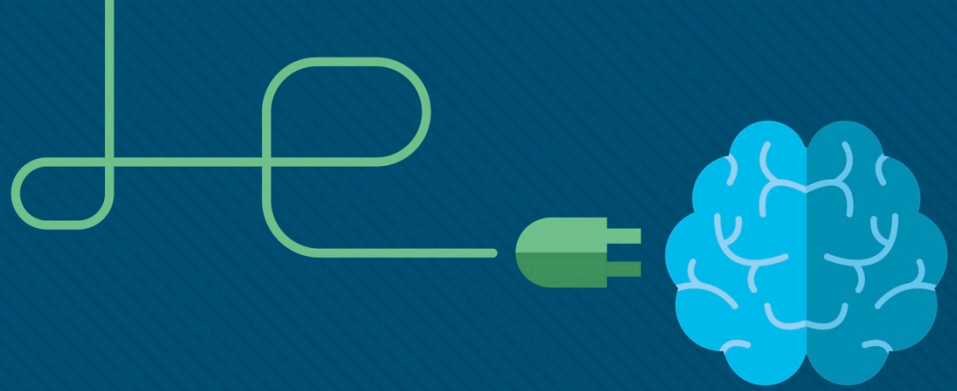


Глава 7. Списки контроля доступа (ACL)

Материалы для инструктора

CCNA Routing and Switching

Routing and Switching Essentials v6.0

Материалы для инструкторов. Глава 7. Руководство по планированию

- Эта презентация PowerPoint состоит из двух частей:
- Руководство по планированию для инструкторов
  - Ознакомительная информация по главе
  - Методические пособия
- Презентация перед классом для инструктора
  - Дополнительные слайды, которые можно использовать в классе
  - Начало на слайде № 12

- **Примечание.** Перед предоставлением общего доступа удалите руководство по планированию из данной презентации.

Глава 7. Списки контроля доступа (ACL)

Routing and Switching Essentials 6.0.
Руководство по планированию

Глава 7. Упражнения

Какие упражнения относятся к данной главе?

Страница №	Тип упражнения	Название упражнения	Необязательно?
7.1.1.4	Cisco Packet Tracer	Наглядное представление работы списка контроля доступа (ACL)	Рекомендуется
7.1.2.6	Интерактивное упражнение	Определите корректную шаблонную маску	Рекомендуется
7.1.2.7	Интерактивное упражнение	Определите: разрешить или запретить	Рекомендуется
7.1.3.3	Интерактивное упражнение	Принцип работы списков контроля доступа	Рекомендуется
7.2.1.5	Интерактивное упражнение	Настройка стандартных списков контроля доступа (ACL) IPv4	Рекомендуется
7.2.1.6	Cisco Packet Tracer	Настройка стандартных нумерованных списков контроля доступа (ACL) для IPv4	Рекомендуется
7.2.1.7	Packet Tracer	Настройка стандартных именованных списков ACL для IPv4	Рекомендуется
7.2.2.6	Лабораторная работа	Настройка стандартных нумерованных списков контроля доступа (ACL) для IPv4	Необязательно
7.2.3.1	Инструмент проверки синтаксиса	Обеспечение безопасности линий VTY с помощью стандартного списка контроля доступа (ACL) IPv4	Рекомендуется
7.2.3.3	Packet Tracer	Настройка списка контроля доступа (ACL) IPv4 для линий VTY	Рекомендуется

В этой главе для выполнения упражнений с программой Packet Tracer используйте следующий пароль: **PT_ccna5**

Глава 7. Упражнения (продолжение)

Какие упражнения относятся к данной главе?

Страница №	Тип упражнения	Название упражнения	Необязательно?
7.2.3.4	Лабораторная работа	Настройка и проверка ограничений VTY	Необязательно
7.3.2.4	Packet Tracer	Устранение неполадок в работе стандартных списков ACL для IPv4	Рекомендуется
7.4.1.1	Задание	FTP запрещен	Необязательно
7.4.1.2	Packet Tracer	Отработка комплексных практических навыков	Рекомендовано

В этой главе для выполнения упражнений с программой Packet Tracer используйте следующий пароль: **PT_ccna5**

Глава 7. Проверочная работа

- После прохождения главы 7 учащиеся должны выполнить проверочную работу по материалам главы 7.
- Для неформальной оценки успехов учащихся можно использовать контрольные работы, лабораторные работы, работу с симулятором Packet Tracer и другие упражнения.

Глава 7. Практические рекомендации

Прежде чем излагать материал главы 7, обратите внимание на следующее:

- Инструктор должен выполнить проверочную работу на знание материала главы 7.
- Цели этой главы:
  - Объясните, как фильтруется трафик с использованием списков контроля доступа (ACL).
  - Объясните, как используются шаблонные маски в списках контроля доступа (ACL).
  - Объясните, как создать списки контроля доступа (ACL).
  - Объясните, как разместить списки контроля доступа (ACL).
  - Настройте стандартные списки контроля доступа (ACL) IPv4 для фильтрации трафика в соответствии с требованиями сети.
  - Используйте порядковые номера для редактирования существующих стандартных списков контроля доступа (ACL) IPv4.
  - Настройка стандартных списков контроля доступа (ACL) для защиты доступа VTY.
  - Объяснение процесса обработки маршрутизатором пакетов в случае применения списка контроля доступа (ACL).
  - С помощью команд CLI выполните поиск и устранение типичных неполадок, связанных со стандартными списками контроля доступа (ACL) IPv4.

Глава 7. Практические рекомендации (продолжение)

- Лучший способ изучить списки контроля доступа — настроить их и выполнить поиск и устранение неполадок. При изучении данной главы выделите как можно больше времени на практическую работу.
- Приведите побольше примеров и попросите студентов определить, что должно происходить, исходя из того, как настроены списки контроля доступа. Например:
  - Что делает каждый из этих списков контроля доступа?
  - Настраиваются ли они в направлении и на правильном интерфейсе?
  - Какие затрагиваются устройства?
- Важно пояснить студентам, что маршрутизаторы не применяют списки контроля доступа для себя, поэтому на любой трафик, исходящий из маршрутизатора, списки контроля доступа не распространяются.
- 7.1.1.2
  - Стандартные списки контроля доступа (ACL) обеспечивают фильтрацию только на уровне 3. Расширенные списки контроля доступа обеспечивают фильтрацию на уровнях 3 и 4.
  - Расширенные списки контроля доступа не рассматриваются в рамках данного курса.

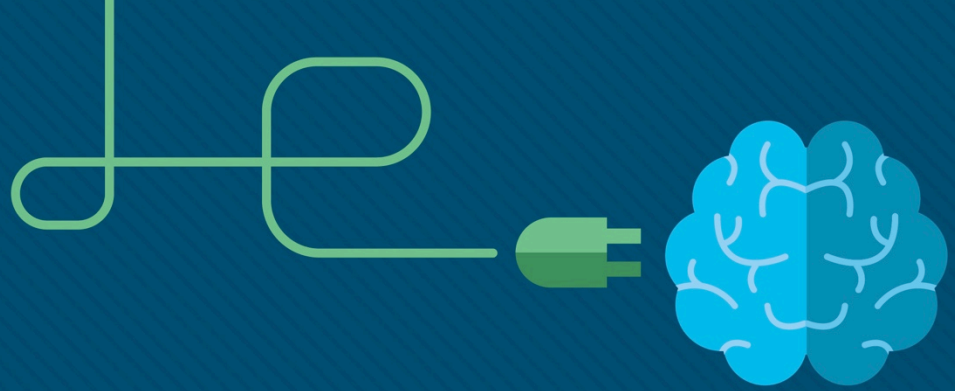
Глава 7. Практические рекомендации (продолжение)

- 7.1.2.2
  - Проработайте побольше примеров шаблонных масок списков контроля доступа.
- 7.2.2.1
  - Поясните студентам, что при использовании команды **no access-list** разные версии ПО IOS ведут себя по-разному.
  - Если ACL-список, который был удален, все еще применяется на интерфейсе, некоторые версии IOS действуют, как будто нет ACL-списков, защищающих сеть, в то время как другие версии блокируют весь трафик.
  - Рекомендуется удалить из интерфейса ссылку на список контроля доступа перед внесением изменений в этот список контроля доступа.
  - Если в новом списке обнаруживается ошибка, отключите его, найдите и устраните проблему. Таким образом, проблему можно исправить без настроенного списка контроля доступа.
- 7.2.2.3
  - Обсудите рекомендуемые способы нумерации списков контроля доступа и сохранения возможности для изменений или добавлений

Глава 7. Дополнительная помощь

- Дополнительные справочные материалы, содержащие различные стратегии обучения, в том числе планы занятий, описание аналогий для сложных понятий и темы обсуждений, доступны на веб-сайте сообщества сертифицированных сетевых специалистов (CCNA) по адресу https://www.netacad.com/group/communities/community-home.
- Практические рекомендации специалистов со всего мира для обучения по программе CCNA Routing and Switching. https://www.netacad.com/group/communities/ccna
- Если вы хотите поделиться с другими преподавателями планами занятий и другой полезной информацией, вы можете разместить ее на сайте сообщества сертифицированных компанией Cisco сетевых специалистов (CCNA).
- Студенты могут записаться на курс **Introduction to Packet Tracer** (для самостоятельного изучения).


CISCO



Глава 7. Списки контроля доступа (ACL)

