IE3x00のアクセスリストのトラブルシューティング

内容

概要

このドキュメントでは、Industrial Ethernet 3x00シリーズのアクセスコントロールリスト(ACL)エントリとハードウェア制限をトラブルシューティングして確認する方法について説明します。

前提条件

要件

ACL設定に関する基本的な知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、Cisco IOS® XEソフトウェアバージョン16.12.4が稼働するIE-3300に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

関連製品

このドキュメントは、次のバージョンのハードウェアにも使用できます。

1. IE-3200（固定）
2. IE-3300（モジュラ）
3. IE-3400（高度なモジュール型）。

背景説明

レイヤ3スイッチのアクセスリスト(ACL)は、ネットワークの基本的なセキュリティを提供します。ACLが設定されていない場合、スイッチを通過するすべてのパケットをネットワークのすべての部分に許可できます。ACLは、ネットワークのさまざまな部分にアクセスできるホストを制御したり、ルータインターフェイスで転送またはブロックされるトラフィックのタイプを決定します。ACLは、着信トラフィック、発信トラフィック、またはその両方をブロックするように設定できます。

例：電子メールトラフィックの転送を許可できますが、ネットワーク外部のTelnetトラフィックは許可できません。

IE3x00のサポートと制限事項：

- VLANアクセスリスト(VACL)は、スイッチ仮想インターフェイス(SVI)ではサポートされません。
- VACLとポートACL(PACL)の両方がパケットに適用される場合、PACLはVACLよりも優先され、この場合はVACLは適用されません。
- VACLあたり最大255のアクセスコントロールエントリ(ACE)。
- TCAMはコンポーネントに分割されないため、TCAMの領域が新しい設定を受け入れるのに十分でないときは常に、エラーがsyslogとともにスローされ、VLANの総数に明確な制限は定義されません。
- Logging は出力ACLではサポートされません。
- レイヤ3 ACLでは、非IP ACLはサポートされません。
- ACLのレイヤ4オペレータ(L4OP)は、ハードウェアによって、UDPの場合は最大8つのL4OP、TCPの場合は最大8つのL4OP、合計16のグローバルL4OPに制限されます。
- **range**演算子は2つのL4OPを消費することに注意してください。

  注：L4OPには次のものがあります。gt（より大きい）、lt（より小さい）、neq（等しくない）、eq（等しい）、range（包含範囲）

- 入力ACLは物理インターフェイスでのみサポートされ、VLAN、ポートチャネルなどの論理インターフェイスではサポートされません。
- ポートACL(PACL)はサポートされており、次の種類があります。非IP、IPv4、およびIPv6です。
- 非IPおよびIPv4 ACLには1つの暗黙フィルタがあり、IPv6 ACLには3つの暗黙フィルタがあります。
- 時間範囲ベースのACLがサポートされます。
- IPv4 ACLとTTL、IPオプションベースの一致はサポートされていません。

トラブルシュート

ステップ1：問題が疑われるACLを**特定**します。ACLのタイプに基づいて、次のコマンドを使用できます。

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
```

コマンド出力の目的は、Cisco IOSの現在のACL設定を特定することです。

ステップ2：ハードウェアエントリテーブルに同じACLが存在することを**確認**します。

show platform hardware acl asic 0 tcam { **all** | **index** | **interface** | **static** | **statistics** | **usage** | **vlan-statistics** } – スイッチのTCAMを確認するために使用できるコマンドオプション。

