# 排除IE3x00上的訪問清單故障

## 目錄



## 簡介

本檔案介紹如何對工業乙太網路3x00系列上的存取控制清單(ACL)專案與硬體限制進行疑難排解和驗證。

## 必要條件

### 需求

思科建議您瞭解ACL組態的基本知識。

### 採用元件

本檔案中的資訊是根據搭載Cisco IOS® XE軟體版本16.12.4的IE-3300。

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

### 相關產品

本檔案也適用於以下硬體版本：

1. IE-3200（固定）
2. IE-3300（模組化）
3. IE-3400（高級模組化）。

# 背景資訊

第3層交換器上的存取清單(ACL)可為網路提供基本安全性。如果沒有設定ACL，則允許經過交換器的所有封包進入網路的所有部分。ACL控制哪些主機可以訪問網路的不同部分，或者決定哪些型別的流量在路由器介面被轉發或阻止。可以將ACL設定為封鎖傳入流量、傳出流量或兩者均有。

**範例：**您可以允許轉發電子郵件流量，但不能允許網路外部的Telnet流量。

IE3x00支援和限制：

- 交換器虛擬介面(SVI)不支援VLAN存取清單(VACL)。
- 當VACL和連線埠ACL(PACL)都適用於封包時，PACL優先於VACL，在這種情況下不會應用VACL。
- 每個VACL最多支援255個訪問控制條目(ACE)。
- 未定義對總VLAN的明確限制，因為TCAM未刻入元件，當TCAM中沒有足夠的空間可用於接受新配置時，系統日誌將引發錯誤。
- Logging 輸出ACL上不支援。
- 在第3層ACL上，不支援非IP ACL。
- ACL中的第4層操作員(L4OP)受到硬體的限制，UDP最多為8個L4OP，TCP最多為8個L4OP，總共為16個全域L4OP。
- 請記住，**range**運算子耗用2個L4OP。

  **附註**：L4OP包括：gt（大於）、lt（小於）、neq（不等於）、eq（等於）、range（範圍）

- 輸入ACL僅支援物理介面，不支援邏輯介面（如VLAN、埠通道等）。
- 支援連線埠ACL(PACL)，可以是：非IP、IPv4和IPv6。
- 非IP和IPv4 ACL具有1個隱式篩選器，而IPv6 ACL具有3個隱式篩選器。
- 支援時間範圍型ACL。
- 不支援TTL和IP選項匹配的IPv4 ACL。

# 疑難排解

步驟1. **識別**您懷疑發生問題的ACL。根據ACL的型別，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
```

命令輸出的目的是識別Cisco IOS上的當前ACL配置。

步驟2. **檢查**硬體條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** } — 可用於檢查交換機TCAM的命令選項。

