排除IE3x00上的访问列表故障

目录

简介

本文档介绍如何对工业以太网3x00系列的访问控制列表(ACL)条目和硬件限制进行故障排除和验证。

先决条件

要求

Cisco建议您具备ACL配置的基本知识。

使用的组件

本文档中的信息基于采用Cisco IOS® XE软件版本16.12.4的IE-3300。

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

本文档还可用于以下硬件版本：

1. IE-3200（固定）
2. IE-3300（模块化）
3. IE-3400（高级模块化）。

背景信息

第3层交换机上的访问列表(ACL)为您的网络提供基本的安全性。如果未配置ACL，则允许通过交换机的所有数据包到达网络的所有部分。ACL控制哪些主机可以访问网络的不同部分，或者决定哪些类型的流量在路由器接口被转发或阻止。可以将ACL配置为阻止入站流量、出站流量或同时阻止两者。

示例：您可以允许转发电子邮件流量，但不允许在网络外部转发Telnet流量。

IE3x00支持和限制：

- 交换机虚拟接口(SVI)不支持VLAN访问列表(VACL)。
- 当VACL和端口ACL(PACL)都适用于数据包时，PACL优先于VACL，在这种情况下不应用VACL。
- 每个VACL最多255个访问控制条目(ACE)。
- 没有定义对总VLAN的明确限制，因为TCAM没有划分到组件中，当TCAM中没有足够的空间可用于接受新配置时，系统日志会引发错误。
- Logging 不支持出口ACL。
- 在第3层ACL上，不支持非IP ACL。
- ACL中的第4层运算符(L4OP)受硬件限制，UDP的最大值为8 L4OP，TCP的最大值为8 L4OP，总共为16个全局L4OP。
- 请记住，**range**运算符会消耗2 L4OP。

  注意：L4OP包括：gt（大于）、lt（小于）、neq（不等于）、eq（等于）、range（范围）

- 入口ACL仅支持物理接口，不支持逻辑接口，如VLAN、端口通道等。
- 支持端口ACL(PACL)，它们可以：非IP、IPv4和IPv6。
- 非IP和IPv4 ACL具有1个隐式过滤器，而IPv6 ACL具有3个隐式过滤器。
- 支持基于时间范围的ACL。
- 不支持基于TTL和IP选项的IPv4 ACL匹配。

故障排除

步骤1.**确**定您怀疑遇到问题的ACL。根据ACL的类型，可以使用以下命令：

show access-list { *acl-no* | *acl-name* } **show mac access-group interface** *interface_name* show ipv6 access-list *acl_name* show ip access-list { *acl-no* | *acl-name* } show ipv6 access-list *acl_name*

```
IE3300#show access-list 103
Extended IP access list 103
    10 permit udp any any eq 2222
    20 permit udp any eq 2222 any
IE3300#show ip access-list 103
Extended IP access list 103
    10 permit udp any any eq 2222
    20 permit udp any eq 2222 any
```

