Меры по предотвращению исчерпания TCAM для ACL и QoS на коммутаторах Catalyst 4500

Содержание

Введение

Коммутаторы Cisco Catalyst серий 4500 и 4948 поддерживают списки управления доступом (ACL) и функции QoS с использованием троичной ассоциативной памяти (TCAM). Включение ACL и политик не уменьшает производительности коммутатора при коммутации или маршрутизации, покуда ACL полностью загружены в TCAM. Если же объем TCAM исчерпан, пакеты могут передаваться через тракт центрального процессора, что поможет ухудшить производительность их обработки. Этот документ содержит подробные данные о:

- Различные типы TCAM, что Catalyst 4500 и использование Catalyst 4948
- Как Catalyst 4500 программирует TCAM
- Как оптимально настроить ACL и TCAM на коммутаторе во избежание истощения TCAM

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Коммутаторы серии Catalyst 4500
- Catalyst коммутаторы серии 4948

Примечание: Этот документ применяет только к Cisco коммутаторы IOS® Software-based и не применяется к операционной системе Catalyst (CatOS) - коммутаторы на основе.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

Для реализации различных типов ACL и политик QoS в аппаратных средствах, таблицы поиска оборудования программ Catalyst 4500 (TCAM) и различные аппаратные регистры в Supervisor Engine. Когда пакет поступает, коммутатор выполняет аппаратный поиск таблиц (поиск TCAM) и решает любому, permit or deny пакет.

Catalyst 4500 поддерживает различные типы ACL. Таблица 1 выделяет эти типы ACL.

Таблица 1 – типы ACL, которые поддерживаются на коммутаторах Catalyst 4500

Тип ACL	Где это применено	Управляемый трафик	Направление
RACL 1	Порт [L32], канал L3 или [SVI3] (VLAN)	Маршрутизируемый IP-трафик	Входящий или исходящий
VACL 4	VLAN (через **команду vlan filter**)	Все пакеты, которые маршрутизируются в или из VLAN или которые соединены в VLAN	Бесцельный
PACL 5	Порт [L26] или канал L2	Весь IP - трафик и трафик [non-IPv47] (через ACL MAC)	Входящий или исходящий

[1] RACL = ACL маршрутизатора

2 L3 = уровень 3

[3] SVI = коммутируемый виртуальный интерфейс

[4] VACL = ACL VLAN

[5] PACL = ACL порта

[6] L2 = уровень 2

[7] IPv4 = IP версии 4

ACL Catalyst 4500 и архитектура программирования аппаратного обеспечения QoS

TCAM Catalyst 4500 имеет следующее количество записей:

- 32,000 записей для списка управления доступом, который также известен как ACL функции
- 32,000 записей для ACL QoS

И для списка управления доступом и для ACL QoS, записи выделены следующим образом:

- 16,000 записей для входного направления
- 16,000 записей для выходного направления

Рисунок 3 показывает посвящение множества технических разделов. Посмотрите Типы раздела TCAM для получения дополнительной информации о TCAM.

Таблица 2 показывает ресурсы ACL, которые доступны для различных Supervisor Engine Catalyst 4500 и коммутаторов.

Таблица 2 – ресурсы ACL Catalyst 4500 на различных Supervisor Engine и коммутаторах

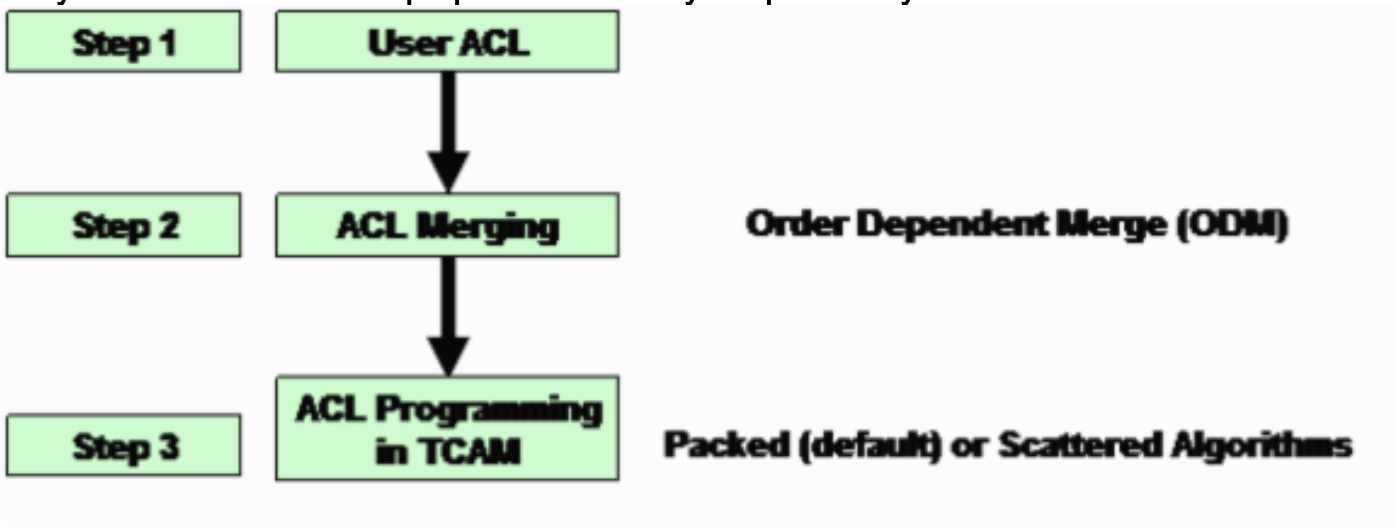
Продукт	Версия TCAM	TCAM функции (на направление)	TCAM QoS (на направлении)
Supervisor Engine II +	2	8000 записей, 1000 масок	8000 записей, 1000 масок
Supervisor Engine II+TS/III/IV/V и WS-C4948	2	16,000 записей, 2000 масок	16,000 записей, 2000 масок
Supervisor Engine V-10GE и WS-C4948-10GE	3	16,000 записей, 16,000 масок	16,000 записей, 16,000 масок

