Solucionar problemas de listas de acceso en IE3x00

Contenido

Introducción

Este documento describe cómo resolver problemas y verificar entradas de Listas de control de acceso (ACL) y límites de hardware en Industrial Ethernet 3x00 Series.

Prerequisites

Requirements

Cisco recomienda tener conocimientos básicos de la configuración de ACL.

Componentes Utilizados

La información de este documento se basa en IE-3300 con la versión 16.12.4 del software Cisco IOS® XE.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Productos Relacionados

Este documento también se puede utilizar con estas versiones de hardware:

1. IE-3200 (fijo)
2. IE-3300 (modular)
3. IE-3400 (modular avanzado).

Antecedentes

Las listas de acceso (ACL) en un switch de capa 3 proporcionan seguridad básica para la red. Si no se configuran las ACL, todos los paquetes que atraviesan el switch se pueden permitir en todas las partes de la red. Las ACL controlan qué hosts pueden acceder a diferentes partes de una red o decidir qué tipos de tráfico se reenvían o bloquean en las interfaces del router. Las ACL se pueden configurar para bloquear el tráfico entrante, el tráfico saliente o ambos.

Ejemplo: Puede permitir que se reenvíe el tráfico de correo electrónico, pero no el tráfico Telnet fuera de la red.

Compatibilidad y limitaciones con IE3x00:

- Las listas de acceso VLAN (VACL) no son compatibles con la interfaz virtual de switch (SVI).
- Cuando VACL y la ACL de puerto (PACL) son aplicables para un paquete, PACL tiene prioridad sobre VACL y VACL no se aplica en tal caso.
- 255 entradas de control de acceso (ACE) como máximo por VACL.
- No se ha definido ningún límite explícito en las VLAN totales, ya que TCAM no se divide en componentes. Siempre que no haya espacio suficiente en TCAM disponible para aceptar la nueva configuración, se producirá un error con un registro del sistema.
- Logging no es compatible con ACL de salida.
- En la ACL de capa 3, no se admite ACL que no sea IP.
- El operador de capa 4 (L4OP) en ACL está limitado por el hardware a un máximo de 8 L4OP para UDP y 8 L4OP para TCP, para un total de 16 L4OP globales.
- Tenga en cuenta que el operador de **rango** consume 2 L4OP.

  Nota: Las L4OP incluyen: gt (mayor que), lt (menor que), neq (no igual), eq (igual), range (rango inclusivo)

- Las ACL de entrada se soportan solamente en interfaces físicas, no en interfaces lógicas como VLAN, Port-channel, etc.
- Se admiten ACL de puerto (PACL), que pueden ser: No IP, IPv4 e IPv6.
- Las ACL que no son IP e IPv4 tienen 1 filtro implícito, mientras que las ACL IPv6 tienen 3 filtros implícitos.
- Se admiten ACL basadas en rango de tiempo.
- ACL IPv4 con TTL; no se admiten coincidencias basadas en opciones IP.

Troubleshoot

Paso 1. **Identifique** la ACL con la que sospecha problemas. Según el tipo de ACL, estos

comandos están disponibles:

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
```

El propósito de los resultados del comando es identificar la configuración de ACL actual en Cisco IOS.

Paso 2. **Verifique** que la misma ACL esté presente en la tabla de entrada de hardware.

show platform hardware acl asic 0 tcam { **all** | **index** | **interface** | **static** | **statistics** | **usage** | **vlan-statistics** } - Opciones de comando disponibles para verificar el TCAM del switch.

