

# Применение списков доступа на интернет-маршрутизаторах серии Cisco 12000

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Обзор поддержки ACL на интернет-маршрутизаторе серии Cisco 12000](#)

[Сравнение списков управления доступом на основе специализированной интегральной схемы и CPU](#)

[Фильтрация для панели контроля и управления](#)

[Настройка списков управления доступом \(ACL\) путей получения IP](#)

[Поддержка IPv4 ACL линейной платой данного типа](#)

[Engine 0 - обработка ACL](#)

[Модуль Engine 1 – обработка ACL](#)

[Модуль 2 – обработка ACL](#)

[ISE \(IP Services Engine\), ядро 3 - обработка ACL](#)

[Ядро 4 \(POS\) — обработка ACL](#)

[Модуль 4+ \(POS и DPT\) — обработка ACL](#)

[Engine 4+ \(Ethernet\) — Обработка ACL](#)

[Запись ACL](#)

[IPv4 Output ACL – матрица взаимодействия линейных плат](#)

[Поддержка ACL в IPv6](#)

[Справочник по командам Cisco 12000 ACL](#)

[Глоссарий](#)

[Дополнительные сведения](#)

## **Введение**

Этот документ описывает поддержку списков контроля доступа (ACL) на Интернет-маршрутизаторах Cisco 12000 серии.

## **Предварительные условия**

### **Требования**

Cisco рекомендует ознакомиться с основами того, как ACL работает на маршрутизатор Cisco.

См. эти документы для получения общей информации на ACL и их приложениях:

- [Списки управления доступом: краткий обзор и инструкции](#)
- [IP-сервисы Настройки: пакеты IP фильтра](#)

## [Используемые компоненты](#)

Сведения в этом документе основываются на Интернет-маршрутизаторах Cisco 12000 серии.

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.](#)

## [Обзор поддержки ACL на интернет-маршрутизаторе серии Cisco 12000](#)

На Интернет-маршрутизаторе Cisco 12000 серии ACL могут быть обработаны в аппаратных средствах (Специализированная интегральная схема - ASIC), программное обеспечение (ЦП линейной карты), или как гибридная функция – обработанный в программном обеспечении с аппаратной поддержкой. Обработан ли ACL в аппаратных средствах, или программное обеспечение зависит от приложения ACL, типа модуля линейной карты и взаимодействия от ACL в других линейных картах.

Модули линейной платы Cisco серии 12000 предоставляют различные возможности ACL. Для сведений о поддержке ACL для механизма карты частичного канала перейдите к соответствующему разделу в этом документе.

**Примечание:** ACL Групповой IP-адресации не поддерживаются в Выпуске 12.0S программного обеспечения Cisco IOS. Функция IP Multicast boundary может быть использована, где требуется фильтрация групповой адресации. См. [Multicast Forwarding Fast-Path на Engine 2 Серии Cisco 12000 и Линейных картах ISE](#) для получения дополнительной информации.

## [Сравнение списков управления доступом на основе специализированной интегральной схемы и CPU](#)

Cisco 12000 поддерживает все поколения Обработки ACL. Понимание практических аспектов того, как каждый из этих режимов обработки работает, взаимодействуйте и поддерживайте друг друга, важно для эффективного использования ACL на Cisco 12000.

Первые поколения Обработки ACL использовали программируемый ЦП для обработки ACL. В течение долгого времени требования к скорости обработки пакета в секунду (PPS) превысили способность новых ЦПУ поддержать на высоком уровне. ASIC-схемы были

созданы для достижения более высоких скоростей PPS для передачи маршрутизатора и функциональных возможностей. ACL, которые были загружены на ЦП линейной платы (LC), были тогда загружены на ASIC LC. ASIC-схемы продолжили быть импровизированными для обработки более высоких скоростей PPS. Эти ASIC-схемы второго поколения были основаны на новаторской работе генерации прежде и предлагают большие поддержки ASIC. Поскольку Cisco 12000 является распределенной платформой маршрутизации, взаимодействие между различными поколениями Обработки ACL может создать некоторый беспорядок в работе.

Термины, такие как Список управления доступом на основе ASIC, ACL на основе ЦПУ, Быстрый маршрут, Медленный Путь и Избыточные направления ASIC использованы всюду по этому документу, чтобы помочь объяснять, что происходит при Обработке ACL. Вот пояснения этих сроков:

- Списки управления доступом на основе ASIC (Быстрый маршрут) — ACL загружены и обработаны в оборудовании ASIC. Блок производительности ASIC определяет глубину ACL, быстродействие и функциональные возможности. Быстрый маршрут использовался в пути для иллюстрирования различия между на основе ASIC обработкой и обработкой, сделанной в поддерживающем LC ЦП. Больше общего термина, на основе ASIC, использовано в этом документе.
- ACL на основе ЦПУ (Медленный Путь) — ACL обработаны в программном обеспечении на ЦП линейной карты. Для карт первых поколений (Механизм 0 и в некоторых случаях Механизм 1), вся обработка сделана на ЦП LC. На основе ASIC LC выполняют Обработку ACL на пакетах, которые плывутся на плоскодонке от ASIC. Медленный Путь использовался в прошлом, чтобы проиллюстрировать, как избыточные направления к ЦП LC были медленнее, чем ASIC. Больше общего термина, основанного на ЦП, использовано в этом документе.
- Избыточные направления ASIC — ASIC-схемы имеют определенные шаблоны конверта. Когда пакет превышает разработанный конверт, он плывется на плоскодонке от ASIC, который будет обработан или на ЦП поддержки LC или передан до Процессора маршрута (RP). Пакеты избыточного направления Списков управления доступом на основе ASIC, которые выходят за пределы дизайна ASIC. Примером является ACL, который имеет ACE с журналом или ключевым словом регистрации-входа. Данные, необходимые для регистрации запросов пакета, следует обрабатывать вне ASIC, то есть пакеты автоматически перенаправляются из ASIC в LC CPU и обрабатываются как обычные ACL на основе CPU.

