Solucionar problemas de listas de acesso no IE3x00

Contents

Introduction

Este documento descreve como solucionar problemas e verificar as entradas das Listas de Controle de Acesso (ACL) e os limites de hardware na série Industrial Ethernet 3x00.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento básico da configuração da ACL.

Componentes Utilizados

As informações neste documento são baseadas no IE-3300 com o software Cisco IOS® XE versão 16.12.4.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Produtos Relacionados

Este documento também pode ser usado com estas versões de hardware:

1. IE-3200 (fixo)
2. IE-3300 (modular)
3. IE-3400 (modular avançado).

Informações de Apoio

As listas de acesso (ACL) em um switch de Camada 3 fornecem segurança básica para sua rede. Se as ACLs não estiverem configuradas, todos os pacotes que atravessam o switch poderão ter permissão para entrar em todas as partes da rede. As ACLs controlam quais hosts podem acessar diferentes partes de uma rede ou decidir que tipos de tráfego são encaminhados ou bloqueados nas interfaces do roteador. As ACLs podem ser configuradas para bloquear o tráfego de entrada, de saída ou ambos.

Exemplo: Você pode permitir que o tráfego de e-mail seja encaminhado, mas não o tráfego Telnet fora da rede.

Suporte e limitações do IE3x00:

- As listas de acesso de VLAN (VACL) não são suportadas na interface virtual do switch (SVI).
- Quando a VACL e a ACL de porta (PACL) são aplicáveis a um pacote, o PACL tem precedência sobre a VACL e a VACL não é aplicada nesse caso.
- Máximo de 255 entradas de controle de acesso (ACE) por VACL.
- Nenhum limite explícito no total de VLANs definido, porque a TCAM não é gravada em componentes, sempre que não houver espaço suficiente disponível na TCAM para aceitar a nova configuração, um erro será lançado com um syslog.
- Logging não é suportado na ACL de saída.
- Na ACL da camada 3, a ACL não IP não é suportada.
- O Operador de Camada 4 (L4OP) nas ACLs é limitado pelo hardware a um máximo de 8 L4OP para UDP e 8 L4OP para TCP, para um total de 16 L4OP globais.
- Tenha em mente que o operador **range** consome 2 L4OP.

  Note: Os L4OP incluem: gt (maior que), lt (menor que), neq (diferente), eq (igual), range (intervalo inclusivo)

- As ACLs de entrada são suportadas apenas em interfaces físicas, não suportadas em interfaces lógicas como VLAN, canal de porta e assim por diante.
- As ACLs de porta (PACLs) são suportadas e podem ser: Não IP, IPv4 e IPv6.
- As ACLs não IP e IPv4 têm 1 filtro implícito, enquanto as ACLs IPv6 têm 3 filtros implícitos.
- Há suporte para ACLs baseadas em intervalo de tempo.
- ACL IPv4 com TTL, correspondência baseada em opções de IP não suportada.

Troubleshoot

Etapa 1. **Identifique** a ACL com a qual você suspeita de problemas. Com base no tipo de ACL,

estes comandos estão disponíveis:

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
```

A finalidade das saídas do comando é identificar a configuração atual da ACL no Cisco IOS.

Etapa 2. Verifique se a mesma ACL está presente na tabela de entrada de hardware.

show platform hardware acl asic 0 tcam { **all** | **index** | **interface** | **static** | **statistics** | **usage** | **vlan-statistics** } - Opções de comando disponíveis para verificar a TCAM do 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]
```

Há três pares de regras na saída da tabela de hardware da qual:

P: Representa padrão = estes são os IPs ou sub-redes na ACE.

M: Representa máscara = esses são os bits curinga na ACE.

Entrada ACE	Índice	SIP	DIP	Protocolo	DSCP
permit udp any any eq 2222	0P, 0M, 0	0.0.0.0 (qualquer)	0.0.0.0 (qualquer)	0x11	0x00 (melhor esforço)
permit udp any eq 2222 any	1 P, 1 M, 1	0.0.0.0 (qualquer)	0.0.0.0 (qualquer)	0x11	0x00 (melhor esforço)
deny ip any any (implicit)	2P, 2M, 2	0.0.0.0 (qualquer)	0.0.0.0 (qualquer)	0x00	0x00 (melhor esforço)

Entrada ACE	OC src	Src port1	Src port2	Dst OP	Dst port1	Dst port2
permit udp any any eq 2222	------	---------	---------	EQ.	2222	---------
permit udp any eq 2222 any	EQ	2222	---------	---------	---------	---------
deny ip any any (implicit)	------	---------	---------	---------	---------	---------

> **Note**: Exemplos de entradas de máscara: palavra-chave host = ff.ff.ff.ff, curinga 0.0.0.255 = ff.ff.ff.00, qualquer palavra-chave = 00.00.00.00

Índice - Número da regra. Temos índices 0, 1 e 2 no exemplo.

