Fehlerbehebung bei Zugriffslisten im IE3x00

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung und Überprüfung von Zugriffskontrolllisten (ACL)-Einträgen und Hardware-Beschränkungen für die Industrial Ethernet 3x00-Serie beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie Grundkenntnisse der ACL-Konfiguration haben.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem IE-3300 mit der Cisco IOS® XE Software-Version 16.12.4.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Verwandte Produkte

Dieses Dokument kann auch mit folgenden Hardwareversionen verwendet werden:

1. IE-3200 (fest)
2. IE-3300 (modular)
3. IE-3400 (erweiterte modulare Bauweise)

Hintergrundinformationen

Zugriffslisten (ACLs) auf einem Layer-3-Switch bieten grundlegende Sicherheit für Ihr Netzwerk. Wenn keine ACLs konfiguriert sind, können alle Pakete, die den Switch passieren, in alle Teile des Netzwerks übertragen werden. ACLs steuern, welche Hosts auf verschiedene Teile eines Netzwerks zugreifen können oder entscheiden, welche Arten von Datenverkehr an den Router-Schnittstellen weitergeleitet oder blockiert werden. ACLs können so konfiguriert werden, dass eingehender und/oder ausgehender Datenverkehr blockiert wird.

Beispiel: Sie können die Weiterleitung von E-Mail-Verkehr zulassen, jedoch keinen Telnet-Verkehr außerhalb des Netzwerks.

Unterstützung und Einschränkungen für IE3x00:

- VLAN-Zugriffslisten (VACLs) werden auf der Switch Virtual Interface (SVI) nicht unterstützt.
- Wenn VACL und Port ACL (PACL) für ein Paket gelten, hat PACL Vorrang vor VACL, und VACL wird in diesem Fall nicht angewendet.
- Max. 255 Access Control Entries (ACE) pro VACL.
- Es wurde keine explizite Beschränkung für die Gesamtzahl der VLANs definiert. Da TCAM nicht in die Komponenten unterteilt ist, wird ein Fehler mit einem Syslog ausgelöst, wenn nicht genügend Speicherplatz im TCAM zur Verfügung steht, um die neue Konfiguration zu akzeptieren.
- Logging wird auf der Ausgangs-ACL nicht unterstützt.
- Auf Layer-3-ACLs wird keine Nicht-IP-ACL unterstützt.
- Layer-4-Operator (L4OP) in ACLs wird durch die Hardware auf maximal 8 L4OP für UDP und 8 L4OP für TCP begrenzt, sodass insgesamt 16 L4OP global sind.
- Beachten Sie, dass der **Range** Operator 2 L4OP verbraucht.

  Anmerkung: Zu den L4OP gehören: gt (größer als), lt (kleiner als), neq (ungleich), eq (gleich), Bereich (einschließlich Bereich)

- Eingangs-ACLs werden nur auf physischen Schnittstellen unterstützt, nicht jedoch auf logischen Schnittstellen wie VLAN, Port-Channel usw.
- Port-ACLs (PACLs) werden unterstützt und können: Nicht-IP, IPv4 und IPv6.
- Für Nicht-IP- und IPv4-ACLs gibt es einen impliziten Filter, für IPv6-ACLs drei implizite Filter.
- Zeitbereichsbasierte Zugriffskontrolllisten werden unterstützt.
- IPv4-ACL mit TTL, Übereinstimmung basierend auf IP-Optionen wird nicht unterstützt.

Fehlerbehebung

Schritt 1: **Identifizieren** Sie die ACL, bei der Sie Probleme vermuten. Je nach ACL-Typ stehen die folgenden Befehle zur Verfügung:

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
```

Die Befehlsausgaben dienen dazu, die aktuelle ACL-Konfiguration in Cisco IOS zu identifizieren.

Schritt 2: Überprüfen Sie, ob die gleiche ACL in der Hardware-Eintragstabelle vorhanden ist.

show platform hardware acl asic 0 tcam { **all** | **index** | **interface** | **static** | **statistics** | **usage** | **vlan-statistics** } - Verfügbare Befehlsoptionen zum Überprüfen des TCAM des Switches