CCNA Routing and Switching

Routing and Switching Essentials v6.0

Глава 7. Разделы и задачи

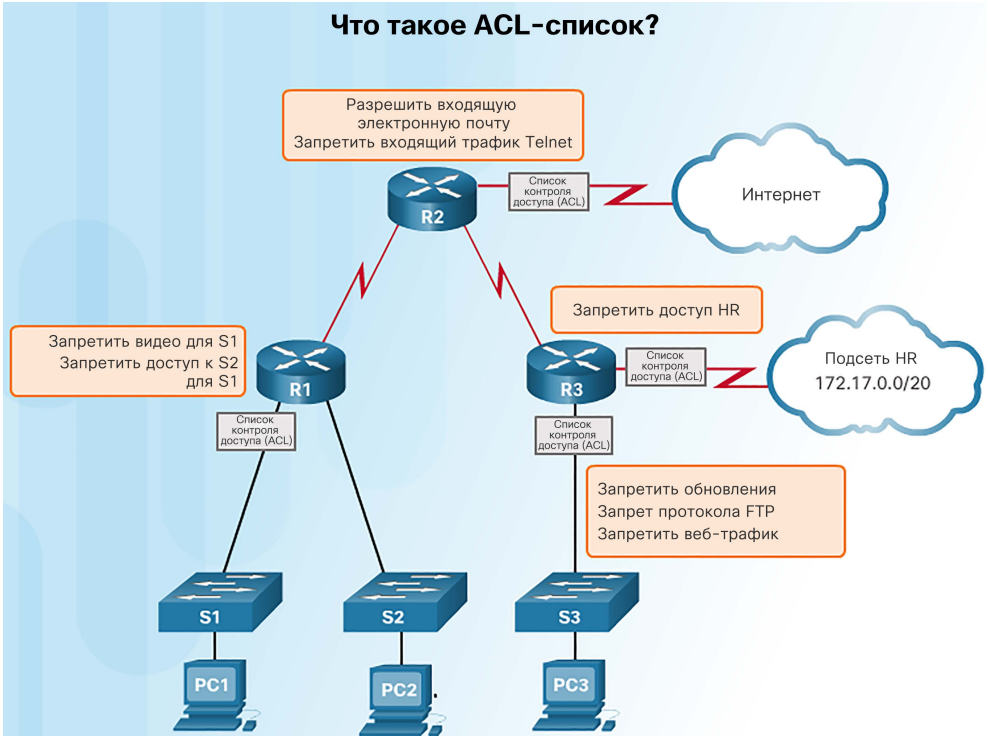
- 7.1. Действие списка контроля доступа (ACL)
  - Объяснить назначение и принципы работы списков контроля доступа (ACL) в сетях предприятий малого и среднего бизнеса.
    - Объясните, как фильтруется трафик с использованием списков контроля доступа (ACL).
    - Объясните, как используются шаблонные маски в списках контроля доступа (ACL).
    - Объясните, как создать списки контроля доступа (ACL).
    - Объясните, как разместить списки контроля доступа (ACL).
- 7.2. Стандартные списки контроля доступа (ACL) IPv4
  - Настроить стандартные списки контроля доступа IPv4 для фильтрации трафика в сетях предприятий малого и среднего бизнеса.
    - Настройте стандартные списки контроля доступа (ACL) IPv4 для фильтрации трафика в соответствии с требованиями сети.
    - Используйте порядковые номера для редактирования существующих стандартных списков контроля доступа (ACL) IPv4.
    - Настройка стандартных списков контроля доступа (ACL) для защиты доступа VTY.

Глава 7. Разделы и цели (продолжение)

- 7.3. Поиск и устранение неполадок, связанных со списками контроля доступа
  - Выполнить поиск и устранение неполадок, связанных со списками контроля доступа IPv4.
    - Объяснение процесса обработки маршрутизатором пакетов в случае применения списка контроля доступа (ACL).
    - С помощью команд CLI выполните поиск и устранение типичных неполадок, связанных со стандартными списками контроля доступа (ACL) IPv4.

7.1. Принципы работы списков контроля доступа

Что такое список контроля доступа?



- ACL-список — это ряд команд IOS, определяющих, пересылает ли маршрутизатор пакеты или сбрасывает их, исходя из информации в заголовке пакета. По умолчанию на маршрутизаторе списки контроля доступа не настроены.
- Списки контроля доступа могут выполнять следующие задачи.
  - Ограничение сетевого трафика для повышения производительности сети. Например, можно заблокировать видеотрафик, если он недопустим.
  - Управление потоком трафика. Списки контроля доступа позволяют обеспечить получение обновлений маршрутизации только из известных источников.
  - Списки контроля доступа обеспечивают безопасность сетевого доступа и позволяют блокировать хост или сеть.
  - Фильтрация трафика на основе типа трафика, такого как трафик Telnet.
  - Проверка узлов для разрешения или запрета доступа к сетевым сервисам, таким как FTP или HTTP.

Предназначение списков контроля доступа.

Фильтрация пакетов

- Список контроля доступа (ACL) — это последовательный список разрешающих или запрещающих операторов, называемых записями списка контроля доступа (ACE).
  - Записи списка контроля доступа обычно называют утверждениями списка контроля доступа.
- При прохождении сетевого трафика через интерфейс, где действует список контроля доступа (ACL), маршрутизатор последовательно сопоставляет информацию из пакета с каждой записью в списке контроля доступа на предмет соответствия. Это называется фильтрацией пакетов.
- Фильтрация пакетов:
  - позволяет анализировать входящие и исходящие пакеты;
  - может выполняться на уровне 3 или 4.
- Последняя запись в списке контроля доступа всегда содержит косвенный запрет трафика. Она автоматически вставляется в конец каждого списка контроля доступа и блокирует весь трафик. Поэтому в каждом списке контроля доступа должно быть хотя бы одно разрешающее утверждение.

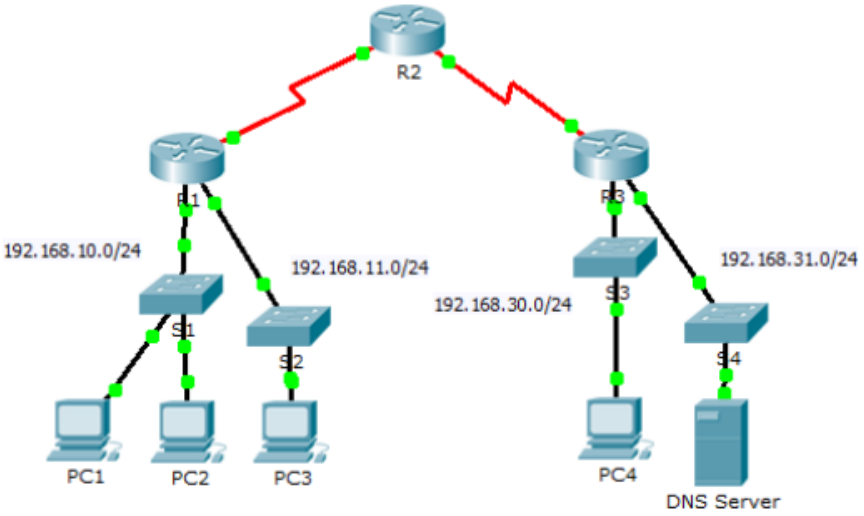
Принципы работы списков контроля доступа

- Списки контроля доступа не применяются к пакетам, созданным маршрутизатором.
  - 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 можно настроить для применения к входящему трафику и к исходящему трафику.
  - Входящие ACL — входящие пакеты обрабатываются перед отправкой в выходной интерфейс.
  - Исходящие ACL — входящие пакеты направляются в выходной интерфейс, а затем обрабатываются исходящим ACL.

Packet Tracer. Демонстрация работы списка контроля доступа

Packet Tracer – Access Control List Demonstration

Topology



Objectives

Part 1: Verify Local Connectivity and Test Access Control List

Part 2: Remove Access Control List and Repeat Test

- В этом упражнении для Packet Tracer будет показано, как с помощью списка контроля доступа можно не позволить ping-запросу попасть на узлы в сети.
- После удаления ACL-списка из конфигурации эхо-запросы будут успешными.

Знакомство с шаблонными масками списков контроля доступа

- Списки контроля доступа IPv4 используют шаблонные маски.
- Шаблонная маска — это строка из 32 двоичных цифр (1 и 0), используемая маршрутизатором для определения битов адреса, которые будут рассматриваться на предмет совпадения.
- Шаблонные маски часто называют обратными масками, так как в отличие от маски подсети, где двоичное значение 1 означает совпадение, в шаблонных масках совпадение означает двоичное значение 0. Например:

	Десятичный адрес	Двоичный адрес
IP-адрес для обработки	192.168.10.0	11000000.10101000.00001010.00000000
Шаблонная маска	0.0.255.255	00000000.00000000.11111111.11111111
Итоговый IP-адрес	192.168.0.0	11000000.10101000.00000000.00000000

Примеры шаблонных масок списков контроля доступа

Расчёт шаблонных масок для соответствия узлам и подсетям IPv4

Пример 1

	Десятичные	Двоичные
IP-адрес	192.168.1.1	11000000.10101000.00000001.00000001
Шаблонная маска	0.0.0.0	00000000.00000000.00000000.00000000
Результат	192.168.1.1	11000000.10101000.00000001.00000001

Пример 2

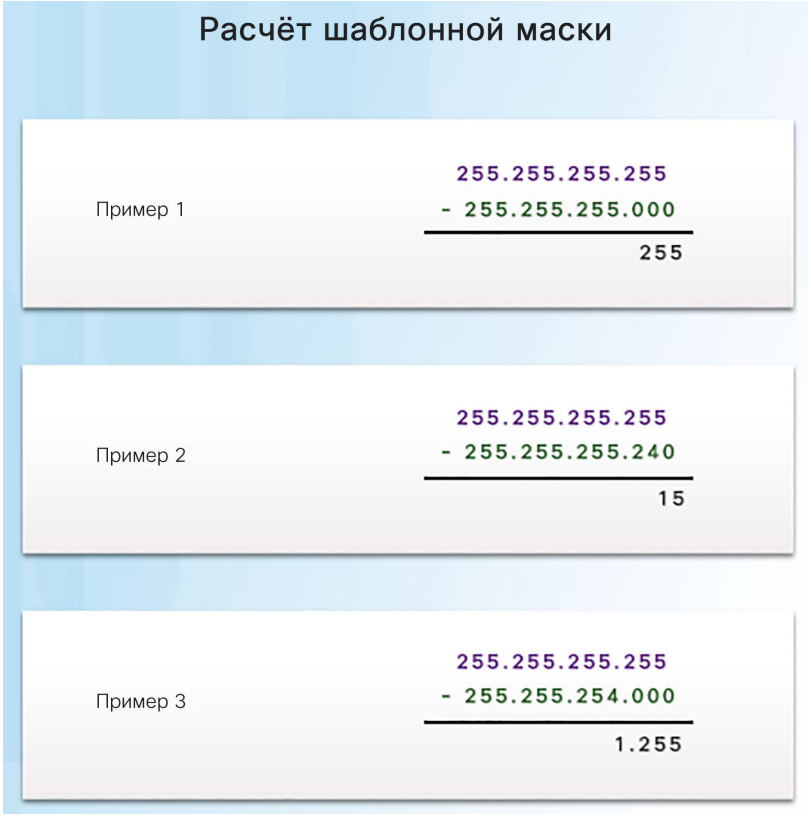
	Десятичные	Двоичные
IP-адрес	192.168.1.1	11000000.10101000.00000001.00000001
Шаблонная маска	255.255.255.255	11111111.11111111.11111111.11111111
Результат	0.0.0.0	00000000.00000000.00000000.00000000

Пример 3

	Десятичные	Двоичные
IP-адрес	192.168.1.1	11000000.10101000.00000001.00000001
Шаблонная маска	0.0.0.255	00000000.00000000.00000000.11111111
Результат	192.168.1.0	11000000.10101000.00000001.00000000

- Чтобы научиться вычислять шаблонную маску, соответствующую подсетям IPV4, требуется практика. В первом слева:
  - Пример 1. Шаблонная маска предусматривает, что каждый бит в адресе IPv4 192.168.1.1 должен точно соответствовать.
  - Пример 2. Шаблонная маска предусматривает, что соответствовать будет все.
  - Пример 3. Шаблонная маска предусматривает, что соответствовать будет любой хост в сети 192.168.1.0/24.

