Troubleshoot Access Lists on IE3x00

Contents

Introduction

This document describes how to troubleshoot and verify Access Control Lists (ACL) entries and hardware limits on Industrial Ethernet 3x00 series.

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of ACL configuration.

Components Used

The information in this document is based on IE-3300 with Cisco IOS® XE software version 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. If your network is live, ensure that you understand the potential impact of any command.

Related Products

This document can also be used with these hardware versions:

1. IE-3200 (fixed)
2. IE-3300 (modular)
3. IE-3400 (advanced modular).

Background Information

Access Lists (ACL) on a Layer 3 switch provide basic security for your network. If ACLs are not configured, all packets which traverse through the switch can be allowed onto all parts of the network. ACLs controls which hosts can access different parts of a network or decide which types of traffic are forwarded or blocked at router interfaces. ACLs can be configured to block inbound traffic, outbound traffic, or both.

Example: You can allow e-mail traffic to be forwarded but not Telnet traffic outside the network.

IE3x00 Support and Limitations:

- VLAN access lists (VACL) are not supported on Switch Virtual Interface (SVI).
- When VACL and Port ACL (PACL) both are applicable for a packet then PACL takes precedence over VACL and VACL is not applied in such a case.
- Max 255 Access Control Entries (ACE) per VACL.
- No explicit limit on total VLANs defined, because TCAM is not carved into components, whenever enough space in TCAM is not available to accept the new configuration, error shall be thrown with a syslog.
- Logging is not supported on egress ACL.
- On layer 3 ACL, Non-IP ACL is not supported.
- Layer 4 Operator (L4OP) in ACLs is limited by the hardware to a maximum of 8 L4OP for UDP and 8 L4OP for TCP, for a total of 16 global L4OP.
- Keep in mind that the **range** operator consumes 2 L4OP.

  Note: The L4OPs include: gt (greater than), lt (less than), neq (not equal), eq (equal), range (inclusive range)

- Ingress ACLs are supported only on physical interfaces, not supported on logical interfaces like VLAN, Port-channel, and so on.
- Port ACLs (PACLs) are supported, and they can be: Non-IP, IPv4 and IPv6.
- Non-IP and IPv4 ACLs have 1 implicit filter whereas IPv6 ACLs have 3 implicit filters.
- Time-range based ACLs are supported.
- IPv4 ACL with TTL, IP Options based match not supported.

Troubleshoot

Step 1. **Identify** the ACL you suspect issues with. Based on the type of the ACL, these commands are available:

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
```

The purpose of the command outputs is to identify the current ACL configuration on Cisco IOS.

Step 2. **Check** the same ACL is present in the hardware entry table.

show platform hardware acl asic 0 tcam { **all** | **index** | **interface** | **static** | **statistics** | **usage** | **vlan-statistics** } - Command options available to check the TCAM of the 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]

<asic,port> pair bind to this ACL:< 0, 1>
```

There are three rule pairs in the output of the hardware table from which:

P: Stands for pattern = these are the IPs or subnets in the ACE.

M: Stands for mask = these are the wildcard bits in the ACE.

ACE Entry	Index	SIP	DIP	Protocol	DSCP
permit udp any any eq 2222	0P, 0M, 0	0.0.0.0 (any)	0.0.0.0 (any)	0x11	0x00 (best effort)

permit udp any eq 2222 any	1P, 1M, 1	0.0.0.0 (any)	0.0.0.0 (any)	0x11	0x00 (best effort)
deny ip any any (implicit)	2P, 2M, 2	0.0.0.0 (any)	0.0.0.0 (any)	0x00	0x00 (best effort)

ACE Entry	Src OP	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**: Examples of Mask entries: host keyword = ff.ff.ff.ff, wildcard 0.0.0.255 = ff.ff.ff.00, any keyword = 00.00.00.00

Index - Number of the rule. We have 0, 1 and 2 indexes in the example.

SIP - Indicates Source IP in HEX format. Since the rules have the 'any' keyword, the source IP is all zeros.

DIP - Indicates Destination IP in HEX format. The 'any' keyword in the rule translates to all zeros.

Protocol - Indicates the protocol of the ACEs. 0x11 goes for UDP.

