

# 了解Catalyst 9000交换机上的QoS硬件资源

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[术语](#)

[查看与QoS相关的系统日志](#)

[验证硬件利用率和策略状态](#)

[了解QoS硬件资源的当前利用率](#)

[使用示例\(9200L 17.3.4\)](#)

[排除硬件使用故障](#)

[场景：QoS TCAM规模估计](#)

[场景：QoS TCAM规模增加（未超过）](#)

[场景：超出QoS TCAM规模](#)

[补救技术](#)

[为TAC收集的命令](#)

[相关信息](#)

[思科漏洞ID](#)

## 简介

本文档介绍如何了解并验证基于UADP ASIC的Catalyst 9000系列交换机上的服务质量(QoS)硬件利用率

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- Cisco MQC QoS配置；策略映射、类映射、访问控制列表、访问控制条目

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Catalyst 9200L Cisco IOS®-XE 17.3.4

其他Cisco Catalyst 9000系列交换机上可以了解一般概念、想法和各种输出。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 相关产品

本文档也可用于以下硬件和软件版本：

- Catalyst 9300 - 9600系列交换机
- Catalyst 9300X和9400X
- Cisco IOS® XE 16.x和17.x软件版本

## 背景信息

- Catalyst 9000系列交换机的各种功能消耗有限的硬件资源。这些资源的存在是为了提高这些功能的性能，并提供交换机预期的预期高转发速率。
- 这些资源的规模可能因交换机型号而异，但在使用UADP ASIC的Catalyst 9000系列交换机中，故障排除的基本方法保持不变
- 通常，带有交换机的主要有限硬件资源称为TCAM — 三重内容可寻址存储器
- 在Catalyst 9000系列交换机中，在TCAM之外使用多种内存类型，以满足给定功能的特定需求

本文档可帮助您：

- 了解服务质量(QoS)如何消耗硬件条目
- 了解指示QoS硬件资源问题的日志或错误消息
- 确定要采取哪些操作来修复与QoS相关的硬件资源问题

## 术语

服务质量	服务质量	与网络设备进出流量的分类、标记、排队和调度相关的概念/组
TCAM	三重内容可寻址存储器	一种内存，用于存储和查询具有三个不同输入（0、1和X）的。这种内存类型用于存在多个匹配项的情况，并且每个匹配项的结果散列不会是唯一的。此表包含一个掩码或X值，通过该值，以知道它是否与此条目匹配。
DSCP	差分服务代码点	数据包的IP报头中包含的流量分类机制
CoS	服务类别	数据包的以太网帧报头中包含的流量分类机制
ACE	访问控制项	访问控制列表(ACL)中的单个规则或线路
ACL	访问控制列表	各种功能使用的一组访问控制条目(ACE)来匹配流量并采取措
美联储	转发引擎驱动程序	对设备硬件进行编程的软件组件

## 查看与QoS相关的系统日志

如果与QoS相关的资源耗尽，系统将生成SYSLOG消息：

QoS相关系统日志消息	定义	恢复操作
%FED_QOS_ERRMSG-4-TCAM_OVERFLOW : 交换机1 R0/0: fed : 无法在GigabitEthernet1/0/10上为策略映射ingress_pmap2编程TCAM。	为QoS实体保留的硬件(TCAM)空间已用尽	确保您具有有效/支持的配置。查看本文档的其余部分，验证交换机的当前规模利用率，以及过度使用可能采取的减少措施。
%FED_QOS_ERRMSG-3-QUEUE_SCHEDULER_HW_ERROR : 交换机1 R0/0: fed : 无法为GigabitEthernet1/0/27配置队列调度程序	QoS队列调度程序的硬件安装失败	验证您的配置是否受支持，查看平台和软件版本的QoS配置指南。仅适用于9200L：查看Cisco Bug ID <a href="#">CSCvz54607</a> 和Cisco Bug ID <a href="#">CSCvz76172</a>
FED_QOS_ERRMSG-3-QUEUE_BUFFER_HW_ERROR: R0/0: fed : 无法配置默认队列缓冲区	QoS队列缓冲区的硬件安装失败	验证您的配置是否受支持，查看平台和软件版本的QoS配置指南。 查看思科漏洞ID <a href="#">CSCvs49401</a>

