# Содержание



# Введение

Этот документ объясняет, как Коммутаторы Catalyst 3850 внедряют Контрольные списки безопасности доступа (ACL) в аппаратных средствах и как Ternary Content Addressable Memory (TCAM) безопасности используется среди различных типов ACL.

# Общие сведения

Этот список предоставляет определения для различных типов ACL:

- **Список контроля доступом VLAN (VACL)** - VACL является ACL, который применен к VLAN. Это может только быть применено к VLAN и никакому другому типу интерфейса. Граница безопасности должна permit or deny трафик, который перемещается между VLAN, и permit or deny трафик в VLAN. ACL VLAN поддерживается в аппаратных средствах и не имеет никакого эффекта на производительность.
- **Список контроля доступа порта (PACL)** - PACL является ACL, применился к интерфейсу порта коммутатора Уровня 2. Граница безопасности должна permit or deny трафик в VLAN. PACL поддерживается в аппаратных средствах и не имеет никакого эффекта на производительность.
- **ACL маршрутизатора (RACL)** - RACL Является ACL, который применен к интерфейсу, которому назначили адрес Уровня 3 на него. Это может быть применено к любому порту, который имеет IP-адрес, такой как маршрутизируемые интерфейсы, интерфейсы обратной связи и интерфейсы виртуальной локальной сети (VLAN). Граница безопасности должна permit or deny трафик, который перемещается между подсетями или сетями. RACL поддерживается в аппаратных средствах и не имеет никакого эффекта на производительность.
- **Основанный на группе ACL (GACL)** - GACL является основанным на группе ACL, определенным в Групповых объектах для ACL.

# Проблема

На Catalyst 3850/3650 коммутаторы, входной PACL и выходные данные PACL Access Control Entities (ACE) установлены в двух отдельных областях/банках. Эти области/банки называют TCAM ACL (TAQs). ACE ввод/вывода VACL сохранены в одиночной области (TAQ). Из-за Доплеровского аппаратного ограничения, VACL не может использовать обоих TAQs.

Поэтому VACL/vlmap только имеют половину пространства Результата маски значения (VMR), доступного спискам управления доступом. Когда любой из этих аппаратных пределов превышен, эти журналы появляются:

Когда эти журналы появляются, Однако TCAM ACE Безопасности, могло бы казаться, не был бы полон.

# Решение

Неправильно предположить, что один ACE всегда использует один VMR. Данный ACE может использовать:

- 0 VMRs, если это объединено с предыдущим ACE.
- 1 VMR, если биты VCU доступны для обработки диапазона.
- 3 VMRs, если это расширено, потому что никакие биты VCU не доступны.

Таблица данных Catalyst 3850 предполагает, что поддерживаются 3,000 записей списка управления доступом. Однако эти правила определяют, как могут быть настроены эти 3,000 ACE:

- VACL/vlmaps поддерживают в общей сложности 1.5K записи, поскольку они могут использовать только один из двух TAQs.
- MAC VACL/vlmap нужны три VMR/ACEs. Это означает, что 460 ACE должны поддерживаться в каждом направлении.
- IPv4 VACL/vlmap нужны два VMR/ACEs. Это означает, что 690 ACE должны поддерживаться в каждом направлении.
- PACL IPv4, RACL и GACL нужен один VMR/ACE. Это означает, что 1,380 ACE должны поддерживаться в каждом направлении.
- PACL MAC, RACL и GACL нужны два VMR/ACEs. Это означает, что 690 ACE должны поддерживаться в каждом направлении.
- PACL IPv6, RACL и GACL нужны два VMR/ACEs. Это означает, что 690 ACE должны поддерживаться в каждом направлении.

## Устранение проблем TCAM списка управления доступом на коммутаторах Catalyst 3850

- Использование TCAM безопасности проверки:

  **Примечание:** Даже при том, что установленные ACE безопасности - меньше чем 3,072, один из пределов, ранее упомянутых, возможно, был достигнут. Например, если у клиента есть большинство RACL, примененных во входном направлении, они могут израсходовать 1,380 записей, доступных для входящего RACL. Однако журналы истощения TCAM могут обнаружиться, прежде чем все 3,072 записи используются.

```
3850#show platform tcam utilization asic all
CAM Utilization for ASIC# 0
 Table                                              Max Values       Used Values
 ------------------------------------------------------------------------------
 Unicast MAC addresses                              32768/512         85/22
 Directly or indirectly connected routes            32768/7680       125/127
 IGMP and Multicast groups                          8192/512          0/16
```

```
 QoS Access Control Entries                       3072              68
 Security Access Control Entries                  3072            1648
 Netflow ACEs                                     1024              15
 Input Microflow policer ACEs                      256               7
 Output Microflow policer ACEs                     256               7
 Flow SPAN ACEs                                    256              13
 Control Plane Entries                             512             195
 Policy Based Routing ACEs                        1024               9
 Tunnels                                           256              12
 Input Security Associations                       256               4
 Output Security Associations and Policies         256               9
 SGT_DGT                                        4096/512           0/0
 CLIENT_LE                                      4096/64            0/0
 INPUT_GROUP_LE                                   6144               0
 OUTPUT_GROUP_LE                                  6144               0
```