> **Note**: List of well-known protocols: 0x01 - ICMP, 0x06 - TCP, 0x11 - UDP, 0x29 - IPv6.

DSCP - Differentiated Services Code Point (DSCP) present in the rule. The value if not specified is 0x00 (best effort).

IGMP Type - Specifies if the ACE contains IGMP types.

ICMP Type - Specifies if the ACE contains ICMP types.

ICMP Code - Specifies if the ACE contains ICMP code types.

TCP Flags - Specifies if the ACE has TCP flags.

Src OP - Indicates the source L4OP used in the rule. There is none in the first ACE entry. The second ACE entry has EQ as the operator.

Src port1 - Indicates the first source port if the ACE is UDP or TCP based.

Src port2 - Indicates the second source port if the ACE is UDP or TCP based.

Dst OP - Indicates the destination L4OP used in the rule. The first ACE entry has EQ as the operator, there is none in the second ACE entry.

Dst port1 - Indicates the first destination port if the ACE is UDP or TCP based.

Dst port2 - Indicates the second destination port if the ACE is UDP or TCP based.

Rules are bound to port **ACL:<0,x>** in which 0 stands for ASIC = 0, and X maps to ASIC port number = 1.

You can also see the Action taken per ACE statement in the table.

ACE Index	Action
0	ASIC_ACL_PERMIT[1]
1	ASIC_ACL_PERMIT[1]
2	ASIC_ACL_DENY[0]

Step 3. **Verify** the same ACL entries with different commands listed next:

ACL Entries at a Given Index

show platform hardware acl asic 0 tcam index *acl_id* **[detail] -** This command shows you the list of rules under specific ACL Id.

```
IE3300#show platform hardware acl asic 0 tcam index 45 detail
ACL_KEY_TYPE_v4 - ACL Id 45

Ingress ACL_KEY_TYPE_v4 -
Index  SIP          DIP          Protocol  DSCP  Frag/Tiny  IGMP type  ICMP type  ICMP code  TCP
flags
Src OP  Src port1  Src port2  Dst OP  Dst port1  Dst port2  Src Port   PCLId
=====  ===========  ===========  ========  ====  ==========  =========  =========  =========
=========
======  =========  =========  ======  =========  =========  ========   ====
  0P   00.00.00.00  00.00.00.00  0x11      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  EQ.     2222       ---------  1     0
  0M   00.00.00.00  00.00.00.00  0xff      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------   0xFF     0xFFFF    --------- 3f   3ff
  0 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
  1P   00.00.00.00  00.00.00.00  0x11      0x00  0/00    ---------  ---------  ---------  ------
---
EQ.     2222       ---------  ------  ---------  ---------  1     0
  1M   00.00.00.00  00.00.00.00  0xff      0x00  0/00    ---------  ---------  ---------  ------
---
 0xFF     0xFFFF   ---------  ------  ---------  --------- 3f   3ff
  1 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
  2P   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  ------  ---------  ---------  1     0
  2M   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  ------  ---------  --------- 3f   3ff
  2 Action: ASIC_ACL_DENY[0], Match Counter[0]
```

Here index is the offset at which the rule is programmed in the TCAM.

To check which ACL index is used, you need to identify the port where the ACL is applied and use the command show platform hardware acl asic 0 tcam interface *interface_name* ipv4 detailto obtain the ACL Id number.

Note: Keep in mind this command does not display the ASIC/Port mapping. Also, if you apply the same ACL to different interfaces, the TCAM creates a different ACL ID entry. This means there is no index reusage for the same ACL applied to different interfaces in the TCAM space.

ACL Entries Programmed in Hardware

show platform hardware acl asic 0 tcam all [detail] - Shows all the information on the 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]
```

This output displays all the ACL IDs stored in the hardware table. There are two separate ACL IDs (45, 46), however the structure of each block is exactly the same. This indicates both ACL IDs belong to the same ACL configured in 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
```

Which is applied to different 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
```

TCAM Usage

show platform hardware acl asic 0 tcam usage - This command displays ACL usage in the ASIC. IE3x00 only has one 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 is 24-byte wide; Extended ACE is 48-byte wide; Ultra ACE is 72-byte wide.

ACL Static Entries

show platform hardware acl asic 0 tcam static [detail]- Displays static ACL configurations (control protocol specific).