## 验证硬件利用率和策略状态

### 验证当前QoS TCAM利用率

```
show platform hardware fed switch active fwd-asic resource tcam utilization
```

注：有关此命令的详细信息，请参阅

#### 16.X versions:

```
CAM Utilization for ASIC [0]
```

Table	Max Values	Used Values
Unicast MAC addresses	16384/256	15/21
L3 Multicast entries	1024/256	0/7
L2 Multicast entries	1024	9
Directly or indirectly connected routes	8192/3072	2/19
<b>QoS Access Control Entries</b>	<b>1024</b>	<b>40 &lt;&lt;&lt; QoS Entries</b>
Security Access Control Entries	1408	125
Ingress Netflow ACEs	128	8
Policy Based Routing ACEs	512	9
Egress Netflow ACEs	128	8
Flow SPAN ACEs	256	13
Control Plane Entries	512	211
Tunnels	128	17
Lisp Instance Mapping Entries	128	3
SGT_DGT	2048/256	0/1
CLIENT_LE	2048/64	0/0

```

INPUT_GROUP_LE          1024          0
OUTPUT_GROUP_LE        1024          0
Macsec SPD              128           2

```

**17.x Versions:**

Codes: EM - Exact\_Match, I - Input, O - Output, IO - Input & Output, NA - Not Applicable CAM

Utilization for ASIC [0] Table Subtype Dir Max Used %Used V4 V6 MPLS Other -----

```

----- Mac Address
Table EM I 16384 17 0.10% 0 0 0 17 Mac Address Table TCAM I 256 21 8.20% 0 0 0 21 L3 Multicast
EM I 1024 0 0.00% 0 0 0 0 L3 Multicast TCAM I 256 9 3.52% 3 6 0 0 L2 Multicast TCAM I 1024 11
1.07% 3 8 0 0 IP Route Table EM I 4096 3 0.07% 2 0 1 0 IP Route Table TCAM I 2048 19 0.93% 6 10
2 1  QOS ACL          TCAM          IO          1024          85          8.30%          28          38
0 19 <-- QoS Entries
Security ACL          TCAM          IO          1408          129          9.16%          26          58          0
45
Netflow ACL          TCAM          I           128           6           4.69%          2           2           0
2
PBR ACL              TCAM          I           512           9           1.76%          3           6           0
0
Netflow ACL          TCAM          O           128           6           4.69%          2           2           0
2
Flow SPAN ACL        TCAM          IO          256           13          5.08%          3           6           0
4
Control Plane        TCAM          I           512           262          51.17%          114          106          0
42
Tunnel Termination   TCAM          I           128           18           14.06%          8           10           0
0
Lisp Inst Mapping    TCAM          I           128           1           0.78%          0           0           0
1
CTS Cell Matrix/VPN  Label          EM          O           2048          0           0.00%          0           0           0
0
CTS Cell Matrix/VPN  Label          TCAM          O           256           1           0.39%          0           0           0
1
Client Table         EM          I           2048          0           0.00%          0           0           0
0
Client Table         TCAM          I           64            0           0.00%          0           0           0
0
Input Group LE       TCAM          I           1024          0           0.00%          0           0           0
0
Output Group LE      TCAM          O           1024          0           0.00%          0           0           0
0
Macsec SPD           TCAM          I           128           2           1.56%          0           0           0
2

```

验证QoS策略是否已成功安装在硬件中。确保状态为VALID和SET\_INHW。查看列表底部的物理接口条目。在交换机堆叠或堆叠式虚拟中，使用交换机编号或主用/备用交换机准确反映您想要验证硬件安装的交换机。

```

C9200(config)#policy-map egress_pmap
C9200(config-pmap)#interface gi2/0/9
C9200(config-if)#service-policy output egress_pmap