```
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]
```

In der Ausgabe der Hardwaretabelle gibt es drei Regelpaare, aus denen:

P: Steht für Muster = dies sind die IPs oder Subnetze im ACE.

M: Steht für Maske = Dies sind die Platzhalterbits im ACE.

ACE-Eintrag	Index	SIP	DIP	Protokolle	DSCP
permit udp any any eq 2222	0P, 0M, 0	0.0.0.0 (beliebige)	0.0.0.0 (beliebige)	0 x 11	0x00 (bestmögliche Leistung)
permit udp any eq 2222 any	1 P, 1 M, 1	0.0.0.0 (beliebige)	0.0.0.0 (beliebige)	0 x 11	0x00 (bestmögliche Leistung)
deny ip any any (implicit)	2P, 2M, 2	0.0.0.0 (beliebige)	0.0.0.0 (beliebige)	0x00	0x00 (bestmögliche Leistung)

ACE-Eintrag	Quelle OP	Quellport1	Quellport2	Ziel OP	Ziel-Port1	Ziel-Port 2
permit udp any any eq 2222	------	---------	---------	EQ:	2222	---------
permit udp any eq 2222 any	EQ	2222	---------	---------	---------	---------
deny ip any any (implicit)	------	---------	---------	---------	---------	---------

> **Anmerkung:** Beispiele für Maskeneinträge: host-Schlüsselwort = ff.ff.ff.ff, Platzhalter 0.0.0.255 = ff.ff.ff.00, beliebiges Schlüsselwort = 00.00.00.00

Index - Nummer der Regel Im Beispiel gibt es den Index 0, 1 und 2.

SIP - gibt die Quell-IP im HEX-Format an. Da die Regeln das Schlüsselwort "any" haben, ist die Quell-IP alle Nullen.

DIP - Zeigt die Ziel-IP im HEX-Format an. Das Schlüsselwort "any" in der Regel wird in alle Nullen übersetzt.

Protokoll - Gibt das Protokoll der ACEs an. 0x11 für UDP.

> **Anmerkung:** Liste bekannter Protokolle: 0x01 - ICMP, 0x06 - TCP, 0x11 - UDP, 0x29 - IPv6.

DSCP: Differentiated Services Code Point (DSCP) in der Regel Ohne Angabe ist der Wert 0x00 (bestmögliche Leistung).

IGMP Type (IGMP-Typ): Gibt an, ob der ACE IGMP-Typen enthält.

ICMP Type - Gibt an, ob der ACE ICMP-Typen enthält.

ICMP-Code - Gibt an, ob der ACE ICMP-Codetypen enthält.

TCP-Flags - Gibt an, ob der ACE über TCP-Flags verfügt.

Src OP - Gibt die Quelle L4OP in der Regel verwendet. Im ersten ACE-Eintrag ist keiner vorhanden. Der zweite ACE-Eintrag hat EQ als Operator.

Src port1 - Gibt den ersten Quellport an, wenn der ACE UDP- oder TCP-basiert ist.

Src port2 - Zeigt den zweiten Quellport an, wenn der ACE UDP- oder TCP-basiert ist.

Dst OP - Zeigt das Ziel L4OP in der Regel verwendet. Der erste ACE-Eintrag hat EQ als Operator, im zweiten ACE-Eintrag ist keiner vorhanden.

Dst port1 - Gibt den ersten Zielport an, wenn der ACE UDP- oder TCP-basiert ist.

Dst port2 - Gibt den zweiten Zielport an, wenn der ACE UDP- oder TCP-basiert ist.

Regeln werden an Port gebunden **ACL:<0,x>** wobei 0 für ASIC = 0 und X für ASIC-Portnummer = 1 steht.

Sie können auch die Aktion sehen, die per ACE-Anweisung in der Tabelle durchgeführt wurde.

ACE-Index	Aktion
0	ASIC_ACL_PERMIT [1]
1	ASIC_ACL_PERMIT [1]
2	ASIC_ACL_DENY[0]

Schritt 3: **Überprüfen Sie** die gleichen ACL-Einträge mit den folgenden Befehlen:

ACL-Einträge in einem bestimmten Index

show platform hardware acl asic 0 tcam index *acl_id* **[detail]** - Dieser Befehl zeigt die Liste der Regeln unter der jeweiligen ACL-ID an.