命令输出的目的是确定Cisco IOS上的当前ACL配置。

步骤2.**检查**硬件条目表中是否存在同一ACL。

show platform hardware acl asic 0 tcam { **all** | **index** | **interface** | **static** | **statistics** | **usage** | **vlan-statistics** } — 可用于检查交换机TCAM的命令选项。

```
IE3300#show platform hardware acl asic 0 tcam interface GigabitEthernet 1/4 ipv4 detail
ACL_KEY_TYPE_v4 - ACL Id 45

Ingress ACL_KEY_TYPE_v4 -
Index  SIP          DIP          Protocol  DSCP  Frag/Tiny  IGMP type  ICMP type  ICMP code  TCP
flags
Src OP  Src port1  Src port2  Dst OP  Dst port1  Dst port2  Src Port   PCLId
=====  ===========  ===========  ========  ====  ==========  =========  =========  =========
=========
======  =========  =========  ======  =========  =========  ========   ====
  0P   00.00.00.00  00.00.00.00  0x11      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  EQ.     2222       ---------  1     0
  0M   00.00.00.00  00.00.00.00  0xff      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------   0xFF     0xFFFF   --------- 3f   3ff
  0 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
  1P   00.00.00.00  00.00.00.00  0x11      0x00  0/00    ---------  ---------  ---------  ------
---
EQ.     2222       ---------  ------  ---------  ---------  1     0
  1M   00.00.00.00  00.00.00.00  0xff      0x00  0/00    ---------  ---------  ---------  ------
---
 0xFF     0xFFFF   ---------  ------  ---------  --------- 3f   3ff
  1 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
  2P   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  ------  ---------  ---------  1     0
  2M   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  ------  ---------  --------- 3f   3ff
  2 Action: ASIC_ACL_DENY[0], Match Counter[0]
```

硬件表的输出中有三个规则对，分别用于：

P:表示模式=这些是ACE中的IP或子网。

M :代表掩码=这些是ACE中的通配符位。

ACE条目	索引	SIP	DIP	协议	DSCP
permit udp any any eq 2222	0P、0M、0	0.0.0.0（任意）	0.0.0.0（任意）	0x11	0x00（尽力而为）
permit udp any eq 2222 any	1P、1M、1	0.0.0.0（任意）	0.0.0.0（任意）	0x11	0x00（尽力而为）
deny ip any any (implicit)	2P、2M、2	0.0.0.0（任意）	0.0.0.0（任意）	0x00	0x00（尽力而为）

ACE条目	源OP	源端口1	源端口2	Dst OP	目标端口1	目标端口2
permit udp any any eq 2222	------	---------	---------	等价	2222	---------
permit udp any eq 2222 any	EQ	2222	---------	---------	---------	---------
deny ip any any (implicit)	------	---------	---------	---------	---------	---------

注意：掩码条目示例：host关键字= ff.ff.ff.ff，通配符0.0.0.255 = ff.ff.ff.00,any关键字= 00.00.00.00

Index — 规则的编号。示例中包含0、1和2个索引。

SIP — 以十六进制格式表示源IP。由于规则具有“any”关键字，因此源IP全部为零。

DIP — 以十六进制格式表示目标IP。规则中的“any”关键字将转换为全零。

Protocol — 指示ACE的协议。0x11用于UDP。

注意：公认协议列表：0x01 - ICMP、0x06 - TCP、0x11 - UDP、0x29 - IPv6。

DSCP — 规则中存在的差分服务代码点(DSCP)。如果未指定，则值为0x00（尽力而为）。

IGMP Type — 指定ACE是否包含IGMP类型。

ICMP Type — 指定ACE是否包含ICMP类型。

ICMP Code — 指定ACE是否包含ICMP代码类型。

TCP Flags — 指定ACE是否具有TCP标志。

源OP — 指示规则中使用的源L4OP。第一个ACE条目中没有任何条目。第二个ACE条目将EQ作为运算符。

Src port1 — 如果ACE基于UDP或TCP，则表示第一个源端口。

Src port2 — 如果ACE基于UDP或TCP，则表示第二个源端口。

Dst OP — 指示规则中使用的目标L4OP。第一个ACE条目将EQ作为运算符，第二个ACE条目中没有运算符。

Dst port1 — 如果ACE基于UDP或TCP，则表示第一个目标端口。

Dst port2 — 指示ACE基于UDP或TCP时的第二个目标端口。

规则绑定到端口 **ACL:<0,x>** 其中0表示ASIC = 0,X映射到ASIC端口号= 1。

您还可以在表中看到每个ACE语句采取的操作。

ACE索引	操作
0	ASIC_ACL_PERMIT [1]
1	ASIC_ACL_PERMIT

2	[1] ASIC_ACL_DENY[0]