```

```

C9200#show platform software fed switch 2 qos policy target status <-- switch 2 is used
because the interface in question is Gi2/0/9 which is on switch 2

```

TCG status summary:

```

Loc Interface          IIF-ID          Dir State:(cfg,opr) Policy
-----

```

```

<snip> L:0 GigabitEthernet2/0/9 0x00000000000010 OUT VALID,SET_INHW egress_pmap <-- VALID /

```

SET\_INHW indicates the policy is understood by software and installed to hardware successfully  
如果发现无效策略或错误，而不是目标接口的VALID / SET\_INHW，请检查QoS策略并验证长度和语法。还要验证硬件利用率。本文档后面的部分详细介绍如何了解策略可以使用的资源。

```
C9200#show run policy-map egress_pmap
```

```
Current configuration : 624 bytes
```

```
!  
policy-map egress_pmap  
  class COS_DSCP6  
    priority level 1  
    queue-buffers ratio 5  
  class COS_DSCP5  
    bandwidth remaining percent 10  
    queue-buffers ratio 5  
<snip...>
```

```
C9200#show run class-map COS_DSCP6
```

```
Current configuration : 66 bytes
```

```
!  
class-map match-any COS_DSCP6  
match ip dscp ef  
!  
end
```

## 了解QoS硬件资源的当前利用率

### 使用示例(9200L 17.3.4)

```
C9200#show platform hardware fed switch active fwd-asic resource tcam utilization | i
```

```
Codes|ASIC|-|QOS
```

```
Codes: EM - Exact_Match, I - Input, O - Output, IO - Input & Output, NA - Not Applicable CAM
```

```
Utilization for ASIC [0] Table Subtype Dir Max Used %Used V4 V6 MPLS Other
```

```
-----  
-----  
QOS ACL TCAM IO 1024 85 8.30% 28 38 0
```

```
19 <-- Baseline utilization with minimal configuration
```

配置并附加空白策略映射 — 在此策略映射中未调用类映射，因此此策略没有预期效果。

```
C9200(config)#policy-map egress_pmap
```

```
C9200(config-pmap)#interface gi1/0/9
```

```
C9200(config-if)#service-policy output egress_pmap
```

```
C9200#show platform hardware fed switch active fwd-asic resource tcam utilization | i
```

```
Codes|ASIC|-|QOS
```

```
Codes: EM - Exact_Match, I - Input, O - Output, IO - Input & Output, NA - Not Applicable CAM
```

```
Utilization for ASIC [0] Table Subtype Dir Max Used %Used V4 V6 MPLS
```

```
Other
```

```
-----  
-----  
QOS ACL TCAM IO 1024 89 8.69% 29 40 0
```

```
20 <-- 4 additional entries consumed
```

请注意，即使连接了零类映射或已执行操作，仍会使用4个硬件条目，这些条目在V4、V6和其他版本之间拆分。

在本例中，添加了一个空白测试类。在正常情况下，此match-any类映射将允许匹配多种类型的DSCP、CoS或IPP标签。但在本例中，未调用任何值，因此类映射不匹配任何流量。

```
C9200(config)#class-map match-any TEST_CLASS
C9200(config-cmap)#policy-map egress_pmap
C9200(config-pmap)#class TEST_CLASS
```

```
C9200#show platform hardware fed switch active fwd-asic resource tcam utilization | i
Codes|ASIC|-|QOS
```

```
Codes: EM - Exact_Match, I - Input, O - Output, IO - Input & Output, NA - Not Applicable CAM
Utilization for ASIC [0] Table Subtype Dir Max Used %Used V4 V6 MPLS Other
```

```
-----
QOS ACL TCAM IO 1024 92 8.92% 30 42 0
20 <-- 3 additional entries consumed
```