Вычисление шаблонных масок



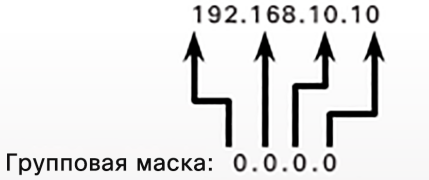
- Примеры вычисления шаблонных масок:
  - Пример 1. Предположим, требуется разрешить доступ всем пользователям из сети 192.168.3.0 с маской подсети 255.255.255.0. Вычтите подсеть из 255.255.255.255 — в результате получается 0.0.0.255.
  - Пример 2. Предположим, требуется разрешить доступ к сети 14 пользователям из подсети 192.168.3.32/28 с маской подсети 255.255.255.240. После вычитания маски подсети из 255.255.255.255 получается 0.0.0.15.
  - Пример 3. Предположим, что требуется сопоставить только сети 192.168.10.0 и 192.168.11.0 с маской подсети 255.255.254.0. После вычитания маски подсети из 255.255.255.255 получается 0.0.1.255.

Ключевые слова для шаблонных масок

Сокращения шаблонной маски

Пример 1

- 192.168.10.10 0.0.0.0 сопоставляет все биты адреса
- Сократите эту шаблонную маску, используя IP-адрес, перед которым указано ключевое слово `host` (`host 192.168.10.10`)

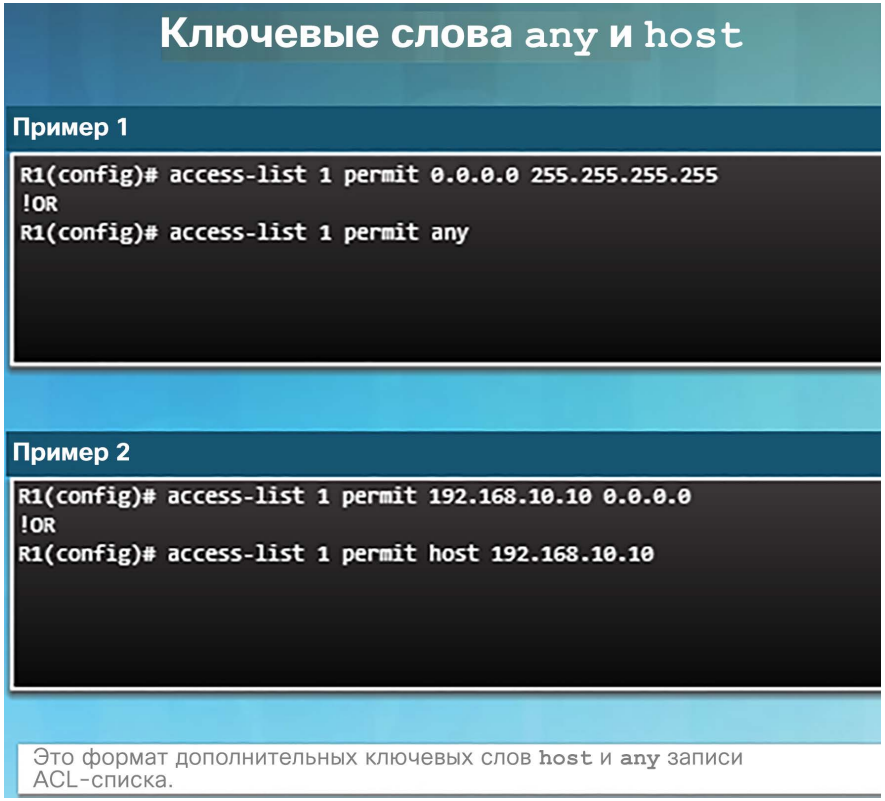


Пример 2

- 0.0.0.0 255.255.255.255 игнорирует все биты адреса
- Это выражение можно сократить с помощью ключевого слова `any`

- Для упрощения чтения шаблонных масок используются ключевые слова **host** и **any**, помогающие определить наиболее распространенные варианты применения шаблонных масок.
  - **host** замещает маску 0.0.0.0
  - **any** замещает маску 255.255.255.255
- Если требуется сопоставить адрес 192.169.10.10, можно использовать выражение **192.168.10.10 0.0.0.0** или **host 192.168.10.10**
- В примере 2 вместо ввода выражения **0.0.0.0 255.255.255.255** можно использовать одно ключевое слово **any**.

Примеры с ключевыми словами для шаблонных масок



- В примере 1 на рисунке иллюстрируется применение ключевого слова **any** вместо адреса IPv4 0.0.0.0 с шаблонной маской 255.255.255.255.
- В примере 2 показывается, как использовать ключевое слово **host** для замены шаблонной маски при определении одного хоста.

Общие рекомендации по созданию списков контроля доступа

Фильтрация трафика на маршрутизаторе с помощью списков контроля доступа (ACL)

По одному списку для каждого интерфейса, направления и протокола

Обладая двумя интерфейсами и двумя работающими протоколами, этот маршрутизатор способен поддерживать до 8 отдельных списков контроля доступа (ACL).

Правила применения списков контроля доступа (ACL)

У вас может быть только по одному списку контроля доступа на каждый протокол, интерфейс и направление:

- Один список контроля доступа (ACL) на каждый протокол (например, IPv4 или IPv6)
- Один список контроля доступа (ACL) на каждое направление (например, IN или OUT)
- Один список контроля доступа (ACL) на каждый интерфейс (например, GigabitEthernet0/0)

- Используйте ACL-списки в межсетевых экранах маршрутизаторов, размещенных между внутренней и внешней сетями, например, Интернетом.
- Используйте списки контроля доступа на маршрутизаторе, расположенном между двумя частями сети, для контроля трафика, входящего или исходящего из определенной части этой внутренней сети.
- Настраивайте списки контроля доступа на граничных маршрутизаторах, например, расположенных на периметре сети. Это обеспечит базовый буфер от внешней сети, которую вы не контролируете.
- Настройте ACL-списки для каждого протокола сети, настроенного на интерфейсе пограничного маршрутизатора.

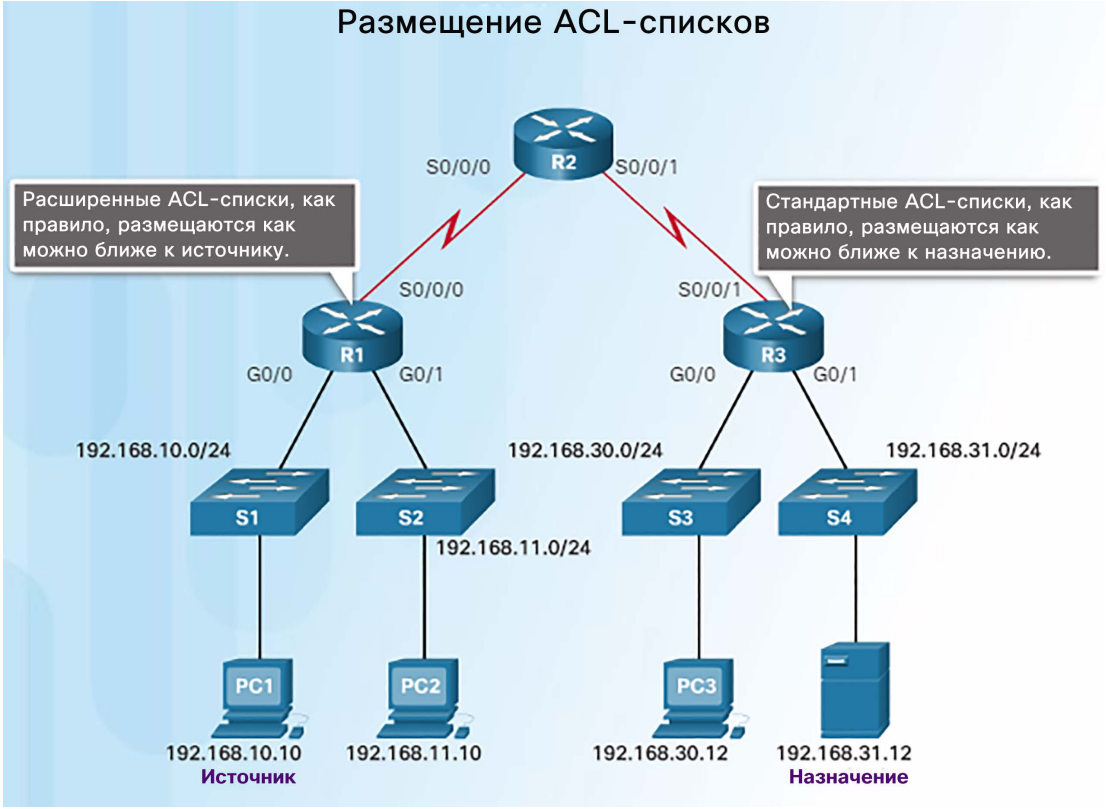
Практические рекомендации по спискам контроля доступа

Рекомендации по созданию ACL-списков

Рекомендации	Преимущество
Создавайте ACL-списки, исходя из корпоративной политики обеспечения информационной безопасности.	Соблюдение рекомендации обеспечивает соответствие требованиям информационной безопасности компании.
Подготовьте описание обязательных действий ваших ACL-списков.	Соблюдение рекомендации поможет избежать непреднамеренного создания потенциальных проблем доступа.
Используйте текстовый редактор для создания, редактирования и сохранения ACL-списков.	Соблюдение рекомендации поможет создать библиотеку повторно используемых ACL-списков.
Проверьте работу ACL-списков в пробной сети перед внедрением в реальную действующую сеть.	Соблюдение рекомендации поможет избежать дорогостоящих ошибок.

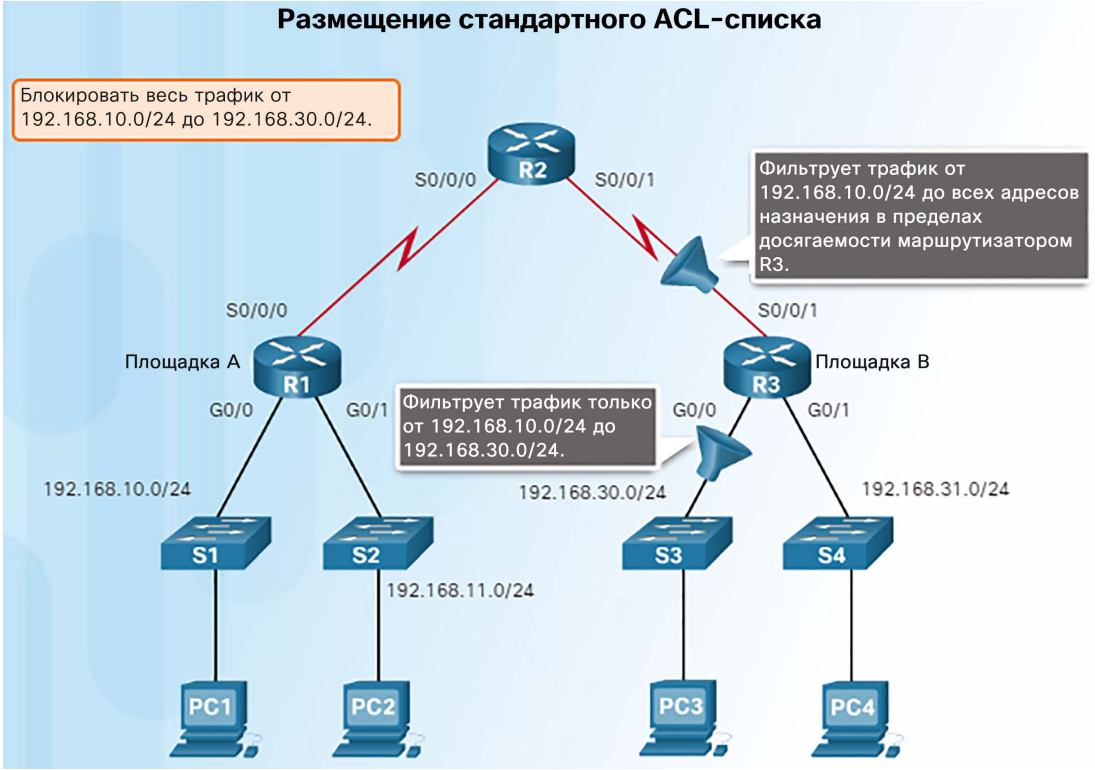
- При использовании списков контроля доступа значительное внимание необходимо уделять деталям. Ошибки могут привести к серьезным последствиям и значительным затратам, связанным с простоями, поиском и устранением неполадок, а также со сниженной производительностью работы сети.

