# Глава 9 Списки контроля доступа (ACL)

# Введение

Тема сетевой безопасности очень обширна, многие её аспекты не входят в материал настоящего курса обучения. В данной главе мы рассмотрим один из важнейших навыков сетевого администратора - управление списками контроля доступа (ACL-списков).

Специалисты по проектированию сетей используют межсетевые экраны для обеспечения защиты сети от несанкционированного использования. Межсетевые экраны или брандмауэры представляют собой аппаратные или программные решения, направленные на повышение степени защищённости сети. Рассмотрим в качестве примера заблокированную дверь помещения внутри здания. Благодаря блокировке в помещение могут войти только авторизованные лица, имеющие ключ или карту доступа. Аналогичным образом межсетевой экран фильтрует неавторизованные или потенциально опасные пакеты, предотвращая их проникновение в сеть. На маршрутизаторе Cisco можно настроить простой межсетевой экран, который позволяет фильтровать трафик на базовом уровне с помощью ACL-списков. Использование ACL-списков позволяет администраторам останавливать трафик или допускать в сеть только определённый трафик.

Список контроля доступа (ACL) — это последовательный список правил разрешения или запрета, применяемых по отношению к адресам или протоколам более высокого уровня. ACL-списки позволяют эффективно контролировать входящий и исходящий трафик сети. ACL-списки также можно настраивать для всех маршрутизируемых протоколов сети.

Самой важной причиной для настройки ACL-списка является обеспечение безопасности сети. В этой главе объясняется, как использовать стандартные и расширенные ACL-списки на маршрутизаторе Cisco в рамках обеспечения сетевой безопасности. Материал главы включает советы, решения, общие рекомендации и инструкции по применению ACL-списков.

Данная глава даёт возможность развить ваши навыки создания и управления ACL-списками посредством упражнений для выполнения в аудитории, интерактивных заданий и лабораторных работ.

# Вопрос сотрудничества

**Вопрос сотрудничества**

**Сценарий**

Каждый учащийся приготовит пять вопросов кандидату на вакансию специалиста по сетевой безопасности на предприятии малого или среднего бизнеса. Последовательность вопросов в списке должна соответствовать степени важности при выборе хорошего специалиста на рассматриваемую должность. Кроме вопросов вам также необходимо записать предпочтительные ответы.

Из учащихся отбираются два интервьюера. Начинается собеседование. Кандидатам на вакансию будет предоставлена возможность (или отказано в таковой) перейти на следующий уровень вопросов по итогам их ответов.

Для ознакомления с полными инструкциями к данному упражнению обратитесь к PDF-файлу.

Затем учащиеся собираются вместе и обсуждают свои наблюдения за процессом, далее по результатам обсуждения выносится решение, проходит ли кандидат на следующий уровень интервью.

[Работа в аудитории. Вопрос сотрудничества. Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.0.1.2%20Permit%20Me%20to%20Assist%20You%20Instructions.pdf)

**Что такое ACL-список?**

ACL-список — это ряд команд IOS, определяющих, пересылает ли маршрутизатор пакеты или сбрасывает их, исходя из информации в заголовке пакета. ACL-списки являются одной из наиболее используемых функций операционной системы Cisco IOS.

В зависимости от конфигурации ACL-списки выполняют следующие задачи:

* Ограничение сетевого трафика для повышения производительности сети. Например, если корпоративная политика запрещает видеотрафик в сети, необходимо настроить и применить ACL-списки, блокирующие данный тип трафика. Подобные меры значительно снижают нагрузку на сеть и повышают её производительность.
* Вторая задача ACL-списков — управление потоком трафика. ACL-списки могут ограничивать доставку обновлений маршрутизации. Настройка сети, устраняющая необходимость в обновлениях маршрутизации, позволяет избежать лишнего использования полосы пропускания.
* Списки контроля доступа обеспечивают базовый уровень безопасности в отношении доступа к сети. ACL-списки могут открыть доступ к части сети одному узлу и закрыть его для других узлов. Например, доступ к сети отдела кадров может быть ограничен и разрешён только авторизованным пользователям.
* ACL-списки осуществляют фильтрацию трафика на основе типа трафика. Например, ACL-список может разрешать трафик электронной почты, но при этом блокировать весь трафик протокола Telnet.
* Списки контроля доступа осуществляют сотировку узлов в целях разрешения или запрета доступа к сетевым службам. С помощью ACL-списков можно разрешать или запрещать доступ к определённым типам файлов, например FTP или HTTP.

По умолчанию ACL-списки не сконфигурированы на маршрутизаторе, поэтому маршрутизатор не фильтрует трафик. Трафик, поступающий на маршрутизатор, маршрутизируется исключительно на основе информации таблицы маршрутизации. Однако если ACL-список используется на интерфейсе, маршрутизатор выполняет дополнительную задачу, оценивая все сетевые пакеты, проходящие через интерфейс, с целью определения разрешения пересылки пакета.

Помимо разрешения или запрета трафика, ACL-списки можно использовать для анализа, пересылки или обработки отдельных видов трафика. Например, при помощи ACL-списков можно классифицировать трафик для включения обработки данных в соответствии с приоритетом. Данная возможность ACL-списков аналогична наличию VIP-пропуска на концерт или спортивное мероприятие. VIP-пропуск даёт избранным гостям привилегии, недоступные обладателям обычных билетов, такие как приоритет входа или доступ в закрытую зону.

На рисунке приводится пример топологии с используемыми ACL-списками.

# Сеанс связи по протоколу TCP

ACL-списки позволяют администраторам контролировать входящий и исходящий трафик. Подобный контроль может сводиться к простому запрету или разрешению трафика на основе сетевых адресов или представлять собой комплекс мер по управлению сетевым трафиком на основе запросов порта TCP. Понять, как ACL-список фильтрует трафик, будет легче, если рассмотреть диалог, возникающий при сеансе связи по протоколу TCP, например, при запросе веб-страницы.

**Обмен данными по протоколу TCP**

Когда клиент запрашивает данные от веб-сервера, протокол IP отвечает за взаимодействие между компьютером (источник) и сервером (назначение). Протокол TCP управляет обменом данных между браузером (приложение) и программным обеспечением сетевого сервера.

При отправке электронной почты, просмотре веб-страницы или загрузке файла протокол TCP отвечает за разбивку данных по сегментам для протокола IP перед тем, как они будут отправлены. Протокол TCP также управляет сбором поступивших из сегментов данных. Действие протокола TCP очень похоже на разговор, в котором два сетевых узла договариваются о передаче данных от одного узла к другому.

TCP обеспечивает надежный сервиc передачи потока байтов. Говорят, что протокол TCP ориентирован на установление соединения (connection-oriented protocol). Термин «с установлением соединения» означает, что два приложения должны установить TCP-соединение перед тем, как осуществлять обмен данными. TCP является полнодуплексным протоколом. Это означает, что каждое TCP-соединение поддерживает пару потоков байтов, и каждый поток байтов следует в одном направлении. Протокол TCP включает механизм управления потоками для каждого потока байтов, позволяющий получателю ограничивать объём данных, передаваемых отправителем. Протокол TCP также реализует механизм отслеживания перегрузки сети.

Анимация на рис. 1 иллюстрирует процесс обмена данными по протоколу TCP/IP. Сегменты TCP маркированы флагами, отмечающими их назначение: SYN начинает сеанс синхронизации, ACK подтверждает, что ожидаемый сегмент принят, и FIN — завершает сеанс. SYN/ACK подтверждает синхронизацию передачи. Сегменты данных TCP несут информацию протоколов более высокого уровня. Эта информация необходима для корректного направления данных к соответствующему приложению.

Сегмент данных TCP также определяет порт, соответствующий запрошенной службе. Например, HTTP соответствует порт 80, SMTP — порт 25, а FTP — порты 20 и 21. На рис. 2 показаны диапазоны портов UDP и TCP.

На рис. 3-5 приводится информация о портах TCP/UDP.

**Фильтрация пакетов**

Каким образом ACL-список использует информацию, переданную в сеансе связи по протоколу TCP/IP, для фильтрации трафика?

С помощью фильтрации пакетов, иногда называемой статической фильтрацией пакетов, осуществляется управление доступом к сети путём анализа входящих и исходящих пакетов и пропускания или отбрасывания пакетов на основе заданных критериев, например, IP-адреса источника, IP-адреса назначения и протокола внутри пакета.

Маршрутизатор работает как фильтр пакетов, когда перенаправляет или отбрасывает пакеты на основе правил фильтрации. Фильтрующий пакеты маршрутизатор извлекает определённую информацию из поступающего на него пакета. Используя эту информацию, маршрутизатор принимает решения на основе установленных правил фильтрации относительно того, можно ли пропустить пакет или его необходимо сбросить. Как показано на рисунке, фильтрация пакетов может работать на разных уровнях модели взаимодействия открытых систем (OSI) или на уровне межсетевого протокола TCP/IP.

Маршрутизатор, фильтрующий пакеты, использует определённые правила пропуска или отклонения трафика. Маршрутизатор также может фильтровать пакеты на уровне 4 — транспортном уровне. Маршрутизатор может фильтровать пакеты на основе порта источника и порта назначения сегмента TCP или UDP. Эти правила задаются с помощью ACL-списков.

Список контроля доступа (ACL) — это последовательный список разрешающих или запрещающих операторов, называемых записями контроля доступа (ACE). Записи контроля доступа также часто называют правилами ACL-списка. ACE-записи можно создать для фильтрации трафика на основании определённых критериев, таких как адрес источника, адрес назначения, протокол и номера портов. При прохождении сетевого трафика через интерфейс, настроенный с ACL-списком, маршрутизатор последовательно сопоставляет информацию внутри пакета с каждой записью ACE, определяя, соответствует ли пакет одному из правил. Если совпадение найдено, пакет обрабатывается в соответствии с записями ACL-списка. Таким образом, ACL-списки можно настроить для управления доступом к сети или подсети.

Для оценки сетевого трафика, ACL-список извлекает следующую информацию из заголовка пакета уровня 3:

* IP-адрес источника;
* IP-адрес назначения;
* тип сообщения протокола ICMP.

ACL-список также может извлекать информацию более высокого уровня из заголовка уровня 4, включая:

* порт источника TCP/UDP;
* порт назначения TCP/UDP.

**Фильтрация пакетов (продолжение)**

**Пример фильтрации пакетов**

Для того чтобы понять концепцию использования маршрутизатором функции фильтрации пакетов представим запертую дверь, на которой висит предупредительная табличка. Согласно этой табличке, в дверь могут войти только те, чьи имена перечислены в списке. Таким образом, предупредительная табличка фильтрует людей по критерию наличия их имён в списке авторизованных лиц. По аналогичной схеме работает ACL-список — все решения принимаются на основе установленных критериев.

Например, ACL-список может быть настроен логически: «Разрешить веб-доступ к пользователям сети А, но запретить все остальные службы для пользователей сети А. Запретить доступ к протоколу HTTP пользователям сети B, но разрешить пользователям сети B доступ ко всем остальным службам». Обратитесь к рисунку для изучения пути принятия решения о фильтрации пакета для выполнения этой задачи.

В рамках данного сценария фильтр пакетов оценивает каждый пакет, исходя из следующих условий:

* Если пакетом является пакет TCP SYN из сети А, использующий порт 80, то пересылка разрешена. Весь остальной доступ этим пользователям запрещён.
* Если пакетом является пакет TCP SYN из сети B, использующий порт 80, то пересылка запрещена. Однако все другие виды доступа разрешены.

Это лишь простой пример. Для разрешения или запрета службы определённым пользователям можно настроить множество правил.

**Принцип работы ACL-списков**

Списки контроля доступа определяют набор правил, обеспечивающих дополнительный контроль над пакетами, которые принимаются интерфейсами, транзитными пакетами, которые передаются через маршрутизатор, а также пакетами, которые отправляются из интерфейсов маршрутизатора. Списки контроля доступа не применяются к пакетам, созданным маршрутизатором.

ACL-списки сконфигурированы для применения к входящему или исходящему трафику, как показано на рисунке.

* **Входящие ACL-списки** — входящие пакеты обрабатываются перед отправкой на исходящий интерфейс. Входящий ACL-список эффективен, поскольку он сохраняет ресурсы на поиск маршрута, если пакет сбрасывается. Если пакет успешно проходит проверку, он передается на обработку для дальнейшей маршрутизации. Входящие ACL-списки являются оптимальным решением для фильтрации пакетов, когда сеть, подключенная к входящему интерфейсу, является единственным источником пакетов, требующих анализа.
* **Исходящие ACL-списки** — входящие пакеты маршрутизируются на исходящий интерфейс, а затем обрабатываются исходящим списком контроля доступа. Исходящие ACL-списки лучше всего использовать, когда одинаковые фильтры применяются к пакетам, поступающим с множества входящих интерфейсов, перед выходом на тот же исходящий интерфейс.

Последняя запись любого ACL-списка — это всегда "косвенный отказ" (эта строчка не видна). Это правило автоматически вставляется в конец каждого ACL-списка, хотя и не присутствует в нём физически. Косвенный отказ блокирует весь трафик. По причине этого неявного запрета ACL-список, не содержащий хотя бы одного разрешающего правила, блокирует весь трафик.

# Packet Tracer. Наглядное представление работы ACL-списка

В рамках этого задания вы получите представление о том, как можно использовать ACL-список для блокирования эхо-запросов, отправленных на узлы удалённых сетей. После удаления ACL-списка из настроек эхо-запросы будут успешно выполняться.