```
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.
```

This command output displays the system programmed ACL entries for different control protocols of the switch.

ACL Statistics

show platform hardware acl asic 0 tcam statistics *interface_name* - Displays ACL statistics in real time, counter is not cumulative. After you display the command the first time, the counters get reset if traffic that hits the ACL stops.

```
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
```

This command tells you how many hits in the Permits have occurred for the ACL on the specified interface, and how many drops have been hit as well while traffic is actively enqueue in the port. The counters reset once the command has been displayed for the first time.

> **Tip**: Since the counters get reset after each run of the command, it is recommended that you run the command several times and keep a record of the previous outputs for a cumulative permit/drop counter.

Port to ASIC Mapping

show platform pm port-map - Displays the ASIC/Port mapping for all the interfaces of the 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**

Debug Commands

debug platform acl all - This command enables all the ACL manager events.

```
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 - Displays Hardware Abstraction Layer (HAL) related events.

For a remove/apply ACL event on an interface, it displays if the rule was programmed in hardware and print the information in 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
```

Direction 0 = Inbound (ACL was applied in ingress)

Direction 1 = Outbound (ACL was applied in egress)

debug platform acl ipv4 - Displays ACL IPv4 related events.

debug platform acl ipv6- Displays ACL IPv6 related events.

debug platform acl mac - Displays ACL MAC related events.

debug platform acl error - Displays ACL error related events.

```
[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 - Displays ACL Order Dependant Merge (ODM) related events.

```
[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 - Displays port ACL related events.

```
[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 - Displays ACL Value Mask Result (VMR) related events. If there are issues with VMR, you can see them here.

```
[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>
```

Common issues

L4OP Exhaustion

L4OPs comparator exhaustion can be identified after you enable these debugs:

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

> **Note**: The debug commands do not display information to the log buffer of the switch. Instead, the information is shown in the show platform software trace message ios R0command.

Run the command **show platform software trace message ios R0** to display the information on the 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] :
```

For the IE3x00 there is a limit of 8 L4OP for UDP and 8 L4OP for TCP, for a maximum total of 16 L4OP in all the ACLs implemented in the switch. (The restriction is global, not per ACL).

> **Note**: Currently there is no available command to check the amount of consumed/free comparators in the CLI.

If you encounter this issue:

- Check with debug commands if the errors are related to the L4OP limitation.
- You need to reduce the number of L4OP in use in the ACL. Each range command consumes 2 port comparators.
- If you can use ACEs with the **range** command, these can be converted to use **eq** keyword instead, so it won’t consume the L4OP available for UDP and TCP, that is:

Line:
permit tcp any any range 55560 55567

Can turn into:
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

Refer to the Cisco bug ID CSCvv07745. Only registered Cisco users can access internal bug information.

Layer 4 ACLs are not Summarized in TCAM

When L4 ACLs with consecutive IP addresses and/or port numbers are entered, these are automatically summarized by the system before they are written into TCAM to conserve space. The system does its best based on the ACL entries to summarise with the appropriate MVR to cover a range of entries where it can. This can be verified when you check the TCAM and how many lines where programmed for the ACL. That is:

```
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>
```

The issue is that the mask value is not read properly so the only entry that actually gets programmed (with the ACL in the example) is **permit tcp any any eq 8**,as this is the top-level summarization ACL. The entries for port-numbers 9-11 are not seen because the mask of 0.0.0.3 is not read correctly.

Refer to the Cisco bug ID CSCvx66354 . Only registered Cisco users can access internal bug information.

Commands to Collect for TAC

The most common problems related to Access Lists on IE3x00 are covered in this guide, with appropriate remediation steps. However, in the event that this guide did not resolve your issue please collect the command list shown and attach them to your TAC service request.

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
```

Copy the file out of the switch and upload it to the TAC case.

Tech support ACL output is required as a starter point when you troubleshoot issues related to ACL in IE3x00 platforms.

Related Information

- **Release Notes for Cisco Catalyst IE3x00 Rugged, IE3400 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches, Cisco IOS XE Gibraltar 16.12.x**
- **Technical Support & Documentation - Cisco Systems**