Общие рекомендации по созданию списков контроля доступа



- Правильное размещение ACL-списка может повысить эффективность сети. Например, можно разместить список контроля доступа для сокращения объема ненужного трафика.
- Каждый список контроля доступа (ACL) должен быть размещен там, где он может демонстрировать максимальную эффективность.
  - Расширенные списки контроля доступа. Расширенные списки контроля доступа следует размещать как можно ближе к источнику фильтруемого трафика. Это предотвращает нежелательный трафик максимально близко к источнику без пересечения им сетевой инфраструктуры.
  - Стандартные списки контроля доступа. Так как в стандартных списках контроля доступа не указываются адреса назначения, их следует размещать их как можно ближе к месту назначения.

Размещение стандартных списков контроля доступа



- В этом примере показано правильное размещение стандартного списка контроля доступа, который настроен для блокирования трафика, идущего из сети 192.168.10.0/24 в сеть 192.168.30.0/24.
- Есть два возможных места, в которых можно настроить этот список контроля доступа на маршрутизаторе R3.
- Если этот список контроля доступа применить к интерфейсу S0/0/1, он будет блокировать трафик к сети 192.168.30.0/24**, но также** и к сети 192.168.31.0/24.
- Лучше место для применения этого списка контроля доступа — интерфейс G0/0 маршрутизатора R3. Список контроля доступа следует применить к трафику, исходящему из интерфейса G0/0. Пакеты из сети 192.168.10.0/24 по-прежнему могут достигать сети 192.168.31.0/24.

7.2. Стандартные списки контроля доступа (ACL) IPv4

Настройка стандартных списков контроля доступа IPv4

Синтаксис стандартных нумерованных списков контроля доступа IPv4

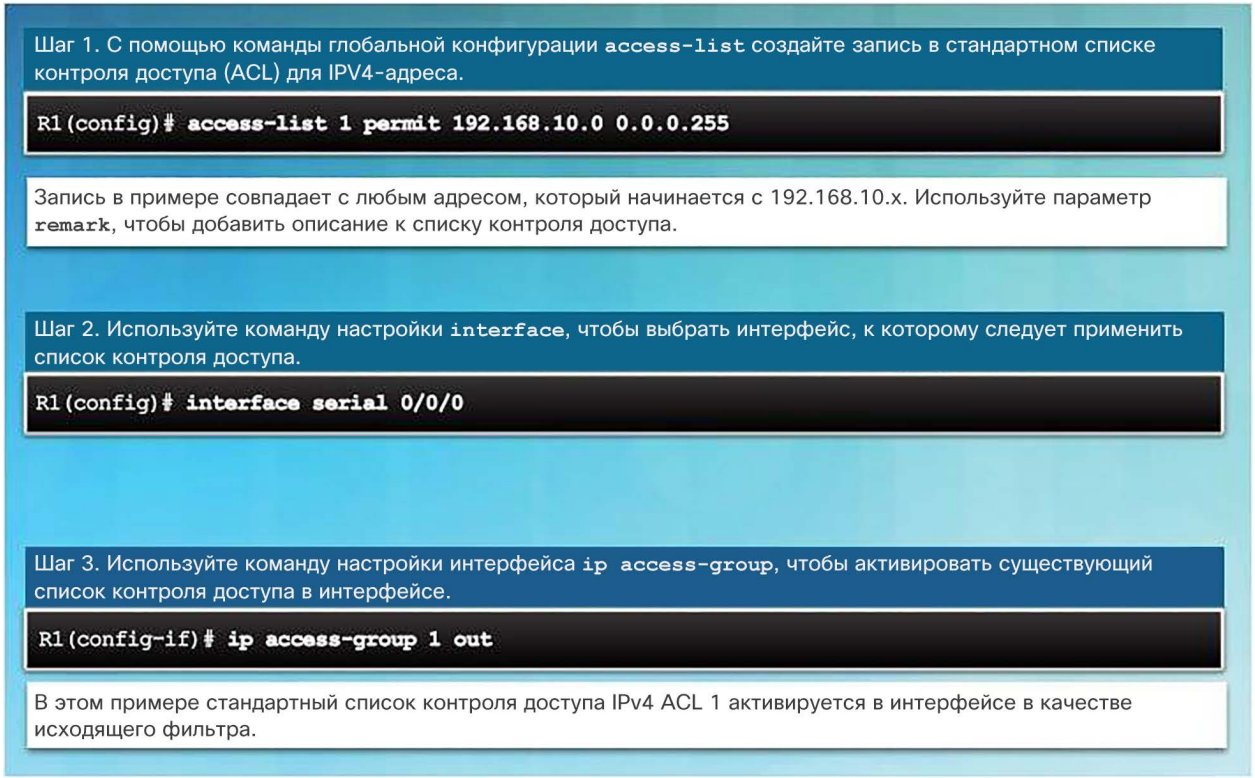
Параметр	Описание
access-list-number	Номер ACL-списка. Это десятичное число от 1 до 99 или от 1300 до 1999 (для стандартного ACL-списка).
deny	Запрещает доступ при совпадении условий.
permit	Разрешает доступ при совпадении условий.
remark	Чтобы сделать список проще для понимания и прочтения, добавьте комментарий о записях в списке доступа IP.
source	Номер сети или узла, с которых отправляется пакет. Два способа определить адрес *источника*: • Используйте 32-битный адрес, записанный в виде четырех 8-битовых целых чисел, разделенных точками. • Используйте ключевое слово **any** как сокращение для адреса ***источника и групповой маски источника*** 0.0.0.0 255.255.255.255.
source-wildcard	(Опционально). 32-битная шаблонная маска должна применяться к адресу источника. Разряды в позиции битов, которые вы хотите игнорировать.
log	(Опционально). Вызывает информационное сообщение журнала о пакете, соответствующем записи, которая должна быть отправлена на консоль. (Уровень сообщений, регистрируемых на консоли, регулируется командой **logging console**). Сообщение включает номер ACL-списка, указание, был ли пакет разрешен или запрещен, адрес источника и количество пакетов. Сообщение создается для первого соответствующего пакета, затем – с пятиминутным интервалом, включая количество разрешенных и запрещенных пакетов в предшествующем пятиминутном интервале.

- Команда глобальной конфигурации **access-list** определяет стандартный ACL-список с номером в диапазоне от 1 до 99.
- Полный синтаксис команды стандартного ACL-списка:

  Router(config)# **access-list** *номер-списка-контроля-доступа* { **deny** | **permit** | **remark** } *источник* [*шаблонная-маска-источника*][**log**]

Для удаления ACL-списка используется команда глобальной конфигурации **no access-list**. Для проверки удаления списка контроля доступа используется команда **show access-list**.

Применение стандартных списков контроля доступа IPv4 к интерфейсам



- Создав стандартный список контроля доступа (ACL), его необходимо связать с интерфейсом при помощи команды **ip access-group**, которая вводится в режиме интерфейсной настройки:

  Router(config-if)# **ip access-group** { *номер-списка-доступа* | *имя-списка-доступа* } { **in** | **out** }

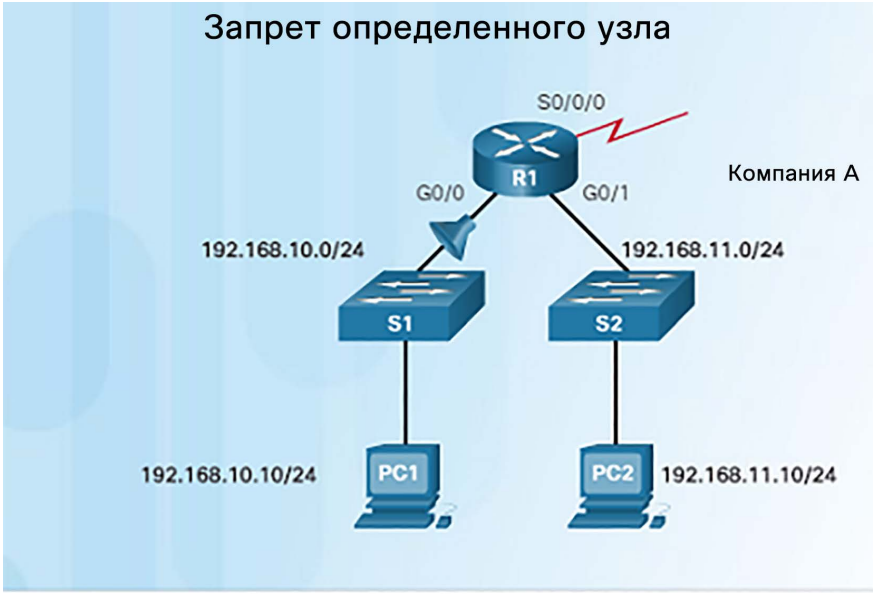
- Для удаления всего списка контроля доступа из интерфейса сначала следует ввести команду **no ip access-group** на интерфейсе, а затем ввести глобальную команду **no access-list**.

Примеры стандартных нумерованных списков контроля доступа IPv4


```
R1(config)# no access-list 1
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 1 out
```

- На рисунке слева показан пример списка контроля доступа, который разрешает трафик от определенной подсети, но запрещает трафик от конкретного хоста из этой подсети.
  - Команда **no access-list 1** удаляет предыдущую версию списка контроля доступа ACL 1.
  - Следующая инструкция списка контроля доступа запрещает хост 192.168.10.10.
  - Каким еще способом можно задать эту команду без использования ключевого слова **host**?
  - Затем разрешаются все остальные узлы из сети 192.168.10.0/24.
  - Здесь присутствует неявный запрет, соответствующий всем остальным сетям.
  - Далее этот список контроля доступа заново применяется к интерфейсу в исходящем направлении.