**Примечание:** При настройке маршрутизации на основе политик (PBR) с сообщениями о совпадении для соответствия с ACL, ACL не должны совпадать с исходным портом. Маршрутизатор гигабитного коммутатора (GSR) не поддерживает аппаратную коммутацию для PBR с ACL, которые совпадают с исходным портом. Это инициирует коммутацию в контексте процесса, и производительность GSR ухудшается.

## [Фильтрация для панели контроля и управления](#)

Процессор маршрутизатора предоставляет контроль и сервисы панели управления в распределенной архитектуре Серии Cisco 12000. ACL Тракта приема (rACL) предоставляют простую распределенную возможность фильтрации контроля и трафика управления, предназначенного для RP. Это может быть логически просмотрено как дополнительный уровень безопасности, которая использует преимущества сильных мест распределенной

архитектуры.

## [Настройка списков управления доступом \(ACL\) путей получения IP](#)

RACL был представлен через специальную документацию по предварительному релизу в дроссель обслуживания релиза 12.0 программного обеспечения Cisco IOS (21) S2. Это официально поддерживается в программном обеспечении Cisco IOS версии 12.0(22)S. См. [IP Получают ACL](#) для получения дополнительной информации.

Процессор маршрутизатора предусматривает поддержку служб плоскости управления для распределенной архитектуры маршрутизаторов Cisco серии 12000. Получить ACL предоставляют возможности фильтрации контрольного трафика, предназначенного для RP, такие как запросы Протокола SNMP и обновления маршрута.

RACL считают Фазой 1 многофазного усилия добавить новые меры защиты к контролю и управлению трафика плоскости. Новые усовершенствования ограничения скорости добавляются через обновления ПО.

## [Поддержка IPv4 ACL линейной платой данного типа](#)

Линейные платы серии 12000 имеют различные возможности ACL для каждого типа модуля. В этом разделе описываются возможности ACL других механизмов линейной карты. Для сведений о поддержке ACL для механизма карты частичного канала посмотрите соответствующий раздел этого документа.

Существуют некоторые общие характеристики для всех ACL (ASIC и основанный ЦП):

- Только один ACL может быть применен к интерфейсу для каждого направления. Например, interface POS 0/0 может иметь только один ввод для ACL и один список ACL для выходных данных.
- Тестирование пакета по списку управления доступом останавливается при нахождении соответствия. Если ACL, который является 300 записями долго, совпадает с пакетом на Записи Access-list (ACE) #45, то пакет обработан, и Обработка ACL остановлена.
- Существует неявное, **не разрешают весь** въезд в конце каждого ACL. В результате, если там не идет ни в какое сравнение на ACL, пакет отброшен. ACL Cisco созданы с *явным разрешением архитектуры ACL*. Это означает, что должен быть ACE для соответствия с пакетом для него, чтобы быть обработанным и переданным.
- Недавно добавленные ACE всегда добавляются до конца ACL. Каждый раз, когда ACL требует обновлений, это - полезный прием для удаления ACL (используйте **команду по access-list**), и повторно добавьте новый ACL.
- Поскольку IP - фрагменты неначальных не содержат сведения о протоколе Уровня 4 в IP - заголовке, только стандартные условия соответствия поддерживаются для неначальный фрагментов. Полное изложение о том, как ACL Cisco соответствуют фильтрации IP - фрагмента, может быть найдено в [Списках контроля доступа и IP - фрагментах](#).
- Пронумерованные ACL обработаны и применены, как только они введены через интерфейс командной строки (CLI). С большими ACL это иногда приводит к Всплеску нагрузки ЦПУ на RP или ЦП LC.

## Engine 0 - обработка ACL

Механизм 0 является первой линейной картой, отправленной для Cisco 12000. Это - вся Процессорная обработка и передача. Следовательно, Механизм 0 линейных карт обрабатывает ACL в ЦП LC.

Эти линейные карты основываются на Механизме 0:

Тип линейной карты	Тип интерфейса	Подключение
12 x DS3	Коаксиальный	SMB
12 x DS3	Коаксиальный	SMB
12 x E3	Коаксиальный	SMB
1xCHOC12->DS3		ИК
1xCHOC12/STM4->OC3/STM1	POS	ИК
4xOC3c/STM1c	POS	SR
4xOC3c/STM1c	POS	LR
4xOC3c/STM1c	POS	MM
1xOC12c/STM4c	POS	ИК
1xOC12c/STM4c	POS	MM
6xCT3->DS1		SMB
2xCHOC3/STM1->DS1/E1		ИК
4xOC3c/STM1c	ATM	ИК
4xOC3c/STM1c	ATM	MM
1xOC12c/STM4c	ATM	ИК
1xOC12c/STM4c	ATM	MM

## Поддерживаемые условия соответствия

Весь Cisco IOS Software Release 12.0S Стандарт, Расширенный список ACL и Турбо ACL поддерживается на Механизме 0.

## Количество поддерживаемых ACE

Размер ACL ограничен только ресурсами доступной памяти и требованиями к производительности.

## Обработка выходных данных ACL

Полученные списки контроля доступа обрабатываются другими линейными картами в системе на установленном маршруте. Толчок Списка ACL для выходных данных входной стороне других LC защищает объединительную плату от передачи пакетов, которые будут отброшенными. Это - наследованная функция от распределенной архитектуры на Cisco 7500. Подробное объяснение, причины и рекомендации по эксплуатации предоставлены в

[Списке ACL для выходных данных IPv4 - Межоперационная матрица линейной карты.](#)

## [Линейная карта определенные команды](#)

Нет.