步骤3.**使用**下面列出的不同命令检验相同的ACL条目：

给定索引处的ACL条目

show platform hardware acl asic 0 tcam index *acl_id* **[detail]** — 此命令显示特定ACL ID下的规则列表。

```
IE3300#show platform hardware acl asic 0 tcam index 45 detail
ACL_KEY_TYPE_v4 - ACL Id 45

Ingress ACL_KEY_TYPE_v4 -
Index  SIP          DIP          Protocol  DSCP  Frag/Tiny  IGMP type  ICMP type  ICMP code  TCP
flags
Src OP  Src port1  Src port2  Dst OP  Dst port1  Dst port2  Src Port   PCLId
=====  ===========  ===========  ========  ====  ==========  =========  =========  =========
=========
======  =========  =========  ======  =========  =========  ========   ====
  0P   00.00.00.00  00.00.00.00  0x11      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  EQ.     2222       ---------  1     0
  0M   00.00.00.00  00.00.00.00  0xff      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------   0xFF     0xFFFF   --------- 3f   3ff
  0 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
  1P   00.00.00.00  00.00.00.00  0x11      0x00  0/00    ---------  ---------  ---------  ------
---
EQ.     2222       ---------  ------  ---------  ---------  1     0
  1M   00.00.00.00  00.00.00.00  0xff      0x00  0/00    ---------  ---------  ---------  ------
---
 0xFF     0xFFFF   ---------  ------  ---------  --------- 3f   3ff
  1 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
  2P   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  ------  ---------  ---------  1     0
  2M   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  ------  ---------  --------- 3f   3ff
  2 Action: ASIC_ACL_DENY[0], Match Counter[0]
```

此处 index 是在TCAM中编程规则的偏移。

要检查使用哪个ACL索引，您需要确定应用ACL的端口并使用命令 show platform hardware acl asic 0 tcam interface *interface_name* ipv4 detail获取ACL ID编号。

> **注意：**请记住，此命令不会显示ASIC/端口映射。此外，如果您将同一ACL应用于不同的接口，则TCAM会创建不同的ACL ID条目。这意味着对于TCAM空间中应用于不同接口的相同ACL，没有索引重复使用。

硬件中编程的ACL条目

show platform hardware acl asic 0 tcam all [detail] — 显示TCAM上的所有信息。

```
IE3300#show platform hardware acl asic 0 tcam all
ACL_KEY_TYPE_v4 - ACL Id 45

Ingress ACL_KEY_TYPE_v4 -
Index  SIP          DIP          Protocol  DSCP  Frag/Tiny  IGMP type  ICMP type  ICMP code  TCP
flags
Src OP  Src port1  Src port2  Dst OP  Dst port1  Dst port2  Src Port   PCLId
=====  ===========  ===========  ========  ====  ==========  =========  =========  =========
=========
======  =========  =========  ======  =========  =========  ========   ====
  0P   00.00.00.00  00.00.00.00  0x11      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  EQ.     2222       ---------  1     0
  0M   00.00.00.00  00.00.00.00  0xff      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------   0xFF     0xFFFF   --------- 3f   3ff
  0 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
  1P   00.00.00.00  00.00.00.00  0x11      0x00  0/00    ---------  ---------  ---------  ------
---
EQ.     2222       ---------  ------  ---------  ---------  1     0
  1M   00.00.00.00  00.00.00.00  0xff      0x00  0/00    ---------  ---------  ---------  ------
---
 0xFF     0xFFFF   ---------  ------  ---------  --------- 3f   3ff
  1 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
  2P   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  ------  ---------  ---------  1     0
  2M   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  ------  ---------  --------- 3f   3ff
  2 Action: ASIC_ACL_DENY[0], Match Counter[0]

ACL_KEY_TYPE_v4 - ACL Id 46

Ingress ACL_KEY_TYPE_v4 -
Index  SIP          DIP          Protocol  DSCP  Frag/Tiny  IGMP type  ICMP type  ICMP code  TCP
flags
Src OP  Src port1  Src port2  Dst OP  Dst port1  Dst port2  Src Port   PCLId
=====  ===========  ===========  ========  ====  ==========  =========  =========  =========
=========
======  =========  =========  ======  =========  =========  ========   ====
  0P   00.00.00.00  00.00.00.00  0x11      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  EQ.     2222       ---------  0     0
  0M   00.00.00.00  00.00.00.00  0xff      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------   0xFF     0xFFFF   --------- 3f   3ff
  0 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
  1P   00.00.00.00  00.00.00.00  0x11      0x00  0/00    ---------  ---------  ---------  ------
---
EQ.     2222       ---------  ------  ---------  ---------  0     0
  1M   00.00.00.00  00.00.00.00  0xff      0x00  0/00    ---------  ---------  ---------  ------
---
 0xFF     0xFFFF   ---------  ------  ---------  --------- 3f   3ff
  1 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
  2P   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  ------  ---------  ---------  0     0
  2M   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  ------  ---------  --------- 3f   3ff
  2 Action: ASIC_ACL_DENY[0], Match Counter[12244]
```