```
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]
```

Hay tres pares de reglas en la salida de la tabla de hardware desde las cuales:

P: Representa el patrón = son las IP o subredes de la ACE.

M: Significa máscara = estos son los bits comodín en la ACE.

Entrada ACE	Índice	SIP	BAÑO	Protocolo	DSCP
permit udp any any eq 2222	0P, 0M, 0	0.0.0.0 (cualquiera)	0.0.0.0 (cualquiera)	0x11	0x00 (mejor esfuerzo)
permit udp any eq 2222 any	1P, 1M, 1	0.0.0.0 (cualquiera)	0.0.0.0 (cualquiera)	0x11	0x00 (mejor esfuerzo)
deny ip any any (implicit)	2P, 2M, 2	0.0.0.0 (cualquiera)	0.0.0.0 (cualquiera)	0x00	0x00 (mejor esfuerzo)

Entrada ACE	Orig OP	Puerto Src1	Puerto de origen 2	Dst OP	Puerto Dst1	Puerto Dst2
permit udp any any eq 2222	------	---------	---------	EC.	2222	---------
permit udp any eq 2222 any	EQ	2222	---------	---------	---------	---------
deny ip any any (implicit)	------	---------	---------	---------	---------	---------

> **Nota:** Ejemplos de entradas de máscara: palabra clave host = ff.ff.ff.ff, comodín 0.0.0.255 = ff.ff.ff.00, cualquier palabra clave = 00.00.00.00

Índice: número de la regla. Tenemos 0, 1 y 2 índices en el ejemplo.

SIP: indica la IP de origen en formato HEX. Dado que las reglas tienen la palabra clave 'any', la IP de origen es todo ceros.

DIP: Indica la IP de destino en formato HEXADECIMAL. La palabra clave 'any' en la regla se traduce a todos ceros.

Protocol - Indica el protocolo de las ACE. 0x11 va para UDP.

> **Nota:** Lista de protocolos conocidos: 0x01 - ICMP, 0x06 - TCP, 0x11 - UDP, 0x29 - IPv6.

DSCP: punto de código de servicios diferenciados (DSCP) presente en la regla. El valor si no se especifica es 0x00 (mejor esfuerzo).

Tipo IGMP: Especifica si la ACE contiene tipos IGMP.

ICMP Type (Tipo de ICMP): Especifica si la ACE contiene tipos de ICMP.

Código ICMP: especifica si la ACE contiene tipos de código ICMP.

Indicadores TCP: especifica si la ACE tiene indicadores TCP.

Src OP: indica el origen L4OP utilizado en la regla. No hay ninguno en la primera entrada ACE. La segunda entrada ACE tiene a EQ como operador.

Src port1 - Indica el primer puerto de origen si la ACE está basada en UDP o TCP.

Src port2 - Indica el segundo puerto de origen si la ACE está basada en UDP o TCP.

Dst OP: indica el L4OP de destino utilizado en la regla. La primera entrada ACE tiene EQ como operador, no hay ninguna en la segunda entrada ACE.

Dst port1 - Indica el primer puerto de destino si la ACE está basada en UDP o TCP.

Dst port2 - Indica el segundo puerto de destino si la ACE está basada en UDP o TCP.

Las reglas están vinculadas al puerto **ACL:<0,x>** en la que 0 significa ASIC = 0 y X se asigna al número de puerto ASIC = 1.

También puede ver la Acción tomada por la sentencia ACE en la tabla.

Índice ACE	Acción
0	ASIC_ACL_PERMIT [1]
1	ASIC_ACL_PERMIT [1]
2	ASIC_ACL_DENY[0]

Paso 3. **Verifique** las mismas entradas de ACL con diferentes comandos listados a continuación:

Entradas de ACL en un Índice Dado

show platform hardware acl asic 0 tcam index *acl_id* **[detail]** - Este comando muestra la lista de reglas bajo un ID de ACL específico.

```
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]
```

Aquí index es el desplazamiento en el que se programa la regla en TCAM.

Para verificar qué índice ACL se utiliza, debe identificar el puerto donde se aplica la ACL y utilizar el comando show platform hardware acl asic 0 tcam interface *interface_name* ipv4 detailpara obtener el número de ID de ACL.

> **Nota:** Tenga en cuenta que este comando no muestra la asignación de ASIC/puerto. Además, si aplica la misma ACL a diferentes interfaces, TCAM crea una entrada de ID de ACL diferente. Esto significa que no hay reutilización del índice para la misma ACL aplicada a diferentes interfaces en el espacio TCAM.

Entradas de ACL Programadas en Hardware

show platform hardware acl asic 0 tcam all [detail] - Muestra toda la información del TCAM.

```
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]
```

Este resultado muestra todos los ID de ACL almacenados en la tabla de hardware. Existen dos ID de ACL independientes (45, 46); sin embargo, la estructura de cada bloque es exactamente la misma. Esto indica que ambos ID de ACL pertenecen a la misma ACL configurada en el software:

```
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
```

Que se aplica a diferentes interfaces.

```
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
```

Uso de TCAM

show platform hardware acl asic 0 tcam usage - Este comando muestra el uso de ACL en el ASIC. IE3x00

solo tiene un 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
```

La ACE estándar tiene un ancho de 24 bytes; La ACE ampliada tiene 48 bytes de ancho; Ultra ACE tiene un ancho de 72 bytes.

Entradas estáticas de ACL

show platform hardware acl asic 0 tcam static [detail]- Muestra configuraciones de ACL estáticas (específicas del protocolo de control).

```
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.
```

Este resultado del comando muestra las entradas de ACL programadas por el sistema para los diferentes protocolos de control del switch.

Estadísticas de ACL

show platform hardware acl asic 0 tcam statistics *interface_name* - Muestra las estadísticas de ACL en tiempo real; el contador no es acumulativo. Después de mostrar el comando por primera vez, los contadores se restablecen si el tráfico que llega a la ACL se detiene.

```
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
```

Este comando le indica cuántos aciertos en los Permisos se han producido para la ACL en la interfaz especificada, y cuántas caídas se han alcanzado también mientras el tráfico se pone en cola activamente en el puerto. Los contadores se restablecen una vez que el comando se ha mostrado por primera vez.