## [Руководство по эксплуатации и взаимодействие линейных плат](#)

- Если NetFlow настроен на Механизме, 0 линейных карт и список ACL для выходных данных настроены на выходном механизме 3 или 4 + линейная карта, список ACL для выходных данных обработан и входными линейными платами и выходными линейными платами, чтобы позволить NetFlow составлять пакеты, запрещенные ACL, а также переданными пакетами.

## [Рекомендации](#)

Cisco рекомендует использование Турбо ACL на Механизме 0 для больших ACL. Малые линейные ACL более эффективны для меньших ACL, поскольку Turbo ACL требуют дополнительной памяти.

## [Модуль Engine 1 – обработка ACL](#)

### [Обзор](#)

Механизм 1 линейная карта является мостом между Процессорной обработкой на Механизме 0 и ASIC передачи/функции первого поколения на Engine 2. Механизм 1 линейная карта обрабатывает ACL в программном обеспечении по умолчанию. С программным обеспечением Cisco IOS версии 12.0(10)S и позже, Механизм 1 предоставляет аппаратные ACL для карт, оборудованных версиями 4 или 5 ASIC Salsa (см. Справочник по командам Линейной карты ниже для определения, которой версией Salsa конкретная карта оборудована).

Эти линейные карты основываются на Механизме 1:

Тип линейной карты	Тип интерфейса	Подключение
8xFE	(RJ45)	100BaseT
8xFE	(MM)	100BaseF
8xFE	(RJ45)	100BaseT
8xFE	(MM)	100BaseF
1xGE	SX,	GBIC:
1xGE	SX,	GBIC:
2xOC12c/STM4 c	DPT	ИК
2xOC12c/STM4 c	DPT	LR
2xOC12c/STM4 c	DPT	XLR
2xOC12c/STM4 c	DPT	MM
2xOC12c/STM4 c	DPT	ИК

2xOC12c/STM4 c	DPT	LR
2cOC12c/STM4c	DPT	XLR
2xOC12c/STM4 c	DPT	MM

### [Поддерживаемые условия соответствия](#)

Весь Cisco IOS Software Release 12.0S поддерживаемый Стандарт, Расширенный, и Турбо ACL, поддерживается в ЦП LC (Медленный Путь). Кроме того, Механизм 1 может ACL входных данных процесса в ASIC Salsa. ASIC Salsa обрабатывает обработку ввода для ACL наряду с поиском маршрута, приводящим к повышению производительности когда по сравнению с Традиционной Линейной Обработкой ACL и обработкой Turbo ACL. SALSА ASIC не удастся обработать выходные ACL или ACL дочерних интерфейсов.

### [Количество поддерживаемых ACE](#)

Размер ACL ограничен только ресурсами доступной памяти и требованиями к производительности.

### [Обработка выходных данных ACL](#)

Полученные списки контроля доступа обрабатываются другими линейными картами в системе на установленном маршруте. Посмотрите [Список ACL для выходных данных IPv4 - раздел Межоперационной матрицы линейной карты](#) для получения дополнительной информации.

### [Линейная карта определенные команды](#)

- `access-list hardware salsa`
- покажите, что контроллер I3 | включает ASIC

### [Руководство по эксплуатации и взаимодействие линейных плат](#)

- Salsa ASIC и PSA ASIC не могут функционировать одновременно. Команда `access-list hardware` принимает только либо PSA (Модуль 2), либо Salsa (Модуль 1), но не оба.
- Если NetFlow настроен на Механизме, 1 линейная карта и список ACL для выходных данных настроены на выходном механизме 3 или 4 + линейная карта, список ACL для выходных данных обработан и входными линейными платами и выходными линейными платами, чтобы позволить NetFlow составлять пакеты, запрещенные ACL, а также переданными пакетами.

### [Рекомендации](#)

Для версий модуля 1 линейная карта, которые не поддерживают аппаратные ACL, Cisco, рекомендует использование Турбо ACL для больших ACL. Некоторые ACL (которые имеют менее 20 линий) можно использовать как линейные ACL для экономии памяти.

### [Модуль 2 – обработка ACL](#)

## Обзор

Модуль Engine 2 стал первой платой, в которой была применена функциональная схема пересылки ASIC. С программным обеспечением Cisco IOS версии 12.0(10)S и позже, линейные карты Engine 2 предоставляют аппаратные возможности ACL в высокоэффективном ASIC коммутации пакетов (PSA). Как со всеми ASIC-схемами передачи/функции, строгими огибающими производительности задаются границы на возможности ASIC. Конверт ключевой производительности на ACL Engine 2 происходит из-за ограничений памяти в ASIC PSA.

Пересылка пакетов в Engine 2 сделана ASIC PSA. PSA Имеет три основных внешних памяти:

- PLU (поиск Пути) — Используемый для хранения узлов mtree
- TLU (Поиск таблиц) — Используемый для хранения отключений FIB и возможно loadbalance структуры. Также используемый для удержания многих структур данных ACL PSA
- SRAM — основное расположение для структур распределения нагрузки

Характеристика ACL PSA является основанной на микрокоде реализацией проверки ACL. Специальный набор инструкций загружен в микросхему PSA, которая позволяет основной ACL проверять. Существует много ограничений к этой функции, которая должна быть тщательно понята перед развертыванием. Один главный недостаток к ACL PSA является большим количеством требуемой памяти аппаратной переадресации.

Характеристика ACL PSA требует, чтобы большой блок памяти PLU/TLU был предварительно выделен независимо от количества префиксов и т.д. Поскольку это выделение прибывает прежде всего из области TLU, оно оказывает значительное влияние на количество маршрутов, которые могут быть поддержаны на этих картах, когда настроены ACL PSA.