Примеры стандартных нумерованных списков контроля доступа IPv4 (продолжение)

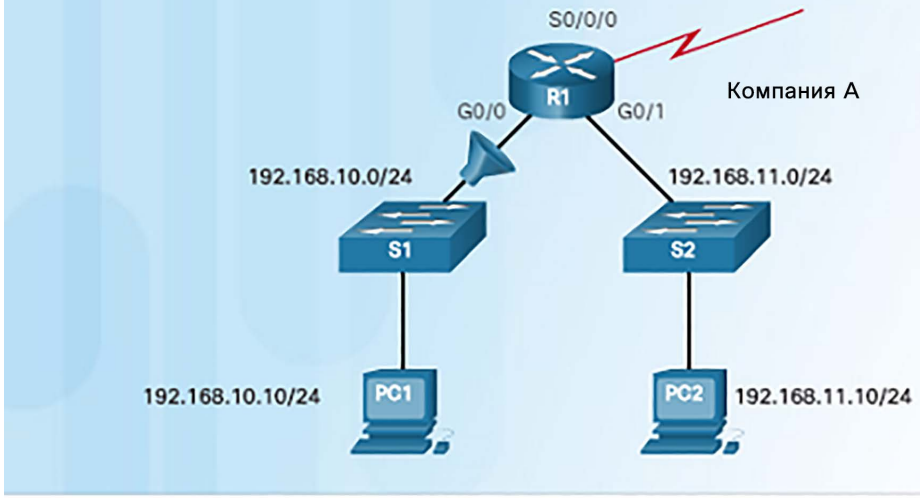



```
R1(config)# no access-list 1
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 permit any
R1(config)# interface g0/0
R1(config-if)# ip access-group 1 in
```

- В этом примере демонстрируется список контроля доступа, запрещающий определенный хост, но разрешающий весь остальной трафик.
  - Первое утверждение списка контроля доступа удаляет предыдущую версию ACL 1.
  - Следующая команда с помощью ключевого слова deny будет отклонять трафик от хоста PC1, расположенного в сети 192.168.10.10.
  - Утверждение **access-list 1 permit any** будет разрешать все остальные узлы.
  - Этот список контроля доступа применяется к интерфейсу G0/0 во входящем направлении, так как он затрагивает только локальную сеть 192.168.10.0/24.

Синтаксис именованных стандартных списков контроля доступа IPv4

Пример именованного списка контроля доступа (ACL)

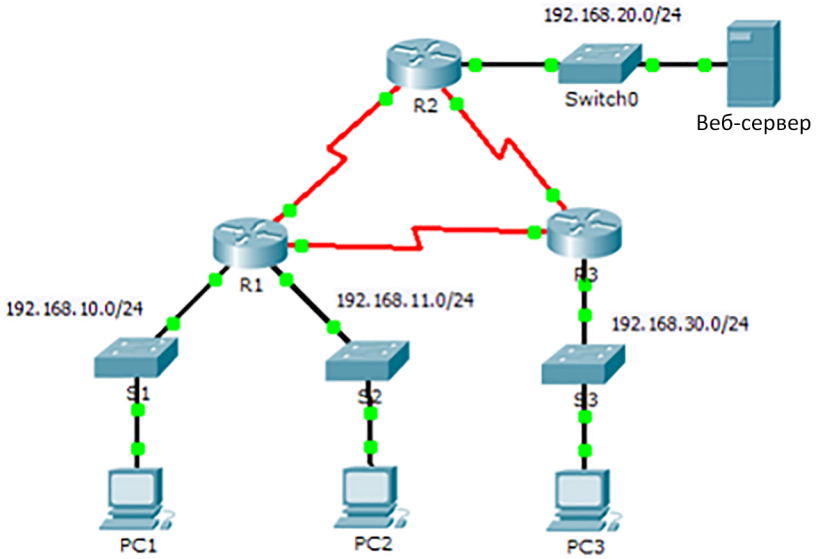



```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group NO_ACCESS out
```

- Обозначение списка контроля доступа по имени, а не по номеру, упрощает понимание его функции.
- В приведенном слева примере показано, как настроить именованный стандартный список контроля доступа. Обратите внимание, что команды немного отличаются.
  - Для создания именованного списка контроля доступа используется команда **ip access-list**. Имена списков контроля доступа состоят из букв и цифр, учитывают регистр и должны быть уникальными.
  - При необходимости используйте утверждение permit или deny. Можно также добавлять комментарии с помощью команды **remark**.
  - Для применения списка контроля доступа к интерфейсу служит команда **ip access-group** *имя*.

Packet Tracer. Настройка нумерованных стандартных списков контроля доступа IPv4

Топология



Общие сведения/сценарий

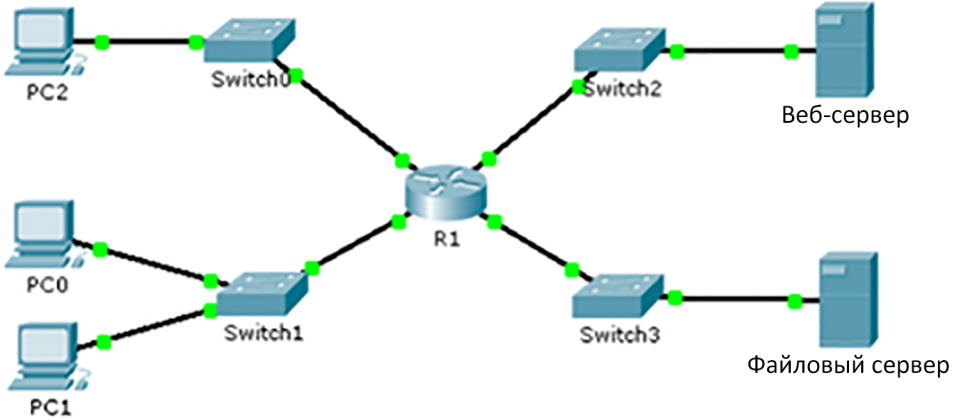
Стандартные списки контроля доступа (ACL-списки) являются скриптами конфигурации маршрутизатора, которые разрешают или запрещают маршрутизатору пропускать пакеты, исходя из адреса источника. Данное интерактивное задание фокусируется на определении критериев фильтрации, конфигурации стандартных ACL-списков,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

- Это упражнение для Packet Tracer позволяет попрактиковаться в определении критериев фильтрации и настройке стандартных списков контроля доступа в предварительно настроенной сети.
- Потребуется также выполнить проверку настроенных и примененных списков контроля доступа.

Packet Tracer. Настройка именованных стандартных списков контроля доступа IPv4

Packet Tracer. Настройка стандартных именованных списков контроля доступа IPv4

Топология

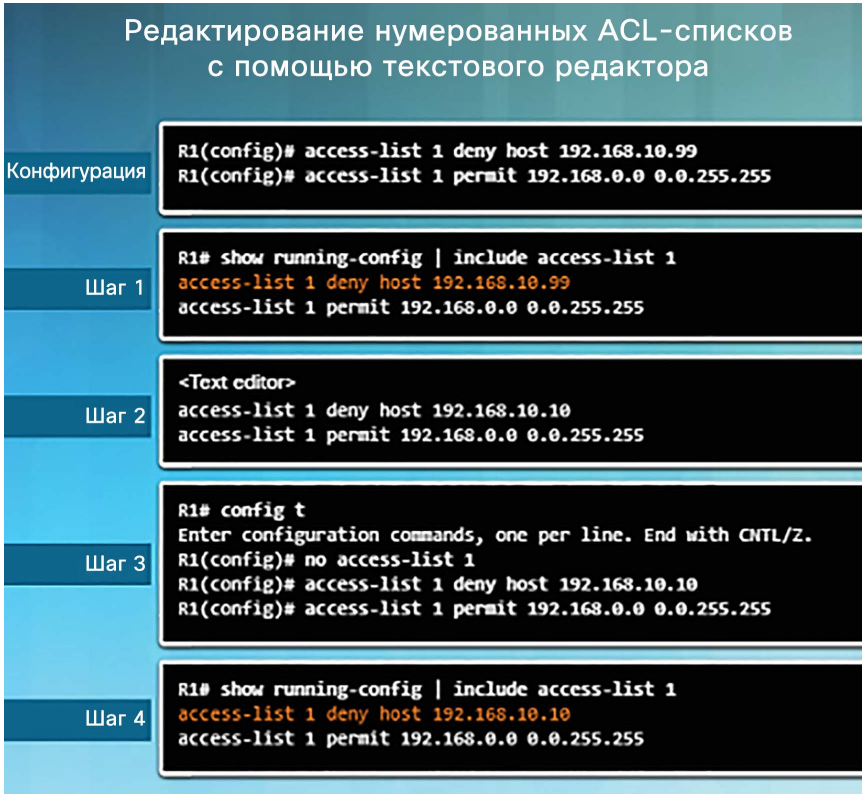


Общие сведения/сценарий

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 определенной рабочей станции другой сети.

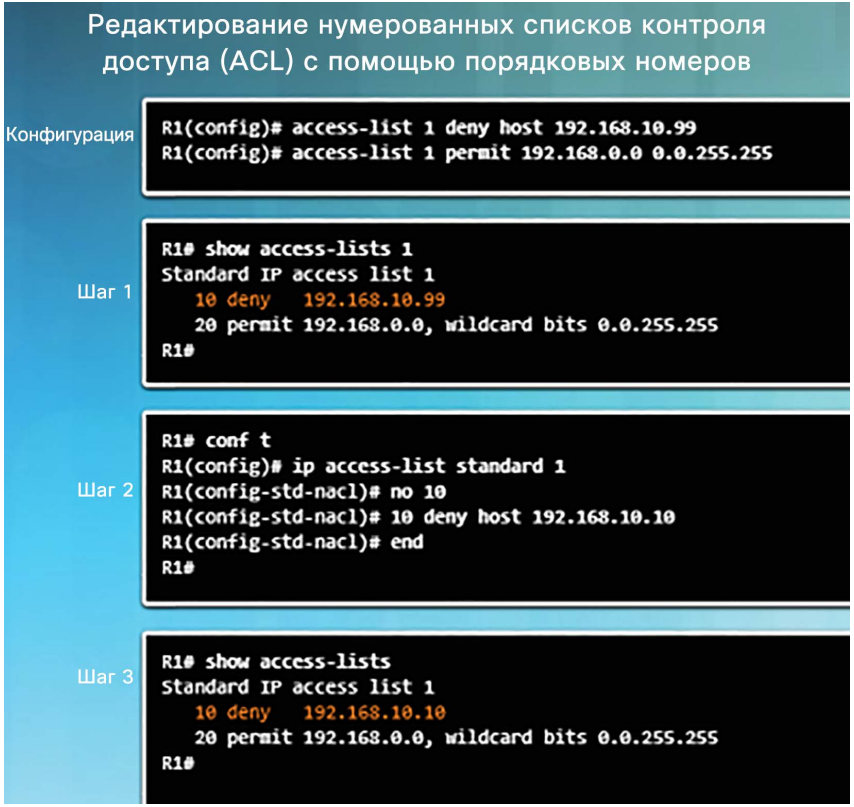
- В этом упражнении для Packet Tracer требуется настроить именованный стандартный список контроля доступа.
- Необходимо будет проверить этот список контроля доступа после его применения к соответствующему интерфейсу.

