IE3x00의 액세스 목록 문제 해결

목차

소개

이 문서에서는 Industrial Ethernet 3x00 Series에서 ACL(Access Control List) 항목 및 하드웨어 제한을 트러블슈팅하고 확인하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

ACL 컨피그레이션에 대한 기본 지식이 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco IOS® XE 소프트웨어 버전 16.12.4의 IE-3300을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 문서는 다음 하드웨어 버전에서도 사용할 수 있습니다.

1. IE-3200(고정)
2. IE-3300(모듈형)
3. IE-3400(고급 모듈형).

배경 정보

레이어 3 스위치의 액세스 목록(ACL)은 네트워크에 대한 기본 보안을 제공합니다. ACL을 구성하지 않으면 스위치를 통과하는 모든 패킷이 네트워크의 모든 부분에 허용됩니다. ACL은 어떤 호스트가 네트워크의 서로 다른 부분에 액세스할 수 있는지 또는 어떤 유형의 트래픽이 라우터 인터페이스에서 전달 또는 차단되는지를 결정합니다. 인바운드 트래픽, 아웃바운드 트래픽 또는 둘 모두를 차단하도록 ACL을 구성할 수 있습니다.

예: 이메일 트래픽의 전달을 허용할 수 있지만 네트워크 외부의 텔넷 트래픽은 허용할 수 없습니다.

IE3x00 지원 및 제한 사항:

- VACL(VLAN Access List)은 SVI(Switch Virtual Interface)에서 지원되지 않습니다.
- VACL과 포트 ACL(PACL)이 모두 패킷에 적용 가능한 경우 PACL이 VACL보다 우선하며, 이러한 경우 VACL이 적용되지 않습니다.
- VACL당 최대 255개의 ACE(Access Control Entries)
- 총 VLAN에 대한 명시적 제한이 정의되지 않습니다. TCAM이 구성 요소에 새겨지지 않기 때문에 TCAM의 충분한 공간이 새로운 구성을 수용할 수 없을 때마다 syslog와 함께 오류가 발생합니다.
- Logging 이그레스 ACL에서는 지원되지 않습니다.
- 레이어 3 ACL에서는 비 IP ACL이 지원되지 않습니다.
- ACL의 L4OP(Layer 4 Operator)는 하드웨어에 의해 UDP의 경우 최대 8개의 L4OP, TCP의 경우 최대 8개의 L4OP(총 16개의 전역 L4OP)로 제한됩니다.
- **범위** 연산자는 2개의 L4OP를 소비합니다.

  참고: L4OP에는 다음이 포함됩니다. gt(보다 큼), lt(보다 작음), neq(같지 않음), eq(같음), 범위(포함 범위)

- 인그레스 ACL은 물리적 인터페이스에서만 지원되며 VLAN, 포트 채널 등과 같은 논리적 인터페이스에서는 지원되지 않습니다.
- PACL(Port ACL)은 지원되며 다음과 같을 수 있습니다. 비 IP, IPv4 및 IPv6.
- 비 IP 및 IPv4 ACL에는 1개의 암시적 필터가 있는 반면 IPv6 ACL에는 3개의 암시적 필터가 있습니다.
- 시간 범위 기반 ACL이 지원됩니다.
- TTL이 있는 IPv4 ACL, IP 옵션 기반 일치는 지원되지 않습니다.

문제 해결

1단계. **문제**가 의심되는 ACL을 확인합니다. ACL의 유형에 따라 다음 명령을 사용할 수 있습니다.

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
```

명령 출력의 목적은 Cisco IOS의 현재 ACL 컨피그레이션을 식별하는 것입니다.

2단계. 하드웨어 항목 테이블에 동일한 ACL이 있는지 **확인합니다**.

show platform hardware acl asic 0 tcam { **all** | **index** | **interface** | **static** | **statistics** | **usage** | **vlan-statistics** } - 스위치의 TCAM을 확인하는 데 사용할 수 있는 명령 옵션입니다.