SIP - Indica o IP de origem no formato HEX. Como as regras têm a palavra-chave 'any', o IP de origem é totalmente igual a zero.

DIP - Indica o IP de destino no formato HEX. A palavra-chave 'any' na regra é convertida em apenas zeros.

Protocol - Indica o protocolo das ACEs. 0x11 vai para UDP.

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

DSCP - Ponto de Código de Serviços Diferenciados (DSCP) presente na regra. O valor, se não for especificado, é 0x00 (melhor esforço).

Tipo de IGMP - Especifica se a ACE contém tipos de IGMP.

Tipo ICMP - Especifica se a ACE contém tipos ICMP.

Código ICMP - Especifica se a ACE contém tipos de código ICMP.

Sinalizadores TCP - Especifica se a ACE tem sinalizadores TCP.

OC Origem - Indica o L4OP origem usado na regra. Não há nenhum na primeira entrada ACE. A segunda entrada ACE tem EQ como operador.

Src port1 - Indica a primeira porta origem se a ACE for baseada em UDP ou TCP.

Src port2 - Indica a segunda porta origem se a ACE for baseada em UDP ou TCP.

Dst OP - Indica o L4OP de destino usado na regra. A primeira entrada ACE tem EQ como o operador, não há nenhuma na segunda entrada ACE.

Dst port1 - Indica a primeira porta de destino se a ACE for baseada em UDP ou TCP.

Dst port2 - Indica a segunda porta de destino se a ACE for baseada em UDP ou TCP.

As regras estão vinculadas à porta **ACL:<0,x>** em que 0 significa ASIC = 0 e X é mapeado para número de porta ASIC = 1.

Você também pode ver a Ação realizada por instrução ACE na tabela.

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

Etapa 3. **Verificar** as mesmas entradas da ACL com comandos diferentes listados a seguir:

Entradas de ACL em um Índice Específico

show platform hardware acl asic 0 tcam index *acl_id* **[detail]** - Esse comando mostra a lista de regras sob uma ID de ACL específica.

```
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]
```

Aqui index é o deslocamento no qual a regra é programada no TCAM.

Para verificar qual índice de ACL é usado, você precisa identificar a porta onde a ACL é aplicada e usar o comando show platform hardware acl asic 0 tcam interface *interface_name* ipv4 detailpara obter o número de ID da ACL.

> **Note**: Lembre-se de que esse comando não exibe o mapeamento ASIC/Porta. Além disso, se você aplicar a mesma ACL a interfaces diferentes, o TCAM criará uma entrada de ID de ACL diferente. Isso significa que não há reutilização de índice para a mesma ACL aplicada a diferentes interfaces no espaço TCAM.

Entradas ACL programadas no hardware

show platform hardware acl asic 0 tcam all [detail] - Mostra todas as informações no 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]
```

Esta saída exibe todas as IDs de ACL armazenadas na tabela de hardware. Há dois IDs de ACL separados (45, 46), no entanto, a estrutura de cada bloco é exatamente a mesma. Isso indica que ambas as IDs de ACL pertencem à mesma ACL configurada no 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 é aplicado 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 - Esse comando exibe o uso da ACL no ASIC. O IE3x00 tem

apenas um 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
```

A ACE padrão tem largura de 24 bytes; A ACE estendida tem largura de 48 bytes; O Ultra ACE tem largura de 72 bytes.

Entradas estáticas da ACL

show platform hardware acl asic 0 tcam static [detail]- Exibe configurações de ACL estáticas (específica do protocolo de controle).

```
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.
```

Esta saída de comando exibe as entradas de ACL programadas pelo sistema para diferentes protocolos de controle do switch.

Estatísticas de ACL

show platform hardware acl asic 0 tcam statistics *interface_name* - Exibe as estatísticas da ACL em tempo real, o contador não é cumulativo. Depois que você exibir o comando pela primeira vez, os contadores serão redefinidos se o tráfego que atingir a ACL parar.

```
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
```

Esse comando informa quantos acertos nas Permissões ocorreram para a ACL na interface especificada e quantas quedas foram atingidas enquanto o tráfego estava ativamente enfileirado na porta. Os contadores são redefinidos quando o comando é exibido pela primeira vez.