```
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]
```

硬體表的輸出中有三個規則對，從中：

**P:**代表模式=這些是ACE中的IP或子網。

**M:**代表掩碼=這些是ACE中的萬用字元位。

| ACE條目 | 索引 | SIP | DIP | 通訊協定 | DSCP |
|---|---|---|---|---|---|
| permit udp any any eq 2222 | 0P、0M、0 | 0.0.0.0（任意） | 0.0.0.0（任意） | 0x11 | 0x00（盡最大努力） |
| permit udp any eq 2222 any | 1P、1M、1 | 0.0.0.0（任意） | 0.0.0.0（任意） | 0x11 | 0x00（盡最大努力） |
| deny ip any any (implicit) | 2P、2M、2 | 0.0.0.0（任意） | 0.0.0.0（任意） | 0x00 | 0x00（盡最大努力） |

| ACE條目 | 源OP | Src port1 | Src port2 | Dst OP | Dst埠1 | Dst埠2 |
|---|---|---|---|---|---|---|
| permit udp any any eq 2222 | ------ | --------- | --------- | EQ。 | 2222 | --------- |
| permit udp any eq 2222 any | EQ | 2222 | --------- | --------- | --------- | --------- |
| deny ip any any (implicit) | ------ | --------- | --------- | --------- | --------- | --------- |

**附註**：掩碼條目示例：host關鍵字= ff.ff.ff.ff，萬用字元0.0.0.255 = ff.ff.ff.00,any關鍵字= 00.00.00.00

**Index** — 規則的編號。本例中包含0、1和2個索引。

**SIP** — 以十六進位制格式表示源IP。由於規則具有「any」關鍵字，因此源IP全部為零。

**DIP** — 以十六進位制格式表示目標IP。規則中的「any」關鍵字轉換為所有零。

**Protocol** — 指示ACE的協定。0x11用於UDP。

**附註**：公認協定清單：0x01 - ICMP、0x06 - TCP、0x11 - UDP、0x29 - IPv6。

DSCP — 規則中存在的區別服務代碼點(DSCP)。如果未指定，則值為0x00（盡力而為）。

IGMP型別 — 指定ACE是否包含IGMP型別。

ICMP型別 — 指定ACE是否包含ICMP型別。

ICMP Code — 指定ACE是否包含ICMP代碼型別。

TCP Flags — 指定ACE是否具有TCP標誌。

Src OP — 指示規則中使用的源L4OP。第一個ACE條目中沒有任何條目。第二個ACE條目將EQ作為運算子。

Src port1 — 如果ACE基於UDP或TCP，則表示第一個源埠。

Src port2 — 如果ACE基於UDP或TCP，則表示第二個源埠。

Dst OP — 指示規則中使用的目標L4OP。第一個ACE條目具有EQ作為運算子，第二個ACE條目中沒有運算子。

Dst port1 — 如果ACE基於UDP或TCP，則表示第一個目的埠。

Dst port2 — 如果ACE基於UDP或TCP，則表示第二個目的埠。

規則繫結到埠 **ACL:<0,x>** 其中0表示ASIC = 0,X對映到ASIC埠號= 1。

您還可以在表中看到每個ACE語句所採取的操作。

| ACE索引 | 動作 |
|---|---|
| 0 | ASIC_ACL_PERMIT [1] |
| 1 | ASIC_ACL_PERMIT |

| | |
|---|---|
| 2 | [1]<br>ASIC_ACL_DENY[0<br>] |

步驟3. **使用**下面列出的不同命令檢驗相同的ACL條目：

## 指定索引中的ACL專案

**show platform hardware acl asic 0 tcam index** *acl_id* **[ detail ]** — 此命令會顯示特定ACL ID下的規則清單。

```
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]
```

此處 index 是在TCAM中程式設計規則的偏移。

要檢查使用哪個ACL索引，您需要確定應用ACL的埠並使用命令 show platform hardware acl asic 0 tcam interface *interface_name* ipv4 detail獲取ACL ID編號。

> **附註**：請記住，此命令不顯示ASIC/埠對映。此外，如果您將相同的ACL應用到不同的介面，則TCAM會建立不同的ACL ID條目。這表示應用於TCAM空間中不同介面的相同ACL沒有索引重複使用。

## 在硬體中程式設計的ACL條目

**show platform hardware acl asic 0 tcam all [ detail ]** — 顯示TCAM上的所有資訊。

```
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]
```

此輸出顯示儲存在硬體表中的所有ACL ID。有兩個獨立的ACL ID(45、46)，但是每個塊的結構完全相同。這表示兩個ACL ID屬於在軟體中設定的同一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
```

適用於不同的介面。

```
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使用情況

show platform hardware acl asic 0 tcam usage — 此命令顯示ASIC中的ACL使用情況。IE3x00隻有一個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
```

標準ACE為24位元組寬；擴展ACE為48位元組寬；Ultra ACE為72位元組寬。

## ACL靜態專案

show platform hardware acl asic 0 tcam static [ detail ] — 顯示靜態ACL配置（特定於控制協定）。

```
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.
```

此命令輸出顯示了交換機不同控制協定的系統程式設計ACL條目。

## ACL統計資訊

**show platform hardware acl asic 0 tcam statistics** *interface_name* — 即時顯示ACL統計資訊，計數器不是累積的。第一次顯示命令後，如果命中ACL的流量停止，計數器就會重置。

```
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
```