Метод 1. Текстовый редактор



- Иногда проще создавать и редактировать списки контроля доступа в текстовом редакторе, например в Блокноте Microsoft, чем вносить изменения непосредственно на маршрутизаторе.
- Если список контроля доступа уже существует, выведите его на экран с помощью команды **show running-config**, скопируйте и вставьте его в текстовый редактор, внесите необходимые изменения, а затем скопируйте и вставьте его обратно в интерфейс маршрутизатора.
- Важно отметить, что при применении команды no access-list разные версии ПО IOS ведут себя по-разному.
  - Если список контроля доступа, который был удален, все еще значится примененным к интерфейсу, одни версии IOS действуют так, будто никакие списки контроля доступа не защищают сеть, в то время как другие версии блокируют весь трафик.

Метод 2. Порядковые номера



- На рисунке слева показаны действия для внесения изменений в нумерованный список контроля доступа с использованием порядковых номеров.
- На шаге 1 выявляется проблема. Утверждение **deny 192.168.10.99** неправильное. Хост, который требуется заблокировать, имеет адрес 192.168.10.10.
- На шаге 2 показано, как перейти в стандартный список контроля доступа 1 и внести изменения. Неправильное утверждение удаляется с помощью команды no: **no 10**
- После удаления добавляется новое утверждение с правильным узлом: **10 deny host 192.168.10.10**

Изменение именованных стандартных списков контроля доступа

```
R1# show access-lists
Standard IP access list NO_ACCESS
    10 deny   192.168.11.10
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# 15 deny host 192.168.11.11
R1(config-std-nacl)# end
R1# show access-lists
Standard IP access list NO_ACCESS
    10 deny   192.168.11.10
    15 deny   192.168.11.11
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

- Команда именованного списка контроля доступа **no** *последовательный-номер* используется для удаления отдельных утверждений.

- Используя порядковые номера утверждений, можно легко вставлять или удалять отдельные утверждения.
- На рисунке слева показан пример вставки строки в именованный список контроля доступа.
- Так как эта команда имеет номер 15, она будет помещена между утверждениями 10 и 20.
- Обратите внимание, что при первоначальном создании списка контроля доступа сетевой администратор назначил каждой команде номера с шагом 10, чтобы оставить место для изменений и дополнений.

Проверка списков контроля доступа

```
R1# show ip interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.1/30
<output omitted>
  Outgoing access list is 1
  Inbound access list is not set
<output omitted>

R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
<output omitted>
  Outgoing access list is NO_ACCESS
  Inbound access list is not set
<output omitted>
```

```
R1# show access-lists
Standard IP access list 1
   10 deny 192.168.10.10
   20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
   15 deny 192.168.11.11
   10 deny 192.168.11.10
   20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

- Для проверки правильности применения списка контроля доступа к интерфейсу используйте команду **show ip interface**.
- В выходных данных этой команды приводится имя списка контроля доступа и направление, в котором он был применен к интерфейсу.
- Чтобы отобразить списки контроля доступа, настроенные на маршрутизаторе, используйте команду **show access-lists**.
- Обратите внимание, что для списка контроля доступа NO_ACCESS утверждения отображаются не в последовательном порядке. Эта ситуация будет рассмотрена далее в этом разделе.

Статистика по ACL

```
R1# show access-lists
Standard IP access list 1
    10 deny 192.168.10.10 (8 match(es))
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
    15 deny 192.168.11.11
    10 deny 192.168.11.10 (4 match(es))
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1# clear access-list counters 1
R1#
R1# show access-lists
Standard IP access list 1
    10 deny 192.168.10.10
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
    15 deny 192.168.11.11
    10 deny 192.168.11.10 (4 match(es))
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
```

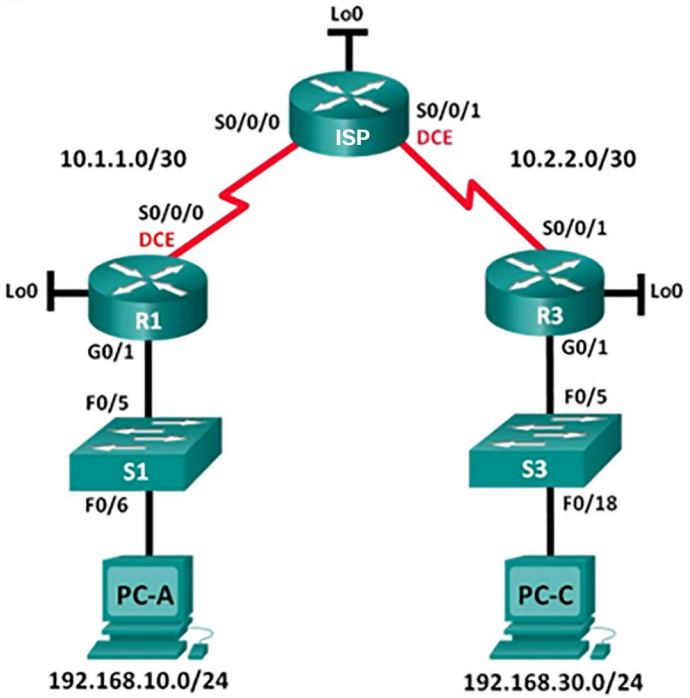
Совпадения очищены

- С помощью команды **show access-lists** можно отобразить соответствующую статистику после применения списка контроля доступа к интерфейсу и выполнения проверки.
- Когда создается трафик, который должен соответствовать какому-либо утверждению списка контроля доступа, количество совпадений, отображаемых в выходных данных команды **show access-lists**, должно увеличиться.
- Напомним, что в каждом списке контроля доступа есть неявное последнее утверждение **deny any**. Статистика для этой неявной команды не отображается. Однако если эта команда настроена вручную, результаты будут отображаться.
- Чтобы очистить счетчики для тестирования, можно использовать команду clear access-list counters.

Лабораторная работа. Настройка и изменение стандартных списков контроля доступа IPv4

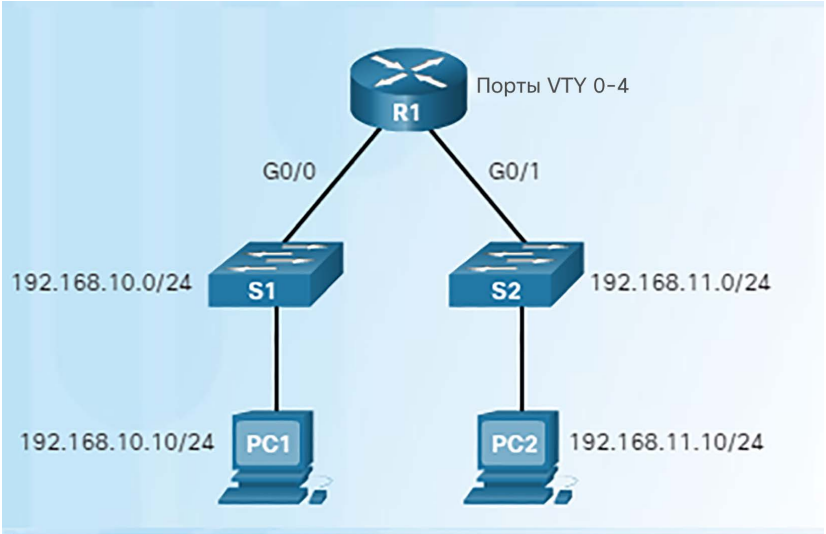
Лабораторная работа. Настройка и проверка стандартных списков контроля доступа для IPv4

Топология



- В этой лабораторной работе требуется установить и настроить устройства в соответствии с указанной топологией.
- Также необходимо будет выполнить настройку, изменение и тестирование стандартных и именованных списков контроля доступа.

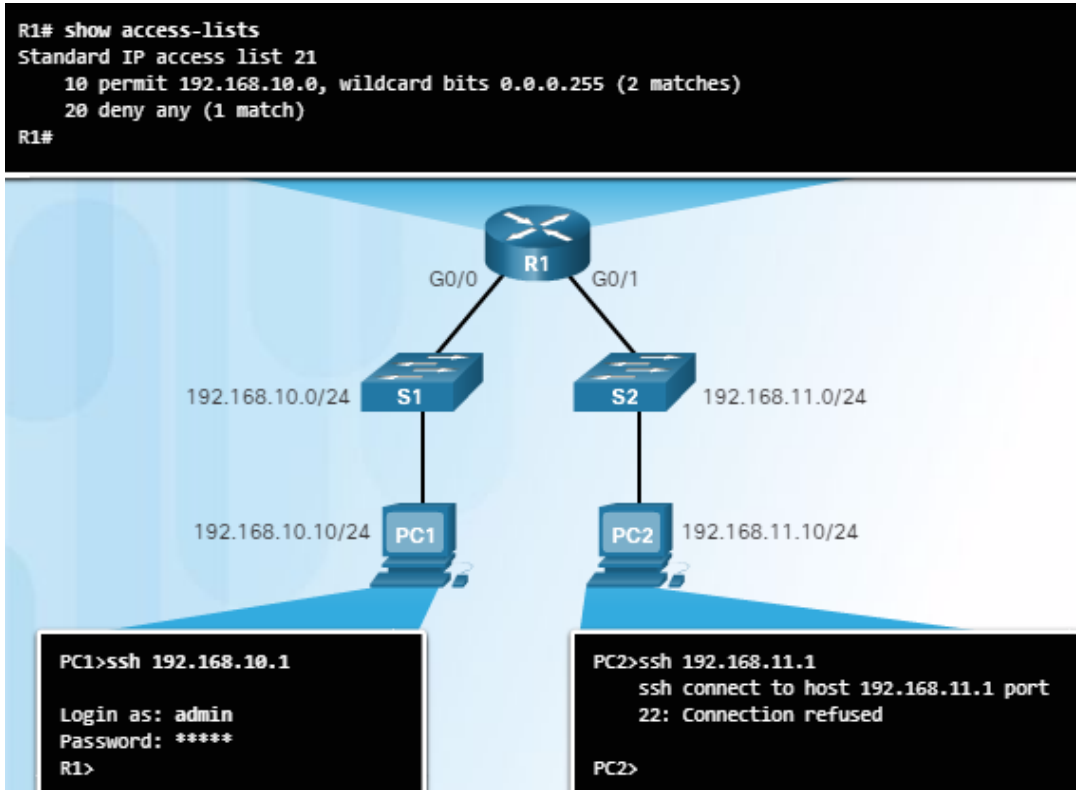
Команда access-class




```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# access-class 21 in
R1(config-line)# exit
R1(config)# access-list 21 permit 192.168.10.0 0.0.0.255
R1(config)# access-list 21 deny any
```

- Для повышения информационной безопасности необходимо ограничивать административный доступ VTY к устройствам Cisco.
- Ограничение доступа VTY позволяет задать перечень IP-адресов, которым разрешен удаленный доступ к процессу EXEC на маршрутизаторе.
- Команда access-class, настроенная в режиме линейного конфигурирования, будет ограничивать входящие и исходящие соединения между конкретным VTY (на устройстве Cisco) и адресами в списке контроля доступа.
- Router(config-line)# **access-class** *номер-списка-контроля-доступа* {in [vrf-also] | out }

Проверка безопасности порта VTY

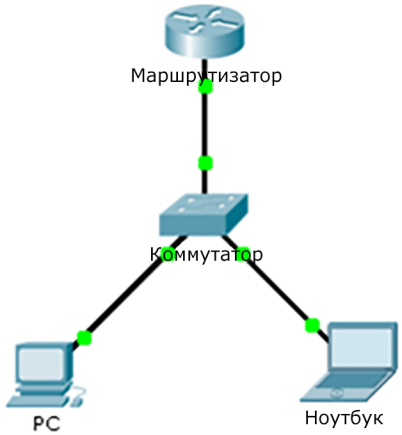


- Проверка конфигурации списка контроля доступа, используемого для ограничения доступа VTY, очень важна.
- На рисунке слева показаны два устройства, пытающиеся установить соединение по протоколу SSH с двумя разными устройствами.
- В выходных данных команды show access-lists показаны результаты после попыток PC1 и PC2 установить соединение SSH.
- Обратите внимание на совпадения в утверждениях permit и deny.