Catalyst 4500 использует отдельные, специализированные TCAM для одноадресного IP - трафика и многоадресной маршрутизации. Catalyst 4500 может иметь до 128,000 записей маршрута, которые совместно используют индивидуальная рассылка и многоадресные маршруты. Однако эти подробные данные выходят за рамки этого документа. Этот документ только обсуждает безопасность и проблемы истощения TCAM QoS.

Рисунок 1 показывает шаги для программирования ACL в аппаратных таблицах на Catalyst

4500.

Рисунок 1 - шагает в ACL программы на коммутаторах Catalyst 4500



Шаг 1

Этот шаг включает одно из этих действий:

- Конфигурация и приложение ACL или политики QoS к интерфейсу или VLANСоздание ACL может произойти динамично. Пример имеет место Защиты IP-источника (IPSG) функция. С этой функцией коммутатор автоматически создает PACL для IP-адресов, которые привязаны к порту.
- Модификация ACL, который уже существует

Примечание: Одна только конфигурация из ACL не приводит к программированию TCAM. ACL (политика QoS) должен к примененному к интерфейс для программирования ACL в TCAM.

Шаг 2

ACL должен быть объединен, прежде чем он сможет быть запрограммирован в аппаратных таблицах (TCAM). Программы слияния множественные ACL (PACL, VACL или RACL) в аппаратных средствах объединенной формой. Таким образом только одиночный поиск оборудования необходим для проверки против всех применимых ACL в пакете логического пути переадресации.

Например, на рисунке 2, пакет, который маршрутизируется от ПК-A до PCC потенциально, может иметь эти ACL:

- Входной PACL на порту ПК-A
- VACL на VLAN 1
- Входной RACL на интерфейсе VLAN1 во входном направлении

Эти три ACL объединены так, чтобы одиночного поиска во входном TCAM было достаточно для создания решения по перенаправлению для permit or deny. Точно так же только одиночные выходные данные lookup необходимы, потому что TCAM запрограммирован с объединенным результатом этих трех ACL:

- Выходные данные RACL на интерфейсе VLAN 2

- VACL VLAN 2
- Выходные данные PACL на порту PCC

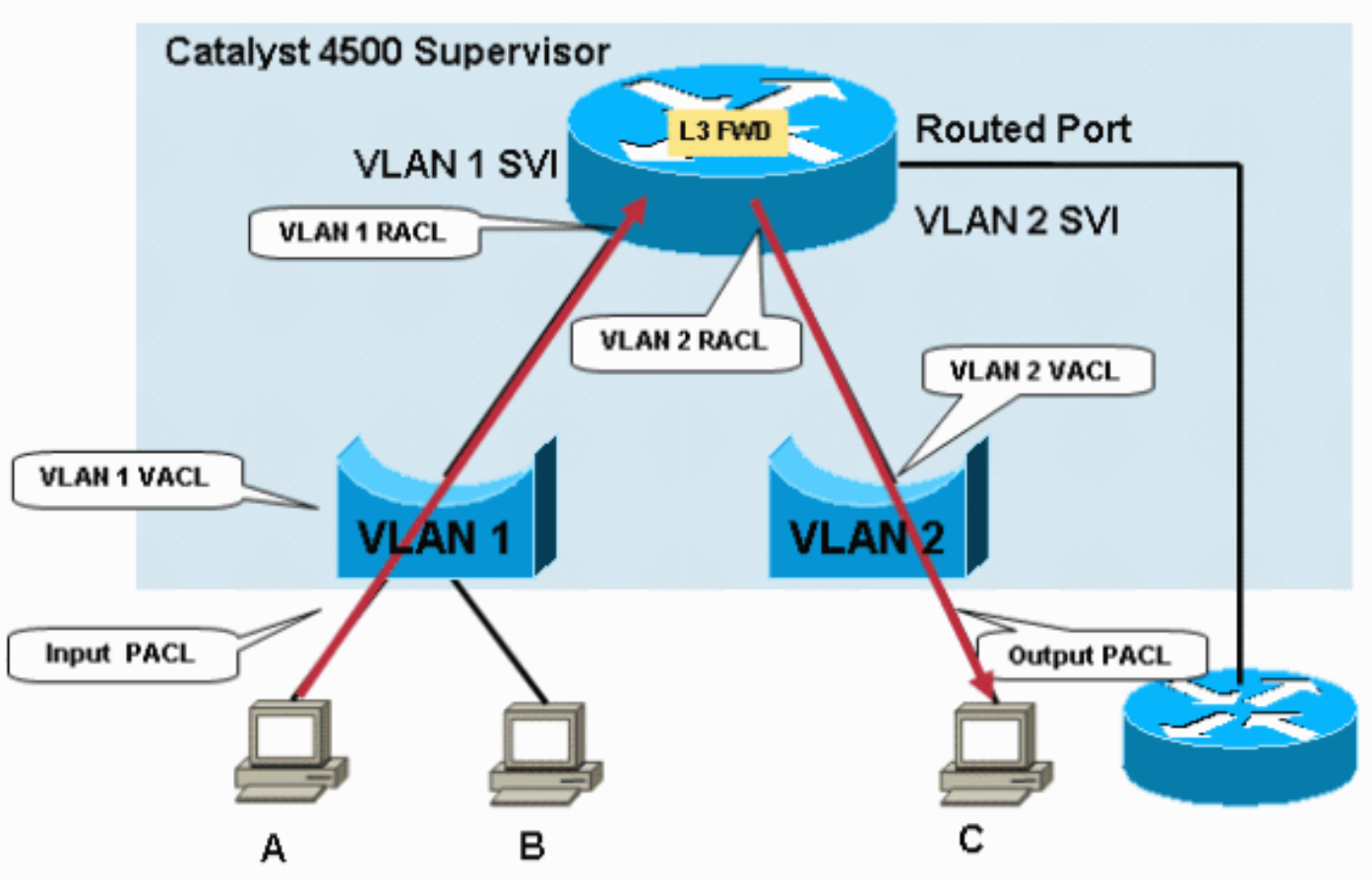
Когда любые из этих ACL находятся в пути пересылки пакетов, с одиночным поиском для ввода и один для выходных данных, нет никакой аппаратной переадресации штрафа пакетов.