В дополнение к начальным издержкам памяти PLU/TLU каждый префикс, сохраненный в памяти TLU, требует значительно большей памяти. Минимальный объем памяти для каждого префикса варьируется, на основе направления примененного ACL (вход по сравнению с выходом) и тип линейной платы. В целом выходные ACL требуют большей памяти, чем вход, и линейные платы с большим количеством физических портов требуют большей памяти что те с меньшим количеством портов.

В случае, где линейная плата Engine 2 не использует ACL, структуры данных для ACL созданы независимо от фактических настроенных ACL. Для изменения на меньшие структуры не-ACL необходимо настроить **аппаратный psa никакого access-list** на маршрутизаторе. Эта команда отключает всю Обработку ACL на всех линейных платах Engine2 во всех направлениях. Cisco recomms для использования их с экстремальным вниманием.

## Обзор

Для обеспечения производительности Обработки ACL, которая является независимом от точности совпадения, ACL Engine 2 интегрированы в таблицу переадресации оборудования. Посмотрите ниже для пояснений о том, как это может повлиять на префиксную масштабируемость.



Эти линейные карты основываются на Engine 2:

Тип линейной карты	Тип интерфейса	Подключение
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	LR
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	LR
1xOC192c/STM64c	Включатель	SR
16xOC3c/STM1c	POS	ИК
16xOC3c/STM1c	POS	ММ
4xOC12c/STM4c	POS	ИК
4xOC12c/STM4c	POS	ММ
4xOC12c/STM4c	POS	ИК
4xOC12c/STM4c	POS	ММ
4xOC12c/STM4c	ATM	ИК
4xOC12c/STM4c	ATM	ММ
8xOC3cSTM1c	ATM/TS	ИК
8xOC3c/STM1c	ATM/TS	ММ
3xGE	SX	GBIC:
3xGE	CWDM	GBIC:
1xOC48c/STM16c	DPT	SR
1xOC48c/STM16c	DPT	LR
1xOC48c/STM16c	DPT	SR
1xOC48c/STM16c	DPT	LR

### [Поддерживаемые условия соответствия](#)

Весь Cisco IOS Software Release 12.0S поддержал условия соответствия Стандарта и Расширенного списка ACL, кроме исходных портов Уровня 4. Прерывистые маски, поля приоритета IP-трафика и исходные порты Уровня 4 плавутся на плоскодонке от ASIC PSA и обрабатываются на ЦП LC.

### [Количество поддерживаемых ACE](#)

До пяти 448-линейных входящих списков ACL в PSA. Один ACL может быть настроен на порт. Дополнительные ACL администрируемы ЦП линейной карты. Посмотрите раздел

“Ограничений” ниже для ограничений на списки ACL для выходных данных.

## Обработка выходных данных ACL

Список ACL для выходных данных, настроенный на этой линейной карте, будет выполнен во входном пути характеристики других линейных карт в системе. Посмотрите [Список ACL для выходных данных IPv4 - Межоперационная матрица линейной карты](#) для подробных данных.

## Линейная карта определенные команды

- **access-list hardware psa limit 128**
- **no access-list hardware psa**
- **psa bypass**
- **show access-list psa detail**
- **show access-list psa summary**
- функция **show controller psa**

## Руководство по эксплуатации и взаимодействие линейных плат

- Обработка ACL быстрого маршрута требует, чтобы были встречены эти условия:Применяемый ACL находится в границе 128- or 448- ACE.Если команда **access-list hardware psa limit 128** настроена, длина должна быть меньше чем 128 ACE.Длина должна быть менее 448 ACE если требуется пакет микрокода ACI на 448 линий.ACL ввода/вывода не настроены вместе на карту.*На этом маршрутизаторе можно настроить до пяти выходных ACL.*
- Только ACL с 128 линиями поддерживаются на 8-и карты Pos линии OC-3/STM-1 с 16 портами. 448 линейка ACL поддерживается на 4-портовой OC-12/STM-4 POS, 1-портовой OC-48/STM-16 POS, и 3-портовой Gigabit Ethernet линейных картах.
- Вводы для ACL берут приоритет в быстром маршруте по спискам ACL для выходных данных, когда оба настроены одновременно на той же карте (список ACL для выходных данных обработан в медленном пути).
- Если список ACL для выходных данных будет настроен на карте Engine 2, и входной линейной платой является Механизм 0/1/2/4, то список ACL для выходных данных будет обработан в карте доступа. Для других типов модуля список ACL для выходных данных будет обработан в медленном пути выхода Engine 2.
- Списки ACL для выходных данных не поддерживаются для IP К ТРАФИКУ MPLS (первый MPLS label, “Выдвигаемый” на пакет IP).
- Информация об обработке ACL интегрирована в аппаратный FIB и может повлиять на префиксную масштабируемость. О префиксном исчерпании памяти сообщают ошибки выделения памяти с “ехтет=1” подписью в сопроводительном сообщении журнала.