Packet Tracer. Настройка списка контроля доступа IPv4 для линий VTY

Packet Tracer. Настройка списка контроля доступа IPv4 в каналах VTY

Топология



В этом упражнении для Packet Tracer необходимо настроить и применить список контроля доступа, разрешающий компьютеру доступ к линиям Telnet на маршрутизаторе, но отклоняющий все другие IP-адреса источника.

Общие сведения

Сетевой администратор должен иметь удаленный доступ к маршрутизатору. Данный доступ не должен быть разрешен другим пользователям сети. В рамках задания нужно будет настроить и применить список контроля доступа, разрешающий **ПК** доступ к линиям Telnet на маршрутизаторе, но отклоняющий все другие IP-адреса источника.

Лабораторная работа. Настройка и проверка ограничений VTY

Лабораторная работа. Настройка и проверка ограничений VTY

Топология

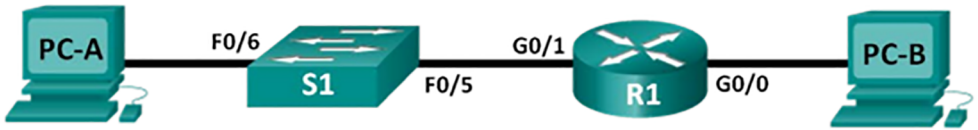


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.0.1	255.255.255.0	–
	G0/1	192.168.1.1	255.255.255.0	–
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Задачи

Часть 1. Настройка базовых параметров устройства

Часть 2. Настройка и применение списка контроля доступа на маршрутизаторе R1

Часть 3. Проверка списка контроля доступа с помощью Telnet

Часть 4. Задание повышенной сложности. Настройка и применение списка контроля доступа на коммутаторе S1

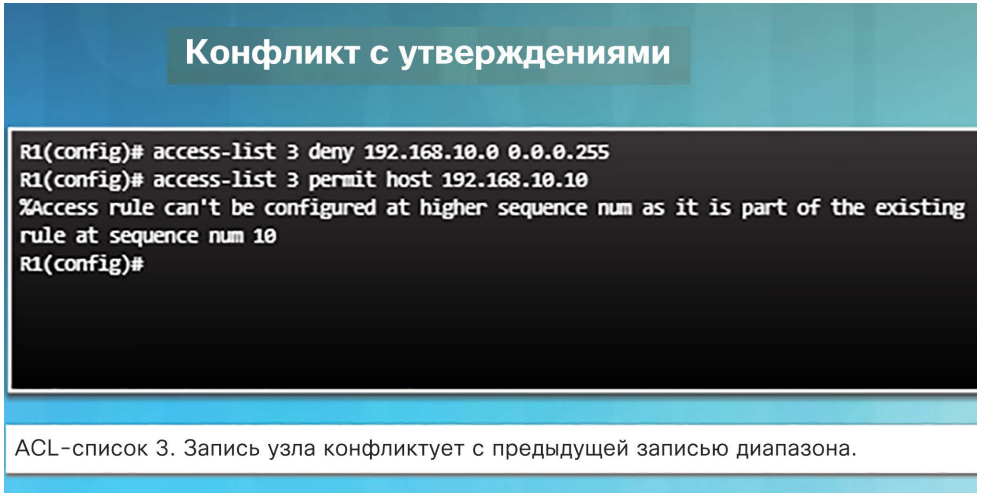
- В этой лабораторной работе требуется будет настроить и проверить ограничения VTY.
- Доступ к линиям VTY на маршрутизаторе будет разрешен только определенным IP-адресам.
- Важно обеспечить, чтобы только компьютеры администраторов имели доступ к маршрутизатору по протоколу Telnet или SSH.

7.3. Поиск и устранение неполадок, связанных со списками контроля доступа

Неявная блокировка трафика (Deny Any)

- Если ACL-список состоит из одной команды запрета, весь трафик будет отклоняться.
- В списке контроля доступа должна быть настроена по крайней мере одна запись разрешения; в противном случае весь трафик будет заблокирован.
- Изучите два списка контроля доступа на рисунке слева.
  - Результаты их применения будут одинаковыми или разными?

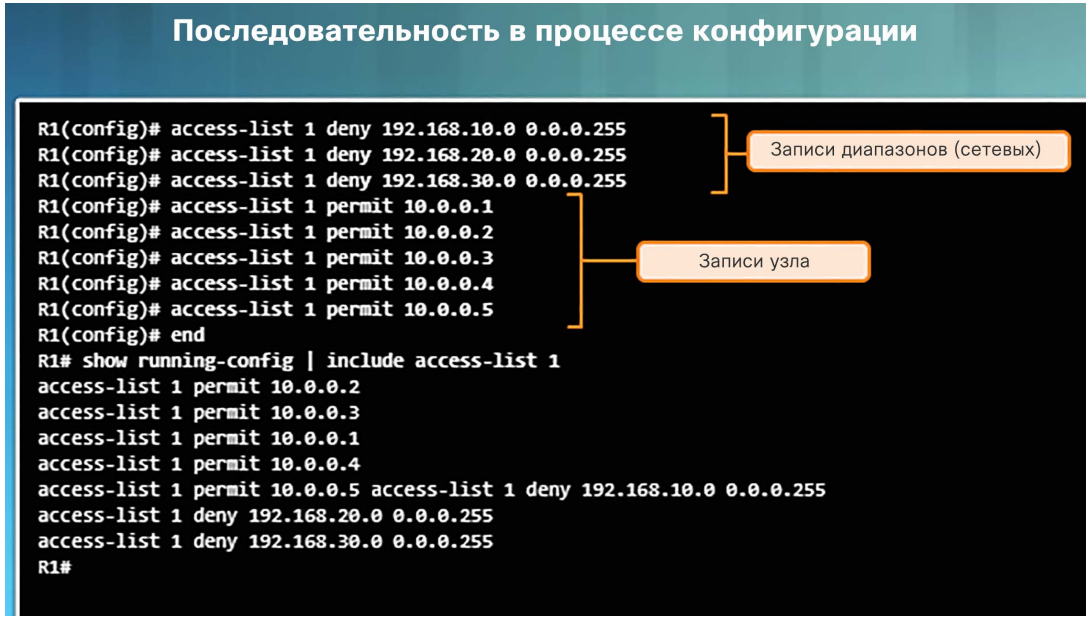
Порядок записей в списке контроля доступа



ACL-список 3. Запись узла конфликтует с предыдущей записью диапазона.

- Порядок записей в списке контроля доступа важен, так как записи списка контроля доступа обрабатываются последовательно.
- На рисунке слева показан конфликт между двумя утверждениями, так как они расположены в неверном порядке.
  - Первое утверждение deny блокирует все из сети 192.168.10.0/24.
  - Однако второе утверждение permit пытается разрешить узел 192.168.10.10.
  - Это утверждение отклоняется, так как узел входит в сеть, указанную в предыдущем утверждении.
  - Чтобы разрешить проблему, достаточно поменять порядок этих двух утверждений.

Изменение порядка стандартных списков контроля доступа в Cisco IOS

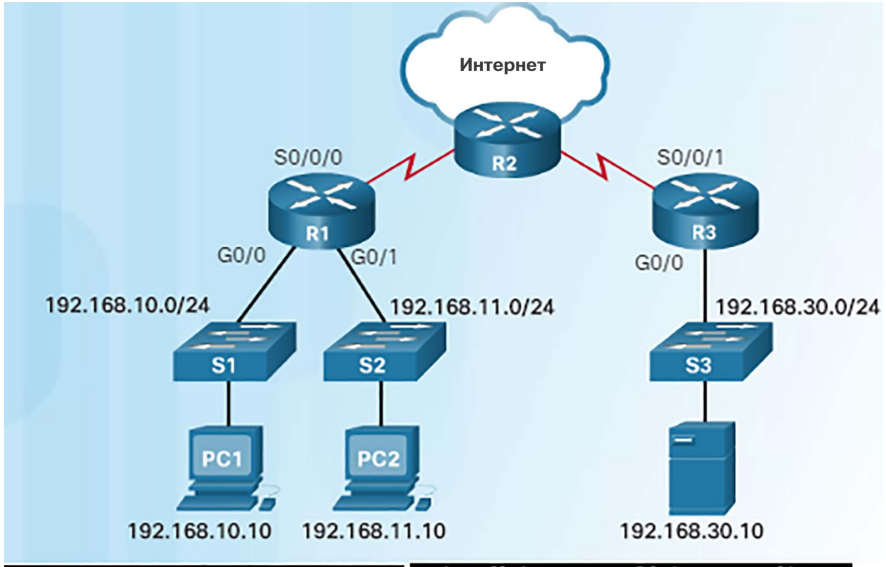


- Запишите порядок, в котором вводились утверждения списка контроля доступа во время настройки.
- Отметьте, что после ввода команды **show running-config** утверждения были отображены в другом порядке.
- Утверждения для хостов перечислены первыми, но не в том порядке, в каком они вводились.
- IOS располагает утверждения для хостов с помощью специальной функции хеширования. В результате такой порядок позволяет оптимизировать поиск записи списка контроля доступа для хоста.
- Порядок расположения утверждений для диапазонов остался неизменным. Функция хеширования применяется только к утверждениям для хостов.

Процессы маршрутизации и списки контроля доступа

- На рисунке проиллюстрированы логика работы маршрутизации и процессов ACL-списка.
- При получении пакета в интерфейсе маршрутизатора процесс маршрутизации остается неизменным независимо от того, настроены ли списки контроля доступа.
- После извлечения информации кадра маршрутизатор проверяет наличие списка контроля доступа на входном интерфейсе. При наличии списка контроля доступа пакет сопоставляется с утверждениями списка.
- Если пакет соответствует одной из записей, он принимается или отклоняется — в зависимости от условия, с которым он совпал.
- Если пакет разрешен, то после обработки пакета маршрутизатор ищет список контроля доступа в выходном интерфейсе.