此输出显示硬件表中存储的所有ACL ID。有两个单独的ACL ID(45、46)，但每个块的结构完全相同。这表示两个ACL ID属于软件中配置的同一ACL:

```
IE3300#show ip access-list 103
Extended IP access list 103
    10 permit udp any any eq 2222
    20 permit udp any eq 2222 any
```

适用于不同接口。

```
IE3300#show run interface GigabitEthernet 1/4
Building configuration...

Current configuration : 60 bytes
!
interface GigabitEthernet1/4
 ip access-group 103 in
end

IE3300#show run interface GigabitEthernet 1/5
Building configuration...

Current configuration : 60 bytes
!
interface GigabitEthernet1/5
 ip access-group 103 in
end
```

TCAM使用情况

show platform hardware acl asic 0 tcam usage — 此命令显示ASIC中的ACL使用情况。IE3x00只有一个ASIC(0)

```
IE3300#show platform hardware acl asic 0 tcam usage
        TCAM Usage For ASIC Num : 0

                Static ACEs      : 18   (0   %)
                Extended ACEs    : 0    (0   %)
                ULTRA ACEs        : 0    (0   %)
                STANDARD ACEs    : 6    (0   %)
                Free  Entries     : 3048 (100 %)
                Total Entries   : 3072
```

标准ACE为24字节宽；扩展ACE为48字节宽；Ultra ACE宽72字节。

ACL静态条目

show platform hardware acl asic 0 tcam static [detail] — 显示静态ACL配置（特定于控制协议）。

```
IE3300-Petra#show platform hardware acl asic 0 tcam static detail
Switch MAC Global Entry:
MAC DA: 01:00:0c:00:00:00/ff:ff:ff:00:00:00
  4 Action: ASIC_ACL_DENY_AND_LOG[2], CPU queue[1], Match Counter[6908]
```

```
Dot1x EAP Global Entry:
Ethertype: 0x888e/0xffff
  1 Action: ASIC_ACL_DENY_AND_LOG[2], CPU queue[2], Match Counter[0]
CISP Global Entry:
Ethertype: 0x0130/0xffff
  0 Action: ASIC_ACL_DENY_AND_LOG[2], CPU queue[2], Match Counter[0]
REP Beacon Global Entry:
Ethertype: 0x0131/0xffff
  2 Action: ASIC_ACL_DENY_AND_LOG[2], CPU queue[1], Match Counter[0]
REP Preferred Global Entry:
MAC DA: 00:00:00:00:00:00/00:00:00:00:00:00
 14 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
REP Preferred Global Entry:
Ethertype: 0x0000/0x0000
 16 Action: ASIC_ACL_DENY_AND_LOG[2], CPU queue[1], Match Counter[25702]
REP Preferred Global Entry:
Ethertype: 0x0129/0xffff
 15 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
DHCP related entries:
None.
MLD related entries:
None.
```