示例显示，对于调用的每个附加类，即使不匹配任何特定流量，也会消耗一个v4条目和两个v6条目的基线。

向每个类添加match语句时，将使用其他条目：

```
C9200(config)#class-map match-any TEST_CLASS
C9200(config-cmap)#match precedence 0
```

```
C9200(config-cmap)#do show platform hardware fed switch ac fwd resource tcam utilization | i QOS
QOS ACL TCAM IO 1024 96 9.38% 31 44 0
21 <-- 4 additional entries
```

```
C9200(config-cmap)#match precedence 1
```

```
C9200(config-cmap)#do show platform hardware fed switch ac fwd resource tcam utilization | i QOS
QOS ACL TCAM IO 1024 99 9.67% 32 46 0
21 <-- 3 additional entries
```

```
C9200(config-cmap)#match cos 1
```

```
C9200(config-cmap)#do show platform hardware fed switch ac fwd resource tcam utilization | i QOS
QOS ACL TCAM IO 1024 100 9.77% 32 46 0
22 <-- 1 additional entry
```

```
C9200(config-cmap)#match dscp 21
```

```
C9200(config-cmap)#do show platform hardware fed switch ac fwd resource tcam utilization | i QOS
QOS ACL TCAM IO 1024 103 10.06% 33 48 0
22 <-- 3 additional entries
```

```
C9200(config-cmap)#match dscp 22
```

```
C9200(config-cmap)#do show platform hardware fed switch ac fwd resource tcam utilization | i QOS
QOS ACL TCAM IO 1024 103 10.06% 33 48 0
22 <-- 0 additional entries
```

```
C9200(config-cmap)#match dscp 23
```

```
C9200(config-cmap)#do show platform hardware fed switch ac fwd resource tcam utilization | i QOS
QOS ACL TCAM IO 1024 106 10.35% 34 50 0
22 <-- 3 additional entries
```

```
C9200(config-cmap)#match dscp 31
```

```
C9200(config-cmap)#do show platform hardware fed switch ac fwd resource tcam utilization | i QOS
QOS ACL TCAM IO 1024 109 10.64% 35 52 0
22 <-- 3 additional entries
```

```
C9200(config-cmap)#match dscp 32
```

```
C9200(config-cmap)#do show platform hardware fed switch ac fwd resource tcam utilization | i QoS
QoS ACL          TCAM          IO          1024          109          10.64%          35          52          0
22 <-- 3 additional entries
```

```
C9200(config-cmap)#match dscp 33
```

```
C9200(config-cmap)#do show platform hardware fed switch ac fwd resource tcam utilization | i QoS
QoS ACL          TCAM          IO          1024          112          10.94%          36          54          0
22 <-- 3 additional entries
```

请注意，在某些情况下，单个match语句不会消耗更多条目。进一步观察到，后续的match语句会占用多个条目。

在实施网络范围内的策略之前，请定期测试策略，并在继续操作时进行优化。

**注意：**对于QoS相关的硬件利用率，硬件使用情况并不总是使用match语句或访问控制条目(ACE)进行一对一扩展。硬件根据值掩码结果或VMR运行。在某些情况下，可能需要多个VMR才能对实现ACE所必需的数据范围进行完全分类。Catalyst 9000系列交换机UADP系列ASIC包含用于优化这些平台的硬件，例如用于具有端口范围操作(L4OP)的ACE，以减少扩展需求。