[Packet Tracer. Наглядное представление работы ACL-списка. Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.1.1.6%20Packet%20Tracer%20-%20ACL%20Demonstration%20Instructions.pdf)

[Packet Tracer. Наглядное представление работы ACL-списка. PKA](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.1.1.6%20Packet%20Tracer%20-%20ACL%20Demonstration.pka)

**Типы ACL-списков Cisco для IPv4**

Существует два типа ACL-списков Cisco для IPv4: стандартные и расширенные ACL-списки.

**Примечание**. ACL-списки Cisco для IPv6 аналогичны расширенным ACL-спискам для IPv4 и будут описаны в следующем разделе.

**Стандартные ACL-списки**

Стандартные ACL-списки можно использовать для разрешения или отклонения прохождения трафика только на основе IPv4-адресов источника. Назначение пакета и порты, участвующие в передаче данных, не оцениваются. В примере на рис. 1 разрешён весь трафик от 192.168.30.0/24. Из-за неявного правила «deny any» в конце списка данный ACL-список блокирует весь остальной трафик. Стандартные ACL-списки создаются в режиме глобальной конфигурации.

**Расширенные ACL-списки**

Расширенные ACL-списки фильтруют IPv4-пакеты, исходя из нескольких признаков:

* тип протокола;
* IPv4-адрес источника;
* IPv4-адрес назначения;
* TCP или UDP порты источника;
* TCP или UDP порты назначения;
* дополнительная информация о типе протокола для оптимизированного контроля.

На рис. 2 ACL-список 103 разрешает трафику с любого адреса сети 192.168.30.0/24 идти в любую IPv4-сеть, если порт назначения — 80 (HTTP). Расширенные ACL-списки создаются в режиме глобальной конфигурации.

Команды для ACL-списков описываются в следующих разделах.

**Примечание**. Стандартные и расширенные ACL-списки рассматриваются более подробно в других разделах данной главы.

# Присваивание номеров и имён ACL-спискам

Стандартные и расширенные списки контроля доступа можно создавать с помощью номера или имени для идентификации ACL-списка и списка его правил.

Использование нумерованных ACL-списков — эффективный способ определения типа ACL-списка в небольших сетях, где в основном используется трафик одного типа. Однако номер не содержит информации о назначении ACL-списка. По этой причине, начиная с операционной системы Cisco IOS версии 11.2, для определения списков контроля доступа Cisco используется присвоенное списку имя.

На рисунке представлено краткий свод правил присвоения имён и номеров ACL-спискам.

Что касается нумерованных ACL-списков, номера с 200 до 1299 опущены, поскольку они используются другими протоколами, многие из которых являются унаследованными или устаревшими. В рамках настоящего учебного курса рассматриваются только списки контроля доступа по протоколу IP. Примеры номеров ACL-списков устаревших протоколов — от 600 до 699, используемые стеком протоколов AppleTalk, и номера от 800 до 899 — используемые протоколом IPX.

**Основные сведения о применении шаблонных масок в ACL**

**Наложение шаблонной маски**

ACL-списки IPv4 используют шаблонные маски. Шаблонная маска представляет собой строку из 32 двоичных цифр, используемую маршрутизатором для определения битов адреса, которые будут рассматриваться на предмет совпадений.

**Примечание**. В отличие от ACL-списков для IPv4, ACL-списки для IPv6 не используют шаблонные маски. В протоколе IPv6 для указания того, какая часть IPv6-адреса источника или назначения должна совпадать, используется длина префикса. ACL-списки для IPv6 будут рассматриваться в данной главе позднее.

Как и в случае с масками подсетей, цифры 1 и 0 в шаблонной маске определяют, как обрабатывать соответствующие биты IP-адреса. Однако в шаблонной маске эти биты используются для других целей и следуют другим правилам.

В масках подсети двоичные единицы и нули используются для определения сети, подсети и узловой части IP-адреса. В шаблонной маске двоичные единицы и нули используются для фильтрации отдельных IP-адресов или групп IP-адресов с целью разрешения или запрета доступа к ресурсам.

Шаблонные маски и маски подсетей различаются по правилам совпадения двоичных единиц и нулей. Для совпадения двоичных единиц и нулей в шаблонных масках используются следующие правила:

* Бит 0 в шаблонной маске означает, что бит в изначальном адресе должен совпадать с битом в адресе результата.
* Бит 1 шаблонной маски означает, что соответствующее значение бита в адресе может быть проигнорировано.

На рис. 1 показано, как разные шаблонные маски фильтруют IP-адреса. Рассматривая приведённый пример, помните, что двоичный ноль означает бит, который должен совпадать, а двоичная единица — бит, который можно игнорировать.

**Примечание**. Шаблонную маску часто называют обратной маской. Это название объясняется тем, что в отличие от маски подсети, где двоичная единица равна совпадению, а двоичный ноль не является совпадением, в шаблонной маске используются обратные значения.

**Использование шаблонной маски**

Таблица на рис. 2 демонстрирует результаты применения шаблонной маски 0.0.255.255 к 32-битному IPv4-адресу. Помните, что двоичный ноль указывает на значение, которое совпадает.

Шаблонные маски также используются при конфигурации некоторых протоколов IPv4-маршрутизации (например, OSPF) с целью включения протокола на конкретных интерфейсах.

# Примеры шаблонной маски

**Расчёт шаблонных масок для соответствия подсетям IPv4**

Расчёт шаблонной маски может потребовать определённого опыта. На рис. 1 представлены три примера шаблонных масок.

В первом примере шаблонной маской предусматривается, что каждый бит в IPv4-адресе 192.168.1.1 должен точно совпадать.

Условием шаблонной маски во втором примере является отсутствие совпадений.

В третьем примере шаблонной маски оговаривается, что любой узел в сети 192.168.1.0/24 будет совпадать.

Приведённые примеры довольно просты и понятны. В действительности, вычисление шаблонных масок может оказаться гораздо более сложной задачей.

**Расчёт шаблонных масок для соответствия диапазонам**

На рис. 2 приводятся более сложные примеры. В примере 1 первые два октета и первые четыре 4 бита третьего октета должны точно совпадать. Последние четыре бита в третьем октете и последний октет могут быть любым допустимым числом. Результатом является маска, которая определяет диапазон сетей от 192.168.16.0 до 192.168.31.0.

В примере 2 показана шаблонная маска, с совпадениями в первых двух октетах и последнем бите третьего октета. Последний октет и первые семь бит в третьем октете могут быть любым допустимым числом. Результатом является маска, позволяющая или запрещающая все узлы из нечетных подсетей основной сети 192.168.0.0.

# Расчёт шаблонной маски

Расчёт шаблонных масок может быть сопряжён с определёнными сложностями. Простым способом является вычитание маски подсети из 255.255.255.255.

**Расчёт шаблонной маски. Пример 1**

Предположим, что в первом примере на рисунке вы хотите разрешить доступ всем пользователям в сети 192.168.3.0. Поскольку маска подсети — 255.255.255.0, вы можете взять 255.255.255.255 и вычесть маску подсети 255.255.255.0. В результате получается шаблонная маска 0.0.0.255.

**Расчёт шаблонной маски. Пример 2**

Предположим, что во втором примере на рисунке вы хотите разрешить сетевой доступ для 14 пользователей в подсети 192.168.3.32/28. Маска подсети для IP-подсети — 255.255.255.240, следовательно, берём 255.255.255.255 и вычитаем маску подсети 255.255.255.240. В результате получается шаблонная маска 0.0.0.15.

**Расчёт шаблонной маски. Пример 3**

Предположим, что в третьем примере на рисунке вы хотите вычислить шаблонную маску для соответствия сетям 192.168.10.0 и 192.168.11.0. И снова берём 255.255.255.255 и вычитаем маску подсети, которая в данном случае будет 255.255.252.0. В итоге получается 0.0.3.255.

Подобный результат можно получить при помощи команд, представленных ниже:

R1(config)# **access-list 10 permit 192.168.10.0**

R1(config)# **access-list 10 permit 192.168.11.0**

Более эффективным способом является конфигурация шаблонной маски следующим образом:

R1(config)# **access-list 10 permit 192.168.10.0 0.0.3.255**

Используйте приведённую ниже конфигурацию для расчёта шаблонной маски, соответствующей сетям в диапазоне между 192.168.16.0 и 192.168.31.0:

R1(config)# **access-list 10 permit 192.168.16.0**

R1(config)# **access-list 10 permit 192.168.17.0**

R1(config)# **access-list 10 permit 192.168.18.0**

R1(config)# **access-list 10 permit 192.168.19.0**

R1(config)# **access-list 10 permit 192.168.20.0**

R1(config)# **access-list 10 permit 192.168.21.0**

R1(config)# **access-list 10 permit 192.168.22.0**

R1(config)# **access-list 10 permit 192.168.23.0**

R1(config)# **access-list 10 permit 192.168.24.0**

R1(config)# **access-list 10 permit 192.168.25.0**

R1(config)# **access-list 10 permit 192.168.26.0**

R1(config)# **access-list 10 permit 192.168.27.0**

R1(config)# **access-list 10 permit 192.168.28.0**

R1(config)# **access-list 10 permit 192.168.29.0**

R1(config)# **access-list 10 permit 192.168.30.0**

R1(config)# **access-list 10 permit 192.168.31.0**

Приведённые выше 16 команд конфигурации можно свести к одной команде при помощи правильной шаблонной маски, как показано ниже:

R1(config)# **access-list 10 permit 192.168.16.0 0.0.15.255**

# Ключевые слова шаблонной маски

**Ключевые слова шаблонной битовой маски**

Работа с десятичными представлениями битов двоичной шаблонной маски может быть трудоёмкой. Ключевые слова **host** и **any** упрощают задачу, помогая определить наиболее часто используемую шаблонную маску. Эти ключевые слова исключают необходимость ввода шаблонных масок при определении конкретного узла или целой сети. Эти ключевые слова облегчают чтение ACL-списка, предоставляя визуальные подсказки относительно критериев источника или назначения.

Ключевое слово **host** применяется для маски 0.0.0.0. Эта маска указывает, что должны совпадать все биты IPv4-адреса, или совпадает только один узел.

Ключевое слово **any** применяется для IP-адреса и маски 255.255.255.255. Эта маска указывает игнорировать весь IPv4-адрес или принять любой адрес.

**Пример 1. Шаблонная маска одного IP-адреса**

В примере 1, представленном на рисунке, вместо введения **192.168.10.10 0.0.0.0** можно ввести строку **host 192.168.10.10**.

**Пример 2. Шаблонная маска любого IP-адреса**

В примере 2, представленном на рисунке, вместо инструкции **0.0.0.0 255.255.255.255** можно ввести отдельно ключевое слово **any.**

**Примечание**. Ключевые слова **host** и **any** также можно использовать при конфигурации ACL-списка IPv6.

# Примеры ключевых слов шаблонной маски

**The** **any and** **host Ключевые слова**

Пример 1 на рисунке показывает, как использовать ключевое слово **any** для замены IPv4-адреса 0.0.0.0 шаблонной маской 255.255.255.255.

Пример 2 показывает, как использовать ключевое слово **host** для замены шаблонной маски при определении одного узла.

**Общие рекомендации по созданию ACL-списков**

Составление ACL-списков может быть сложной задачей. Для каждого интерфейса может существовать несколько правил, необходимых для управления типами трафика, которым разрешено входить или выходить через этот интерфейс. Маршрутизатор на рисунке имеет два интерфейса, сконфигурированных для IPv4 и IPv6. Если для обоих протоколов необходимы ACL-списки на обоих интерфейсах и в обоих направлениях, то потребуется создать 8 отдельных ACL-списков. Каждый интерфейс будет иметь четыре ACL-списка: два списка для протокола IPv4 и два — для протокола IPv6. Для каждого протокола нужен один ACL-список для входящего трафика и один — для исходящего трафика.

**Примечание**. Списки контроля доступа не требуется конфигурировать на оба направления. Номера ACL-списков и их направления, применяемые на интерфейсе, зависят от заявленных требований.

Приведём несколько рекомендаций по использованию ACL-списков.

* Используйте ACL-списки в межсетевых экранах маршрутизаторов, размещённых между внутренней сетью и внешней сетью, например Интернетом.
* Для управления входящим или исходящим трафиком в определённой части внутренней сети используйте ACL-списки на маршрутизаторе, расположенном между двумя частями сети.
* Сконфигурируйте ACL-списки на пограничных маршрутизаторах, то есть маршрутизаторах, расположенных на границах сетей. Это обеспечит базовый буфер от внешней сети или между менее контролируемой и более чувствительной областями сети.
* Сконфигурируйте ACL-списки для каждого протокола сети, настроенного на интерфейсе пограничного маршрутизатора.

**Три «для»**

Запомните три «для», составляющие основные правила применения ACL-списков на маршрутизаторе. Можно сконфигурировать один список контроля доступа для протокола, направления, интерфейса:

* **Один ACL-список для одного протокола —** для управления потоком трафика на интерфейсе ACL-список должен быть определён для каждого протокола, действующего на интерфейсе.
* **Один ACL-список для одного направления —** ACL-списки одновременно контролируют трафик на одном направлении одного интерфейса. Для управления исходящим и входящим трафиком должны быть созданы два отдельных ACL-списка.
* **Один ACL-список для одного интерфейса** — ACL-списки управляют трафиком на одном интерфейсе, например, GigabitEthernet 0/0.