- Проверьте состояние аппаратного обеспечения ACL, установленных в TCAM:

```
3850#show platform acl info acltype ?
 all  Acl type
 ipv4 Acl type
 ipv6 Acl type
 mac  Acl type

3850#show platform acl info acltype all
############################################################
#########                             ##################
#########                             ##################
########     Printing ACL Infos      ##################
#########                             ##################
############################################################
==================================
IPv4 ACL: Guest-ACL
     aclinfo: 0x52c41030
     ASIC255 Input L3 labels: 4
ipv4 Acl: Guest-ACL Version 16 Use Count 0 Clients 0x0
       10 permit udp any 8 host 224.0.0.2 eq 1985
       20 permit udp any 8 any eq bootps
       30 permit ip 10.100.176.0 255.255.255.0 any
<snip>3850#show platform acl info switch 1
############################################################
#########                             ##################
#########                             ##################
########     Printing ACL Infos      ##################
#########                             ##################
############################################################
==================================
IPv4 ACL: Guest-ACL
     aclinfo: 0x52c41030
     ASIC255 Input L3 labels: 4
ipv4 Acl: Guest-ACL Version 16 Use Count 0 Clients 0x0
       10 permit udp any 8 host 224.0.0.2 eq 1985
       20 permit udp any 8 any eq bootps
       30 permit ip 10.100.176.0 255.255.255.0 any
 <snip>
```

- Проверьте журналы событий acl каждый раз, когда ACL установлены/удалены:

```
3850#show mgmt-infra trace messages acl-events switch 1
[04/22/15 21:35:34.877 UTC 3a8 5692] START Input IPv4 L3 label_id 22
asic3 num_les 1 old_unload 0x0, cur_unloaded 0x0, trid 236 num_vmrs 11


[04/22/15 21:35:34.877 UTC 3a9 5692] Trying L3 iif_id 0x104608000000100
```

```
input base FID 14

[04/22/15 21:35:34.878 UTC 3aa 5692] Input IPv4 L3 label_id 22 hwlabel
22 asic3 status 0x0 old_unloaded 0x0 cur_unloaded 0x0 trid 236

[04/22/15 21:35:35.939 UTC 3ab 5692] MAC: 0000.0000.0000
Adding Input IPv4 L3 acl [Postage-Printer] BO 0x1 to leinfo le_id 29on asic 255

[04/22/15 21:35:35.939 UTC 3ac 5692] MAC: 0000.0000.0000 Rsvd
label 0 --> New label 23, asic255

[04/22/15 21:35:35.939 UTC 3ad 5692] START Input IPv4 L3 label_id 23
asic3 num_les 1 old_unload 0x0, cur_unloaded 0x0, trid 237 num_vmrs 5
<snip>
```

- Распечатайте Content Addressable Memory (CAM) ACL:

```
C3850-1#show platform acl cam
======== ACL TCAM (asic 0) =========
Printing entries for region ACL_CONTROL (135)
=====================================================
TAQ-4 Index-0 Valid StartF-1 StartA-1 SkipF-0 SkipA-0:
Entry allocated in invalidated state
Mask1 00f00000:00000000:00000000:00000000:00000000:00000000:00000000:00000000
Key1 00400000:00000000:00000000:00000000:00000000:00000000:00000000:00000000
AD   90220000:2f000000

TAQ-4 Index-1 Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Mask1 00f00000:0f000000:00000000:00000000:00000000:00000000:00000000:00000000
Key1 00400000:01000000:00000000:00000000:00000000:00000000:00000000:00000000
AD   00a00000:00000000
```

- Распечатайте перечисленное соответствие ACL и счетчики сбросов:

```
C3850-1#show platform acl counters hardware switch 1
=====================================================
Ingress IPv4 Forward            (280): 397555328725 frames
Ingress IPv4 PACL Drop          (281):        147 frames
Ingress IPv4 VACL Drop          (282):          0 frames
Ingress IPv4 RACL Drop          (283):          0 frames
Ingress IPv4 GACL Drop          (284):          0 frames
Ingress IPv4 RACL Drop and Log  (292):       3567 frames
Ingress IPv4 PACL CPU           (285):          0 frames
Ingress IPv4 VACL CPU           (286):          0 frames
Ingress IPv4 RACL CPU           (287):          0 frames
Ingress IPv4 GACL CPU           (288):          0 frames
```