## 排除硬件使用故障

本部分介绍多种结合硬件和软件使用的场景，以帮助说明问题场景和补救。

- 平台 — C9200L-48T-4X
- 思科IOS®-XE 17.3.4

所展示的场景说明：

- 添加相对少量条目以实现整体利用率的小型策略
- 一种大型策略，它会在整体利用率中添加相对大量的条目
- 导致无法安装该策略的第二个大型策略
- 修复安装失败

### 场景：QoS TCAM规模估计

**注意：**这些示例使用基于对象组的ACL。对象组有效地代表更大的传统访问列表。它们本身不会消耗更多或更少的TCAM。相反，它们是一种简化的模块化方式，用于表示本来将是很长的模式化ACE列表。

此示例使用入口策略来标记数据包。它涉及基于对象组、IP访问列表和TCP/UDP端口的匹配。

对象组	使用对象组的访问列表	类映射	策略映射
对象组网络RFC1918-Private-IPv4 10.0.0.0 255.0.0.0 172.16.0.0 255.240.0.0	ip access-list extended APP_1_PORTS_1 10 permit udp any object-group app_1 range 1433 1434	class-map match-any BigClass match access-group name APP_1_PORTS_1	policy-map ingress_pma 类BigClass set dscp cs

```

192.168.0.0 255.255.0.0 20 permit udp object-group app_1
range 1433 1434 any
object-group network app_1 30 permit tcp any object-group
app_1 range 1433 1434
group-object RFC1918-Private-IPv4 40 permit tcp object-group app_1
range 1433 1434 any
50 permit tcp any object-group
app_1 range 14300 14400
60 permit tcp object-group app_1
range 14300 14400 any

```

查看图表，注意对象组网络RFC1918-Private-IPv4中有3个子网

```

object-group network app_1
group-object RFC1918-Private-IPv4

object-group network RFC1918-Private-IPv4
10.0.0.0 255.0.0.0
172.16.0.0 255.240.0.0
192.168.0.0 255.255.0.0

```

此外，ip access-list extended APP\_1\_PORTS\_1中还有6条匹配语句。

```

ip access-list extended APP_1_PORTS_1
10 permit udp any object-group app_1 range 1433 1434 <-- permits any source, to group app_1 on
UDP ports 1433 - 1434
20 permit udp object-group app_1 range 1433 1434 any <-- reverse of previous line, reminder
that app_1 is made up of RFC1918-Private-IPv4, which is 3 separate subnets
30 permit tcp any object-group app_1 range 1433 1434
40 permit tcp object-group app_1 range 1433 1434 any
50 permit tcp any object-group app_1 range 14300 14400
60 permit tcp object-group app_1 range 14300 14400 any

```

object-group network app\_1将object-group network RFC1918-Private-IPv4 中的每个条目应用于ip access-list extended APP\_1\_PORTS\_1中的每个条目

这会产生乘法效应，因为对于APP\_1\_PORTS\_1中的每个ACE，它引用对象组app\_1，而该对象组本身代表来自RFC1918-Private-IPv4的3个附加ACE

连接到类映射和策略映射时，ip access-list extended APP\_1\_PORTS\_1的总利用率估计值为：

APP\_1使用6倍x 3对象组ACE = 18

应用策略并观察TCAM利用率：

```

C9200#show platform hardware fed switch 2 fwd-asic resource tcam utilization | i Codes|ASIC|-
|QoS
Codes: EM - Exact_Match, I - Input, O - Output, IO - Input & Output, NA - Not Applicable CAM
Utilization for ASIC [0] Table Subtype Dir Max Used %Used V4 V6 MPLS Other
-----
-----
QOS ACL TCAM IO 1024 85 8.69% 29 40 0
20 <-- baseline utilization

```

```

C9200 (config-pmap) #interface gi1/0/9
C9200 (config-if) #service-policy input ingress_pmap

```



```
C9200#show platform hardware fed switch active fwd-asic resource tcam utilization | i
Codes|ASIC|-|QOS
Codes: EM - Exact_Match, I - Input, O - Output, IO - Input & Output, NA - Not Applicable CAM
Utilization for ASIC [0] Table Subtype Dir Max Used %Used V4 V6 MPLS Other
-----
-----
QOS ACL TCAM IO 1024 107 10.45% 47 40 0
20 <-- 22 entries consumed
```

**摘要**

- ACL定义对象组，由于对象组的乘法效应，对象组会扩展为占用18个额外的条目
- 默认情况下，策略映射使用4个条目
- 这会添加到使用22个条目

**场景：QoS TCAM规模增加 (未超过)**

此示例是上一个策略较大的延续。这样可以确定如何快速消耗大量TCAM。

策略1:

对象组	使用对象组的访问列表	类映射	策略映射
object-group network <b>experimental_1</b> 240.1.192.0 255.255.192.0 240.2.96.0 255.255.224.0 240.3.160.0 255.255.240.0 240.4.32.0 255.255.224.0 240.5.160.0 255.255.224.0 240.6.192.0 255.255.224.0 240.7.128.0 255.255.128.0 240.8.0.0 255.255.0.0 240.9.128.0 255.255.192.0 240.10.224.0 255.255.224.0 240.11.0.0 255.255.240.0 240.12.160.0 255.255.224.0 240.13.192.0 255.255.224.0 240.14.192.0 255.255.240.0 240.15.128.0 255.255.224.0 object-group network	ip access-list extended <b>APP_1_PORTS_1</b> 10 permit udp any object-group <b>app_1</b> range 1433 1434 20 permit udp object-group <b>app_1</b> range 1433 1434 any <4行> ip access-list extended <b>APP_1_PORTS_2</b> 10 permit udp any object-group <b>app_1</b> range 7750 7759 20 permit udp object-group <b>app_1</b> range 7750 7759 any <18行> ip access-list extended <b>APP_1_PORTS_3</b> 10 permit udp any object-group <b>app_1</b> range 22030 22031 20 permit udp object-group <b>app_1</b> range 22030 22031 any <6行> ip access-list extended <b>APP_2_PORTS_1</b> 10 permit udp any object-group <b>app_2</b> range 6000 9291 20 permit udp object-group <b>app_2</b> range 6000 9291 any ip access-list extended <b>APP_3_PORTS_1</b>	class-map match-any <b>BigClass_1</b> match access-group name <b>APP_3_PORTS_2</b> class-map match-any <b>BigClass_2</b> match access-group name <b>APP_4_PORTS_1</b> class-map match-any <b>BigClass_3</b> match access-group name <b>APP_1_PORTS_2</b> match access-group name <b>APP_3_PORTS_3</b> match access-group name <b>APP_2_PORTS_1</b> class-map match-any <b>BigClass_4</b> match access-group name <b>APP_1_PORTS_3</b> match access-group name <b>APP_3_PORTS_4</b> class-map match-any <b>BigClass_5</b> match access-group name <b>APP_1_PORTS_1</b> match access-group name <b>APP_3_PORTS_1</b>	policy-map big_ingress p class <b>BigCl</b> set dscp cs class <b>BigCl</b> set dscp af class <b>BigCl</b> set dscp cs class <b>BigCl</b> set dscp af class <b>BigCl</b> set dscp cs class class default

## experimental\_2

241.0.0.0 255.255.192.0

241.4.0.0 255.252.0.0

241.8.0.0 255.252.0.0

主机241.12.1.1

主机241.13.1.1

主机241.14.1.1

主机241.15.1.1

241.16.0.0 255.252.0.0

主机241.20.1.1

主机241.21.1.1

主机241.22.1.1

主机241.23.1.1

对象组网络RFC1918-

Private-IPv4

10.0.0.0 255.0.0.0

172.16.0.0 255.240.0.0

192.168.0.0 255.255.0.0

object-group network

app\_1

group-object RFC1918-

Private-IPv4

object-group network

app\_2

group-object RFC1918-

Private-IPv4

object-group network

app\_3

group-object RFC1918-

Private-IPv4

object-group network

app\_4

group-object RFC1918-

Private-IPv4

group-object

experimental\_1

group-object

experimental\_2

10 permit tcp any object-group

app\_3 eq 7563

20 permit tcp object-group app\_3

eq 7563 any

<4行>

ip access-list extended

APP\_3\_PORTS\_2

10 permit udp any object-group

app\_3 eq 554

20 permit udp object-group app\_3

eq 554 any

<2行>

ip access-list extended

APP\_3\_PORTS\_3

10 permit udp any object-group

app\_3 eq 22331

20 permit udp object-group app\_3

eq 22331 any

<2行>

ip access-list extended

APP\_3\_PORTS\_4

10 permit tcp any object-group

app\_3 eq 5432

20 permit tcp object-group app\_3

eq 5432 any

<6行>

ip access-list extended

APP\_4\_PORTS\_1

10 permit udp any object-group

app\_4 range 1718 1719

20 permit udp object-group app\_4

range 1718 1719 any

<14行>



## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。