# Рекомендации по созданию ACL-списков

Создание ACL-списков требует внимания к деталям и повышенной осторожности. Ошибки могут привести к серьёзным последствиям и дополнительным затратам, связанным с простоями, поиском и устранением неполадок, а также некорректной работой сетевых служб. Перед конфигурацией ACL-списка необходимо создать базовый план. На рисунке представлен список рекомендаций, составляющих базовую методику составления ACL-списка.

**Где следует размещать ACL-списки**

Правильное размещение ACL-списка может повысить эффективность сети. ACL-список можно разместить для минимизации избыточного трафика. Например, трафик, который будет отклонён удаленным местом назначения, не должен пересылаться с помощью сетевых ресурсов по маршруту к этому месту назначения.

Каждый ACL-список должен быть размещен там, где он может быть максимально полезен. Приведём список базовых правил размещения ACL-списков (см. рис.):

* **Расширенные ACL-списки** — расширенные ACL-списки следует размещать максимально близко к источнику фильтруемого трафика. Таким образом, нежелательный трафик отклоняется близко к сети-источнику, не пересекая инфраструктуру сети.
* **Стандартные ACL-списки** — поскольку стандартные списки контроля доступа не определяют адреса назначения, их размещают максимально близко к месту назначения. Размещение стандартного ACL-списка у источника трафика позволяет предотвратить достижение этим трафиком других сетей через интерфейс, на котором применён ACL-список.

Размещение ACL-списка и, как следствие, тип используемого ACL-списка может также зависеть от следующих параметров:

* **Сфера контроля сетевого администратора** — размещение ACL-списка может зависеть от того, управляет ли сетевой администратор и сетью-источником, и сетью назначения.
* **Пропускная способность задействованных сетей** — фильтрация нежелательного трафика у источника предотвращает передачу трафика до того, как он снижает пропускную способность сети на пути к пункту назначения. Это особенно важно в сетях с низкой пропускной способностью.
* **Простота конфигурации** — для запрета сетевым администратором трафика, поступающего от нескольких сетей, одним из способов может стать использование одного стандартного ACL-списка на ближайшем к месту назначения маршрутизаторе. Недостаток этого способа в том, что трафик из этих сетей будет использовать пропускную способность. Расширенный ACL-список можно применить на каждом маршрутизаторе, с которого идёт трафик. Это позволит сохранить пропускную способность при помощи фильтрации трафика на источнике, но для этого требуется создание расширенных ACL-списков на нескольких маршрутизаторах.

**Примечание**. Общее правило в рамках сертификации CCNA заключается в том, что расширенные ACL-списки размещаются как можно ближе к источнику, а стандартные ACL-списки — как можно ближе к месту назначения.

**Размещение стандартного ACL-списка**

Стандартный ACL-список может фильтровать трафик только по адресу источника. Основное правило размещения стандартного ACL-списка заключается в размещении списка как можно ближе к сети назначения. Это позволяет трафику достичь всех остальных сетей, кроме сети с фильтрацией пакетов.

На рисунке администратор желает запретить трафику из сети 192.168.10.0/24 попадать в сеть 192.168.30.0/24.

Если стандартный ACL-список размещён на исходящем интерфейсе R1, то трафик из сети 192.168.10.0/24 не сможет достичь любой сети, доступной через интерфейс Serial 0/0/0 маршрутизатора R1.

На рисунке показаны два интерфейса маршрутизатора R3, на которых можно настроить использование стандартного ACL-списка, согласно основным рекомендациям по размещению стандартного ACL-списка как можно ближе к месту назначения:

* **Интерфейс S0/0/1 маршрутизатора R3** — использование стандартного ACL-списка для предотвращения трафика из сети 192.168.10.0/24 в интерфейс S0/0/1 также не допустит этот трафик в сеть 192.168.30.0/24 и в другие сети, к которым имеет доступ маршрутизатор R3, включая сеть 192.168.31.0/24. Поскольку целью ACL-списка является фильтрация трафика, предназначенного только для 192.168.30.0/24, стандартный ACL-список не должен применяться на этом интерфейсе.
* **Интерфейс G0/0 R3** — применение стандартного списка контроля доступа к трафику выходного интерфейса G0/0 приведёт к фильтрации пакетов из сетей в диапазоне от 192.168.10.0/24 до 192.168.30.0/24. Применение данного списка не повлияет на другие сети, досягаемые R3. Пакеты из сети 192.16810.0/24 по-прежнему смогут достигнуть сеть 192.168.31.0/24.

**Размещение расширенного ACL-списка**

Как и стандартный ACL-список, расширенный список контроля доступа может фильтровать трафик на основе адреса источника. Однако, помимо этого, расширенный ACL-список может фильтровать трафик на основе адреса назначения, протокола и номера порта. Эти дополнительные возможности дают сетевым администраторам больше гибкости при выборе типа трафика, который можно отфильтровать, и места размещения ACL-списка. Основным правилом размещения расширенного ACL-списка является его размещение максимально близко к источнику. Соблюдение данного правила позволяет предотвратить отправку нежелательного трафика на первоначальном этапе, а не после прохождения нескольких сетей.

Сетевые администраторы могут размещать ACL-списки только на тех устройствах, которые они способны контролировать. Поэтому место размещения определяется, исходя из пределов сферы контроля сетевого администратора. На рисунке администратор компании A, которая включает сети 192.168.10.0/24 и 192.168.11.0/24 (упомянутые как .10 и .11 в рассматриваемом примере), желает управлять трафиком, передаваемым в сети компании B. В частности, администратор хочет запретить трафик протоколов Telnet и FTP из сети .11 в сеть компании В 192.168.30.0/24 (в данном примере — .30). В то же время на весь остальной трафик, исходящий из сети .11, не должно накладываться каких-либо ограничений.

Существует несколько способов достижения этих целей. Расширенный ACL-список на маршрутизаторе R3, блокирующий протоколы Telnet и FTP из сети .11, мог бы выполнить эту задачу, однако администратор не контролирует R3. Кроме того, при таком решении нежелательный трафик сможет проходить через всю сеть только для того, чтобы оказаться заблокированным по достижении места назначения. Это оказывает влияние на общую эффективность сети.

Оптимальным решением в данной ситуации является размещение расширенного ACL-списка на маршрутизаторе R1, который определяет как адреса источника, так и адреса назначения (сеть .11 и сеть .30, соответственно), и обеспечивает соблюдение правила: «Трафику Telnet и FTP-из сети .11 сетей запрещено идти в сеть .30». Рисунок демонстрирует два интерфейса на маршрутизаторе R1, на которых возможно применение расширенного ACL-списка:

* **Интерфейс S0/0/0 R1 (исходящий)** — одно из возможных решений заключается в применении расширенного исходящего ACL-списка на интерфейсе S0/0/0. Поскольку расширенный ACL-список может просмотреть и адрес источника, и адрес назначения, запрещены будут только пакеты FTP и Telnet, исходящие из сети 192.168.11.0/24. Остальной трафик из 192.168.11.0/24 и других сетей будет перенаправляться на R1. Недостаток размещения расширенного ACL-списка на данном интерфейсе заключается в том, что весь трафик, выходя из S0/0/0, должен быть обработан ACL-списком, включая пакеты из 192.168.10.0/24.
* **Интерфейс G0/1 R1 (входящий)** — вторым возможным решением является применение расширенного ACL-списка к трафику, входящему через интерфейс G0/1, что означает, что только пакеты из сети 192.168.11.0/24 являются объектом для ACL-списка, действующего на R1. Поскольку фильтр ограничивается только пакетами, покидающими сеть 192.168.11.0/24, применение расширенного списка контроля доступа на G0/1 — оптимальное решение.

# Задание порядка записей ACL-списка

Когда трафик поступает на маршрутизатор, он сравнивается с записями ACE в порядке, заданном в ACL-списке. Маршрутизатор продолжает обработку ACE, пока не обнаружит совпадение. Маршрутизатор обрабатывает пакет на основе первого найденного совпадения, остальные ACE-записи маршрутизатором не учитываются.

Если к концу списка совпадения не найдены, маршрутизатор отклоняет трафик. Это объясняется тем, что по умолчанию в конце каждого ACL-списка содержится команда запрета для трафика, который не совпали ни с одной записью списка. Если ACL-список состоит из одной команды запрета, весь трафик будет отклоняться. Таким образом, в списке должна быть, по крайней мере, одна команда разрешения, т.к. в противном случае весь трафик будет заблокирован.

Для сети на рисунке применение ACL-списка 1 или ACL-списка 2 на интерфейсе S0/0/0 маршрутизатора R1 на исходящем направлении даёт одинаковые результаты. Для сети 192.168.10.0 будет разрешён доступ к сетям, досягаемым через S0/0/0, в то время как в отношении сети 192.168.11.0 будет действовать запрет доступа этим сетям.

# Настройка стандартного ACL-списка

**Логика стандартного ACL-списка**

На рисунке у пакетов, поступающих на маршрутизатор через интерфейс G0/0, проверяются адреса их источника на основе следующих записей:

**access-list 2 deny 192.168.10.10**

**access-list 2 permit 192.168.10.0 0.0.0.255**

**access-list 2 deny 192.168.0.0 0.0.255.255**

**access-list 2 permit 192.0.0.0 0.255.255.255**

Если пакеты разрешены, они направляются через маршрутизатор к выходному интерфейсу. Если пакеты блокируются, они отбрасываются на входящий интерфейс.

# Настройка стандартного ACL-списка (продолжение)

**Настройка стандартных ACL-списков**

Для использования стандартных нумерованных ACL-списков на маршрутизаторе Cisco необходимо сначала создать стандартный ACL-список и затем активировать его на интерфейсе.

Команда глобальной конфигурации **access-list** определяет стандартный ACL-список с номером в диапазоне от 1 до 99. В ОС Cisco IOS версии 12.0.1 данный диапазон расширен; для стандартных ACL-списков могут использоваться номера от 1300 до 1999. Это позволяет создать до 798 возможных стандартных ACL-списков. Дополнительные номера ссылаются на расширенный ACL-список по протоколу IP.

Ниже приводится полный синтаксис команды стандартного ACL-списка:

Router(config)# **access-list** *access-list-number* { **deny** | **permit** | **remark** } *source* [ *source-wildcard* ][ **log** ]

Рис. 1 содержит подробное описание синтаксиса для стандартного ACL-списка.

Записи ACE могут разрешить или запретить отдельный узел или диапазон адресов узлов. Для создания в нумерованном ACL-списке 10 записи, разрешающей определённый узел с IP-адресом 192.168.10.0, необходимо ввести следующую команду:

R1(config)# **access-list 10 permit host 192.168.10.10**

Как показано на рис. 2, для создания записи, которая разрешит диапазон IPv4-адресов в нумерованном ACL-списке 10, разрешающем все IPv4-адреса в сети 192.168.10.0/24, необходимо ввести следующую команду:

R1(config)# **access-list 10 permit 192.168.10.0 0.0.0.255**

Для удаления ACL-списка используется команда глобальной конфигурации **no access-list**. Ввод команды **show access-list** подтверждает удаление ACL-списка 10.

Как правило, при создании администратором списка контроля доступа применение каждой записи известно и очевидно. Тем не менее, для того, чтобы администратор и другие пользователи могли вспомнить назначение той или иной записи, необходимо добавить соответствующие комментарии. Для документирования и упрощения прочтения ACL-списков используется ключевое слово **remark**. Длина комментария ограничена 100 символами. Довольно простой ACL-список на рис. 3 приводится в качестве примера. При просмотре конфигурации ACL-списка с помощью команды **show running-config** также отображается соответствующий комментарий.

# Внутренний алгоритм работы

Cisco IOS применяет внутренний алгоритм в процессе приёма и обработки стандартных записей ACE. Как уже упоминалось ранее, записи ACE обрабатываются последовательно. Поэтому при введении записей ACE важно соблюдать определённый порядок.

Например, на рис. 1 ACL-список 3 содержит две ACE-записи. Первая ACE использует шаблонную маску для запрещения диапазона адресов, который включает все узлы в сети 192.168.10.0/24. Вторая ACE является записью типа host, который разрешается определённый узел — 192.168.10.10. Это узел находится в диапазоне узлов, запрещённом в первой записи ACE. Другими словами, 192.168.10.10 — узел в сети 192.168.10.0/24. Внутренний алгоритм IOS для стандартных списков доступа отклоняет вторую запись и выдает сообщение об ошибке, поскольку вторая запись противоречит первой. Обратите внимание, что на рисунке маршрутизатор автоматически назначает номер 10 (num 10) в качестве порядкового номера, назначенного первой записи, введённой в рассматриваемом примере. Выходные данные маршрутизатора включают сообщение о том, что вторая запись противоречит правилу номер 10 («part of the existing rule at sequence num 10»), и отклоняет запись.

**Примечание**. В настоящее время расширенные ACL-списки не выдают аналогичных ошибок.

Конфигурация ACL 4 на рис. 2 имеет две аналогичные записи, используемые в обратном порядке. Это верная последовательность записей, поскольку первая запись ссылается на определённый узел, а не на диапазон узлов.

На рис. 3 ACL 5 показывает, что запись узла можно добавить после записи, отмечающей диапазон узлов, однако узел не должен находиться в пределах диапазона, запрещённого в предыдущей записи. Адрес узла 192.168.11.10 не является участником сети 192.168.10.0/24, поэтому запись является допустимой.