> **Consejo:** Dado que los contadores se restablecen después de cada ejecución del comando, se recomienda ejecutar el comando varias veces y mantener un registro de los resultados anteriores para un contador de permiso/descarte acumulativo.

Asignación de puerto a ASIC

show platform pm port-map - Muestra la asignación de ASIC/puerto para todas las interfaces del switch.

```
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**

Comandos de Debug

debug platform acl all - Este comando habilita todos los eventos del administrador ACL.

```
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 - Muestra eventos relacionados con la capa de abstracción de hardware (HAL).

Para un evento de quitar/aplicar ACL en una interfaz, muestra si la regla se programó en hardware e imprime la información en la consola.

```
[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
```

Dirección 0 = Entrante (se aplicó ACL en el ingreso)

Dirección 1 = Saliente (ACL aplicada en salida)

debug platform acl ipv4 - Muestra eventos relacionados con IPv4 de ACL.

debug platform acl ipv6- Muestra eventos relacionados con IPv6 ACL.

debug platform acl mac - Muestra eventos relacionados con MAC de ACL.

debug platform acl error - Muestra eventos relacionados con errores de ACL.

```
[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 - Muestra eventos relacionados con la combinación dependiente del orden (ODM) de ACL.

```
[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 - Muestra eventos relacionados con ACL de puerto.

```
[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 - Muestra eventos relacionados con el resultado de la máscara de valor de ACL (VMR). Si hay problemas con VMR, puede verlos aquí.

```
[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>
```

Problemas comunes

Agotamiento de L4OP

El agotamiento del comparador L4OPs se puede identificar después de habilitar estas depuraciones:

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

> **Nota:** Los comandos debug no muestran información al buffer de registro del switch. En su lugar, la información se muestra en la show platform software trace message ios R0comando.

Ejecute el comando **show platform software trace message ios R0** para mostrar la información sobre los debugs.

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] :
```

Para el IE3x00 hay un límite de 8 L4OP para UDP y 8 L4OP para TCP, para un máximo total de 16 L4OP en todas las ACL implementadas en el switch. (La restricción es global, no por ACL).

> **Nota:** Actualmente no hay ningún comando disponible para verificar la cantidad de comparadores consumidos/libres en la CLI.

Si experimenta este problema:

- Verifique con los comandos debug si los errores están relacionados con la limitación L4OP.
- Debe reducir el número de L4OP en uso en la ACL. Cada comando range consume dos comparadores de puertos.
- Si puede utilizar ACE con el comando **range**, éstos se pueden convertir para utilizar la palabra clave **eq** en su lugar, por lo que no consumirá el L4OP disponible para UDP y TCP, es decir:

Línea:
permit tcp any any range 55560 55567

Puede convertirse en:
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

Consulte el ID de bug de Cisco CSCvv07745. Solamente los usuarios registrados de Cisco pueden acceder a la información de bug interna.

Las ACL de Capa 4 no se resumen en TCAM

Cuando se ingresan ACL L4 con direcciones IP y/o números de puerto consecutivos, el sistema los resume automáticamente antes de que se escriban en TCAM para ahorrar espacio. El sistema hace todo lo posible basándose en las entradas de ACL para resumir con el MVR apropiado y

cubrir un rango de entradas donde pueda. Esto se puede verificar al verificar el TCAM y cuántas líneas se programaron para la ACL. Es decir:

```
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>
```

El problema es que el valor de la máscara no se lee correctamente, por lo que la única entrada que realmente se programa (con la ACL en el ejemplo) es **permit tcp any any eq 8,**ya que esta es la ACL de resumen de nivel superior. Las entradas para los números de puerto 9-11 no se ven porque la máscara de 0.0.0.3 no se lee correctamente.

Consulte el ID de bug Cisco CSCvx6354 . Solo los usuarios registrados de Cisco pueden acceder a la información de bug interno.

Comandos a recopilar para TAC

Los problemas más comunes relacionados con las listas de acceso en IE3x00 se tratan en esta guía, con los pasos de corrección adecuados. Sin embargo, en caso de que esta guía no haya resuelto su problema, recopile la lista de comandos mostrada y adjúntela a su solicitud de servicio TAC.

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
```

Copie el archivo fuera del switch y cárguelo en el caso TAC.

La salida de ACL de soporte técnico es necesaria como punto de partida cuando se solucionan problemas relacionados con ACL en plataformas IE3x00.

Información Relacionada

- Notas de la versión para Cisco Catalyst IE3x00 Rugged, IE3400 Rugged, IE3400 Heavy Duty y ESS3300 Series Switches, Cisco IOS XE Gibraltar 16.12.x
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).