Примечание: Поиски TCAM ввод/вывода происходят в то же время в аппаратных средствах. Общее несовпадение - то, что выходной поиск TCAM происходит после входного поиска TCAM, как логический поток пакетов предполагает. Эта информация важна для понимания, потому что политика вывода Catalyst 4500 не может совпасть на модифицируемых параметрах QoS политики для входящих пакетов. В случае списка управления доступом происходит большая часть жесткого действия. Пакет отброшен в любой из этих ситуаций:

- Если входной результат поиска является отбрасыванием, и выходной результат поиска является разрешением
- Если входной результат поиска является разрешением, и выходной результат поиска является отбрасыванием

Примечание: Пакет разрешен, если оба результаты поиска ввод/вывода являются разрешением.

Рисунок 2 – фильтрация через Списки управления доступом на Коммутаторах Catalyst 4500



Слияние ACL на Catalyst 4500 зависимо от инструкции. Процесс также известен как зависимое слияние заказа (ODM). С ODM записи ACL запрограммированы в заказе, в котором они появляются в ACL. Например, если ACL содержит две записи управления доступом (ACE), ACE программ коммутатора 1 первое и затем ACE программ 2. Однако зависимость заказа только между ACE в определенном ACL. Например, ACE в ACL 120 могут запуститься перед ACE в ACL 100 в TCAM.

Шаг 3

Объединенный ACL запрограммирован в TCAM. TCAM Ввода или вывода для ACL или QoS далее разделен на две области, PortAndVlan и PortOrVlan. Если конфигурация имеет *оба* из этих ACL в том же пути пакета, объединенный ACL запрограммирован в регионе PortAndVlan TCAM:

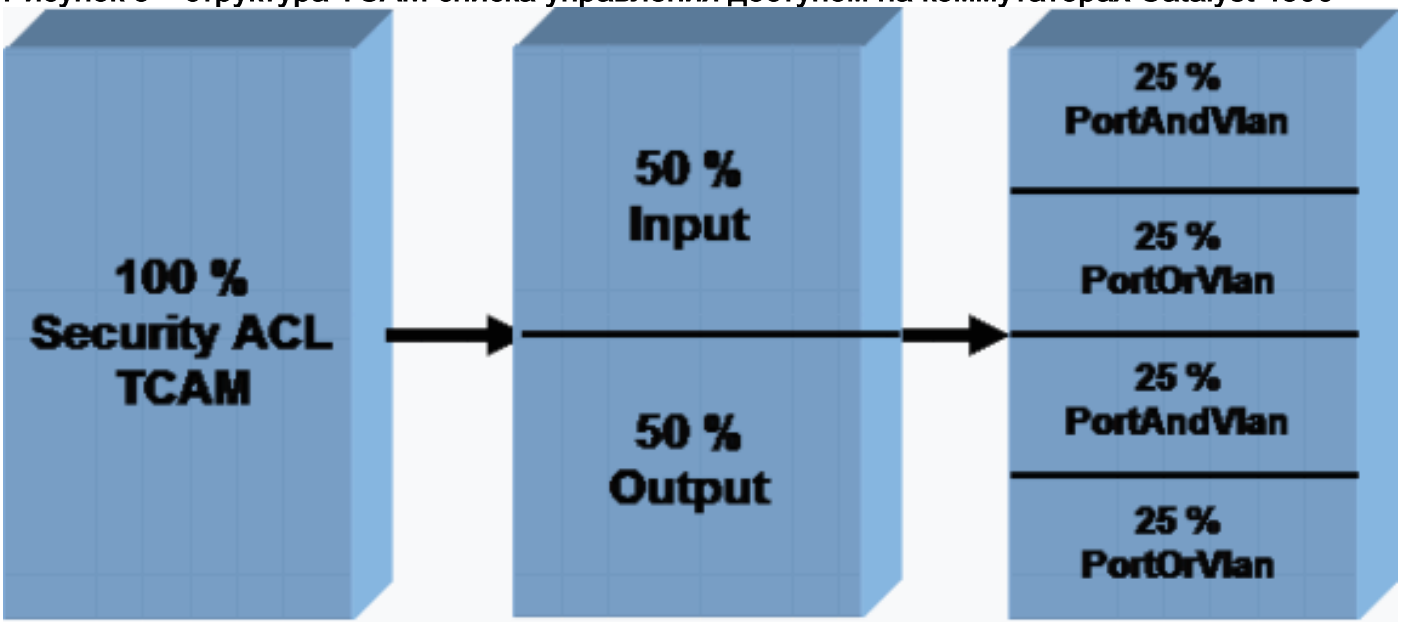
- PACL**Примечание:** PACL является обычным ACL фильтрации или созданным IPSG динамическим ACL.
- VACL или RACL