**Примечание**. Порядок, в котором вводятся стандартные ACE-записи, может не совпадать с порядком, в котором они сохраняются, отображаются или обрабатываются маршрутизатором. Это будет описано в последующих разделах.

# Применение стандартных ACL-списков на интерфейсах

**Порядок действий при конфигурации стандартного ACL-списка**

После конфигурации стандартного ACL-списка, он привязывается к интерфейсу при помощи команды режима настройки интерфейса **ip access-group**:

Router(config-if)# **ip access-group** { *access-list-number* | *access-list-name* } { **in** | **out** }

Для удаления всего ACL-списка из интерфейса сначала следует ввести команду **no ip access-group** на интерфейсе, а затем ввести глобальную команду **no access-list**.

На рис. 1 перечислены этапы и синтаксис для настройки и применения нумерованного стандартного списка контроля доступа на маршрутизаторе.

На рис. 2 приведен пример ACL-списка для разрешения одной сети.

Этот ACL-список разрешает пересылать трафик только из сети источника 192.168.10.0 с интерфейса S0/0/0. Трафик из сетей, отличных от 192.168.10.0, заблокирован.

Первая строка задаёт список контроля доступа как список доступа 1. Таким образом, разрешается трафик, соответствующий заданным параметрам. В этом случае IPv4-адрес и шаблонная маска, определяющая сеть источника — 192.168.10.0 0.0.0.255. Помните о существовании косвенной команды «deny all», эквивалентной добавлению строки **access-list 1 deny 0.0.0.0 255.255.255.255**.

Команда конфигурации интерфейса **ip access-group 1 out** связывает и привязывает ACL 1 к интерфейсу Serial 0/0/0 в качестве исходящего фильтра.

Поэтому ACL-список 1 разрешает выход через маршрутизатор R1 только узлам из сети 192.168.10.0/24. В то же время он запрещает любую другую сеть, включая 192.168.11.0.

# Применение стандартных ACL-списков на интерфейсах (продолжение)

На рис. 1 приведён пример ACL-списка, разрешающего исключить определённую подсеть за исключением конкретного узла в этой подсети.

Этот ACL-список заменяет предыдущий пример, но при этом дополнительно блокирует трафик с определённого адреса. Первая команда удаляет предыдущую версию ACL-списка 1. Следующая запись списка контроля доступа запрещает узел PC1, расположенный в сети 192.168.10.10. Все остальные узлы сети 192.168.10.0/24 разрешены. И снова косвенная запись отказа соответствует каждой иной сети.

ACL-список повторно применён на исходящем направлении интерфейса S0/0/0.

На рис. 2 приведён пример ACL-списка, который запрещает определённый узел. Этот ACL-список является заменой предыдущему примеру. В этом примере по-прежнему блокируется трафик от узла PC1, но разрешён весь остальной трафик.

Первые две команды аналогичны командам из предыдущего примера. Первая команда удаляет предыдущую версию ACL 1, в то время как следующая команда списка контроля доступа запрещает узел PC1, расположенный в сети 192.168.10.10.

Третья команда введена заново — в ней разрешаются все другие узлы. Это означает, что разрешены все узлы сети 192.168.10.0/24, за исключением PC1, который был запрещён в предыдущей записи.

Рассматриваемый ACL-список применяется на входящем направлении интерфейса G0/0. Поскольку фильтр затрагивает только на LAN 192.168.10.0/24 на G0/0, более эффективным будет применить ACL-список на входящем интерфейсов. ACL-список может быть применён на s0/0/0 в исходящем направлении, но с другой стороны, R1 будет вынужден проверять пакеты от всех сетей, включая 192.168.11.0/24.

# Создание стандартных именованных ACL-списков

Присвоение имён ACL-спискам упрощает понимание функции того или иного списка. Например, ACL-списку, настроенному для запрета FTP, можно присвоить имя «NO\_FTP». При присвоении ACL-списку имени вместо номера, режим конфигурации и синтаксис команд немного меняются.

На рис. 1 представлены последовательные действия, которые необходимо предпринять для создания стандартного именованного ACL-списка.

**Шаг 1.** Для созданием именованного ACL-списка начните с выполнения команды режима глобальной конфигурации **ip access-list**. Имена ACL-списков состоят из буквенно-цифровых символов, они чувствительны к регистру и должны быть уникальными. Команда **ip access-list standard** *name* используется для создания стандартного именованного ACL-списка, в то время как команда **ip access-list extended** *name* применяется для создания расширенного списка доступа. После ввода команды маршрутизатор входит в режим конфигурации стандартного именованного ACL-списка, как указано в командной строке.

**Примечание**. Для нумерованных ACL-списков используется команда глобальной конфигурации **access-list**, в то время как к именованным ACL-спискам IPv4 применяется команда **ip access-list**.

**Шаг 2.** В режиме конфигурации именованных ACL-списков примените команды **permit** или **deny**, чтобы задать одно или более условий определения отправки или отклонения пакета.

**Шаг 3.** Примените ACL-список к интерфейсу при помощи команды **ip access-group**. Определите, должен ли ACL-список применяться к пакетам, когда они приходят на интерфейс (**in**), или когда они покидают его (**out**).

На рис. 2 показаны команды, используемые для конфигурации стандартного именованного ACL-списка на интерфейсе G0/0 маршрутизатора R1, запрещающего доступ узла 192.168.11.10 к сети 192.168.10.0. ACL-списку присвоено имя «NO\_ACCESS».

Указывать имена ACL-списков заглавными буквами не обязательно, но это делает их более заметными при просмотре выходных данных текущей конфигурации. Это также снижает вероятность случайного создания двух разных ACL-списков с одинаковыми именами, но различающимися использованием заглавных и строчных букв.

# Комментарии к ACL-спискам

Для добавления комментариев (замечаний) о записях любого стандартного или расширенного ACL-списка можно использовать ключевое слово **remark**. Комментарии упрощают понимание и просмотр ACL-списков. Длина комментария ограничена 100 символами.

Комментарий можно добавлять до или после команды **permit** или **deny**. Однако при добавлении комментариев следует использовать систематичный подход, чтобы пользователь всегда мог понять, к какой команде **permit** или **deny** относится тот или иной комментарий. Например, размещение одних комментариев до соответствующих команд **permit** или **deny**, а других комментариев — после команд, может привести к путанице.

Для добавления комментария к нумерованному стандартному или расширенному ACL-списку IPv4 используйте команду глобальной конфигурации **access-list** *access-list\_number* **remark** *remark*. Чтобы удалить комментарий, используйте форму **no** этой команды.

В первом примере нумерованный ACL-список запрещает доступ гостевой рабочей станции 192.168.10.10 за пределы S0/0/0, но разрешает любые другие устройства из 192.168.0.0/16.

Для добавления комментария в именованном стандартном или расширенном ACL-списке используйте команду конфигурации списка доступа **remark**. Чтобы удалить комментарий, используйте форму **no** этой команды. В примере 2 показан стандартный именованный ACL-список. В этом примере комментарий операторов означает, что лабораторная рабочая станция с адресом узла 192.168.11.10 запрещена, но устройствам из всех других сетей доступ разрешен.

# Packet Tracer. Настройка стандартных ACL-списков

Стандартные списки контроля доступа (ACL-списки) являются сценариями конфигурации маршрутизатора, которые разрешают или запрещают маршрутизатору пропускать пакеты, исходя из адреса источника. Данное интерактивное задание фокусируется на определении критериев фильтрации, конфигурации стандартных ACL-списков, применении их на интерфейсах маршрутизатора и проверке и тестировании реализации ACL-списка. Маршрутизаторы уже сконфигурированы, в том числе установлены IP-адреса и настроена маршрутизация EIGRP.

[Packet Tracer. Настройка стандартных ACL-списков. Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.2.1.10%20Packet%20Tracer%20Configuring%20Standard%20ACLs%20Instructions.pdf)

[Packet Tracer. Настройка стандартных ACL-списков. PKA](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.2.1.10%20Packet%20Tracer%20Configuring%20Standard%20ACLs.pka)

# Packet Tracer. Настройка стандартных именованных ACL-списков

Старший сетевой администратор поставил перед вами задачу создать стандартный именованный ACL-список для предотвращения доступа к файловому серверу. Доступ должен быть запрещен всем клиентам одной сети и определённой рабочей станции другой сети.

[Packet Tracer. Настройка стандартных именованных ACL-списков. Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.2.1.11%20Packet%20Tracer%20-%20Configuring%20Named%20Standard%20ACLs%20Instructions.pdf)

[Packet Tracer. Настройка стандартных именованных ACL-списков. PKA](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.2.1.11%20Packet%20Tracer%20-%20Configuring%20Named%20Standard%20ACLs.pka)

# Редактирование стандартных нумерованных ACL-списков

**Редактирование нумерованных ACL-списков**

При настройке стандартного ACL-списка в текущую конфигурацию добавляются команды. Однако для этого не предусмотрена встроенная функция редактирования, позволяющая вносить изменения в ACL-список.

Существует два способа редактирования стандартного нумерованного ACL-списка.

**Метод 1.Использование текстового редактора**

После ознакомления с процессами создания и редактирования ACL-списков, более простым способом составления ACL будет использование текстового редактора, например блокнот от Майкрософт. Он позволяет создавать или вносить изменения в ACL-список, а затем вставить его в маршрутизатор. Выполните команду **show running-config**, чтобы отобразить ACL-список, после чего список нужно скопировать, вставить в текстовый редактор, внести необходимые изменения и затем вставить его обратно.

**Конфигурация**. Предположим, что IPv4-адрес узла на рисунке указан неправильно. Вместо узла 192.168.10.99 должен быть узел 192.168.10.10. Ниже приведён порядок действий при редактировании ACL 1:

**Шаг 1.** Отобразите текущий ACL-список с помощью команды **show running-config**. В примере на рисунке используется ключевое слово **include** для отображения только записей ACE.

**Шаг 2.** Выделите ACL-список, скопируйте его и вставьте в Блокнот. Внесите необходимые изменения. После корректировки ACL-списка в Блокноте, выделите его и скопируйте.

**Шаг 3.** В режиме глобальной конфигурации удалите список доступа с помощью команды **no access-list 1**. В противном случае новые операторы можно добавить в существующий список контроля доступа. Затем вставьте новый список контроля доступа в конфигурацию маршрутизатора.

**Шаг 4.** Используя команду **show running-config**, проверьте внесённые изменения.

Необходимо пояснить, что при применении команды **no access-list**, версии ОС IOS ведут себя по-разному. Если ACL-список, который был удалён, всё ещё применяется на интерфейсе, некоторые версии IOS действуют, как будто нет ACL-списков, защищающих сеть, в то время как другие версии блокируют весь трафик. По этой причине рекомендуется удалить ссылки на списки доступа с интерфейса перед внесением изменений в список доступа. Также имейте в виду, что если в заново созданном списке обнаружена ошибка, список необходимо отключить для устранения проблемы. Опять же, на время внесения изменений сеть не будет иметь ACL-списка.

# Редактирование стандартных нумерованных ACL-списков (продолжение)

**Метод 2. Использование порядкового номера**

Как показано на рисунке, начальная конфигурация ACL 1 включает запись узла для узла 192.168.10.99. Данная запись ошибочна. Узел должен быть сконфигурирован как 192.168.10.10. Чтобы изменить список контроля доступа с использованием порядковых номеров, выполните следующие действия:

**Шаг 1.** Ещё раз отобразите текущий ACL-список с помощью команды **show access-lists 1**. Выходные данные этой команды будут подробно обсуждаться далее в этом разделе. Порядковый номер отображается в начале каждой записи. Порядковый номер автоматически присваивается при добавлении записи в список. Обратите внимание, что запись с неправильной конфигурацией имеет порядковый номер 10.

**Шаг 2.** Введите команду **ip access-lists standard**, используемую для конфигурации именованного ACL-списка. Номер ACL-списка, 1,используется как его имя. Сначала необходимо удалить некорректно сконфигурированную запись с помощью команды **no 10**, где 10 ссылается на порядковый номер. Затем добавьте новую запись с порядковым номером 10 при помощи команды **10 deny host 192.168.10.10**.

**Примечание**. Записи нельзя перезаписать с теми же порядковыми номерами, что и у существующих записей. Сначала необходимо удалить текущую запись, а затем можно создавать новую.

**Шаг 3.** Проверьте внесённые изменения, используя команду **show access-lists**.

Как уже упоминалось ранее, Cisco IOS реализует внутреннюю логику для стандартных списков доступа. Порядок, в котором вводятся стандартные ACE-записи, может не совпадать с порядком, в котором они сохраняются, отображаются или обрабатываются маршрутизатором. Команда **show access-lists** отображает ACE-записи с их порядковыми номерами.

**Редактирование стандартных именованных ACL-списков**

В предыдущем примере для редактирования стандартного нумерованного ACL-списка использовались порядковые номера. Используя порядковые номера записей, отдельные записи можно легко вставить или удалить. Данный метод также можно использовать при редактировании стандартных именованных ACL-списков.

На рисунке приводится пример вставки строки в именованный список контроля доступа.