## Рекомендации

- Информация об обработке ACL интегрирована в таблицу пересылки CEF, которая уменьшает префиксную масштабируемость. Приложения, которые не используют ACL, могут отключить поддержку ACL в таблице CEF и таким образом увеличить доступную

- префиксную память путем запуска **команды no access-list hardware psa**.
- Конфигурация **команды no access-list hardware psa** отключает всю Обработку ACL картами Engine 2 в дополнение к отключению поддержки PSA ACL. Это не вызывает выполнение программного обеспечения ACL. Данное условие также применяется в том случае, если настроены выходные ACL для выходной линейной платы.
  - Конфигурация **команды access-list compiled** после **команды access-list hardware psa** преобразовывает ACE, которые превышают емкость PSA в Turbo ACL. Это обеспечивает оптимальную работу списков ACL длиной свыше 448 ACE. По умолчанию микрокод ACL равен 128 (в соответствии с версией Cisco IOS Software Release 12.0(14)S/ST). Если меньшие ACL используются, и возможность с 448 линиями не требуется, настраивание **команды access-list hardware psa limit 128** сохраняет передачу (TLU) память, которая улучшает префиксную масштабируемость). Обработка Turbo ACL должна быть включена с **командой access-list compiled** для ACL дольше, чем 129 линий наряду с **командой access-list hardware psa limit 128**. Эта комбинация обрабатывает первые 128 линий в ASIC PSA и остающиеся линии с Турбо ACL, который оптимизирует производительность при сохранении передачи памяти.
  - Карта линии ATM OC12 с 4 портами не поддерживает вводы для ACL, но предоставляет обнаружение списка ACL для выходных данных в микрокоде, который позволяет процесс списков ACL для выходных данных в медленном пути.
  - 8xOC3 поддержки плат линии ATM для каждого VC 128 ACL линии с программным обеспечением Cisco IOS версии 12.0(23)S и позже. Максимум 16 отдельных вводов для ACL может быть настроен в быстром маршруте. 448 вводов для ACL поддерживаются на виртуальном канале в медленном пути только. Списки ACL для выходных данных не поддерживаются.

## [ISE \(IP Services Engine\), ядро 3 - обработка ACL](#)

### [Обзор](#)

Механизм 3 является первой Двойной передающей линейной картой этапа. На входном и выходном пути Engine 3 имеет ASIC-микросхемы расширения/переадресации. Это позволяет размещать списки ACL в ASIC как для входных, так и для выходных путей. Кроме того, структура ASIC Механизма 3 является гибридным массивом конвейера/параллели. Структура ASIC внедряет Обработку ACL в параллельном высокоскоростном Ternary Content Addressable Memory (TCAM), который предоставляет обработку скорости линии до ACE 20K на вход и ACE 20K на выход.

Эти линейные карты основываются на Механизме 3:

Тип линейной карты	Тип интерфейса	Подключение
4xOC12c/STM4c	POS	ИК
4xOC12c/STM4c	POS	ММ
4xCHOC12/STM4 -> OC3/STM1-> DS3/E3	POS	ИК
16xOC3c/STM1c	POS	ИК
16xOC3c/STM1c	POS	ММ

8xOC3/STM1c	POS	ИК
8xOC3c/STM1c	POS	ММ
4xOC3c/STM1c	POS	ИК
4xOC3c/STM1c	POS	ММ
4xOC3c/STM1c	POS	LR
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	LR
1xCHOC48/STM16-> STM4-> OC3/STM1-> DS3/E3	POS	SR
4xOC12c/STM4c	ATM/IP	ИК
4xOC12c/STM4c	ATM/IP	ММ
4xGE	GE	
4xOC12c/STM4c	DPT	ИК
4xOC12c/STM4c	DPT	XLR

### [Поддерживаемые условия соответствия](#)

Весь Cisco IOS Software Release 12.0S Стандартные и Расширенные условия соответствия поддерживаются в быстром маршруте за исключением регистрационных ACE, которые обработаны ЦП линейной карты.

### [Количество поддерживаемых ACE](#)

- Обработка скорости линии и во входе и в выходном направлении на порт, на VLAN, на подинтерфейс Frame Relay, и на подчиненного интерфейс ATM. Поддерживается до 20 000 расширенных ACE на одно направление и одну карту.
- Условия соответствия для источника/порта назначения TCP/UDP “диапазон”, “lt”, и “gt” все обрабатываются в аппаратных средствах с помощью “ресурсы” оператора L4.
- Количество отдельных компонентов операции L4 ограничено 32 для всей линейной платы. Операторы исходного порта ограничены максимумом шесть.

### [Обработка выходных данных ACL](#)

Собственная поддержка fast-path на скорости пропускной способности обработки списка ACL для выходных данных в Пакетном ASIC Обработки тракта передачи. Посмотрите [Список ACL для выходных данных IPv4 - Межоперационная матрица линейной карты](#) для подробных данных.

### [Линейная карта определенные команды](#)

- **hw-module** <слот #> no-merge компиляции tcam!---12.0 (21) S3
- аппаратный интерфейс **show-access-list** <имя интерфейса>

- `show cef INT POS [x/y] | inc if_number`

## [Руководство по эксплуатации и взаимодействие линейных плат](#)

- Пакетные ACE регистрации соответствия обработаны в медленном пути.
- Пакеты, согласующие отклонение ACE (прерывание для обеспечения защиты против системного прерывания), обрабатываются в медленном маршруте.
- Когда ACL включает диапазон адресов, аппаратные средства используют специальные ACE, вызванные “ACE Диапазона”, которые требуют до трех ACE.
- Объединение ACL может сохранить ресурсы TCAM путем совместного использования общих ACE через отдельные ACL. **Чтобы определить, объединены ли ACL, используйте команду интерфейса оборудования `show-access-list`.**
- Счетчики ACL не поддерживаются для объединенных ACL. С программным обеспечением Cisco IOS версии 12.0(21)S3 и позже, Объединение ACL может быть отключено с `hw-module <слот #> команда no-merge компиляции tcam`. Чтобы определить, объединен ли ACL, используйте команду `show-access-list hardware interface`.
- Если NetFlow будет настроен на Механизме 0/1 линейная карта, и список ACL для выходных данных настроен на выходном Механизме 3 или 4 + линейная карта, то список ACL для выходных данных будет обработан и входными линейными платами и выходными линейными платами, чтобы позволить NetFlow составлять пакеты, запрещенные ACL, а также переданными пакетами.