> **Tip**: Como os contadores são redefinidos após cada execução do comando, é recomendável executar o comando várias vezes e manter um registro das saídas anteriores para um contador de permissão/queda cumulativo.

Mapeamento de porta para ASIC

show platform pm port-map - Exibe o mapeamento de ASIC/Porta para todas as interfaces do 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 debug

debug platform acl all - Esse comando ativa todos os eventos do gerenciador de 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 - Exibe eventos relacionados à HAL (Hardware Abstraction Layer, Camada de Abstração de Hardware).

Para um evento de remoção/aplicação de ACL em uma interface, ele exibe se a regra foi programada no hardware e imprime as informações no console.

```
[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
```

Direção 0 = Entrada (ACL foi aplicada na entrada)

Direção 1 = Saída (ACL aplicada na saída)

debug platform acl ipv4 - Exibe eventos relacionados ao IPv4 da ACL.

debug platform acl ipv6- Exibe eventos relacionados ao IPv6 da ACL.

debug platform acl mac - Exibe eventos relacionados ao MAC da ACL.

debug platform acl error - Exibe eventos relacionados a erros da 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 - Exibe eventos relacionados ao ODM (Order Dependant Merge) da 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 - Exibe eventos relacionados à ACL de porta.

```
[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 - Exibe eventos relacionados ao resultado da máscara de valor (VMR) da ACL. Se houver problemas com o VMR, você poderá vê-los aqui.

```
[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 comuns

Esgotamento L4OP

O esgotamento do comparador L4OPs pode ser identificado depois que você ativar estas depurações:

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

> **Note**: Os comandos debug não exibem informações para o buffer de registro do switch. Em vez disso, as informações são exibidas na show platform software trace message ios R0comando.

Execute o comando **show platform software trace message ios R0 para exibir as informações nas depurações.**

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 o IE3x00 há um limite de 8 L4OP para UDP e 8 L4OP para TCP, para um total máximo de 16 L4OP em todas as ACLs implementadas no switch. (A restrição é global, não por ACL).

> **Note**: Atualmente não há nenhum comando disponível para verificar a quantidade de comparadores consumidos/livres na CLI.

Se você encontrar esse problema:

- Verifique com comandos debug se os erros estão relacionados à limitação de L4OP.
- Você precisa reduzir o número de L4OP em uso na ACL. Cada comando range consome 2 comparadores de porta.
- Se você puder usar ACEs com o comando **range**, elas poderão ser convertidas para usar a palavra-chave **eq**, de modo que não consumirá o L4OP disponível para UDP e TCP, ou seja:

Linha:
permit tcp any any range 55560 55567

Pode se transformar em:
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 o bug da Cisco ID CSCv07745. Somente usuários registrados da Cisco podem acessar informações de bug internas.

As ACLs da camada 4 não são resumidas no TCAM

Quando ACLs L4 com endereços IP e/ou números de porta consecutivos são inseridos, eles são automaticamente resumidos pelo sistema antes de serem gravados no TCAM para conservar espaço. O sistema faz o melhor com base nas entradas da ACL para resumir com o MVR apropriado para cobrir uma gama de entradas onde pode. Isso pode ser verificado quando você verifica o TCAM e quantas linhas foram programadas para a ACL. Ou seja:

```
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>
```

O problema é que o valor da máscara não é lido corretamente, portanto, a única entrada que é realmente programada (com a ACL no exemplo) é **permit tcp any any eq 8**,pois esta é a ACL de sumarização de nível superior. As entradas para os números de porta 9-11 não são vistas porque a máscara de 0.0.0.3 não é lida corretamente.

Consulte o bug da Cisco ID CSCvx6354 . Somente usuários registrados da Cisco podem acessar informações de bug internas.

Comandos a serem coletados para o TAC

Os problemas mais comuns relacionados às Listas de Acesso no IE3x00 são abordados neste guia, com as etapas de correção apropriadas. No entanto, caso este guia não resolva o problema, colete a lista de comandos mostrada e anexe-a à sua solicitação de serviço do 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 o arquivo do switch e carregue-o no caso TAC.

A saída da ACL de suporte técnico é necessária como um ponto de partida quando você soluciona problemas relacionados à ACL em plataformas IE3x00.

Informações Relacionadas

- Notas de versão para switches Cisco Catalyst IE3x00 Rugged, IE3400 Rugged, IE3400 Heavy Duty e ESS3300 Series, Cisco IOS XE Gibraltar 16.12.x
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.