* В выходных данных команды **show** можно увидеть, что ACL-списку присвоено имя «NO\_ACCESS», он имеет две нумерованных строки, указывающих правила доступа для рабочей станции с IPv4-адресом 192.168.11.10.
* Команда **ip access-list standard** применяется для конфигурации именованных списков контроля доступа. В режиме конфигурации именованного списка доступа можно вставить или удалить запись. Команда **no** *sequence-number* применяется для удаления отдельных записей.
* Для добавления записи, содержащей запрет другой рабочей станции, требуется добавление нумерованной строки. В этом примере добавляется рабочая станция с IPv4-адресом 192.168.11.11 с новым порядковым номером 15.
* Заключительные выходные данные команды **show** подтверждают, что теперь для новой рабочей станции доступ запрещён.

# Проверка ACL-списков

Как показано на рис. 1, команда **show ip interface** используется для проверки ACL-списка на интерфейсе. Выходные данные этой команды включают номер или имя списка доступа и направление, к которому был привязан ACL-список. Выходные данные показывают, что маршрутизатор R1 имеет список доступа 1, применённый на исходящем интерфейсе S0/0/0, и список доступа NO\_ACCESS, применённый на его исходящем интерфейсе g0/0.

Пример на рис. 2 демонстрирует результаты выполнения команды **show access-lists** на маршрутизаторе R1. Чтобы просмотреть отдельный список доступа, примените команду **show access-lists**, а затем введите номер или имя списка доступа. Записи NO\_ACCESS могут выглядеть странным образом. Обратите внимание, что порядковый номер 15 отображается перед порядковым номером 10. Это результат внутреннего процесса маршрутизатора, который будет рассматриваться позже в рамках данного раздела.

# ACL-статистика

После применения ACL-списка на интерфейсе и завершения проверки с помощью команды **show access-lists** отображается статистика для каждой совпадающей записи. Заметьте, что некоторые записи в выходных данных на рис. 1 совпадают. Когда создаётся трафик, который должен соответствовать какой-либо записи ACL-списка, количество совпадений, отображаемых в выходных данных команды **show access-lists**, должно увеличиться. Например, если эхо-запрос исходит от PC1 к PC3 или PC4, выходные данные покажут увеличение количества совпадений для записи ACL 1, содержащей запрет.

Записи разрешения и запрета отслеживают статистику совпадений, однако необходимо помнить, что каждый список контроля доступа имеет косвенный отказ в последней строке. Данная запись не отображается при выполнении команды **show access-lists**, следовательно, статистика его не учитывает. Для просмотра статистики по косвенной записи «deny any», запись можно сконфигурировать вручную, после чего она появится в выходных данных. При ручной конфигурации команды «deny any» необходимо соблюдать крайнюю осторожность, поскольку она применяется ко всему трафику. Если данная запись не сконфигурирована как последняя запись ACL-списка, это может привести к неожиданным результатам.

В процессе тестирования ACL-списка, счётчики можно обнулить, выполнив команду **clear access-list counters**. Эту команду можно применять отдельно или с указанием номера или имени конкретного ACL-списка. Как показано на рис. 2, эта команда обнуляет счётчики статистики для списка контроля доступа.

# Порядковые номера стандартного ACL-списка

Cisco IOS реализует внутреннюю логику применительно к стандартным ACL-спискам. Как уже говорилось, частью этой логики является предотвращение операторов узла от конфигурации после операторов диапазона, если узел является участником этого диапазона, как показано на рис. 1.

Другой частью внутренней логики IOS является внутреннее упорядочение стандартных ACE. На рис. 2 показана конфигурация стандартных списков доступа. Операторы диапазона, блокирующие три сети, конфигурируются в первую очередь, далее конфигурируются операторы остальных пяти узлов. Все операторы узлов являются значимыми, поскольку IP-адреса их узлов не являются частью ранее введённых операторов.

Команда **show running-config** применяется для проверки конфигурации ACL-списка. Обратите внимание, что операторы перечислены в ином порядке, чем они были введены. Мы будем использовать команду **show access-lists**, чтобы понять эту логику.

Как показано на рис. 3, команда **show access-lists** отображает записи ACE в соответствии с их порядковыми номерами. Можно ожидать, что в выходных данных записи будут отображены в том же порядке, в котором они были введены. Однако выходные данные команды **show access-lists** показывают, что это не так.

Порядок, в котором перечислены стандартные ACE-записи — это последовательность, используемая IOS при обработке списка. Обратите внимание, что записи сгруппированы в два раздела — операторы узла следуют после операторов диапазона. Порядковый номер указывает порядок, в котором записи были введены, а не порядок, в котором они будут обрабатываться.

Операторы узла перечислены первыми, однако это не означает, что они были добавлены в этом порядке. IOS располагает операторы узлов с помощью специальной функции расстановки (hash function). Полученный порядок позволяет оптимизировать поиск оператора узла в ACL-списке.

Операторы диапазона отображаются после операторов узла. Эти операторы располагаются в том порядке, в котором они были введены.

Помните, все стандартные и нумерованные списки контроля доступа можно редактировать с помощью порядковых номеров. Порядковый номер, указанный в выходных данных команды **show access-lists**, является номером, используемым при удалении отдельной записи из списка. При добавлении новой записи в ACL-список порядковый номер будет влиять только на местоположение в списке оператора диапазона. Операторы узла всегда будут располагаться в определённом порядке благодаря функции расстановки.

Продолжая предыдущий пример, необходимо указать, что после сохранения текущей конфигурации маршрутизатор перезагружается (перезапускается). Как показано на рисунке 3, команда **show access-lists** отображает ACL-список в том же порядке, однако операторы перенумерованы. Порядковые номера теперь расположены в цифровой последовательности.

**Примечание**. Функция расстановки применяется только к операторам узла в стандартном списке контроля доступа IPv4. Алгоритм не применяется для расширенных ACL-списков IPv4 или IPv6. Это связано с тем, что фильтр расширенных и IPv6 ACL-списков больше, чем просто один адрес источника. Подробные сведения о функции расстановки не рассматривается в этой учебной программе.

**Лабораторная работа. Настройка и проверка стандартных ACL-списков**

**В ходе лабораторной работы необходимо выполнить следующие задания:**

* Часть 1. Создание топологии и запуск устройств
* Часть 2. Настройка устройств и проверка подключения
* Часть 3. Настройка и проверка стандартных нумерованных ACL-списков и стандартных именованных ACL-списков
* Часть 4. Внесение изменений в стандартный ACL-список

[Лабораторная работа. Настройка и проверка стандартных ACL-списков](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.2.2.7%20Lab%20-%20Configuring%20and%20Verifying%20Standard%20ACLs.pdf)

**Настройка стандартного ACL-списка для защиты порта VTY**

**Использование ACL-списка для управления доступом к VTY**

Cisco рекомендует использовать протокол SSH для административных подключений к маршрутизаторам и коммутаторам. Если образ Cisco IOS на маршрутизаторе не поддерживает протокол SSH, можно повысить безопасность административных каналов путем ограничения доступа к VTY. Ограничение доступа к VTY — метод, позволяющий определить, какому IP-адресу разрешён доступ Telnet к процессу EXEC маршрутизатора. Можно проконтролировать, какая административная рабочая станция или сеть управляет маршрутизатором с помощью ACL-списка и оператора **access-class**, сконфигурированного на каналах VTY. Также можно использовать этот метод с протоколом SSH для дальнейшего улучшения безопасности административного доступа.

Команда **access-class**, установленная в режиме конфигурации канала, ограничивает входящие и исходящие соединения между указанным VTY (в устройстве Cisco) и адресами в списке доступа.

Стандартные и расширенные списки контроля доступа применяются к пакетам данных, передающимся через маршрутизатор. Они не предназначены для блокировки пакетов, создающихся внутри маршрутизатора. Расширенный ACL-список по исходящему протоколу Telnet не препятствует открытию Telnet-сессий, инициированных маршрутизатором по умолчанию.

Фильтрация трафика Telnet или SSH, как правило, рассматривается как расширенная функция ACL-списка IP, поскольку подразумевает фильтрацию трафика протокола высшего уровня. Между тем, поскольку для фильтрации входящего и исходящего трафика Telnet/SSH используется команда **access-class**, можно применять стандартный ACL-список.

Синтаксис команды **access-class** выглядит следующим образом:

Router(config-line)# **access-class** *access-list-number* { **in** [ **vrf-also** ] | **out** }

Параметр **in** ограничивает входящие соединения между адресами в списке доступа и устройством Cisco, в то время как параметр **out** ограничивает исходящие соединения между отдельным устройством Cisco и адресами в списке доступа.

На рис. 1 показан пример, в котором у диапазона адресов есть доступ к каналам VTY 0-4. ACL-список на рисунке настроен на разрешение доступа для сети 192.168.10.0 к каналам VTY 0-4 и на запрет доступа для всех остальных сетей.

Следующие положения должны учитываться при конфигурации списка доступа к каналам VTY.

* Только нумерованные списки доступа могут применяться к VTY.
* Одинаковые ограничения должны быть установлены на все каналы VTY, поскольку пользователь может попытаться подключиться к любому из них.

Используйте инструмент проверки синтаксиса на рис. 2 для отработки навыков обеспечения защиты доступа к VTY.

# Проверка стандартного ACL-списка, использующегося для защиты порта VTY

После настройки ACL-списка для ограничения доступа к каналам VTY, важно убедиться в его надлежащем функционировании. На рисунке изображены два устройства, пытающиеся подключиться к R1 с помощью протокола SSH. Список доступа 21 настроен на каналы VTY маршрутизатора R1. PC1 успешно установил SSH-соединение, в то время как PC2 не удалось это сделать. Это прогнозируемое поведение, поскольку настроенный список доступа обеспечивает доступ к VTY из сети 192.168.10.0/24, запрещая доступ всем остальным устройствам.

Выходные данные для R1 показывают результат выполнения команды **show access-lists** после попыток PC1 и PC2 установить SSH-соединение. Совпадение в строке разрешения выходных данных является результатом успешного SSH-соединения PC1. Совпадение в строке запрета является следствием неудачной попытки установить SSH-подключение PC2, устройством в сети 192.168.11.0/24.

# Packet Tracer. Настройка ACL-списка для каналов VTY

Как администратору сети вам необходим удаленный доступ к маршрутизатору. Такой доступ не должны иметь другие пользователи сети. Таким образом, необходимо создать и применить ACL-список, позволяющий компьютеру подключаться к каналам Telnet и отклоняющий все другие IP-адреса источников.

[Packet Tracer. Настройка ACL-списка для каналов VTY. Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.2.3.3%20Packet%20Tracer%20-%20Configuring%20an%20ACL%20on%20VTY%20Lines%20Instructions.pdf)

[Packet Tracer. Настройка ACL-списка для каналов VTY. PKA](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.2.3.3%20Packet%20Tracer%20-%20Configuring%20an%20ACL%20on%20VTY%20Lines.pka)

**Лабораторная работа. Настройка и проверка ограничений VTY**

**В ходе лабораторной работы необходимо выполнить следующие задания** **:**

* Часть 1. Настроить основные параметры устройств
* Часть 2. Настроить и применить список контроля доступа на маршрутизаторе R1
* Часть 3. Проверить список контроля доступа с помощью Telnet
* Часть 4. Задание повышенной сложности. Настроить и применить список контроля доступа на коммутаторе S1

[Лабораторная работа. Настройка и проверка ограничений VTY](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.2.3.4%20Lab%20-%20Configuring%20and%20Verifying%20VTY%20Restrictions.pdf)

# Расширенные ACL-списки

**Проверка пакетов с помощью расширенных ACL-списков**

Для более точного контроля над фильтрацией трафика управления можно создать расширенные списки контроля доступа IPv4. Расширенные ACL-списки нумеруются от 100 до 199 и от 2000 до 2699, обеспечивая 799 возможных расширенных нумерованных ACL-списков. Расширенным ACL-спискам также можно присваивать имена.

Расширенные ACL-списки используются чаще, чем стандартные, поскольку они обеспечивают больший объем контроля. На рисунке показано, что, как и стандартные, расширенные ACL-списки проверяют адреса источников пакетов, а также адрес назначения, протоколы и номера портов (или службы). Это обеспечивает более широкий спектр критериев, на которых можно строить ACL-список. Например, расширенный ACL-список может разрешить трафик электронной почты из сети к определённому месту назначения с одновременным запретом передачи файлов и просмотром веб-страниц.

# Расширенные ACL-списки (продолжение)

**Проверка портов и служб**

Возможность фильтрации по протоколу и номеру порта позволяет сетевым администраторам создавать весьма специфические расширенные ACL-списки. Применение определяется путем настройки номера порта или имени известного порта.

На рис.1 показаны некоторые примеры того, как администратор определяет номера портов TCP или UDP, помещая его в конец оператора расширенного списка контроля доступа. Можно применить логические действия, такие как «равно» (eq), «не равно» (neq), «более чем» (gt) и «менее чем» (lt).

На рис. 2 показано, как отобразить список номеров портов и ключевых слов, которые можно использовать при создании ACL-списка, используя команду:

R1(config)# **access-list 101 permit tcp any any eq ?**

# Настройка расширенных ACL-списков

Последовательность шагов настройки расширенных ACL-списков такая же, как для стандартных ACL-списков. Сначала расширенный ACL-список настраивается, а затем активируется на интерфейсе. При этом следует учитывать, что синтаксис команды и параметры более сложны для обеспечения поддержки дополнительных функций, предоставляемых расширенными ACL-списками.

