这些交换机上未启用分散算法选项。

此示例位于为IPSG功能配置的Supervisor引擎II+上。输出显示，尽管仅使用49%的条目，但89%的掩码被使用：

```
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，编程算法从默认的打包算法到散乱算法的更改会有所帮助。散乱算法将总掩码使用率从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
```

有关Catalyst 4500交换机上安全功能最佳实践的信息，请参阅Catalyst 4500安全功能管理引擎最佳实践。

在ACL中过度使用L4Op

术语L4Ops是指在ACL配置中使用**gt**、**lt**、**neq**和**range**关键字。Catalyst 4500对可在单个ACL中使用的这些关键字的数量有限制。限制因管理引擎和交换机而异，即每个ACL有6个或8个L4Op。表3显示了每个Supervisor引擎和每个ACL的限制。

表3 — 不同Catalyst 4500管理引擎和交换机上每个ACL的L4Op限制

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

如果超过每个ACL的L4Op限制，则控制台上会显示警告消息。消息类似于以下内容：

```
%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，如果超过L4Op限制，则在TCAM中扩展特定ACE。其他TCAM使用结果。此ACE用作示例：

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

在ACL中使用此ACE时，交换机仅使用一个条目和一个L4Op。但是，如果此ACL中已使用6个L4Op，则此ACE在硬件中扩展为10个条目。这种扩展可能会占用TCAM中的许多条目。谨慎使用这些L4Ops可防止TCAM溢出。

注意：如果本例涉及Supervisor引擎V-10GE和WS-C4948-10GE，则ACL中以前使用的八个L4Ops会导致ACE扩展。

在Catalyst 4500交换机上使用L4Op时，请记住以下事项：

- 如果运算符或操作数不同，则L4运算被视为不同。例如，此ACL包含三种不同的L4操作，因**为gt 10**和**gt 11**被视为两种不同的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
  ```
- 如果同一运算符/操作数对对源端口应用一次，对目标端口应用一次，则L4运算被视为不同。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交换机在可能时共享L4Ops。在本例中，粗体斜体中的***行演示***了此场景：ACL 101的L4Op使用率= 5ACL 102的L4Op使用率= 4 **注意： eq**关键字不消耗任何L4Op硬件资源。L4Op总使用量= **8注意：**ACL 101和102共享一个L4Op。**注意：**即使TCP或用户数据报协议(UDP)等协议不匹配或允许/拒绝操作不匹配，L4Op也是共享的。

管理引擎或交换机类型的ACL过多

如表2所示，TCAM是有限的资源。如果配置了大量IPSG条目的过多ACL或功能（如IPSG），则可以超出任何Supervisor引擎的TCAM资源。

如果超出Supervisor引擎的TCAM空间，请执行以下步骤：

- 如果您有Supervisor引擎II+，并且运行的Cisco IOS软件版本早于Cisco IOS软件版本12.2(18)EW，请升级到最新的Cisco IOS软件版本12.2(25)EWA维护版本。TCAM容量在后续版本中已增加。
- 如果您使用DHCP监听和IPSG，并且开始耗尽TCAM，请使用最新的Cisco IOS软件版本12.2(25)EWA维护版本，并在TCAM 2产品中使用分散算法。**注意：**Cisco IOS软件版本12.2(20)EW及更高版本中提供了散乱算法。最新版本还增强了DCHP监听和动态地址解析协议(ARP)检测(DAI)功能，可提高TCAM利用率。
- 如果由于超出L4Op限制而开始耗尽TCAM，请尝试减少ACL中的L4Op使用，以防止TCAM溢出。
- 如果在同一VLAN中的不同端口上使用许多类似的ACL或策略，请将它们聚合到VLAN接口上的单个ACL或策略中。此聚合可节省一些TCAM空间。例如，应用基于语音的策略时，默认基于端口的QoS用于分类。此默认QoS可能导致超出TCAM容量。如果将QoS切换为基于VLAN，则可减少TCAM的使用。

- 如果TCAM空间仍有问题，请考虑高端Supervisor引擎，如Supervisor引擎V-10GE或Catalyst 4948-10GE。这些产品使用最高效的TCAM 3硬件。

摘要

Catalyst 4500使用TCAM对已配置的ACL进行编程。TCAM允许在硬件转发路径中应用ACL，而不会影响交换机的性能。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已经实施了大量优化，并提供了改变TCAM编程算法的命令，以实现最大效率。TCAM 3产品（如管理引擎V-10GE和Catalyst 4948-10GE）为安全ACL和QoS策略提供最多的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