```
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]
```

하드웨어 테이블 출력에는 다음과 같은 세 가지 규칙 쌍이 있습니다.

P: 패턴 = ACE의 IP 또는 서브넷입니다.

M: mask = 는 ACE의 와일드카드 비트입니다.

ACE 항목	색인	SIP	복각	프로토콜	DSCP
permit udp any any eq 2222	0P, 0M, 0	0.0.0.0(모두)	0.0.0.0(모두)	0x11	0x00(최선형)
permit udp any eq 2222 any	1P, 1M, 1	0.0.0.0(모두)	0.0.0.0(모두)	0x11	0x00(최선형)
deny ip any any (implicit)	2P, 2M, 2	0.0.0.0(모두)	0.0.0.0(모두)	0x00	0x00(최선형)

ACE 항목	소스 OP	소스 포트1	소스 포트2	Dst OP	Dst 포트1	Dst 포트2
permit udp any any eq 2222	------	---------	---------	EQ.	2222	---------
permit udp any eq 2222 any	EQ	2222	---------	---------	---------	---------
deny ip any any (implicit)	------	---------	---------	---------	---------	---------

참고: 마스크 항목의 예: host 키워드 = ff.ff.ff.ff, wildcard 0.0.0.255 = ff.ff.ff.00, any 키워드 = 00.00.00.00

Index - 규칙의 번호입니다. 예제에는 0, 1, 2개의 인덱스가 있습니다.

SIP - 소스 IP를 16진수 형식으로 나타냅니다. 규칙에는 'any' 키워드가 있으므로 소스 IP는 모두 0입니다.

DIP - 16진수 형식의 대상 IP를 나타냅니다. 규칙의 'any' 키워드는 모두 0으로 변환됩니다.

Protocol - ACE의 프로토콜을 나타냅니다. 0x11은 UDP에 적용됩니다.

참고: 잘 알려진 프로토콜 목록: 0x01 - ICMP, 0x06 - TCP, 0x11 - UDP, 0x29 - IPv6.

DSCP - 규칙에 DSCP(Differentiated Services Code Point)가 있습니다. 지정하지 않은 경우 값은 0x00(best effort)입니다.

IGMP Type(IGMP 유형) - ACE에 IGMP 유형이 포함되는지 여부를 지정합니다.

ICMP Type(ICMP 유형) - ACE에 ICMP 유형이 포함되는지 여부를 지정합니다.

ICMP Code - ACE에 ICMP 코드 유형이 포함되는지 여부를 지정합니다.

TCP Flags - ACE에 TCP 플래그가 있는지 여부를 지정합니다.

Src OP - 규칙에 사용된 소스 L4OP를 나타냅니다. 첫 번째 ACE 항목에 없습니다. 두 번째 ACE 항목은 EQ를 연산자로 가집니다.

Src port1 - ACE가 UDP 또는 TCP 기반인 경우 첫 번째 소스 포트를 나타냅니다.

Src port2 - ACE가 UDP 또는 TCP 기반인 경우 두 번째 소스 포트를 나타냅니다.

Dst OP - 규칙에 사용된 대상 L4OP를 나타냅니다. 첫 번째 ACE 엔트리에는 EQ가 연산자로 있고 두 번째 ACE 엔트리에는 없습니다.

Dst port1 - ACE가 UDP 또는 TCP 기반인 경우 첫 번째 목적지 포트를 나타냅니다.

Dst port2 - ACE가 UDP 또는 TCP 기반인 경우 두 번째 목적지 포트를 나타냅니다.

규칙은 포트에 바인딩됩니다. **ACL:<0,x>** 여기서 0은 ASIC = 0을 나타내고 X는 ASIC 포트 번호 = 1에 매핑됩니다.

표에서 ACE별로 수행한 Action(작업) 명령문도 확인할 수 있습니다.

ACE 인덱스	작업
0	ASIC_ACL_PERMIT [1]
1	ASIC_ACL_PERMIT [1]
2	ASIC_ACL_DENY[0]

3단계. **다음**에 나열된 서로 다른 명령으로 동일한 ACL 항목을 확인합니다.

지정된 인덱스의 ACL 항목

show platform hardware acl asic 0 tcam index *acl_id* **[detail]** - 이 명령은 특정 ACL ID 아래의 규칙 목록을 표시합니다.