**Примечание**. Внутренний алгоритм применяется для упорядочения записей стандартного списка контроля доступа и не применяется для расширенных ACL-списков. Записи отображаются и обрабатываются в том порядке, в котором они вводились в процессе настройки.

На рис. 1 изображён общий синтаксис команд для расширенного списка контроля доступа IPv4. Обратите внимание, что существует множество ключевых слов и параметров для расширенных ACL-списков. Нет необходимости использовать все ключевые слова и параметры при конфигурации расширенного списка контроля доступа. Помните, что **?** может использоваться для получения помощи при вводе сложных команд.

На рис. 2 приведён пример расширенного списка контроля доступа. В этом примере сетевой администратор настроил ACL-списки для ограничения сетевого доступа любой внешней сети, чтобы разрешить просмотр веб-сайтов только из LAN, подключённой к G0/0. ACL 103 разрешает трафику, поступающий от любого адреса в сети 192.168.10.0, перейти к любому месту назначения с учетом ограничения, что трафик использует только порты 80 (HTTP) и 443 (HTTPS).

Характер протокола HTTP требует, чтобы трафик возвращался обратно в сеть от веб-сайтов, к которым обращались внутренние клиенты. Сетевой администратор хочет ограничить возвращающийся трафик до HTTP-обменов от запрашиваемых веб-сайтов, запрещая весь остальной трафик. Эту задачу выполняет ACL 104, блокируя весь входящий трафик за исключением трафика от ранее установленных подключений. Запись permit в ACL 104 разрешает входящий трафик параметром **established.**

Параметр **established** разрешает возврат в сеть 192.168.10.0/24 только того трафика, который изначально исходил из этой сети. Пакет удовлетворяет условиям, если обратный сегмент протокола TCP имеет биты ACK и RST, которые указывают, что пакет принадлежит существующему подключению. Без параметра **established** записи ACL-списка клиент может послать трафик на веб-сервер, но не получить обратный трафик, возвращающийся от веб-сервера.

# Применение расширенных ACL-списков на интерфейсах

В предыдущем примере сетевой администратор настроил ACL-список, чтобы разрешить пользователям из сети 192.168.10.0/24 просматривать как защищённые, так и ненадёжные веб-сайты. Даже настроенный ACL не будет фильтровать трафик до того, как будет применён на интерфейсе. Перед применением ACL на интерфейсе необходимо определить, какой вид трафика будет фильтроваться: входящий или исходящий. Когда пользователь внутренней LAN получает доступ к веб-сайту в Интернете, трафик идёт в Интернет. Когда внутренний пользователь получает электронную почту из Интернета, трафик идёт на локальный маршрутизатор. Однако в случае с применением списка контроля доступа на интерфейсе, «из» и «в» приобретают другие значения. С точки зрения ACL-списка, «из» и «в» являются ссылками на интерфейс маршрутизатора.

В топологии, изображённой на рисунке, маршрутизатор R1 обладает тремя интерфейсами. Это последовательный интерфейс S0/0/0 и два интерфейса Gigabit Ethernet: G0/0 и G0/1. Помните, что расширенный список контроля доступа обычно должен быть применён как можно ближе к источнику. В этой топологии ближайший к источнику целевого трафика интерфейс — это интерфейс G0/0.

Трафик веб-запросов от пользователей LAN 192.168.10.0/24 — входящий трафик на интерфейс G0/0. Обратный трафик от установленных соединений к пользователям локальной сети считается исходящим с интерфейса G0/0. Пример применения ACL-списка на интерфейсе G0/0 в обоих направлениях. Входящий ACL 103 проверяет тип трафика. Исходящий ACL 104 проверяет трафик, возвращающийся от установленных соединений. Это ограничивает доступ в Интернет для сети 192.168.10.0, чтобы разрешить только просмотр веб-страниц.

**Примечание**. Список доступа можно применить на интерфейсе S0/0/0, но в этом случае при обработке списка контроля доступа маршрутизатор будет просматривать все пакеты, приходящие на него, а не только трафик в сеть 192.168.11.0 и из неё. Это может стать причиной излишней нагрузки на маршрутизатор.

# Фильтрация трафика с использованием расширенных ACL-списков

В примере на рис. 1 запрещён трафик FTP из подсети 192.168.11.0, который направляется в подсеть 192.168.10.0, но разрешён любой другой тип трафика. Обратите внимание на использование шаблонной маски и косвенной команды отказа deny any. Не забывайте, что протокол FTP использует порты TCP 20 и 21; таким образом, для запрета доступа FTP ACL-списку требуется оба ключевых слова имени порта: **ftp** и **ftp-data** или **eq 20** и **eq 21**.

Если используется номер порта вместо имени порта, команды будут иметь следующий вид:

**access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20**

**access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21**

Чтобы исключить блокирование всего трафика командой deny any, представленной в виде косвенной записи в конце каждого ACL-списка, необходимо добавить команду **permit ip any any**. При отсутствии, по крайней мере, одной разрешающей команды **permit** в ACL-списке весь трафик на интерфейсе, где применён ACL, будет сброшен. Список контроля доступа должен применяться на входящем интерфейсе G0/1, для того чтобы трафик из локальной сети 192.168.11.0/24 фильтровался при поступлении на интерфейс маршрутизатора.

В примере на рис. 2 запрещён трафик протокола Telnet из любого источника в LAN 192.168.11.0/24, но разрешён весь остальной IP-трафик. Поскольку трафик, предназначенный для локальной сети 192.168.11.0/24, является исходящим на интерфейсе G0/1, ACL-список будет применён на G0/1 с ключевым словом **out**. Обратите внимание на использование ключевых слов **any** в командах разрешения. Запись, содержащая разрешение, добавляется, чтобы избежать ненужной блокировки трафика.

**Примечание**. В примерах на рис. 1 и 2 в конце ACL-списка приводится команда **permit ip any any**. Для обеспечения большей безопасности можно применить команду **permit 192.168.11.0 0.0.0.255 any**.

# Создание расширенных именованных ACL-списков

Именованные расширенные списки доступа создаются практически тем же способом, что и именованные стандартные ACL-списки. Для создания расширенного ACL-списка с присвоением имени необходимо выполнить следующие действия:

**Шаг 1.** В режиме глобальной конфигурации выполните команду **ip access-list extended** *name* для определения имени расширенного ACL-списка.

**Шаг 2.** В режиме конфигурации именованного ACL-списка укажите условия для **permit** или **deny**.

**Шаг 3.** Вернитесь в привилегированный режим EXEC и проверьте ACL-список при помощи команды **show access-lists** *name*.

**Шаг 4.** Сохраните записи в файле конфигурации, выполнив команду **copy running-config startup-config**.

Для удаления именованного расширенного ACL-списка выполните команду глобальной конфигурации **no ip access-list extended** *name*.

На рисунке показаны именованные версии ACL-списков, созданных в предыдущих примерах. Именованный ACL-список SURFING разрешает пользователям локальной сети 192.168.10.0/24 доступ к веб-сайтам. Именованный ACL-список BROWSING разрешает обратный трафик от установленных соединений. С использованием имён ACL-списка правила применяются на входящем и исходящем направлениях интерфейса G0/0.

# Проверка расширенных ACL-списков

После того, как ACL-список настроен и применён на интерфейсе, выполните проверку конфигурации при помощи команд Cisco IOS **show**. На рисунке верхний пример показывает команду Cisco IOS для отображения содержимого всех списков контроля доступа. Нижний пример показывает результаты применения команды **show ip interface g0/0** на маршрутизаторе R1.

В отличие от стандартных списков контроля доступа, расширенные ACL-списки не реализуют ту же внутреннюю логику и функцию расстановки. Выходные данные и порядковые номера, отображаемые в выходных данных команды **show access-lists**, демонстрируют порядок, в котором были введены записи. Записи узла не перечисляются автоматически перед записями диапазона.

Команда **show ip interface** используется для проверки ACL-списка на интерфейсе и направления, к которому был привязан список. Выходные данные этой команды включают номер или имя списка доступа и направление, к которому был привязан ACL-список. Написанные заглавными буквами имена ACL-списков — BROWSING и SURFING — выделяются на экране выходных данных.

После проверки конфигурации ACL-списка нужно подтвердить, что ACL-списки работают, как запланировано, т.е. блокируют и пропускают трафик согласно требованиям.

Согласно рекомендациям, приведённым выше в этом разделе, конфигурацию ACL-списка желательно первоначально проверять в экспериментальной сети, и только после этого применять ACL-список в реальной действующей сети.

**Редактирование расширенных ACL-списков**

Внесение изменений в расширенный ACL-список осуществляется по аналогии с внесением изменений в стандартный ACL-список. Расширенный ACL-список можно изменить с помощью следующих инструментов:

* **Метод 1. Текстовый редактор** — при использовании этого метода ACL-список копируется и вставляется в текстовый редактор, в котором производятся изменения. Текущий список доступа удаляется командой **no access-list**. Отредактированный ACL-список затем вставляется обратно в конфигурацию.
* **Метод 2. Порядковые номера** — порядковые номера используются для удаления или вставки записи ACL-списка. Команда **ip access-list extended** *name* применяется для запуска режима конфигурации именованного ACL-списка. Если ACL-списку присвоен номер, а не имя, номер ACL-списка используется в параметре *name*. ACE-записи можно вставить или удалить.

На рисунке администратору необходимо отредактировать стандартный список контроля доступа с именем SURFING — исправить опечатку в записи сети источника. Для просмотра текущих порядковых номеров используется команда **show access-lists**. Запись, подлежащая редактированию, определяется как запись 10. Исходная запись удаляется командой **no** *sequence\_#*. Исправленная запись замещает исходную запись.

# Packet Tracer. Настройка расширенных ACL-списков. Сценарий 1

**Сценарий**

Двум работникам предприятия требуется доступ к службам, предоставляемым сервером. PC1 требуется доступ только к FTP, в то время как PC2 нужен доступ только к веб-сети. Оба компьютера могут отправлять эхо-запросы серверу, но не друг другу.

[Packet Tracer. Настройка расширенных ACL-списков. Сценарий 1. Инструкции.](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.3.2.10%20Configuring%20Extended%20ACLs%20Scenario%201%20Instructions.pdf)

[Packet Tracer. Настройка расширенных ACL-списков. Сценарий 1. PKA](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.3.2.10%20Configuring%20Extended%20ACLs%20Scenario%201.pka)

# Packet Tracer. Настройка расширенных ACL-списков. Сценарий 2

**Сценарий**

В этом сценарии устройствам в одной LAN разрешается удалённый доступ к устройствам другой LAN посредством протокола Telnet. Весь трафик, кроме ICMP, от других сетей запрещён.

[Packet Tracer. Настройка расширенных ACL-списков. Сценарий 2. Инструкции.](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.3.2.11%20Configuring%20Extended%20ACLs%20Scenario%202%20Instructions.pdf)

[Packet Tracer. Настройка расширенных ACL-списков. Сценарий 2. PKA](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.3.2.11%20Configuring%20Extended%20ACLs%20Scenario%202.pka)

# Packet Tracer. Настройка расширенных ACL-списков. Сценарий 3

**Исходные данные/Сценарий**

В этом сценарии конкретным устройствам сети LAN разрешается доступ к различным службам серверов, размещённым в сети Интернет.

[Packet Tracer. Настройка расширенных ACL-списков. Сценарий 3. Инструкции.](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.3.2.12%20Configuring%20Extended%20ACLs%20Scenario%203%20Instructions.pdf)

[Packet Tracer. Настройка расширенных ACL-списков. Сценарий 3. PKA](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.3.2.12%20Configuring%20Extended%20ACLs%20Scenario%203.pka)

**Лабораторная работа. Настройка и проверка расширенных ACL-списков**

**В ходе лабораторной работы необходимо выполнить следующие задания** **:**

* Часть 1. Создание топологии и запуск устройств
* Часть 2. Настройка устройств и проверка подключения
* Часть 3. Настройка и проверка стандартных нумерованных ACL-списков и стандартных именованных ACL-списков.
* Часть 4. Редактирование и проверка расширенных ACL-списков

[Лабораторная работа. Настройка и проверка расширенных ACL-списков](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.3.2.13%20Lab%20-%20Configuring%20and%20Verifying%20Extended%20ACLs.pdf)

**Логика работы входящего и исходящего ACL-списков**

**Логика работы входящего ACL-списка**

На рис. 1 проиллюстрирована логика работы входящего ACL-списка. Если данные в заголовке пакета соответствуют первой записи ACL-списка, остальные записи списка опускаются, и пакет принимается или отклоняется, в зависимости от условия, с которым он совпал. Если заголовок пакета не соответствует первой записи ACL-списка, пакет проверяется на соответствие следующей записи в списке. Этот процесс повторяется до тех пор, пока не будут проверены все записи списка.

Последней записью в конце каждого ACL-списка является косвенная команда «deny any». Данная запись не отображается в выходных данных. Команда «deny any» применяется ко всем пакетам, не удовлетворяющим условиям проверки. Последнее условие проверки соответствует всем оставшимся пакетам и инициирует в их отношении действие «запретить». Маршрутизатор отбрасывает все оставшиеся пакеты, не передавая их на интерфейс или из интерфейса. Последнюю запись списка часто называют «косвенным отказом deny any» или командой «запретить весь трафик». Из-за этой команды список контроля доступа должен иметь хотя бы одну разрешающую запись, в противном случае весь трафик будет блокироваться.