## [Поддержка счетчика ACL](#)

	Per-ACE	Per-ACE (hardware counters)	Aggregate
21S3/ST3		X	
22S		X	X
23S	X	X	X

### Определения:

- На ACE — Обычная поддержка программного обеспечения Cisco IOS, команда `<number> show access-list` на RP/LC отображает ACL и счетчик, привязанный к каждому ACE. Это доступно только, когда **слияние** отключено перед настройкой любых ACL. Это может быть сделано при помощи этой команды настройки: `Router(config)#hw-module slot <number> tcam compile acl no-merge` Эта опция, когда включено выключает некоторую оптимизацию объединения TCAM и влияет на масштабируемость. Конкретный результат зависит от отдельных ACL. Также обратите внимание, что счетчики не будут корректны, если маршрутизация на основе политик будет применена на тот интерфейс. В этом случае составной счетчик должен использоваться.
- На ACE (TCAM) — Аппаратные счетчики связались с каждым множеством технических разделов. Никакая конфигурация не необходима и нет никакого влияния на производительность/масштабируемость. Доступный только на линейной карте с помощью этого CLI. Эти счетчики невозможно очистить программным методом. `LC-Slot4#show contr tofab alpha acl <if-number> vmr2ace` Новый CLI общего назначения для этой команды будет доступен в 22 Cisco IOS Software Release: `LC-Slot4#show access-list hardware interface p0:1 in` Как со счетчиком на ACE, счетчики TCAM допустимы только, когда PBR не используется на том интерфейсе с ACL.
- Агрегат — Каждый ACL показывает, что сводка разрешает/запрещает счетчик. Это

сумма всех счетчиков ACE. Никакая конфигурация не необходима и нет никакого влияния на производительность или масштабируемость.

## [Рекомендации](#)

Ни один в это время.

## [Ядро 4 \(POS\) — обработка ACL](#)

### [Обзор](#)

Механизм 4 оказывает эту поддержку ACL с программным обеспечением Cisco IOS версии 12.0(18)S и позже:

- Выходные списки ACL поддерживаются линейными картами E0/1/2 в том случае, если линейная карта модуля 4 является платой входа. В этой конфигурации список ACL для выходных данных обработан ЦП выходной линейной платы.

Эти линейные карты основываются на Механизме 4:

Тип линейной карты	Тип интерфейса	Тип модуля	Подключени е
4xOC48c/ST M16c	POS	E4	
4xOC48c/ST M16c	POS	E4	LR
1xOC192c/S TM64c	POS	E4	ИК
1xOC192c/S TM64c	POS	E4	SR
1xOC192c/S TM64c	POS	E4	VSR-1
10xGE	SFP	E4	

## [Модуль 4+ \(POS и DPT\) — обработка ACL](#)

### [Обзор](#)

Механизм 4 + представляет функцию списка прав доступа (ACL) портфелю Серии Cisco 12000 10 гигабитов.

На каждом входном и выходном маршруте поддерживается до 1024 устройств ACE. Оба ACL Ввод/вывода обработаны в скорости линии максимум для 96 ACE. Эффективность для более длинных строк сопоставления изменяется с глубиной сопоставления.

Эти карты Pos линии основываются на Механизме 4 +:

Тип линейной	Тип интерфейса	Подключение
--------------	----------------	-------------

<b>карты</b>		
4xOC48c/STM16c	POS	SR
4xOC48c/STM16c	POS	LR
1xOC192c/STM64c	POS	ИК
1xOC192c/STM64c	POS	SR
1xOC192c/STM64c	POS	VSR-1
1xOC192c/STM64c	POS	LR
4xOC48c/STM16c	DPT	SFP:
1xOC192c/STM64c	DPT	ИК
1xOC192c/STM64c	DPT	SR
1xOC192c/STM64c	DPT	VSR-1
1xOC192c/STM64c	DPT	LR

### [Поддерживаемые условия соответствия](#)

Весь Cisco IOS Software Release 12.0S поддерживаемые критерии Стандарта и Расширенного списка ACL поддерживается в быстром маршруте за исключением ACE фрагмента или журнала.

### [Количество поддерживаемых ACE](#)

Быстрый путь поддерживает в каждом направлении до 1024 ACE.

**Примечание:** 1021 ACE можно настраивать. Три записи зарезервированы для ACE неявный **permit ip any any**, **deny ip any any**, и команды **send to CPU**.

Верхнего предела для количества поддерживаемых ACE не существует. Любые ACE вне этого 1021 предела выполнены в линейной карте медленный путь.

### [Обработка выходных данных ACL](#)

Выходные данные ACL обрабатываются на быстром пути передающей стороны. Посмотрите [Список ACL для выходных данных IPv4 - Межоперационная матрица линейной карты](#) для подробных данных.

### [Линейная карта определенные команды](#)

- **show tcam**, прикладной [acl - в / acl] tcam <метка - нет>
- **show tcam**, прикладной [acl - в / acl] <port> памяти <количество записей>

## [Руководство по эксплуатации и взаимодействие линейных плат](#)

- ACL подчиненного интерфейса не поддерживаются.
- Производительность меняется в зависимости от глубины соответствия.
- Записи диапазона используют два правила ACL (три в случае пересечения двумя записями границы).
- Один ACL поддерживается на каждом физическом интерфейсе.
- До 1024 ACE (на направление) поддерживаются в быстром маршруте.
- Любой из 1024 ACE быстрого маршрута может быть разделен через порты.
- ACE, которые используют ключевое слово фрагмента, фильтруются в медленном пути.
- Отклоненные пакеты не посчитаны для ACE, обрабатываемых в медленном пути.
- Если NetFlow настроен на Механизме, 0 линейных карт и список ACL для выходных данных настроены на выходном механизме 3 или 4 + линейная карта, список ACL для выходных данных будет обработан и входными линейными платами и выходными линейными платами, чтобы позволить NetFlow составлять пакеты, запрещенные ACL, а также переданными пакетами.