```
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]
```

여기 index TCAM에서 규칙이 프로그래밍되는 오프셋입니다.

어떤 ACL 인덱스가 사용되는지 확인하려면 ACL이 적용되는 포트를 식별하고 명령을 사용해야 합니다 show platform hardware acl asic 0 tcam interface *인터페이스 이름* ipv4 detailACL ID 번호를 가져옵니다.

참고: 이 명령은 ASIC/포트 매핑을 표시하지 않습니다. 또한 동일한 ACL을 다른 인터페이스에 적용할 경우 TCAM은 다른 ACL ID 항목을 생성합니다. 즉, TCAM 공간의 다른 인터페이스에 적용되는 동일한 ACL에 대한 인덱스 재사용이 없습니다.

하드웨어에 프로그래밍된 ACL 항목

show platform hardware acl asic 0 tcam all [detail] - TCAM에 대한 모든 정보를 표시합니다.

```
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]
```

이 출력은 하드웨어 테이블에 저장된 모든 ACL ID를 표시합니다. 두 개의 개별 ACL ID(45, 46)가 있지만 각 블록의 구조는 정확히 동일합니다. 이는 두 ACL ID가 소프트웨어에 구성된 동일한 ACL에 속함을 나타냅니다.

```
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
```

다른 인터페이스에 적용됩니다.

```
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 사용

show platform hardware acl asic 0 tcam usage - 이 명령은 ASIC에서 ACL 사용량을 표시합니다. IE3x00에는 하나의 ASIC(0)만 있음

```
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
```

표준 ACE는 24바이트 폭입니다. Extended ACE는 48바이트 너비입니다. Ultra ACE는 72바이트 너비입니다.

ACL 정적 항목

show platform hardware acl asic 0 tcam static [detail]- 정적 ACL 컨피그레이션(제어 프로토콜별)을 표시합니다.

```
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.
```

이 명령 출력은 스위치의 서로 다른 제어 프로토콜에 대한 시스템 프로그래밍 ACL 엔트리를 표시합니다.

ACL 통계

show platform hardware acl asic 0 tcam statistics *interface_name* - ACL 통계를 실시간으로 표시합니다. 카운터는 누적되지 않습니다. 명령을 처음 표시한 후 ACL에 도달하는 트래픽이 중단되면 카운터가 재설정됩니다.

```
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
```

이 명령은 지정된 인터페이스의 ACL에 대해 Permit에서 발생한 적중 수 및 트래픽이 포트에서 대기 중인 동안 적중된 삭제 수를 알려줍니다. 명령이 처음으로 표시되면 카운터가 재설정됩니다.

> **팁:** 카운터는 명령을 실행할 때마다 재설정되므로, 명령을 여러 번 실행하고 누적 허용/삭제 카운터에 대해 이전 출력의 레코드를 유지하는 것이 좋습니다.

포트-ASIC 매핑

show platform pm port-map - 스위치의 모든 인터페이스에 대한 ASIC/포트 매핑을 표시합니다.

```
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**

디버그 명령

debug platform acl all - 이 명령은 모든 ACL 관리자 이벤트를 활성화합니다.

```
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 - HAL(Hardware Abstraction Layer) 관련 이벤트를 표시합니다.

인터페이스에서 ACL 제거/적용 이벤트의 경우 규칙이 하드웨어에서 프로그래밍되었는지 여부를 표시하고 콘솔에서 정보를 인쇄합니다.

```
[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
```

방향 0 = 인바운드(인그레스에 ACL이 적용됨)

방향 1 = 아웃바운드(ACL이 이그레스에 적용됨)

debug platform acl ipv4 - ACL IPv4 관련 이벤트를 표시합니다.

debug platform acl ipv6- ACL IPv6 관련 이벤트를 표시합니다.

debug platform acl mac - ACL MAC 관련 이벤트를 표시합니다.

debug platform acl error - ACL 오류 관련 이벤트를 표시합니다.

```
[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 ODM(Order Dependent Merge) 관련 이벤트를 표시합니다.