```
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]
```

ハードウェアテーブルの出力には、次の3つのルールペアがあります。

P：パターンを表す略語= ACE内のIPまたはサブネットです。

分:maskの略で、これらはACEのワイルドカードビットです。

ACEエントリ	インデックス	SIP	ディップ	プロトコル	DSCP
permit udp any any eq 2222	0P、0M、0	0.0.0.0（任意）	0.0.0.0（任意）	0x11	0x00（ベストエフォート）
permit udp any eq 2222 any	1P、1M、1	0.0.0.0（任意）	0.0.0.0（任意）	0x11	0x00（ベストエフォート）
deny ip any any (implicit)	2P、2M、2	0.0.0.0（任意）	0.0.0.0（任意）	0x00	0x00（ベストエフォート）

ACEエントリ	送信元OP	送信元ポート1	送信元ポート2	宛先OP	宛先ポート1	宛先ポート2
permit udp any any eq 2222	------	---------	---------	等分	2222	---------
permit udp any eq 2222 any	EQ	2222	---------	---------	---------	---------
deny ip any any (implicit)	------	---------	---------	---------	---------	---------

> **注**：マスクエントリの例：hostキーワード= ff.ff.ff.ff、ワイルドカード0.0.0.255 = ff.ff.ff.00、任意のキーワード= 00.00.00.00

Index：ルールの番号。この例では、0、1、2のインデックスがあります。

SIP：送信元IPを16進形式で示します。ルールには「any」キーワードがあるため、送信元IPはすべて0です。

DIP：宛先IPを16進形式で示します。ルール内の「any」キーワードは、すべて0に変換されます。

Protocol:ACEのプロトコルを示します。0x11はUDP用です。

> **注**：既知のプロトコルのリスト：0x01:ICMP、0x06:TCP、0x11:UDP、0x29:IPv6。

DSCP：ルールに存在するDiffServコードポイント(DSCP)。指定しない場合の値は0x00（ベストエフォート）です。

IGMP Type:ACEにIGMPタイプが含まれているかどうかを指定します。

ICMPタイプ：ACEにICMPタイプが含まれるかどうかを指定します。

ICMPコード：ACEにICMPコードタイプが含まれるかどうかを指定します。

TCPフラグ：ACEにTCPフラグがあるかどうかを指定します。

Src OP：ルールで使用される送信元L4OPを示します。最初のACEエントリには何もありません

。2番目のACEエントリの演算子はEQです。

Src port1:ACEがUDPまたはTCPベースの場合は、最初の送信元ポートを示します。

Src port2:ACEがUDPまたはTCPベースの場合は、2番目の送信元ポートを示します。

Dst OP：ルールで使用される宛先L4OPを示します。最初のACEエントリは演算子としてEQを持ち、2番目のACEエントリにはEQがありません。

Dst port1:ACEがUDPまたはTCPベースの場合に、最初の宛先ポートを示します。

Dst port2:ACEがUDPまたはTCPベースの場合は、2番目の宛先ポートを示します。

ルールはポートにバインドされる **ACL:<0,x>** 0はASIC = 0を表し、XはASICポート番号= 1に対応します。

また、ACEステートメントごとに実行されたアクションを表で確認することもできます。

ACEインデックス	アクション
0	ASIC_ACL_PERMIT [1]
1	ASIC_ACL_PERMIT [1]
0	ASIC_ACL_DENY[0]

ステップ3：同じACLエントリを、次に示す異なるコマンドで**確認**します。

特定のインデックスのACLエントリ

show platform hardware acl asic 0 tcam index *acl_id* **[detail]** – このコマンドは、特定のACL IDの下のルールのリストを表示します。

```
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]
```

Here index は、TCAMでルールがプログラムされるオフセットです。

使用されているACLインデックスを確認するには、ACLが適用されているポートを特定し、コマンドを使用する必要があります show platform hardware acl asic 0 tcam interface *interface_name* ipv4 detailACL ID番号を取得します。

> **注**：このコマンドでは、ASIC/ポートマッピングは表示されないことに注意してください。また、同じACLを異なるインターフェイスに適用すると、TCAMは異なるACL IDエントリを作成します。これは、TCAMスペース内の異なるインターフェイスに適用される同じACLに対するインデックスの再利用がないことを意味します。

ハードウェアにプログラムされたACLエントリ

show platform hardware acl asic 0 tcam all [detail] - TCAMのすべての情報を表示します。

```
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]
```

この出力には、ハードウェアテーブルに格納されているすべてのACL IDが表示されます。2つの別個のACL ID(45、46)がありますが、各ブロックの構造はまったく同じです。これは、両方のACL IDがソフトウェアで設定された同じACLに属していることを示しています。

```
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
```

異なるインターフェイスに適用されます。

```
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の使用

show platform hardware acl asic 0 tcam usage – このコマンドは、ASICでのACLの使用状況を表示します。IE3x00には1つのASIC(0)しかありません。

```
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の幅は24バイトです。拡張ACEの幅は48バイトです。Ultra ACEの幅は72バイトです。

ACLスタティックエントリ

show platform hardware acl asic 0 tcam static [detail] – スタティックACLの設定を表示します（制御プロトコル固有）。

```
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.
```

このコマンド出力には、スイッチのさまざまな制御プロトコルに関するシステムプログラムACLエントリが表示されます。

ACL統計情報

show platform hardware acl asic 0 tcam statistics *interface_name* - ACL統計情報をリアルタイムで表示します。カウンタは累積されません。コマンドを最初に表示した後、ACLにヒットするトラフィックが

停止すると、カウンタがリセットされます。