此命令將告訴您在指定介面上的ACL在允許中進行了多少次命中，以及在流量主動入隊到埠時也發生了多少丟棄事件。在首次顯示該命令後，計數器將重置。

> **提示：**由於計數器在每次運行該命令後都會重置，因此建議您多次運行該命令，並保留累計permit/drop計數器的以前輸出的記錄。

## 埠到ASIC對映

show platform pm port-map — 顯示交換機所有介面的ASIC/埠對映。

```
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**

## Debug指令

debug platform acl all — 此命令啟用所有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 — 顯示硬體抽象層(HAL)相關事件。

對於介面上的刪除/應用ACL事件，它會顯示規則是否已在硬體中程式設計，並在控制檯中列印資訊。

```
[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已應用於輸入）

方向1 =出站（ACL應用於輸出）

debug platform acl ipv4 — 顯示ACL IPv4相關事件。

debug platform acl ipv6 — 顯示ACL IPv6相關事件。

**debug platform acl mac** — 顯示ACL MAC相關事件。

debug platform acl error — 顯示ACL錯誤相關事件。

```
[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** — 顯示與ACL順序相關的合併(ODM)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 — 顯示埠ACL相關事件。

```
[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 — 顯示與ACL值掩碼結果(VMR)相關的事件。如果VMR存在問題，您可以在此處看到它們。

```
[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>
```

# 常見問題

## L4OP耗盡

啟用以下調試後，可以識別L4OP比較器耗盡：

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

> **附註**：debug指令不會將資訊顯示到交換器的記錄緩衝區中。相反，資訊顯示在 show platform software trace message ios R0指令。

### 運行命令show platform software trace message ios R0以顯示有關調試的資訊。

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] :
```

對於IE3x00,UDP限製為8 L4OP，TCP限製為8 L4OP，在交換機中實施的所有ACL中，最大總共限製為16 L4OP。（此限製為全域限制，而不是每個ACL）。

> **附註**：當前沒有可用命令來檢查CLI中已使用/可用比較器的數量。

如果您遇到此問題：

- 如果錯誤與L4OP限制相關，請檢查debug命令。
- 您需要減少ACL中使用的L4OP數量。每個range命令使用2個埠比較器。
- 如果可以將ACE與range命令一起使用，則可以將它們轉換為eq關鍵字，這樣它就不會佔用可用於UDP和TCP的L4OP，即：

線路：
permit tcp any any range 55560 55567

可以轉換為：
**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

請參閱思科錯誤ID CSCvv07745。只有註冊的思科使用者才能存取內部錯誤資訊。

## 第4層ACL不會在TCAM中彙總

當輸入具有連續IP地址和/或埠號的L4 ACL時，系統會在將其寫入TCAM之前自動對其進行摘要以節省空間。系統根據ACL條目盡其最大努力來使用適當的MVR進行彙總，以覆蓋可以覆蓋的條目範圍。當您檢查TCAM以及為ACL程式設計的線路數時，可以驗證這一點。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>
```

問題在於遮罩值未正確讀取，因此實際透過範例中的ACL進行程式的唯一專案是 **permit tcp any any eq 8**,這是頂級摘要ACL。未看到埠號9-11的條目，因為未正確讀取0.0.0.3的掩碼。

請參閱思科錯誤ID CSCvx66354。只有註冊思科使用者才能存取內部錯誤資訊。

# 為TAC收集的命令

本指南介紹了與IE3x00上的訪問清單相關的最常見問題，並提供了相應的補救步驟。但是，如果此

指南未解決您的問題，請收集顯示的命令清單，並將它們附加到TAC服務請求。

**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
```

將檔案從交換器複製並上傳到TAC案例。

在對IE3x00平台中的ACL相關問題進行故障排除時，需要以技術支援ACL輸出作為起點。

# 相關資訊

- Cisco Catalyst IE3x00強固型、IE3400強固型、IE3400耐用型和ESS3300系列交換機、Cisco IOS XE直布羅陀版16.12.x的版本說明
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。