此命令输出显示交换机不同控制协议的系统编程ACL条目。

ACL统计信息

show platform hardware acl asic 0 tcam statistics *interface_name* — 实时显示ACL统计信息，计数器不是累积的。第一次显示命令后，如果到达ACL的流量停止，计数器将重置。

```
IE3300#show platform hardware acl asic 0 tcam statistics GigabitEthernet 1/4
         TCAM STATISTICS OF ASIC NUM  :0
         Number Of IPv4 Permits   : 0
         Number Of IPv4 Drops     : 2
IE3300#show platform hardware acl asic 0 tcam statistics GigabitEthernet 1/4
         TCAM STATISTICS OF ASIC NUM  :0
         Number Of IPv4 Permits   : 0
         Number Of IPv4 Drops     : 1
IE3300#show platform hardware acl asic 0 tcam statistics GigabitEthernet 1/4
         TCAM STATISTICS OF ASIC NUM  :0
         Number Of IPv4 Permits   : 0
         Number Of IPv4 Drops     : 1
IE3300#show platform hardware acl asic 0 tcam statistics GigabitEthernet 1/4
         TCAM STATISTICS OF ASIC NUM  :0
         Number Of IPv4 Permits   : 0
         Number Of IPv4 Drops     : 1
IE3300#show platform hardware acl asic 0 tcam statistics GigabitEthernet 1/4
         TCAM STATISTICS OF ASIC NUM  :0
         Number Of IPv4 Permits   : 0
         Number Of IPv4 Drops     : 0
```

此命令将告诉您在指定接口上为ACL执行了多少次命中，以及在流量主动入队到端口时执行了多少次丢弃。在首次显示该命令后，计数器将重置。

> **提示：**由于计数器在每次运行该命令后重置，因此建议您多次运行该命令，并记录累计permit/drop计数器的以前输出。

端口到ASIC的映射

show platform pm port-map — 显示交换机所有接口的ASIC/端口映射。

```
IE3300#show platform pm port-map

interface gid  gpn  asic slot unit gpn-idb
----------------------------------------
Gi1/1     1    1    0/24 1    1    Yes
Gi1/2     2    2    0/26 1    2    Yes
Gi1/3     3    3    0/0  1    3    Yes
Gi1/4     4    4    0/1  1    4    Yes
Gi1/5     5    5    0/2  1    5    Yes
Gi1/6     6    6    0/3  1    6    Yes
Gi1/7     7    7    0/4  1    7    Yes
Gi1/8     8    8    0/5  1    8    Yes
Gi1/9     9    9    0/6  1    9    Yes
Gi1/10    10   10   0/7  1    10   Yes
```

0/**x** under asic column indicates = asic/**asic_port_number**

调试命令

debug platform acl all — 此命令启用所有ACL管理器事件。

```
IE3300#debug platform acl all
ACL Manager debugging is on
ACL MAC debugging is on
ACL IPV4 debugging is on
ACL Interface debugging is on
ACL ODM debugging is on
ACL HAL debugging is on
ACL IPV6 debugging is on
ACL ERR debugging is on
ACL VMR debugging is on
ACL Limits debugging is on
ACL VLAN debugging is on
```

debug platform acl hal — 显示硬件抽象层(HAL)相关事件。

对于接口上的删除/应用ACL事件，它显示规则是否已在硬件中编程，并在控制台中打印信息。

```
[IMSP-ACL-HAL] : Direction 0
[IMSP-ACL-HAL] : TCAM: region_type = 1, lookup_stage = 0, key_type = 1, packet_type = 1,
acl_type = 1, pcl_id = 0, priority = 1
[IMSP-ACL-HAL] : asic_acl_add_port_access_list programmed rule for asic_num=0, region_type=1,
acl_type=1,
port_num=1, lookup stage=0 packet_type=1, key_type=1, pcl_id=0, priority=32, num_aces=3,
acl_handle=0x7F8EA6DC58, acl_dir=0, cpu_log_queue=7 with acl_err=0
[IMSP-ACL-HAL] : Dump acl, acl_handle:0x0x7F8EA6DC58
```