## [Рекомендации](#)

Ни один в это время.

## [Engine 4+ \(Ethernet\) — Обработка ACL](#)

### [Обзор](#)

Механизм 4 + карты Линии Ethernet представляет функциональность ввода для ACL на vlan в аппаратных средствах к портфелю 10 Gigabit Ethernet Cisco 12000. Это некоторые характеристики:

- ACL ввод/вывода могут быть применены одновременно на одном порте без влияния на производительность.
- ACL могут быть применены на VLAN или на порт.
- Производительность Ввода для ACL до ACE 15K не ухудшается с глубиной соответствия.
- Списки ACL для выходных данных обработаны в скорости линии максимум для 96 ACE. Эффективность для более длинных строк сопоставления изменяется с глубиной сопоставления.

Эти карты Линии Ethernet основываются на Механизме 4 +:

Тип линейной карты	Тип интерфейса	Тип модуля
10xGE Rev B ("X-B")	SFP:	E4 +
Модульный	SFP:	E4 +



1x10GE	10G	E4 +
1x10GE	10G	E4 +

### [Поддерживаемые условия соответствия](#)

Весь Cisco IOS Software Release 12.0S поддерживаемые критерии Стандарта и Расширенного списка ACL поддерживаются в быстром маршруте за исключением ACE фрагмента или журнала.

### [Количество поддерживаемых ACE](#)

- До 15,000 вводов для ACL, которые могут быть настроены на порт или на VLAN.
- 1024 выходных данных ACE на карту, которые могут быть применены на на порт. **Примечание:** 1021 ACE можно настраивать. Три записи зарезервированы для ACE неявный `permit ip any any`, `deny ip any any`, и команды `send to CPU`.

### [Обработка выходных данных ACL](#)

Исходящие ACL обрабатываются по стандартной схеме на быстром маршруте на передающей стороне. Посмотрите [Список ACL для выходных данных IPv4 - Межоперационная матрица линейной карты](#) для получения дополнительной информации.

### [Линейная карта определенные команды](#)

- слияние `acl ip <number> hw-module slot`

### [Руководство по эксплуатации и взаимодействие линейных плат](#)

- ACE, которые содержат ключевое слово фрагмента, обработаны в медленном пути.
- Счетчики ACL не поддерживаются для ACL, объединенных с другими функциями.
- Счетчики ACL не поддерживаются для объединенных ACL. Объединенные ACL конфигурируемы с `hw-module slot <номер слота>` команда слияния `acl ip`.
- Операции to168 L4 поддерживаются на линейную карту. Как только это превышено, ACL выполнен в медленном пути.
- Если Механизм, который 1 линейной карте включили дискретный сетевой поток и список ACL для выходных данных, включен на выходном Механизме 3 или 4 + линейная карта, список ACL для выходных данных обработан и входными линейными платами и выходными линейными платами, чтобы позволить NetFlow составлять пакеты, запрещенные ACL, а также переданными пакетами.

### [Рекомендации](#)

Ни один в это время.

## [Запись ACL](#)

Перед программным обеспечением Cisco IOS версии 12.0(21)S информация о Регистрации ACL передавалась RP исключительно по Шине обслуживания (MBUS). Во время высокого уровня действия Регистрации ACL было возможно превысить емкость MBUS. Программное обеспечение Cisco IOS версии 12.0(21)S представляет несколько оптимизации, которая предотвращает этот сценарий.

О ситуациях перегрузки MBUS сообщает программное обеспечение Cisco IOS с этими сообщениями об ошибках:

LCLOG-3-INVSTATE

MBUS\_SYS-3-SEQUENCE

В то время как более низкая серьезность (степени серьезности ошибки 5-7) сообщения журнала отправлена RP через коммутационную матрицу более высокой пропускной способности, с программным обеспечением Cisco IOS версии 12.0(21)S и позже, высокий уровень важности (степени серьезности ошибки 0-4) сообщения регистрации отправлены RP через MBUS. Сообщения журнала ACL являются высоким уровнем важности, таким образом теперь отправлены RP через коммутационную матрицу.

Это добавило, что функциональность регистрации является конфигурируемым использованием этих команд:

- *logging method mbus severity* — Определяет, какие сообщения, степенями серьезности ошибки, будут передаваться RP с помощью MBUS. Сообщения более высокого уровня важности будут передаваться через коммутационную матрицу.
- *show logging method* – Отображает текущий метод регистрации для сообщений всех уровней важности.
- *при регистрации цифр последовательности* — Эта команда включает линейную карту передачи к сообщениям журнала порядкового номера так, чтобы сообщения могли быть должным образом переупорядочены RP. Без этой команды сообщения журнала могут быть отправлены RP в непоследовательном порядке.

## IPv4 Output ACL – матрица взаимодействия линейных плат

Перед Обработкой ACL введения обработки входящего ACL с выпуском Механизма 3 и Механизма 4 +, списки ACL для выходных данных были обработаны входной линейной платой. Выходные списки ACL были обновлены для использования высокопроизводительных функций обработки выходных списков ACL модулей 3 и 4+.