```
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
```

このコマンドを使用すると、指定したインターフェイスでACLに対して許可でヒットした回数と、トラフィックがポートにアクティブにエンキューされている間にヒットしたドロップ数がわかります。コマンドが初めて表示されると、カウンタがリセットされます。

> **ヒント**：コマンドを実行するたびにカウンタがリセットされるため、コマンドを何度か実行し、累積的なpermit/dropカウンタに対する以前の出力を記録しておくことをお勧めします。

ポートからASICへのマッピング

show platform pm port-map – スイッチのすべてのインターフェイスのASIC/ポートマッピングを表示します。

```
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**

デバッグ コマンド

debug platform acl all – このコマンドは、すべてのACLマネージャイベントを有効にします。

```
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 – ハードウェアアブストラクションレイヤ(HAL)関連のイベントを表示します。

インターフェイスでのACLの削除/適用イベントでは、ルールがハードウェアでプログラムされているかどうかを表示し、その情報をコンソールに表示します。

```
[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 =インバウンド（ACLは入力で適用された）

方向1 =アウトバウンド（ACLは出力側に適用された）

debug platform acl ipv4 - ACL IPv4関連イベントを表示します。

debug platform acl ipv6- ACL IPv6関連イベントを表示します。

debug platform acl mac - ACL MAC関連イベントを表示します。

debug platform acl error - ACLエラー関連イベントを表示します。

```
[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 - ACL Order Dependent Merge(ODM)関連のイベントを表示します。

```
[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 – ポートACL関連イベントを表示します。

```
[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 - ACL Value Mask Result(VMR)関連のイベントを表示します。VMRに問題がある場合は、ここで確認できます。

```
[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>
```

一般的な問題

L4OP枯渇

L4OPsのコンパレータの枯渇は、次のデバッグをイネーブルにした後で確認できます。

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

> **注：**debugコマンドは、スイッチのログバッファに情報を表示しません。代わりに、情報がshow platform software trace message ios R0コマンドが表示されない場合もあります。

show platform software trace message ios R0コマンドを実行して、デバッグ情報を表示します。

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] :
```

IE3x00の場合、UDPには8 L4OP、TCPには8 L4OPの制限があり、スイッチに実装されているすべてのACLで最大16 L4OPの制限があります。（制限はACLごとではなく、グローバルです）。

注：現在、CLIには、消費された空き比較器の量を確認するコマンドはありません。

この問題が発生した場合：

- エラーがL4OPの制限に関連しているかどうかをdebugコマンドで確認します。
- ACLで使用するL4OPの数を減らす必要があります。各rangeコマンドは、2つのポートコンパレータを消費します。
- rangeコマンドでACEを使用できる場合は、代わりにeqキーワードを使用するように変換できるため、UDPおよびTCPで使用可能なL4OPは消費されません。次に例を示します。

ライン：
permit tcp any any range 55560 55567

次のようなメリットがあります。
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

Cisco Bug ID CSCv07745を参照してください。内部バグ情報にアクセスできるのは、登録ユーザだけです。

レイヤ4 ACLはTCAMに集約されない

連続するIPアドレスやポート番号を持つL4 ACLを入力すると、スペースを節約するために、これらがTCAMに書き込まれる前にシステムによって自動的に集約されます。システムは、ACLエントリに基づいて最善を尽くし、可能な範囲のエントリをカバーするように適切なMVRで集約します。これは、TCAMを確認し、ACL用にプログラムされている行の数を確認することで確認できます。つまり、次のようになります。

```
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>
```

問題は、マスク値が正しく読み取られないため、（例のACLで）実際にプログラムされる唯一のエントリが **permit tcp any any eq 8,**これはトップレベル集約ACLであるため。0.0.0.3のマスクが正しく読み取られないため、ポート番号9 ~ 11のエントリは表示されません。

Cisco Bug ID CSCvx66354（登録ユーザ専用）を参照してください。内部バグ情報にアクセスできるのは、登録済みのシスコユーザだけです。

TAC用に収集するコマンド

このガイドでは、IE3x00のアクセスリストに関連する最も一般的な問題と、適切な修復手順について説明します。ただし、このガイドで問題が解決しなかった場合は、表示されているコマンドリストを収集し、TACサービスリクエストに添付してください。

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
```

ファイルをスイッチからコピーし、TACケースにアップロードします。

テクニカルサポートIE3x00プラットフォームでACLに関連する問題をトラブルシューティングす

る場合は、ACL出力が出発点として必要です。

関連情報

- Cisco Catalyst IE3x00 Rugged、IE3400 Rugged、IE3400 Heavy Duty、およびESS3300シリーズスイッチ、Cisco IOS XE Gibraltar 16.12.xのリリースノート
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。