方向0 =入站（ACL应用于入口）

方向1 =出站（ACL应用于出口）

debug platform acl ipv4 — 显示ACL IPv4相关事件。

debug platform acl ipv6 — 显示ACL IPv6相关事件。

debug platform acl mac — 显示ACL MAC相关事件。

debug platform acl error — 显示ACL错误相关事件。

```
[IMSP-ACL-ERROR] : asic_acl_delete_access_list successfully deleted rule for asic_num=0,
region_type=1 acl_handle=0x7F8EA6DC58, acl_dir=0 atomic_update=0 with acl_err=0
```

debug platform acl odm — 显示ACL顺序相关合并(ODM)相关事件。

```
[IMSP-ACL-ODM] : ODM: Num. ACEs before collapse - 2
[IMSP-ACL-ODM] : ODM: Num. ACEs after collapse - 2
[IMSP-ACL-ODM] : Number of Aces after ODM Pre Optimization- 2
[IMSP-ACL-ODM] : ODM: ACEs post collapse = 2
[IMSP-ACL-ODM] : Number of Aces after Final ODM Merge- 2
[IMSP-ACL-ODM] : ODM: Num. ACEs before collapse - 2
[IMSP-ACL-ODM] : ODM: Num. ACEs after collapse - 2
<snip>
```

debug platform acl port-acl — 显示端口ACL相关事件。

```
[IMSP-ACL-PORT] : PACL attach common
[IMSP-ACL-PORT] : Dumping List of ACL-Handle pairs...
[IMSP-ACL-PORT] : ACL:103, Handle: 0x7F8EA6DC64, Asic Num: 0,Use Count: 1, Is overloaded: 0
[IMSP-ACL-PORT] : ACL:103, Handle: 0x7F8EA6DC58, Asic Num: 0,Use Count: 1, Is overloaded: 0
[IMSP-ACL-PORT] : ACL Detached from the port
[IMSP-ACL-PORT] : Acl-port handle info, Idb Entry Found
[IMSP-ACL-PORT] : ACL handle=0x7F8EA6DC58 found for port=Gi1/4
[IMSP-ACL-PORT] : Calling HAL asic_acl_remove_port
[IMSP-ACL-PORT] : asic_acl_remove_port successful for asic_num=0, acl_handle=0x7F8EA6DC58,
port_num=1
[IMSP-ACL-PORT] : acl_type: 1, handle: 0x0, dir: 0, acl_name: 0x0, idb: 0x7F4D0AF288
[IMSP-ACL-PORT] : List of HW Programmed Port-ACLs...
[IMSP-ACL-PORT] : Port: Gi1/3
[IMSP-ACL-PORT] : Ingress IPV4: handle = 0x7F8EA6DC64, acl_name = 103, is_acl_overloaded = 0,
auth_proxy_vmr = 0x0, overload_vmr_entries = 0
[IMSP-ACL-PORT] : Port: Gi1/4
[IMSP-ACL-PORT] : Ingress IPV4: handle = 0x7F8EA6DC58, acl_name = 103, is_acl_overloaded = 0,
auth_proxy_vmr = 0x0, overload_vmr_entries = 0
[IMSP-ACL-PORT] : rc = 1
[IMSP-ACL-PORT] : No more acl on this port!!
[IMSP-ACL-PORT] : Free stored_acl_name=0x0
[IMSP-ACL-PORT] : Update_Pacl_info, Updated entries for idb=0x0
<snip>
```