**Логика работы исходящего ACL-списка**

Рис. 2 иллюстрирует логику работы исходящего ACL-списка. Перед тем как пакет пересылается на исходящий интерфейс, маршрутизатор проверяет таблицу маршрутизации, чтобы определить, подлежит ли пакет маршрутизации. Если пакет не подлежит маршрутизации, он отбрасывается и не проверяется на соответствие записям ACE. Следующим этапом маршрутизатор проверяет, задан ли исходящий интерфейс в списке контроля доступа. Если интерфейс не задан, пакет отправляется в выходной буфер. Приведём несколько примеров принципа работы исходящего списка контроля доступа:

* **ACL-список не применён на интерфейсе:** если исходящий интерфейс не связан с исходящим ACL, пакет отправится непосредственно на исходящий интерфейс.
* **ACL-список применён на интерфейсе:** если исходящий интерфейс связан с исходящим ACL, пакет не будет отправлен на исходящий интерфейс до тех пор, пока не будет проверен комбинацией записей ACE, связанных с этим интерфейсом. В зависимости от результата проверки пакет принимается или отклоняется.

Для исходящих списков контроля доступа принятие означает отправку пакета в выходной буфер, а отклонение — отбрасывание пакета.

# Логические действия ACL-списка

**ACL-список, маршрутизация и процессы ACL-списка на маршрутизаторе**

На рисунке проиллюстрированы логика работы маршрутизации и процессов ACL-списка. При получении пакета на интерфейс маршрутизатора, процесс маршрутизации остаётся неизменным, независимо от того, применяются ACL-списки или нет. Поскольку кадр прибывает на интерфейс, маршрутизатор проверяет его на соответствие адреса назначения уровня 2 адресу интерфейса маршрутизатора уровня 2, и является ли кадр кадром широковещательной рассылки.

Если адрес кадра принят, информация кадра удаляется, и маршрутизатор проверяет наличие ACL-списка на входящем интерфейсе. При наличии ACL-списка пакет сопоставляется с записями в списке.

Если пакет соответствует одной из записей, он принимается или отклоняется в зависимости от условия, с которым он совпал. Если пакет принимается, он проверяется на наличие соответствующей записи в таблице маршрутизации с целью определения интерфейса назначения. Если для данного места назначения существует запись в таблице маршрутизации, пакет перенаправляется на выходной интерфейс, если записи нет — пакет отбрасывается.

Далее маршрутизатор проверяет, имеется ли на выходном интерфейсе ACL-список. При наличии ACL-списка пакет сопоставляется с записями в списке.

Если пакет соответствует одной из записей, он принимается или отклоняется в зависимости от условия, с которым он совпал.

Если ACL-список отсутствует, или пакету разрешено прохождение, пакет инкапсулируется в новом протоколе уровня 2 и перенаправляется на интерфейс следующего устройства.

# Процесс принятия решений стандартного ACL-списка

Стандартные ACL-списки анализируют только IPv4-адрес источника. Пункт назначения пакета и задействованные порты не рассматриваются.

Процесс принятия решений стандартного ACL-списка проиллюстрирован на рисунке. Операционная система Cisco IOS поочерёдно проверяет адреса, сопоставляя их с условиями ACL-списка. Первое же совпадение определяет, принимает ли операционная система данный адрес или нет. Поскольку ОС прекращает проверку условий после первого совпадения, порядок размещения условий принципиально важен. При отсутствии совпадений адрес не пропускается.

# Процесс принятия решений расширенного ACL-списка

На рисунке проиллюстрирован логический путь принятия решений расширенным ACL-списком с целью фильтрации трафика по адресам источника и назначения, протоколу и номерам портов. В рассматриваемом примере ACL-список сначала выполняет фильтрацию по адресу источника, а затем — по порту и протоколу источника. Далее он выполняет фильтрацию по адресу назначения, а затем — по порту и протоколу назначения; после этого принимается окончательное решение о разрешении или запрете.

Помните, что записи ACL-списка обрабатываются одна за другой, поэтому решение «нет» не обязательно означает «запретить». По мере продвижения по пути логического принятия решений, обратите внимание, что «нет» означает переход к следующей записи с целью нахождения совпадения с условием.

# Поиск и устранение распространённых ошибок ACL-списка. Пример 1

Использование команд **show**, описанных в предыдущих разделах, позволяет выявить большинство распространённых ошибок ACL-списка. К подобным ошибкам относятся ввод записей ACE в неверном порядке и неприменение соответствующих критериев к правилам ACL-списка.

**Пример ошибки 1**

На приведённом рисунке узел 192.168.10.10 не может подключиться к 192.168.30.12. При просмотре выходных данных команды **show access-lists** обнаружены совпадения для первой запрещающей записи. Это указывает на то, что данное условие совпало по трафику.

**Решение** — проверить порядок записей ACE. Узел 192.168.10.10 не может подключиться к 192.168.30.12 из-за расположения правила 10 в списке доступа. Поскольку маршрутизатор обрабатывает списки контроля доступа, следуя сверху вниз, правило 10 запрещает узел 192.168.10.10, поэтому для правила 20 может никогда не найтись совпадение. Записи 10 и 20 следует поменять местами. Последняя строка разрешает весь остальной трафик, отличный от TCP, соответствующий протоколу IP (UDP, ICMP и т.д.).

# Поиск и устранение распространённых ошибок ACL-списка. Пример 2

**Пример ошибки 2**

На рисунке сеть 192.168.10.0/24 не может использовать протокол TFTP для подключения к сети 192.168.30.0/24.

**Решение** — сеть 192.168.10.0/24 не может использовать протокол TFTP для подключения к сети 192.168.30.0/24, поскольку протокол TFTP использует транспортный протокол UDP. Строка 30 в списке доступа 120 разрешает весь трафик TCP. Но поскольку TFTP использует UDP вместо TCP, он косвенно запрещён. Помните, что косвенный отказ «deny any» не отображается в выходных данных команды **show access-lists** и, следовательно, совпадения также не отображаются.

Запись 30 следует заменить на **ip any any**.

Приведённый ACL-список работает вне зависимости от того, применён ли он на G0/0 R1, S0/0/1 R3 или S0/0/0 R2 во входящем направлении. Однако, основываясь на правиле размещения расширенного ACL-списка как можно ближе к источнику, наиболее оптимальным вариантом будет G0/0 R1, поскольку в данном случае нежелательный трафик будет фильтроваться без необходимости в прохождении через всю инфраструктуру сети.

# Поиск и устранение распространённых ошибок ACL-списка. Пример 3

**Пример ошибки 3**

На рисунке сеть 192.168.11.0/24 может использовать протокол Telnet для соединения с 192.168.30.0/24, но в соответствии с политикой компании, соединение данного типа запрещено. Результаты команды **show access-lists 130** указывают на то, что найдено совпадение с разрешающим условием.

**Решение** — сеть 192.168.11.0/24 может использовать протокол Telnet для подключения к сети 192.168.30.0/24, так как номер порта протокола Telnet в строке 10 списка доступа 130 приведён в неверном месте записи ACL-списка. В настоящее время строка 10 запрещает любой источник пакета с номером порта, равным Telnet. Чтобы запретить трафик Telnet на входящем интерфейсе G0/1, нужно запретить номер порта назначения, равный Telnet, например, **deny tcp any any eq telnet**.

# Поиск и устранение распространённых ошибок ACL-списка. Пример 4

**Пример ошибки 4**

На рисунке узел 192.168.30.12 имеет возможность использовать Telnet для подключения к 192.168.31.12, но согласно политике безопасности компании, подобное подключение должно быть запрещено. Выходные данные команды **show access-lists 140** указывают на то, что найдено совпадение с разрешающим условием.

**Решение** — узел 192.168.30.12 может использовать Telnet для подключения к 192.168.31.12, так как нет правил, запрещающих узел 192.168.30.12 или его сеть в качестве источника. Строка 10 списка доступа 140 запрещает интерфейс маршрутизатора, через который трафик поступает на маршрутизатор. IPv4-адрес узла в записи 10 должен быть равен 192.168.30.12.

# Поиск и устранение распространённых ошибок ACL-списка. Пример 5

**Пример ошибки 5**

На рисунке узел 192.168.30.12 может использовать протокол Telnet для подключения к 192.168.31.12, но в соответствии с политикой безопасности, данное подключение не может быть разрешено. Выходные данные команды **show access-lists 150** указывают на то, что, вопреки ожиданиям, нет ни одного совпадения с запрещающим условием.

**Решение** — узел 192.168.30.12 может подключаться к 192.168.31.12 через протокол Telnet из-за направления, в котором список доступа 150 применён на интерфейсе G0/1. Правило 10 запрещает любой адрес источника для подключения к узлу 192.168.31.12 с использованием telnet. Однако для корректной фильтрации этот фильтр должен быть применён на исходящем G0/1.

**Packet Tracer. Поиск и устранение неполадок ACL-списков**

**Сценарий**

Создание сети с реализацией следующих трёх политик:

* Узлы сети 192.16 8.0.0/24 не могут получить доступ ни к одной службе TCP сервера Server3.
* Узлы сети 10.0.0.0/8 не могут получить доступ к сервису HTTP сервера Server1.
* Узлы сети 172.16.0.0/16 не могут получить доступ к сервису FTP сервера Server2.

[Packet Tracer. Поиск и устранение неполадок ACL-списков. Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.4.2.6%20Packet%20Tracer%20-%20Troubleshooting%20ACLs%20Instructions.pdf)

[Packet Tracer. Поиск и устранение неполадок ACL-списков. PKA](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.4.2.6%20Packet%20Tracer%20-%20Troubleshooting%20ACLs.pka)

**Лабораторная работа. Поиск и устранение неполадок в конфигурации и размещении ACL-списков**

**В ходе лабораторной работы необходимо выполнить следующие задания:**

* Часть 1. Создание сети и настройка основных параметров устройства
* Часть 2. Поиск и устранение неисправностей внутреннего доступа
* Часть 3. Поиск и устранение неисправностей удалённого доступа

[Лабораторная работа. Поиск и устранение неполадок в конфигурации и размещении ACL-списков](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.4.2.7%20Lab%20-%20Troubleshooting%20ACL%20Configuration%20and%20Placement.pdf)

# Packet Tracer. Отработка практических навыков по работе с программой

В рамках этого задания вам необходимо завершить схему адресации, настроить маршрутизацию и применить именованные списки контроля доступа.

[Packet Tracer. Отработка практических навыков по работе с программой. Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.4.2.8%20Packet%20Tracer%20-%20Skills%20Integration%20Challenge%20Instructions.pdf)

[Packet Tracer. Отработка практических навыков по работе с программой. PKA](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.4.2.8%20Packet%20Tracer%20-%20Skills%20Integration%20Challenge.pka)

**Типы ACL-списков для IPv6**

В отношении эксплуатации и конфигурации ACL-списки для IPv6 очень похожи на ACL-списки для IPv4. Предварительно ознакомившись со списками доступа для IPv4, вам будет легче разобраться в принципах работы и конфигурации списков доступа для IPv6.

Существует два типа ACL-списков для протокола IPv4: стандартный и расширенный. ACL-спискам обоих типов можно присвоить номера или имена.

В IPv6 существует только один тип ACL-списка, представляющий собой эквивалент расширенного именованного ACL-списка для IPv4. Нумерованных ACL-списков для IPv6 не существует. Резюмируя, об ACL-списках для IPv6 можно сказать следующее:

* представлены только в виде именованных ACL-списков;
* по функциональности эквивалентны расширенным ACL-спискам для IPv4.

ACL-список для IPv4 и ACL-список для IPv6 не могут иметь одно и то же имя.

**Сравнение ACL-списков для IPv4 и IPv6**

Несмотря на то, что ACL-списки для IPv4 и IPv6 очень схожи, у них есть три серьёзных отличия.

* **Применение ACL-списка для IPv6**

Первым отличием является команда, используемая для применения ACL-списка IPv6 на интерфейсе. IPv4 использует команду **ip access-group** для применения ACL-списка IPv4 на интерфейсе IPv4. IPv6 использует команду **ipv6 traffic-filter** для выполнения аналогичной функции на интерфейсах IPv6.

* **Отсутствие шаблонных масок**

В отличие от ACL-списков для IPv4, ACL-списки для IPv6 не используют шаблонные маски. В протоколе IPv6 для указания того, какая часть IPv6-адреса источника или назначения должна совпадать, используется длина префикса.

* **Дополнительные записи по умолчанию**

Последнее значительное отличие заключается в наличии двух дополнительных записей косвенного разрешения в конце каждого ACL-списка для IPv6. В конце каждого стандартного или расширенного списка доступа IPv4 находится запись косвенного отказа **deny any** или **deny any any**. В конце каждого ACL-списка для IPv6 находится похожее правило — **deny ipv6 any any**. Различие заключается в том, что IPv6 также включает два других косвенных условия по умолчанию:

* **permit icmp any any nd-na**
* **permit icmp any any nd-na**

Эти условия позволяют маршрутизатору пользоваться IPv6-эквивалентом протокола ARP для IPv4. Давайте вспомним, что протокол ARP применяется в IPv4 для разрешения адресов уровня 3 MAC-адресам уровня 2. Как показано на рисунке, IPv6 использует сообщения обнаружения соседних устройств ICMP (ND) для выполнения тех же задач. ND использует сообщения запроса соседнего устройства (NS) и сообщения объявления соседнего устройства (NA).