```
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]
```

Hier index ist der Offset, bei dem die Regel im TCAM programmiert wird.

Um zu überprüfen, welcher ACL-Index verwendet wird, müssen Sie den Port identifizieren, auf den die ACL angewendet wird, und den Befehl show platform hardware acl asic 0 tcam interface *Schnittstellenname* ipv4 detailum die ACL-ID-Nummer zu erhalten.

> **Anmerkung:** Beachten Sie, dass bei diesem Befehl die ASIC/Port-Zuordnung nicht angezeigt wird. Wenn Sie dieselbe ACL auf verschiedene Schnittstellen anwenden, erstellt der TCAM außerdem einen anderen Eintrag für die ACL-ID. Das bedeutet, dass für dieselbe ACL keine Indexwiederverwendung für verschiedene Schnittstellen im TCAM-Bereich erfolgt.

Hardwareprogrammierte ACL-Einträge

show platform hardware acl asic 0 tcam all [detail] - Zeigt alle Informationen zum TCAM an.

```
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]
```

Diese Ausgabe zeigt alle in der Hardwaretabelle gespeicherten ACL-IDs an. Es gibt zwei separate ACL-IDs (45, 46), jedoch ist die Struktur jedes Blocks identisch. Dies weist darauf hin, dass beide ACL-IDs zu derselben ACL gehören, die in der Software konfiguriert wurde:

```
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
```

Die auf verschiedene Schnittstellen angewendet wird.

```
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-Nutzung

show platform hardware acl asic 0 tcam usage - Mit diesem Befehl wird die ACL-Verwendung im ASIC angezeigt. IE3x00 verfügt nur über einen 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
```

Standard-ACE ist 24 Byte breit; Der erweiterte ACE ist 48 Byte breit. Ultra ACE ist 72 Byte breit.

Statische ACL-Einträge

show platform hardware acl asic 0 tcam static [detail]- Zeigt statische ACL-Konfigurationen an (je nach Steuerungsprotokoll).

```
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.
```

Mit diesem Befehl werden die vom System programmierten ACL-Einträge für verschiedene Steuerungsprotokolle des Switches angezeigt.

ACL-Statistik

show platform hardware acl asic 0 tcam statistics *interface_name* - Zeigt ACL-Statistiken in Echtzeit an. Der Zähler ist nicht kumulativ. Nachdem Sie den Befehl zum ersten Mal angezeigt haben, werden die Zähler zurückgesetzt, wenn der Datenverkehr, der die ACL erreicht, stoppt.

```
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
```

Dieser Befehl gibt an, wie viele Treffer in der Zugriffskontrollliste auf der angegebenen Schnittstelle aufgetreten sind und wie viele Löschvorgänge ausgeführt wurden, während der Datenverkehr aktiv in die Warteschlange des Ports eingebunden ist. Die Zähler werden zurückgesetzt, sobald der Befehl zum ersten Mal angezeigt wurde.

> **Tipp:** Da die Zähler nach jedem Ausführen des Befehls zurückgesetzt werden, wird empfohlen, den Befehl mehrmals auszuführen und die vorherigen Ausgaben für einen kumulativen Erlaubniszähler/Drop-Zähler aufzuzeichnen.

Zuordnung von Port zu ASIC

show platform pm port-map - Zeigt die ASIC/Port-Zuordnung für alle Schnittstellen des Switches an.

```
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**

Debugbefehle

debug platform acl all - Mit diesem Befehl werden alle ACL-Manager-Ereignisse aktiviert.

```
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 - Zeigt Ereignisse im Zusammenhang mit der Hardwareabstraktionsschicht (HAL) an.

Bei einem Ereignis zum Entfernen/Anwenden einer ACL auf einer Schnittstelle wird angezeigt, ob die Regel in der Hardware programmiert wurde, und die Informationen werden in der Konsole ausgegeben.

```
[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
```

Richtung 0 = Eingehend (ACL wurde am Eingang angewendet)

Richtung 1 = Ausgehend (ACL wurde am Ausgang angewendet)

debug platform acl ipv4 - Zeigt Ereignisse in Zusammenhang mit ACL IPv4 an.

debug platform acl ipv6- Zeigt Ereignisse in Zusammenhang mit ACL IPv6 an.

debug platform acl mac - Zeigt Ereignisse im Zusammenhang mit ACL MAC an.

debug platform acl error - Zeigt Ereignisse im Zusammenhang mit ACL-Fehlern an.

```
[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 - Zeigt ODM-bezogene Ereignisse (ACL Order Dependant Merge) an.

```
[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 - Zeigt Ereignisse im Zusammenhang mit Port-ACLs an.