Если отдельный путь пакета имеет только PACL или VACL или RACL, ACL запрограммирован в области PortOrVlan TCAM. Рисунок 3 показывает вырезание TCAM списка управления доступом для различных типов ACL. QoS имеет столь же вырезанный, отдельный, специализированный TCAM.

В настоящее время вы не можете модифицировать расположение TCAM по умолчанию. Однако существуют планы предоставить способность изменить распределение TCAM, которое доступно для PortAndVlan и областей PortOrVlan в версиях последующих версий ПО. Это изменение позволит вам увеличивать или уменьшать пространство для PortAndVlan и PortOrVlan в любом TCAM ввода или вывода.

Примечание: Любое увеличение выделения для региона PortAndVlan приведет к эквивалентному уменьшению для области PortOrVlan в TCAM ввода или вывода.

Рисунок 3 – структура TCAM списка управления доступом на коммутаторах Catalyst 4500



Команда show platform hardware ACL statistics utilization brief отображает это использование TCAM для каждого региона и для ACL и для TCAM QoS. Выходные данные команды показывают доступные маски и записи и делят их на область, как на рисунке 3. Этот пример выходных данных от Supervisor Engine II Catalyst 4500 +:

Примечание: Посмотрите Типы раздела TCAM этого документа для получения дополнительной информации о масках и записях.

```
Switch#show platform hardware acl statistics utilization brief Entries/Total(%) Masks/Total(%) -
--------------- --------------- Input Acl(PortAndVlan) 2016 / 4096 ( 49) 252 / 512 ( 49) Input
Acl(PortOrVlan) 6 / 4096 ( 0) 5 / 512 ( 0) Input Qos(PortAndVlan) 0 / 4096 ( 0) 0 / 512 ( 0)
```

```
Input Qos(PortOrVlan) 0 / 4096 ( 0) 0 / 512 ( 0) Output Acl(PortAndVlan) 0 / 4096 ( 0) 0 / 512 (
0) Output Acl(PortOrVlan) 0 / 4096 ( 0) 0 / 512 ( 0) Output Qos(PortAndVlan) 0 / 4096 ( 0) 0 /
512 ( 0) Output Qos(PortOrVlan) 0 / 4096 ( 0) 0 / 512 ( 0) L4Ops: used 2 out of 64
```

Типы TCAM

Catalyst 4500 использует два типа TCAM, поскольку Таблица 2 показывает. Этот раздел представляет различие между двумя версиями TCAM так, чтобы можно было выбрать соответствующий продукт для сети и конфигурации.

TCAM 2 использует структуру, в которой восемь записей совместно используют одну маску. Примером являются восемь IP-адресов в ACE. Записи должны иметь ту же маску как маска, которую они совместно используют. Если ACE имеют другие маски, записи должны использовать отдельные маски по мере необходимости. Это использование отдельных масок может привести к исчерпанию маски. Исчерпание маски в TCAM является одной из обычных причин для истощения TCAM.

TCAM 3 не имеет никакого подобного ограничения. Каждая запись может иметь свою собственную уникальную маску в TCAM. Полное использование всех записей, которые доступны в аппаратных средствах, возможно, независимо от маски тех записей.

Для демонстрации этой архитектуры аппаратного обеспечения пример в этом разделе показывает как TCAM 2 и программа acl TCAM 3 в аппаратных средствах.

```
access-list 101 permit ip host 8.1.1.1 any
access-list 101 deny ip 8.1.1.0 0.0.0.255 any
```

Этот типовой ACL имеет две записи, которые имеют две других маски. ACE 1 является записью хоста и таким образом, он имеет/32 маску. ACE 2 является элементом подсети с /24 маской. Поскольку вторая запись имеет другую маску, пустые записи в Маске 1 не могут использоваться, и отдельная маска используется в случае TCAM 2.