Поиск и устранение неполадок, связанных со стандартными списками контроля доступа IPv4. Пример 1

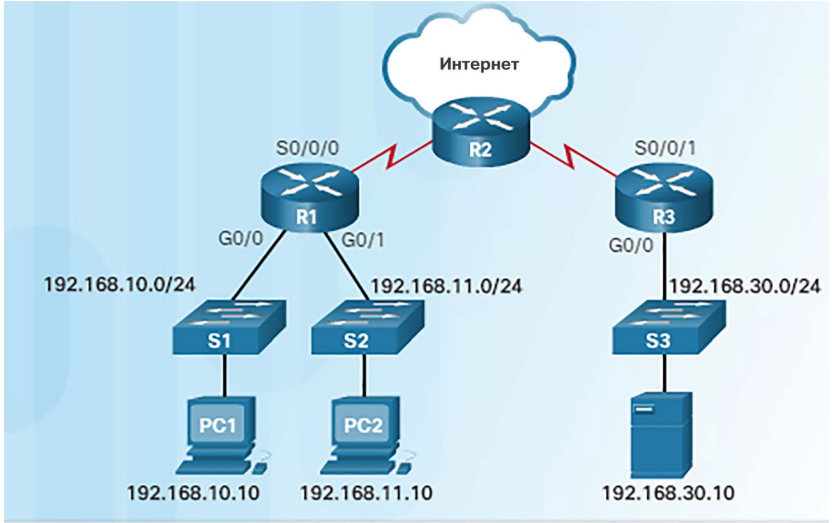



```
R3# show access-list
Standard IP access list 10
    10 deny 192.168.11.10
R3#
```

```
R3(config)# access-list 10 permit any
R3(config)# end
R3# show access-list
Standard IP access list 10
    10 deny 192.168.11.10
    20 permit any (4 match(es))
R3#
```

- Наиболее распространенные ошибки, связанные со списками контроля доступа:
  - Ввод записей списка контроля доступа в неверном порядке
  - Отсутствие приемлемых правил списка контроля доступа
  - Применение списка контроля доступа к неправильному направлению, неправильному интерфейсу или неправильному адресу источника
- На рисунке слева доступ к файловому серверу должен быть запрещен для компьютера PC2. Однако компьютер PC1 тоже не может получить к нему доступ.
- В выходных данных команды show access-list показано одно утверждение deny в списке контроля доступа.
- Решение показано на примере набора команд, приведенного справа. Утверждение permit разрешает доступ другим устройствам, так как неявная команда deny блокировала весь остальной трафик.

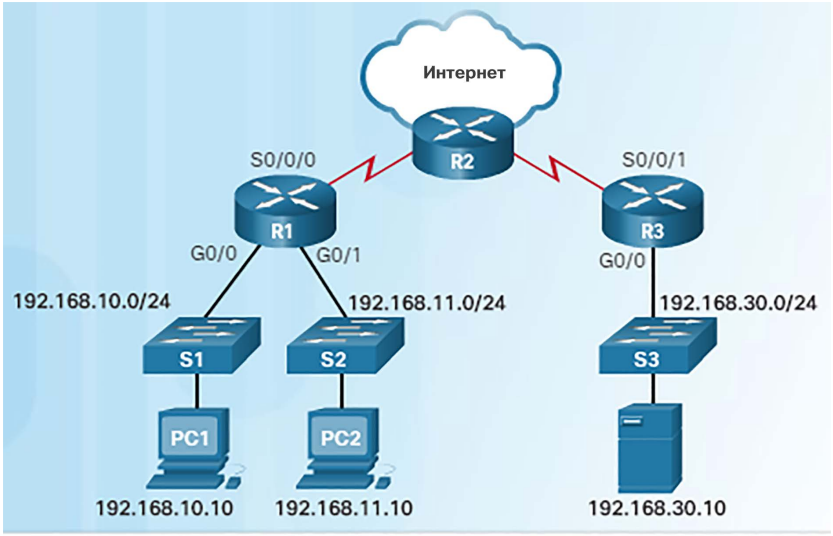
Поиск и устранение неполадок, связанных со стандартными списками контроля доступа IPv4. Пример 2




```
R1# show run | section interface
interface GigabitEthernet0/0
ip address 192.168.10.1 255.255.255.0
duplex auto
speed auto
interface GigabitEthernet0/1
ip address 192.168.11.1 255.255.255.0
ip access-group 20 in
duplex auto
speed auto
<output ommitted>
```

- Сеть 192.168.11.0/24 не должна иметь доступа к сети 192.168.10.0/24.
- Компьютер PC2 не имеет доступа к компьютеру PC1, как и планировалось, однако он также не имеет доступа в Интернет через маршрутизатор R2.
- Ошибка: список контроля доступа 20 был применен к интерфейсу G0/1 на входящем направлении
- Где следует применить список контроля доступа 20 и в каком направлении?
- Чтобы компьютер PC2 имел доступ к Интернету, список контроля доступа 20 нужно удалить из интерфейса G0/1 и применить к интерфейсу G0/0 в исходящем направлении.

Поиск и устранение неполадок, связанных со стандартными списками контроля доступа IPv4. Пример 3




```
R1# show run | section line vty
line vty 0 4
 access-class PC1-SSH in
 login
 transport input ssh
R1# show access-list
Standard IP access list PC1-SSH
    10 permit 192.168.10.1
    20 deny   any (5 match(es))
R1#
```

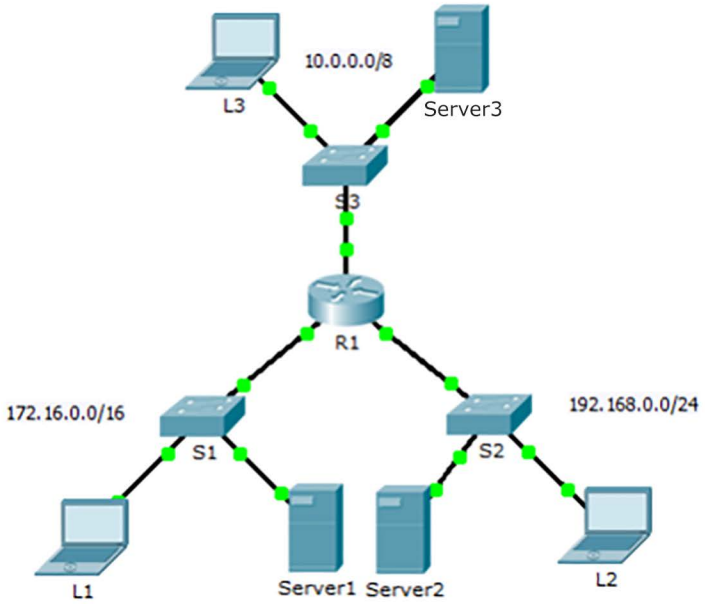
- Доступ к маршрутизатору R1 по протоколу SSH должен быть разрешен только компьютеру PC1.
- В конфигурации, показанной на рисунке слева, есть ошибка, поскольку PC1 не может подключиться к маршрутизатору R1 по протоколу SSH.
- Список контроля доступа разрешает адрес 192.168.10.1, который является интерфейсом G0/0. Разрешен же должен быть адрес хоста PC1 — 192.168.10.10.
- Решение представлено ниже:

```
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip access-list standard PC1-SSH
R1(config-std-nacl)# no 10
R1(config-std-nacl)# 10 permit host 192.168.10.10
R1(config-std-nacl)# end
R1# clear access-list counters
R1# show access-list
Standard IP access list PC1-SSH
    10 permit 192.168.10.10 (2 match(es))
    20 deny   any
R1#
```

Packet Tracer. Поиск и устранение неполадок, связанных со стандартными списками контроля доступа IPv4

Packet Tracer. Устранение неполадок в работе стандартных списков контроля доступа для IPv4

Топология



Сценарий

К этой сети должны применяться три правила.

- Хосты сети 192.168.0.0/24 не могут получить доступ к сети 10.0.0.0/8.
- L3 не может получить доступ к какому-либо устройству в сети 192.168.0.0/24.
- L3 не может получить доступ к **Server1** или **Server2**. L3 может получить доступ только к **Server3**.
- Хосты из сети 172.16.0.0/16 имеют полный доступ к **Server1**, **Server2** и **Server3**.

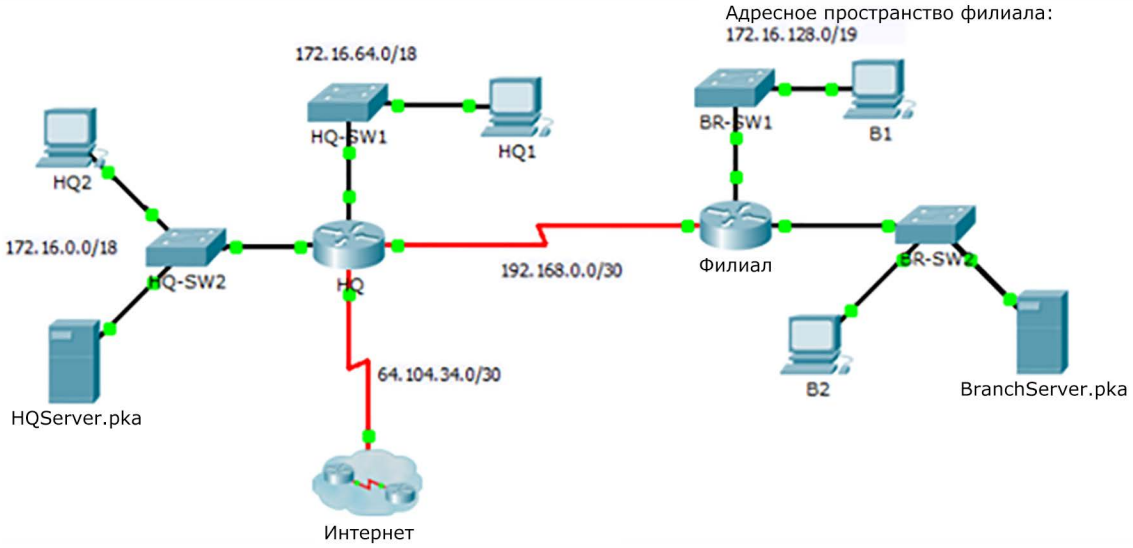
- В этом упражнении для Packet Tracer потребуется выполнить поиск и устранение различных неполадок, связанных со списками контроля доступа IPv4.

7.4. Обзор главы

Packet Tracer. Отработка комплексных практических навыков

Cisco Packet Tracer. Отработка комплексных практических навыков

Топология



- В этом упражнении для Packet Tracer потребуется завершить схему IP-адресации, настроить маршрутизацию и применить именованные списки контроля доступа.

Новые термины и команды

- списки контроля доступа (ACL)
- межсетевые экраны
- Записи списка контроля доступа (ACE) для
- фильтрация пакетов
- Стандартные списки контроля доступа (ACL)
- Расширенные списки контроля доступа (ACL)
- неявный запрет
- Списки контроля доступа (ACL) для входящих подключений
- Списки контроля доступа (ACL) для исходящих подключений
- шаблонные маски
- именованные списки контроля доступа
- инверсная маска


CISCO