```
[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 - 포트 ACL 관련 이벤트를 표시합니다.

```
[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 VMR(Value Mask Result) 관련 이벤트를 표시합니다. VMR에 문제가 있는 경우 여기에서 확인할 수 있습니다.

```
[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>
```

일반적인 문제

L4OP 소모

다음 디버그를 활성화한 후 L4OPs 비교기 소진을 식별할 수 있습니다.

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

> **참고:** debug 명령은 스위치의 로그 버퍼에 정보를 표시하지 않습니다. 대신, 이 정보는 show platform software trace message ios R0명령을 실행합니다.

디버그의 정보를 표시하려면 **show platform software trace message ios R0** 명령을 실행합니다.

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] :
```

IE3x00의 경우 스위치에 구현된 모든 ACL에서 최대 총 16개의 L4OP에 대해 UDP의 경우 8개의 L4OP, TCP의 경우 8개의 L4OP로 제한됩니다. (ACL이 아닌 전역 제한)

참고: 현재 CLI에서 소비된/사용 가능한 비교기의 양을 확인할 수 있는 명령이 없습니다.

이 문제가 발생하는 경우:

- 오류가 L4OP 제한과 관련된 경우 debug 명령을 확인합니다.
- ACL에서 사용 중인 L4OP의 수를 줄여야 합니다. 각 range 명령은 2개의 포트 비교기를 사용합니다.
- **range 명령**과 함께 ACE를 사용할 수 있는 경우 이러한 ACE는 **eq 키워드를** 사용하도록 변환할 수 있으므로 UDP 및 TCP에 사용 가능한 L4OP를 사용하지 않습니다. 즉,

줄:
permit tcp any any range 55560 55567

다음과 같이 전환할 수 있습니다.
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 버그 ID CSCv07745를 참조하십시오. 등록된 Cisco 사용자만 내부 버그 정보에 액세스할 수 있습니다.

레이어 4 ACL은 TCAM에 요약되지 않음

연속 IP 주소 및/또는 포트 번호를 포함한 L4 ACL을 입력하면 공간을 절약하기 위해 TCAM에 기록되기 전에 시스템이 자동으로 요약합니다. 시스템은 ACL 항목을 기준으로 최선을 다해 적절한 MVR을 사용하여 요약함으로써 가능한 범위의 항목을 다룹니다. TCAM을 확인하고 ACL에 대해 프로그래밍된 라인 수를 확인할 수 있습니다. 즉,

```
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>
```

문제는 마스크 값이 제대로 읽히지 않아서 (예제의 ACL로) 실제로 프로그래밍되는 유일한 항목은 다음과 같습니다 **permit tcp any any eq 8,**최상위 요약 ACL입니다. 0.0.0.3의 마스크가 제대로 읽히지 않아 포트 번호 9-11의 항목이 표시되지 않습니다.

Cisco 버그 ID CSCvx66354를 참조하십시오. 등록된 Cisco 사용자만 내부 버그 정보에 액세스할 수 있습니다.

TAC를 위해 수집할 명령

IE3x00의 액세스 목록과 관련된 가장 일반적인 문제는 이 가이드에서 적절한 치료 단계를 통해 다룹니다. 그러나 이 설명서에서 문제를 해결하지 못한 경우 표시된 명령 목록을 수집하여 TAC 서비스 요청에 첨부하십시오.

초how 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
```

스위치에서 파일을 복사하여 TAC 케이스에 업로드합니다.

IE3x00 플랫폼에서 ACL과 관련된 문제를 트러블슈팅할 때 기술 지원 ACL 출력이 시작점으로 필요합니다.

관련 정보

- Cisco Catalyst IE3x00 Rugged, IE3400 Rugged, IE3400 Heavy Duty 및 ESS3300 Series 스위치, Cisco IOS XE Gibraltar 16.12.x 릴리스 정보
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.