Эта таблица показывает, как этот ACL запрограммирован в TCAM 2:

Маски	Записи
Маска 1 Соответствие: все 32 бита IP - адреса источника "Не заботятся": все оставшиеся биты	Source IP = 8.1.1.1
	Пустая запись 2
	Пустая запись 3
	Пустая запись 4
	Пустая запись 5
	Пустая запись

	6
	Пустая запись 7
	Пустая запись 8
Маска 2 Соответствия: старшие значащие 24 бита IP - адреса источника "Не заботятся": все оставшиеся биты	Source IP = 8.1.1.0
	Пустая запись 2
	Пустая запись 3
	Пустая запись 4
	Пустая запись 5
	Пустая запись 6
	Пустая запись 7
	Пустая запись 8

Даже при том, что существуют пустые поля, доступные как часть Маски 1, структура TCAM 2 предотвращает население ACE 2 в пустой записи 2 для Маски 1. Использование этой маски не допустимо, потому что маска ACE 2 не совпадает с/32 маской ACE 1. TCAM 2 должен программировать ACE 2 с использованием отдельной маски,/24 маски.

Это использование отдельной маски может привести к более быстрому исчерпанию доступных ресурсов, поскольку Таблица 2 показывает. Другие ACL могут все еще использовать остающиеся записи в Маске 1. Однако в большинстве случаев эффективность TCAM 2 высока, но не составляет 100 процентов. Эффективность меняется в зависимости от каждого сценария конфигурации.

Эта таблица показывает тот же ACL, запрограммированный в TCAM 3. TCAM 3 выделяет маску для каждой записи:

Маски	**Записи**
Маска 32 бита для IP-адреса 1	Source IP = 8.1.1.1
Маска 24 бита для IP-адреса 2	Source IP = 8.1.1.0

Пустая маска 3	Пустая запись 3
Пустая маска 4	Пустая запись 4
Пустая маска 5	Пустая запись 5
Пустая маска 6	Пустая запись 6
Пустая маска 7	Пустая запись 7
Пустая маска 8	Пустая запись 8
Пустая маска 9	Пустая запись 9
Пустая маска 10	Пустая запись 10
Пустая маска 11	Пустая запись 11
Пустая маска 12	Пустая запись 12
Пустая маска 13	Пустая запись 13
Пустая маска 14	Пустая запись 14
Пустая маска 15	Пустая запись 15
Пустая маска 16	Пустая запись 16

В данном примере 14 остающихся записей могут каждый иметь записи с другими масками без ограничений. Поэтому TCAM 3 очень более эффективен, чем TCAM 2. Данный пример чрезмерно упрощен для иллюстрирования различия между версиями TCAM. Программное обеспечение Catalyst 4500 имеет множественную оптимизацию для увеличения эффективности программирования в TCAM 2 для практического сценария конфигурации. Субоптимальный программный алгоритм TCAM для раздела TCAM 2 этого документа обсуждает эту оптимизацию.

Если тот же ACL применен на другие интерфейсы, и для TCAM 2 и для TCAM 3 на Catalyst 4500, разделены множества технических разделов. Эта оптимизация оставляет свободное место TCAM.

Истощение TCAM устранения неполадок

Когда истощение TCAM происходит на коммутаторах Catalyst 4500 во время программирования списка управления доступом, частичное приложение ACL происходит через путь к программному обеспеченю. Пакеты, которые совпадают с ACE, которые не применены в TCAM, обработаны в программном обеспечении. Эта обработка в программном обеспечении вызывает высокую загрузку ЦП. Поскольку программирование ACL Catalyst 4500 зависимо от инструкции, ACL всегда программируется от вершины вниз. Если определенный ACL действительно не полностью вписывается в TCAM, ACE в нижней части ACL, скорее всего, не запрограммированы в TCAM.

Когда переполнение TCAM происходит, предупреждающее сообщение появляется. Например:

```
%C4K_HWACLMAN-4-ACLHWPROGERRREASON: (Suppressed 1times) Input(null, 12/Normal)
Security: 140 - insufficient hardware TCAM masks.
%C4K_HWACLMAN-4-ACLHWPROGERR: (Suppressed 4 times) Input Security: 140 - hardware TCAM
limit, some packet processing will be software switched.
```

Можно также видеть это сообщение об ошибках в выходных данных **команды show logging** при включении системного журнала. Присутствие этого сообщения окончательно указывает, что некоторая обработка программного обеспечения будет иметь место. Следовательно, может быть высокая загрузка ЦП. ACL, который был уже запрограммирован

в TCAM, остается запрограммированным в TCAM, если исчерпание емкости TCAM происходит во время приложения нового ACL. Пакеты, которые совпадают с ACL, которые были уже запрограммированы, продолжают быть обработанными и переданными в аппаратных средствах.

Примечание: При внесении изменений в большой ACL ПРЕВЫШЕННОЕ К TCAM сообщение может быть отображено. Коммутатор пытается перепрограммировать ACL в TCAM. В большинстве случаев новый, модифицированный ACL может быть повторно запрограммирован полностью в аппаратных средствах. Если коммутатор может успешно перепрограммировать ACL полностью в TCAM, это сообщение появляется:

```
*Apr 12 08:50:21: %C4K_COMMONHWACLMAN-4-ALLACLINHW: All configured ACLs
now fully loaded in hardware TCAM - hardware switching / QoS restored
```

Используйте **входную итоговую интерфейсную** команду *interface-id* **acl программного обеспечения show platform**, чтобы проверить, что ACL полностью запрограммирован в аппаратных средствах.