debug platform acl vmr — 显示ACL值掩码结果(VMR)相关事件。如果VMR存在问题，您可以在此处看到它们。

```
[IMSP-ACL-VMR] : DstIP Mask=00.00.00.00
[IMSP-ACL-VMR] : Protocol Value/Mask=0011/FFFF
[IMSP-ACL-VMR] : Fragment field set to FALSE
[IMSP-ACL-VMR] : SrcPort1 Value/Mask=D908/FFFF
[IMSP-ACL-VMR] : SrcPort2 Value/Mask=D90F/FFFF
[IMSP-ACL-VMR] : SrcL4Op Value is Range
[IMSP-ACL-VMR] : SrcL4Op Mask is FFFFFFFF
[IMSP-ACL-VMR] : Action is PERMIT
[IMSP-ACL-VMR] : ACE number => 30
[IMSP-ACL-VMR] : vmr_ptr 0x7F51D973B0
[IMSP-ACL-VMR] : vmr_ptr->entry 0x7F51D973B0
<snip>
```

常见问题

L4OP耗尽

启用以下调试后，可以识别L4OP比较器耗尽：

debug platform port-asic hal acl errors debug platform port-asic hal tcam errors

> **注意：**debug命令不会向交换机的日志缓冲区显示信息。相反，信息显示在 show platform software trace message ios R0 命令。

运行命令show platform software trace message ios R0以显示有关调试的信息。

show platform software trace message ios R0：

```
2022/08/17 21:04:47.244 {IOSRP_R0-0}{1}: [iosrp] [8748]: (ERR): *Aug 17 21:04:47.244:
%IMSP_ACLMGR-3-INVALIDACL: Add access-list failed
2022/08/17 21:04:47.244 {IOSRP_R0-0}{1}: [iosrp] [8748]: (note): Unable to add access-list
[IMSP-ACL-ERROR]:imsp_acl_program_tcam,2026:
2022/08/17 21:04:47.244 {IOSRP_R0-0}{1}: [iosrp] [8748]: (note):
2022/08/17 21:04:47.244 {IOSRP_R0-0}{1}: [iosrp] [8748]: (note):
asic_acl_add_port_access_list failed for asic_num=0, region_type=1, acl_type=1,
port_num=1, lookup stage=0, packet_type=1, key_type=1, pcl_id=0, priority=32, num_aces=99
acl_handle=0x0, acl_dir=0, cpu_log_queue=7 with acl_err=2
[IMSP-ACL-ERROR]:imsp_acl_add_port_access_list,211:
2022/08/17 21:04:47.244 {IOSRP_R0-0}{1}: [iosrp] [8748]: (note):
ACL ERR:[pc3_add_port_access_list:5471] - not enough available port comparators,asic_num[0],
acl_type[1], num_aces[99]
2022/08/17 21:04:47.244 {IOSRP_R0-0}{1}: [IOSRP] [6472]: (note):

ACL ERR:[prv_check_for_available_port_comparators:5282] - Not enough TCP port comparators
available: Required[20] > Available[8]
2022/08/17 21:04:47.244 {IOSRP_R0-0}{1}: [IOSRP] [6472]: (note):

2022/08/17 21:04:47.244 {IOSRP_R0-0}{1}: [iosrp] [8748]: (note): TCAM: region_type = 1,
lookup_stage = 0, key_type = 1,
packet_type = 1, acl_type = 1, pcl_id = 0, priority = 1
[IMSP-ACL-HAL] :
2022/08/17 21:04:47.244 {IOSRP_R0-0}{1}: [iosrp] [8748]: (note):
2022/08/17 21:04:47.244 {IOSRP_R0-0}{1}: [iosrp] [8748]: (note): Direction 0
[IMSP-ACL-HAL] :
```