```
[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 - Zeigt Ereignisse im Zusammenhang mit dem ACL Value Mask Result (VMR) an. Wenn Probleme mit VMR auftreten, können Sie diese hier sehen.

```
[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>
```

Häufige Probleme

L4OP Erschöpfung

L4OPs Komparator-Erschöpfung kann identifiziert werden, nachdem Sie diese Debugs aktivieren:

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

> **Anmerkung:** Die Debug-Befehle zeigen keine Informationen im Protokollpuffer des Switches an. Stattdessen werden die Informationen im show platform software trace message ios R0aus.

Führen Sie den Befehl **show platform software trace message ios R0 aus**, um die Informationen zu den Debugs anzuzeigen.

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] :
```

Für den IE3x00 gibt es eine Grenze von 8 L4OP für UDP und 8 L4OP für TCP, für eine maximale Summe von 16 L4OP in allen in den Switch implementierten ACLs. (Die Einschränkung gilt global und nicht pro ACL).

> **Anmerkung:** Derzeit ist kein Befehl verfügbar, um die Anzahl der verbrauchten/freien Vergleichswerte in der CLI zu überprüfen.

Wenn dieses Problem auftritt:

- Überprüfen Sie mit den Debug-Befehlen, ob die Fehler mit der L4OP-Einschränkung in Zusammenhang stehen.
- Sie müssen die Anzahl der L4OP in der ACL reduzieren. Jeder Bereichsbefehl benötigt 2 Port-Komparatoren.
- Wenn Sie ACEs mit dem **Range-**Befehl verwenden können, können diese stattdessen in **eq-**Schlüsselwörter konvertiert werden, sodass das für UDP und TCP verfügbare L4OP nicht verwendet wird, d. h.:

Anschluss:
permit tcp any any range 55560 55567

Ergebnis:
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

Unter der Bug-ID "CSCv07745" von Cisco können nur registrierte Benutzer auf interne Bug-Informationen zugreifen.

Layer-4-ACLs werden im TCAM nicht zusammengefasst

Wenn L4-ACLs mit aufeinander folgenden IP-Adressen und/oder Port-Nummern eingegeben werden, werden diese vom System automatisch zusammengefasst, bevor sie in TCAM geschrieben werden, um Platz zu sparen. Das System gibt anhand der ACL-Einträge die besten Möglichkeiten vor, um eine Zusammenfassung mit der entsprechenden MVR für eine Reihe von Einträgen zu erstellen, bei denen dies möglich ist. Dies kann überprüft werden, wenn Sie den

TCAM überprüfen und feststellen, wie viele Leitungen für die ACL programmiert wurden. Das heißt:

```
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>
```

Das Problem ist, dass der Maskenwert nicht richtig gelesen wird, sodass der einzige Eintrag, der tatsächlich programmiert wird (mit der ACL im Beispiel), **permit tcp any any eq 8**,da es sich hierbei um die übergeordnete Zusammenfassung handelt. Die Einträge für die Portnummern 9-11 werden nicht angezeigt, da die Maske 0.0.0.3 nicht richtig gelesen wurde.

Weitere Informationen finden Sie unter der Cisco Bug-ID CSCvx66354 . Nur registrierte Cisco Benutzer können auf interne Fehlerinformationen zugreifen.

Zu sammelnde Befehle für TAC

Die häufigsten Probleme im Zusammenhang mit Zugriffslisten auf IE3x00 werden in diesem Leitfaden behandelt, und es werden geeignete Abhilfemaßnahmen ergriffen. Falls Ihr Problem jedoch nicht durch diesen Leitfaden behoben werden konnte, sammeln Sie die angezeigte Befehlsliste, und fügen Sie sie Ihrer TAC-Serviceanfrage bei.

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
```

Kopieren Sie die Datei aus dem Switch und laden Sie sie in das TAC-Ticket hoch.

Die Ausgabe von technischen Support-ACLs ist als Ausgangspunkt für die Fehlerbehebung bei ACL-Problemen in IE3x00-Plattformen erforderlich.

Zugehörige Informationen

- Versionshinweise für Cisco Catalyst Switches der Serien IE3x00 Rugged, IE3400 Rugged, IE3400 Heavy Duty und ESS3300, Cisco IOS XE Gibraltar 16.12.x
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.