Эти выходные данные показывают конфигурацию ACL 101 к VLAN 1 и проверке, что ACL полностью запрограммирован в аппаратных средствах:

Примечание: Если ACL не полностью запрограммирован, сообщение об ошибках истощения TCAM может отобразиться.

```
Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan 1 Switch(config-if)#ip access-group 101 in Switch(config-if)#end
Switch# Switch#show platform software acl input summary interface vlan 1 Interface
Name                : Vl1  Path(dir:port, vlan)        : (in :null, 1)    Current TagPair(port,
vlan) : (null, 0/Normal)    Current Signature         : {FeatureCam:(Security: 101)}
 Type                         : Current    Direction                 : In    TagPair(port,
vlan)       : (null, 0/Normal)    FeatureFlatAclId(state)   : 0(FullyLoadedWithToCpuAces)
   QosFlatAclId(state)       : (null)    Flags                     : L3DenyToCpu
```

Поле `Flags` (`L3DenyToCpu`) указывает, что, если пакет запрещен из-за ACL, пакет плывется на плоскодонке к ЦП. Коммутатор тогда отсылает Протокол ICMP - недостижимое сообщение. Это поведение является по умолчанию. Когда пакеты плывутся на плоскодонке к ЦП, высокая загрузка ЦП может произойти на коммутаторе. Однако в программном обеспечении Cisco IOS версии 12.1(13)EW и позже, эти пакеты с ограниченной скоростью к ЦП. В большинстве случаев Cisco рекомендует выключить функцию, которая передает сообщения ICMP недостижим.

Эти выходные данные показывают конфигурацию коммутатора для не передачи сообщений ICMP недостижим и проверки TCAM, программируя после изменения. Состоянием ACL 101 является теперь `FullyLoaded`, поскольку выходные данные команды показывают. Отказ в трафике не переходит к ЦП.

```
Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan 1 Switch(config-if)#no ip unreachables Switch(config-if)#end
Switch#show platform software acl input summary interface vlan 1 Interface Name                :
Vl1  Path(dir:port, vlan)        : (in :null, 1)    Current TagPair(port, vlan) : (null,
1/Normal)    Current Signature         : {FeatureCam:(Security: 101)}
 Type                         : Current    Direction                 : In    TagPair(port,
vlan)       : (null, 1/Normal)    FeatureFlatAclId(state)   : 0(FullyLoaded)
   QosFlatAclId(state)       : (null)    Flags                     : None
```

Примечание: Если TCAM QoS превышен во время приложения определенной политики QoS, что определенная политика *не* применена к интерфейсу или VLAN. Catalyst 4500 не внедряет политику QoS в пути к программному обеспеченю. Когда TCAM QoS превышен, Поэтому загрузка ЦПУ не пронзает.

```
*May 13 08:01:28: %C4K_HWACLMAN-4-ACLHWPROGERR: Input Policy Map: 10Mbps - hardware TCAM
limit, qos being disabled on relevant interface.

*May 13 08:01:28: %C4K_HWACLMAN-4-ACLHWPROGERRREASON: Input Policy Map: 10Mbps - no
available hardware TCAM entries.
```

Выполните команду show platform cpu packet statistics. Определите, получает ли ACL очередь большое число пакетов. Большое число пакетов указывает на исчерпание TCAM безопасности. Это истощение TCAM заставляет пакеты передаваться ЦП для передачи программного обеспечения.

```
Switch#show platform cpu packet statistics !--- Output suppressed. Packets Received by Packet
Queue  Queue                 Total          5 sec avg 1 min avg 5 min avg 1 hour avg -----------
---------- -------------- --------- --------- --------- ----------
Control                     57902635       22        16        12         3 Host
Learning                      464678        0         0         0         0 L3 Fwd
Low                           623229        0         0         0         0 L2 Fwd
Low                         11267182        7         4         6         1 L3 Rx
High                            508        0         0         0         0 L3 Rx
Low                           1275695       10         1         0         0 ACL
fwd(snooping)                 2645752        0         0         0         0 ACL log,
unreach                    51443268        9         4         5         5 ACL sw
processing                842889240     1453      1532      1267      1179  Packets Dropped by Packet
Queue  Queue                 Total          5 sec avg 1 min avg 5 min avg 1 hour avg -----------
---------- -------------- --------- --------- --------- ---------- L2 Fwd
Low                           3270        0         0         0         0 ACL sw
processing                   12636        0         0         0         0
```

Если вы находите, что очередь `ACL sw processing` не получает дополнительную оплату трафика, обратитесь к Высокой загрузке ЦП на Коммутаторах Catalyst 4500 на основе ПО Cisco IOS для других возможных причин. Документ предоставляет сведения о том, как устранить неполадки других сценариев высокой загрузки ЦП.