对于IE3x00,UDP限制为8 L4OP，TCP限制为8 L4OP，在交换机中实施的所有ACL中最多总共为16 L4OP。（限制是全局的，而不是每个ACL）。

> **注意：**目前，没有可用命令来检查CLI中已消耗/空闲的比较器的数量。

如果遇到此问题：

- 如果错误与L4OP限制相关，请使用debug命令检查。
- 您需要减少ACL中使用的L4OP数量。每个range命令使用2个端口比较器。
- 如果可以将ACE与range命令一起使用，则可以将它们转换为使用eq关键字，这样它不会使用可用于UDP和TCP的L4OP，即：

线路：
permit tcp any any range 55560 55567

可以变成：
permit tcp any any eq 55560 permit tcp any any eq 55561 permit tcp any any eq 55562 permit tcp any any eq 55563 permit tcp any any eq 55564 permit tcp any any eq 55565 permit tcp any any eq 55566 permit tcp any any eq 55567

请参阅Cisco Bug ID CSCvv0745。只有已注册的Cisco用户可以访问内部Bug信息。

第4层ACL未在TCAM中汇总

当输入具有连续IP地址和/或端口号的L4 ACL时，系统会在将其写入TCAM之前自动对其进行摘要以节省空间。系统根据ACL条目尽其最大努力使用适当的MVR进行总结，以覆盖其能够覆盖的条目范围。当您检查TCAM以及为ACL编程的线路数时，可以验证这一点。即：

```
IE3300#show ip access-list TEST
Extended IP access list TEST
    10 permit tcp any any eq 8
    20 permit tcp any any eq 9
    30 permit tcp any any eq 10
    40 permit tcp any any eq 11
```

```
IE3300#show platform hardware acl asic 0 tcam interface GigabitEthernet 1/4 ipv4 detail
ACL_KEY_TYPE_v4 - ACL Id 45

Ingress ACL_KEY_TYPE_v4 -
Index  SIP          DIP          Protocol  DSCP  Frag/Tiny  IGMP type  ICMP type  ICMP code  TCP
flags
Src OP  Src port1  Src port2  Dst OP  Dst port1  Dst port2  Src Port   PCLId
=====  ===========  ===========  ========  ====  ==========  =========  =========  =========
=========
======  =========  =========  ======  =========  =========  ========   ====
  0P   00.00.00.00  00.00.00.00  0x06      0x00  0/00    ---------  ---------  ---------  0x00
------  ---------  ---------  EQ.     8          ---------  1     0
  0M   00.00.00.00  00.00.00.00  0xff      0x00  0/00    ---------  ---------  ---------  0x00
------  ---------  ---------   0xFF     0xFFFF   --------- 3f   3ff
  0 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
  1P   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  ------  ---------  ---------  1     0
  1M   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  ------  ---------  --------- 3f   3ff
  1 Action: ASIC_ACL_DENY[0], Match Counter[0]

<asic,port> pair bind to this ACL:< 0, 1>
```

问题是掩码值读取不正确，因此实际编程的唯一条目（在本例中为ACL）是 **permit tcp any any eq 8**,这是顶级汇总ACL。未看到端口号9-11的条目，因为未正确读取掩码0.0.0.3。

请参阅Cisco Bug ID CSCvx66354。只有注册的思科用户才能访问内部Bug信息。

为TAC收集的命令

本指南介绍了与IE3x00上的访问列表相关的最常见问题，以及相应的补救步骤。但是，如果此指南

未解决您的问题，请收集显示的命令列表，并将其附加到TAC服务请求。

Show tech-support acl

```
IE3300#show tech-support acl | redir flash:tech-acl.txt
IE3300#dir flash: | i .txt
89249  -rw-            56287  Aug 18 2022 00:50:32 +00:00  tech-acl.txt
```

将文件从交换机复制并上传到TAC案例。

在对IE3x00平台中的ACL相关问题进行故障排除时，需要以技术支持ACL输出作为起点。

相关信息

- Cisco Catalyst IE3x00坚固型、IE3400坚固型、IE3400重型和ESS3300系列交换机、Cisco IOS XE Gibraltar 16.12.x版本说明
- 技术支持和文档 - Cisco Systems

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）。