Сообщения ND инкапсулируются в пакеты IPv6 и требуют служб IPv6 сетевого уровня, в то время как протокол ARP для IPv4 не использует уровень 3. Поскольку IPv6 использует службу уровня 3 для обнаружения соседей, ACL-списки IPv6 нуждаются в косвенном разрешении, чтобы отправлять и получать ND пакеты на интерфейсе. Главным образом, разрешены сообщения обнаружения соседей — сообщения объявления соседей (nd-na) и сообщения обнаружения соседей — сообщения запроса соседей (nd-ns).

# Создание топологии IPv6

Рис.1 иллюстрирует топологию, которая будет использоваться для конфигурации ACL-списков IPv6. Топология схожа с предыдущей топологией IPv4, за исключением схемы IPv6-адресации. Существует три подсети 2001:DB8:CAFE::/64: 2001:DB8:CAFE:10::/64, 2001:DB8:CAFE:11::/64 и 2001:DB8:CAFE:30::/64. Две последовательных сети подключены к трем маршрутизаторам: 2001:DB8:FEED:1::/64 и 2001:DB8:FEED:2::/64.

На рис. 2, 3 и 4 приводится конфигурация IPv6-адресации для каждого маршрутизатора. Для проверки адреса и состояния интерфейса применяется команда **show ipv6 interface brief**.

**Примечание**. Команды **no shutdown** и **clock rate** не отображаются.

# Настройка ACL-списков для IPv6

В протоколе IPv6 существуют только именованные списки контроля доступа. Настройка этих списков аналогична настройке расширенного именованного ACL-списка для IPv4.

На рис. 1 приводится синтаксис команд для ACL-списков IPv6. Опять же, приведённый синтаксис аналогичен синтаксису, применяемому для расширенных ACL-списков IPv4. Одно из наиболее значимых различий заключается в использовании IPv6 длины префикса вместо шаблонной маски IPv4.

Для настройки списка IPv6 ACL требуется выполнение трёх действий:

**Шаг 1.** Для создания ACL-списка IPv6 выполните команду режима глобальной конфигурации **ipv6 access-list** *name*. Как и в случае с именованными ACL-списками для IPv4, имена списков для IPv6 состоят из буквенно-цифровых символов, они чувствительны к регистру и должны быть уникальными. В отличие от IPv4, стандартная или расширенная опция не требуются.

**Шаг 2.** В режиме настройки списка ACL примените команды **permit** или **deny** для указания одного или более условий, согласно которым пакет будет отправлен или отклонён.

**Шаг 3.** Вернитесь в привилегированный режим EXEC с помощью команды **end**.

На рис. 2 продемонстрированы шаги создания ACL-списка для IPv6 на простом примере, построенном на предыдущей топологии. Первой записью списка становится название ACL-списка IPv6 — NO-R3-LAN-ACCESS. Как и в именованных ACL-списках IPv4, указывать имена ACL-списков IPv6 заглавными буквами не обязательно, но это делает их более заметными при просмотре выходных данных текущей конфигурации.

Вторая строка запрещает все IPv6-пакеты из 2001:DB8:CAFE:30::/64, предназначенные для любой IPv6 сети. Третья строка содержит разрешение для всех остальных пакетов IPv6.

На рис. 3 приводится ACL-список в контексте топологии.

# Применение ACL-списка IPv6 на интерфейсе

После создания ACL-списка для IPv6, его необходимо применить к интерфейсу с помощью команды **ipv6 traffic-filter**:

Router(config-if)# **ipv6 traffic-filter** *access-list-name* { **in** | **out** }

На рисунке приводится сконфигурированный ранее ACL-список NO-R3-LAN-ACCESS, а также команды, используемые для применения ACL-списка IPv6 на входящем интерфейсе S0/0/0. Применение ACL-списка на входящем интерфейсе S0/0/0 запретит пакетам из 2001:DB8:CAFE:30::/64 доступ к обеим локальным сетям на R1.

Для удаления ACL-списка из интерфейса сначала следует ввести команду **no ipv6 traffic-filter** на интерфейсе, а затем глобальную команду **no ipv6 access-list** — для удаления списка доступа.

**Примечание**. И IPv4, и IPv6 используют команду **access-class** для применения списка доступа к портам VTY.

# Примеры ACL-списка для IPv6

**Запрет протокола FTP**

Топология для примера приведена на рис. 1.

В первом примере, представленном на рис. 2, маршрутизатор R1 настроен с помощью списка доступа IPv6 на запрет трафика FTP для 2001:DB8:CAFE:11::/64. Порты для данных FTP (порт 20) и управления FTP (порт 21) должны быть заблокированы. Поскольку фильтр применён на входящем интерфейсе G0/0 R1, запрещён будет только трафик из сети 2001:DB8:CAFE:10::/64.

**Ограниченный доступ**

Во втором примере, представленном на рис. 3, ACL-список IPv6 сконфигурирован для предоставления LAN на R3 ограниченного доступа к локальным сетям на R1. Комментарии добавлены в конфигурацию для документации ACL-списка. Следующие функции были отмечены в ACL-списке:

1. Первые два разрешающих правила дают доступ с любого устройства к веб-серверу, расположенному в 2001:DB8:CAFE:10::10.

2. Доступ для всех остальных устройств в сеть 2001:DB8:CAFE:10::/64 запрещён.

3. PC3 в 2001:DB8:CAFE:30::12 разрешён доступ Telnet к PC2, который имеет IPv6-адрес 2001:DB8:CAFE:11::11.

4. Всем остальным устройства доступ Telnet к PC2 запрещён.

5. Для всего остального IPv6-трафика разрешён доступ ко всем остальным местам назначениям.

6. Список доступа IPv6 применяется на интерфейсе G0/0 во входящем направлении, так что задействована только сеть 2001:DB8:CAFE:30::/64.

# Проверка ACL-списков для IPv6

Команды для проверки списка доступа IPv6 аналогичны командам, используемым для проверки списков доступа IPv4. С помощью этих команд можно проверить список доступа IPv6 RESTRICTED-ACCESS, сконфигурированный ранее. Рис. 1 показывает выходные данные команды **show ipv6 interface**. Выходные данные подтверждают, что ACL-список RESTRICTED-ACCESS сконфигурирован на входящем интерфейсе G0/0.

Как показано на рис. 2, команда **show access-lists** отображает все списки доступа на маршрутизаторе, включая оба вида списков доступа — IPv4 и IPv6. Обратите внимание, что порядковые номера ACL-списков IPv6 помещаются в конце строки, а не в начале, как в ACL-списках IPv4. Хотя записи появляются в том порядке, в каком они вводятся, они не всегда возрастают на 10. Это связано с тем, что комментарии к записям добавляются при помощи порядковых номеров, но они не отображаются в выходных данных команды **show access-lists**.

Как и расширенные ACL-списки IPv4, списки доступа IPv6 отображаются и обрабатываются в порядке, в котором были добавлены записи. Помните, что стандартные ACL-списки IPv4 используют внутреннюю логику, которая меняет их порядок и последовательность операций.

Как показано на рис. 3, выходные данные команды **show running-config** включают все записи ACE и комментарии к ним. Комментарии к записям могут идти до или после разрешающего или запрещающего правила **permit** или **deny**, но располагать их следует однообразно.

**Packet Tracer. Настройка ACL-списков для IPv6**

**Задачи**

* Часть 1. Настройте, примените и проверьте ACL-список для IPv6
* Часть 2. Настройте, примените и проверьте второй ACL-список для IPv6

[Packet Tracer. Настройка ACL-списков для IPv6. Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.5.2.6%20Packet%20Tracer%20-%20Configuring%20IPv6%20ACLs%20Instructions.pdf)

[Packet Tracer. Настройка ACL-списков для IPv6. PKA](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.5.2.6%20Packet%20Tracer%20-%20Configuring%20IPv6%20ACLs.pka)

**Лабораторная работа. Настройка и проверка ACL-списков для IPv6**

**В ходе лабораторной работы необходимо выполнить следующие задания:**

* Часть 1. Создание топологии и запуск устройств
* Часть 2. Настройка устройств и проверка подключения
* Часть 3. Настройка и проверка ACL-списка для IPv6
* Часть 4. Внесение изменений в ACL-список для IPv6

[Лабораторная работа. Настройка и проверка ACL-списков для IPv6](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.5.2.7%20Lab%20-%20Configuring%20and%20Verifying%20IPv6%20ACLs.pdf)

**FTP запрещён**

**FTP запрещён**

**Сценарий**

Недавно вы получили сообщение о том, что в пределах сети вашего предприятия малого или среднего бизнеса появились вирусы. Ваш системный администратор отслеживал производительность сети и определил, что один узел постоянно загружает файлы с удаленного FTP сервера. На этом узле, вероятно, имеется источник вирусов, проникший через сеть!

Выполните это задание, используя программу Packet Tracer. Создайте именованный ACL-список, чтобы блокировать доступ с узла на FTP-сервер. Примените ACL-список на наиболее подходящем интерфейсе маршрутизатора.

Для завершения физической топологии необходимо использовать:

* одну станцию узла ПК;
* два коммутатора;
* один маршрутизатор с интегрированными службами серии Cisco 1941;
* один сервер.

С помощью текстового инструмента в Packet Tracer зафиксируйте подготовленный ACL-список. Убедитесь, что ACL-список блокирует доступ к FTP-серверу, предприняв тестовую попытку доступа на этот сервер. В режиме моделирования понаблюдайте за тем, что произойдёт.

Сохраните свой файл и подготовьтесь к тому, чтобы представить его другому учащемуся или всему классу.

[Работа в аудитории. FTP запрещён. Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/9.6.1.1%20FTP%20Denied%20Instructions.pdf)

# Заключение

По умолчанию маршрутизатор не фильтрует трафик. Трафик, поступающий на маршрутизатор, маршрутизируется исключительно на основе информации таблицы маршрутизации.

С помощью фильтрации пакетов осуществляется управление доступом к сети путём анализа входящих и исходящих пакетов и пропускания или отбрасывания пакетов на основе таких критериев, как IP-адрес источника, IP-адрес назначения и протокол внутри пакета. Маршрутизатор, фильтрующий пакеты, использует определённые правила пропуска или отклонения трафика. Маршрутизатор также может фильтровать пакеты на уровне 4 — транспортном уровне.

ACL-список является последовательным списком разрешающих или запрещающих условий. Последней записью ACL-списка всегда является косвенный отказ, блокирующий весь трафик. Для того чтобы отменить действие косвенного отказа, присутствующего в конце любого ACL-списка и запрещающего весь трафик, можно добавить разрешающую команду **permit ip any any**.

При прохождении сетевого трафика через интерфейс, настроенный с помощью ACL-списка, маршрутизатор по порядку сопоставляет информацию внутри пакета с каждой записью списка, пытаясь найти соответствие. Если совпадение найдено, пакет обрабатывается в соответствии с записями ACL-списка.

ACL-списки настраиваются для применения к входящему или исходящему трафику.

Стандартные ACL-списки можно использовать для разрешения или отклонения трафика только с IPv4-адресов источника. Назначение пакета и порты, участвующие в передаче данных, не оцениваются. Основным правилом размещения расширенного ACL-списка является его размещение максимально близко к пункту назначения.

Расширенные ACL-списки фильтруют пакеты на основе нескольких атрибутов: тип протокола, IPv4-адрес источника или назначения и порты источника или назначения. Основным правилом размещения расширенного ACL-списка является его размещение максимально близко к источнику.

Команда глобальной конфигурации **access-list** задаёт стандартный ACL-список с номером в диапазоне от 1 до 99 или расширенный ACL-список с номером в диапазоне от 100 до 199 и от 2000 до 2699. Как стандартным, так и расширенным ACL-спискам можно присваивать имена. Команда **ip access-list standard** *name* используется для создания стандартного именованного ACL-списка, в то время как команда **ip access-list extended** *name* применяется для создания расширенного списка доступа. ACL-списки IPv4 используют шаблонные маски.

После настройки ACL-списка он подключается к интерфейсу с помощью команды **ip access-group** в режиме настройки интерфейса. Не забывайте правило трёх «для» — лишь один ACL-список предусмотрен для каждого протокола, направления и интерфейса.

Для удаления всего ACL-списка из интерфейса сначала следует ввести команду **no ip access-group** на интерфейсе, а затем ввести глобальную команду **no access-list**.

Для проверки настройки ACL-списка используются команды **show running-config** и **show access-lists**. Команда **show ip interface** используется для проверки ACL-списка на интерфейсе и направления, к которому был привязан список.

Команда **access-class**, введённая в режиме конфигурации канала, ограничивает входящие и исходящие соединения между отдельным VTY и адресами в списке доступа.

Как и в случае с именованными ACL-списками для IPv4, имена списков для IPv6 состоят из буквенно-цифровых символов, они чувствительны к регистру и должны быть уникальными. В отличие от IPv4, стандартная или расширенная опция не требуются.

Для создания ACL-списка IPv6 выполните команду режима глобальной конфигурации **ipv6 access-list** *name*. В отличие от ACL-списков для IPv4, ACL-списки для IPv6 не используют шаблонные маски. В протоколе IPv6 для указания того, какая часть IPv6-адреса источника или назначения должна совпадать, используется длина префикса.

После настройки ACL-списка IPv6, он подключается к интерфейсу с помощью команды **ipv6 traffic-filter**.