TCAM Catalyst 4500 может переполниться по этим причинам:

- Субоптимальный программный алгоритм TCAM для TCAM 2
- Злоупотребление операциями Уровня 4 (L4Op) в ACL
- Чрезмерные ACL для Supervisor Engine или типа коммутатора

Субоптимальный программный алгоритм TCAM для TCAM 2

Как Типы раздела TCAM обсуждает, эффективность TCAM 2 ниже вследствие того, что восемь записей совместно используют одну маску. Программное обеспечение Catalyst 4500 обеспечивает два типа алгоритмов программирования TCAM для TCAM 2, которые повышают эффективность TCAM 2:

- Упакованный — Подходящий для большинства сценариев списка управления доступом**Примечание:** !--- Это стандартный вариант.
- Рассеянный — Используемый в сценарии IPSG

Можно изменить алгоритм на рассеянный алгоритм, но это, как правило, не помогает при настройке только списков управления доступом, таких как RACL. Рассеянный алгоритм является только эффективным при сценариях, где то же или подобный, маленький ACL повторены на многочисленных портах. Этот сценарий имеет место с IPSG, который включен на нескольких интерфейсах. В сценарии IPSG, каждом динамическом ACL:

- Имеет небольшое количество записейЭто включает разрешения для позволенных IP-адресов и запрещения в конце для предотвращения доступа порта неавторизованными

IP-адресами.
- Повторен для всех портов настроенного адресаACL повторен максимум для 240 портов на Catalyst 4507R.

Примечание: TCAM 3 использует упакованный алгоритм по умолчанию. Поскольку структура TCAM является одной маской на запись, упакованный алгоритм является самым лучшим алгоритмом. Поэтому рассеянная опция алгоритма не включена на этих коммутаторах.

Данный пример находится на Supervisor Engine II +, который настроен для функции IPSG. Выходные данные показывают, что, невзирая на то, что только 49 процентов записей используются, использованы 89 процентов масок:

```
Switch#show platform hardware acl statistics utilization brief
                                     Entries/Total(%) Masks/Total(%)
                                    ----------------- ---------------
          Input Acl(PortAndVlan) 2016 / 4096 ( 49)  460 / 512 ( 89)
           Input Acl(PortOrVlan)     6 / 4096 ( 0)    4 / 512 ( 0)
           Input Qos(PortAndVlan)    0 / 4096 ( 0)    0 / 512 ( 0)
           Input Qos(PortOrVlan)     0 / 4096 ( 0)    0 / 512 ( 0)            Output
Acl(PortAndVlan)    0 / 4096 ( 0)    0 / 512 ( 0)           Output Acl(PortOrVlan)     0 / 4096
( 0)    0 / 512 ( 0)           Output Qos(PortAndVlan)    0 / 4096 ( 0)    0 / 512 ( 0)
           Output Qos(PortOrVlan)     0 / 4096 ( 0)    0 / 512 ( 0)            L4Ops: used 2 out
of 64
```

В этом случае изменение в алгоритме программирования от упакованного алгоритма по умолчанию до рассеянного алгоритма помогает. Рассеянный алгоритм уменьшает общее использование маски с 89 процентов до 49 процентов.

```
Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#access-list hardware entries scattered Switch(config)#end Switch#show platform
hardware acl statistics utilization brief Entries/Total(%) Masks/Total(%) ----------------- ----
---------- Input Acl(PortAndVlan) 2016 / 4096 ( 49) 252 / 512 ( 49) Input Acl(PortOrVlan) 6 /
4096 ( 0) 5 / 512 ( 0) Input Qos(PortAndVlan) 0 / 4096 ( 0) 0 / 512 ( 0) Input Qos(PortOrVlan) 0
/ 4096 ( 0) 0 / 512 ( 0) Output Acl(PortAndVlan) 0 / 4096 ( 0) 0 / 512 ( 0) Output
Acl(PortOrVlan) 0 / 4096 ( 0) 0 / 512 ( 0) Output Qos(PortAndVlan) 0 / 4096 ( 0) 0 / 512 ( 0)
Output Qos(PortOrVlan) 0 / 4096 ( 0) 0 / 512 ( 0) L4Ops: used 2 out of 64
```

Для получения информации об оптимальных методах для характеристик безопасности на коммутаторах Catalyst 4500 обратитесь к Оптимальным методам Характеристик безопасности Catalyst 4500 для Супервизоров.

Злоупотребление L4Op в ACL

Термин L4Op относится к использованию **gt**, **lt**, **neq** и ключевых слов **диапазона** в конфигурации списков управления доступом (ACL). Catalyst 4500 имеет пределы на количестве этих ключевых слов, которые можно использовать в одиночном ACL. Ограничение, которое варьируется Supervisor Engine и коммутатором, является или шестью или восемью L4Op на ACL. Таблица 3 показывает предел на Supervisor Engine и на ACL.

Предел таблицы 3 - L4Op на ACL на других Supervisor Engine Catalyst 4500 и коммутаторах

Продукт	L4Op
Supervisor Engine II +/II+TS	32 (6 на ACL)
Supervisor Engine III/IV/V и WS-C4948	32 (6 на ACL)
Supervisor Engine V-10GE и WS-C4948-10GE	64 (8 на ACL)

Если предел L4Op на ACL превышен, предупреждающее сообщение отображено на консоли. Сообщение подобно этому:

```
%C4K_HWACLMAN-4-ACLHWPROGERR: Input Security: severn - hardware TCAM limit, some
packet processing will be software switched.
19:55:55: %C4K_HWACLMAN-4-ACLHWPROGERRREASON: Input Security: severn - hardware TCAM L4
operators/TCP flags usage capability exceeded.
```

Кроме того, если предел L4Op превышен, определенный ACE расширен в TCAM. Дополнительные результаты использования TCAM. Этот ACE служит примером:

```
access-list 101 permit tcp host 8.1.1.1 range 10 20 any
```

С этим ACE в ACL коммутатор использует только одну запись и один L4Op. Однако, если шесть L4Op уже используются в этом ACL, этот ACE расширен до 10 записей в аппаратных средствах. Такое расширение может потенциально израсходовать много записей в TCAM. Тщательное использование этих L4Op предотвращает переполнение TCAM.