Эта диаграмма предоставляет сводку того, где списки ACL для выходных данных обработаны для других комбинаций линейной карты:

	Выходная линейная карта					
Входная линейная плата (список ACL для выходных данных применилс	E0	E1	E2	E3	E4	E4 +

я к задействов анному интерфейс у),						
E0	Вход	Вход	Вход	Выхо д	н/д	Выхо д
E1	Вход	Вход	Вход	Выхо д	н/д	Выхо д
E2	Вход	Вход	Вход	Выхо д	н/д	Выхо д
E3	Выхо д	Выхо д	Выхо д	Выхо д	н/д	Выхо д
E4	Выхо д	Выхо д	Выхо д	Выхо д	н/д	Выхо д
E4 +	Выхо д	Выхо д	Выхо д	Выхо д	н/д	Выхо д

## [Поддержка ACL в IPv6](#)

Расширенные списки ACL IPv6 поддерживаются в медленном пути (Вход и Выход) на E0, E1, E2, E3 и E4 + в программном обеспечении Cisco IOS версии 12.0(23)S.

В Механизме 3 функция списка прав доступа (ACL) IPv6 поддерживается в аппаратных средствах в программном обеспечении Cisco IOS версии 12.0(25)S. ACL применены к определенному интерфейсу с неявной инструкцией deny в конце каждого списка доступа. ACL IPv6 настроены с помощью команды `ipv6 access-list` с запрещением и разрешают ключевые слова в режиме глобальной конфигурации. Основанная на механизме 3 фильтрация поддержки карт основанных на трафике заголовков параметра IPv6, теките метки, и дополнительно, информация о типе протокола высшего уровня.

## [Справочник по командам Cisco 12000 ACL](#)

### Механизм 1 команда

- `access-list hardware salsa`
- покажите, что контроллер I3 | включает ASIC

### Команды engine 2

- `access-list hardware psa limit 128`
- `no access-list hardware psa`
- `psa bypass`
- `show access-list psa detail`
- `show access-list psa summary`
- функция `show controller psa`

### Команды механизма 3

- `hw-module <слот #> no-merge компиляции tcam!----с программного обеспечения Cisco`

## *IOS версии 12.0(21)S3*

- аппаратный интерфейс `show-access-list <имя интерфейса>`
- покажите противоречие `[tofab/frfab] альфа-acl <интервал> vmr2ace`

### Механизм 4 + команды

- отметка `show access-list gen7`
- `show tcam`, прикладной `[acl - в / acf] tcam <метка - нет>`
- `show tcam`, прикладной `[acl - в / acf] <port> памяти <количество записей>`

### Механизм 4 + команды настройки Ethernet

- слияние `acl ip <number> hw-module slot`

## Глоссарий

Этот раздел предоставляет определения стандарта соответствующих сроков:

- **Уровни обработки** – сетевое устройство может быть логически поделено на три уровня обработки: Плоскость данных — Обрабатывающий на пакетах, текущих через сетевое устройство. Уровень управления — Обрабатывающий на пакетах использовал склеивать сетевые устройства. Сюда включаются протоколы каналов (например, протокол "точка-точка" - PPP и высокоуровневый протокол управления каналом передачи данных (HDLC)), протоколы маршрутизации (протокол пограничных шлюзов - BGP, протокол маршрутизации информации версии 2 - RIPv2, протокол первоочередного открытия кратчайших маршрутов - OSPF, и пр.) и протоколы синхронизации (например, сетевой протокол синхронизации времени - NTP). Панель управления — Обрабатывающий на пакетах, которые используются для управления сетевыми устройствами. Это включает telnet, Secure Shell (SSH), Протокол FTP, Протокол TFTP, SNMP и другие протоколы управления.
- **Стандартные списки доступа.** Фильтр стандартных списков доступа только для 3 уровня.
- **Расширенные списки ACL** — расширенные списки доступа IP используют адреса источника и назначения для соответствующих операций, а также дополнительную информацию о типе протокола для большой степени детализации контроля.
- **Линейные Обработанные ACL** — Обработанный линейно в программном обеспечении. Производительность зависит от глубины сопоставления (число записей, которое необходимо проверить для определения соответствия).
- **Турбо (Скомпилированные) ACL** — Турбо ACL оптимизируют Обработку ACL программного обеспечения путем компиляции ACL в высоко оптимизированную серию таблиц поиска который обработка программного обеспечения скорости. Быстродействие функции Turbo ACLs не меняется при изменении глубины соответствия.
- **Вводы для ACL** — ACL применен к трафику, вводящему порт, к которому это применено.
- **ACL для выходных данных** – ACL, применяемый к исходящему трафику порта. За некоторыми исключениями списки ACL для выходных данных обработаны картой входной линии.
- **ACL для пути приема.** Списки доступа для пути приема обеспечивают фильтрацию для управления трафиком, предназначенного для маршрутизатора, такого как обновление

маршрутов и запросы SNMP.

- **Двойная Передающая Линейная карта Этапа** — Линейные карты, которые имеют ASIC-схемы передачи/функции и на входе и на исходящем пути. Это позволяет линейной карте выполнять функции и на потоке входящего пакета и на потоке исходящего пакета без избыточно направленных пакетов к ЦП LC. Это также обеспечивает новые волны двойных алгоритмов пересылки этапа, которые будут использоваться в Cisco 12000. Линейная карта Механизма 3 является примером Двойной Передающей Линейной карты Этапа.
- **Линейная карта Single Stage Forwarding** – линейные платы, в которых ASIC продвижения/функций есть только на входном пути. Эти линейные карты только выполняют на основе ASIC обработку на пакетах, которые текут на пути для внешнего доступа. Выходной трафик или не обрабатывается (просто переданный), обрабатывается входными ASIC-схемами других LC или управляется ЦП LC. Engine 2, Механизм 4 и Механизм 4 + являются примерами Одноэтапных Передающих Линейных карт.

## [Дополнительные сведения](#)

- [IP-маршрутизаторы серии Cisco 12000](#)
- [Cisco Systems – техническая поддержка и документация](#)