Примечание: Если этот случай включает Supervisor Engine V-10GE и WS-C4948-10GE, восемь ранее используемых L4Op в результатах ACL в первоклассном расширении.

Помните эти элементы при использовании L4Op на коммутаторах Catalyst 4500:

- Если оператор или операнд отличаются, операции L4 считают другими.Например, этот ACL содержит три других операции L4, потому что **gt 10** и **gt 11** считают двумя другими операциями L4:`access-list 101 permit tcp host 8.1.1.1 any gt 10 access-list 101 deny tcp host 8.1.1.2 any lt 9 access-list 101 deny tcp host 8.1.1.3 any gt 11`
- Если та же пара оператора/операнда применяется однажды к исходному порту и однажды к порту назначения, операции L4 считают другими.Например:`access-list 101 permit tcp host 8.1.1.1 gt 10 any access-list 101 permit tcp host 8.1.1.2 any gt 10`
- Catalyst 4500 переключает общие L4Op, если это возможно.В данном примере линии в ***полужирном курсиве*** демонстрируют этот сценарий:Использование L4Op для ACL 101 = 5Использование L4Op для ACL 102 = 4 **Примечание:** Ключевое слово **eq** не использует ни одного аппаратного ресурса L4Op.Общее использование L4Op = **8Примечание:** ACL 101 и 102 совместно использует один L4Op.**Примечание:** L4Op разделен, даже если протокол, такой как TCP или Протокол UDP, не совпадает, или разрешать/запрещать действие не совпадает.

Чрезмерные ACL для Supervisor Engine или типа коммутатора

Поскольку Таблица 2 показывает, TCAM является ограниченным ресурсом. Можно превысить ресурс TCAM любого Supervisor Engine при настройке чрезмерных ACL или функций как IPSG с большим числом записей IPSG.

Если вы превышаете пространство TCAM для своего Supervisor Engine, делаете эти шаги:

- Если у вас есть Supervisor Engine II +, и вы выполняете Cisco IOS Software Release, который является *ранее*, чем программное обеспечение Cisco IOS версии 12.2 (18) EW, обновление к последнему программному обеспечению Cisco IOS версии 12.2 (25) отладочный релиз EWA.Емкость TCAM была увеличена в более поздних версиях.
- При использовании отслеживание DHCP и IPSG, и вы начинаете заканчиваться TCAM, использовать последнее программное обеспечение Cisco IOS версии 12.2 (25) отладочный релиз EWA и использовать рассеянный алгоритм в случае TCAM 2

продукта.**Примечание:** Рассеянный алгоритм доступен в программном обеспечении Cisco IOS версии 12.2 (20) EW и позже.Последний выпуск также имеет усовершенствования для лучшего использования TCAM с отслеживанием DCHP и Протоколом Разрешения динамических адресов (ARP) Контроль (DAI) функции.
- Если вы начинаете заканчиваться TCAM, потому что предел L4Op превышен, попытайтесь уменьшить использование L4Op в ACL для предотвращения переполнения TCAM.
- При использовании много подобных ACL или политики по различным портам в той же VLAN, объединяете их в одиночный ACL или политику по интерфейсу виртуальной локальной сети (VLAN).Эта агрегация оставляет некоторое свободное место TCAM. Например, при применении основанной на голосе политики QoS на основе портов по умолчанию используется для классификации. Это QoS по умолчанию может заставить емкость TCAM быть превышенной. При коммутации QoS к на основе VLAN вы уменьшаете использование TCAM.
- Если вы все еще имеете проблемы с пространством TCAM, рассматриваете высокопроизводительный Supervisor Engine, такой как Supervisor Engine V-10GE или Catalyst 4948-10GE.Эти продукты используют самые эффективные аппаратные средства TCAM 3.

Сводка

Catalyst 4500 программирует настроенные ACL с использованием TCAM. TCAM Обеспечивает приложение ACL в пути устройств переадресации без влияния на производительность коммутатора. Производительность является постоянной вне зависимости от размера ACL, так как производительность поиска в ACL является скоростью линии. Тем не менее, TCAM является ограниченным ресурсом. Поэтому, настроив чрезмерное количество записей ACL, можно переполнить емкость TCAM. Catalyst 4500 внедрил множественную оптимизацию и предоставил команды для варьирования алгоритма программирования TCAM для достижения максимальной эффективности. TCAM 3 продукта, такие как Supervisor Engine V-10GE и Catalyst 4948-10GE предложение большинство ресурсов TCAM для списка управления доступом и политик QoS.

Дополнительные сведения

- Страницы поддержки продуктов LAN
- Страница поддержки коммутационных решений для локальной сети
- Cisco Systems – техническая поддержка и документация