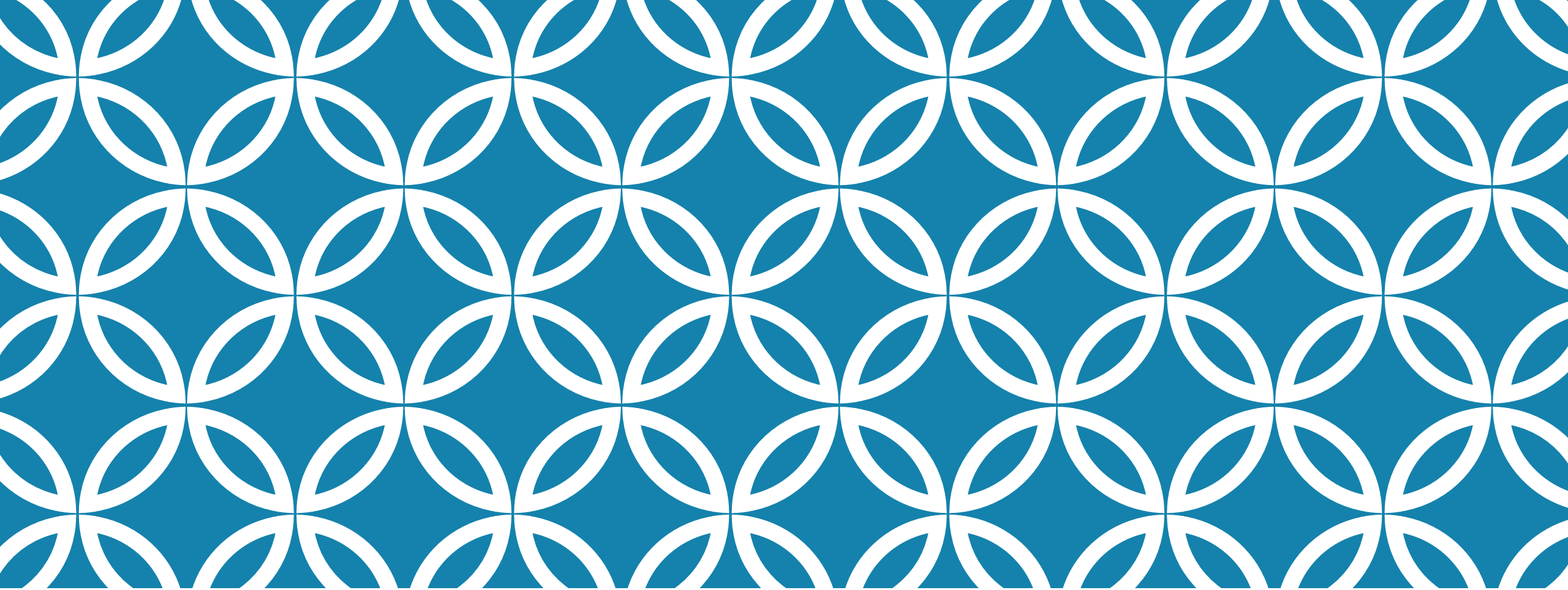


# МОДУЛЬ 4. ПРИНЦИПЫ ACL

КАФЕДРА ТЕЛЕКОММУНИКАЦИЙ

# 4.1 НАЗНАЧЕНИЕ ACL-СПИСКОВ
## 4.1.1 ЧТО ТАКОЕ ACL?

ACL-список — это ряд команд IOS, определяющих, пересылает ли маршрутизатор пакеты или сбрасывает их, исходя из информации в заголовке пакета. По умолчанию маршрутизатор не имеет настроенных списков ACL. Если ACL-список используется на интерфейсе, маршрутизатор выполняет дополнительную задачу, оценивая все сетевые пакеты, проходящие через интерфейс, с целью определения разрешения пересылки пакета.

Список контроля доступа (ACL) — это последовательный список разрешающих или запрещающих операторов, называемых записями списка контроля доступа (ACE).

**Примечание.** Записи списка контроля доступа также часто называют правилами ACL-списка.

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. Этот процесс называется фильтрацией пакетов.

# 4.1 НАЗНАЧЕНИЕ ACL-СПИСКОВ
## 4.1.1 ЧТО ТАКОЕ ACL?

Некоторые задачи, выполняемые маршрутизаторами, требуют использования списков ACL для идентификации трафика:

Ограничение сетевого трафика для повышения производительности сети.

Управление потоком трафика.

Списки контроля доступа обеспечивают базовый уровень безопасности в отношении доступа к сети.

Фильтрация трафика на основе типа трафика.

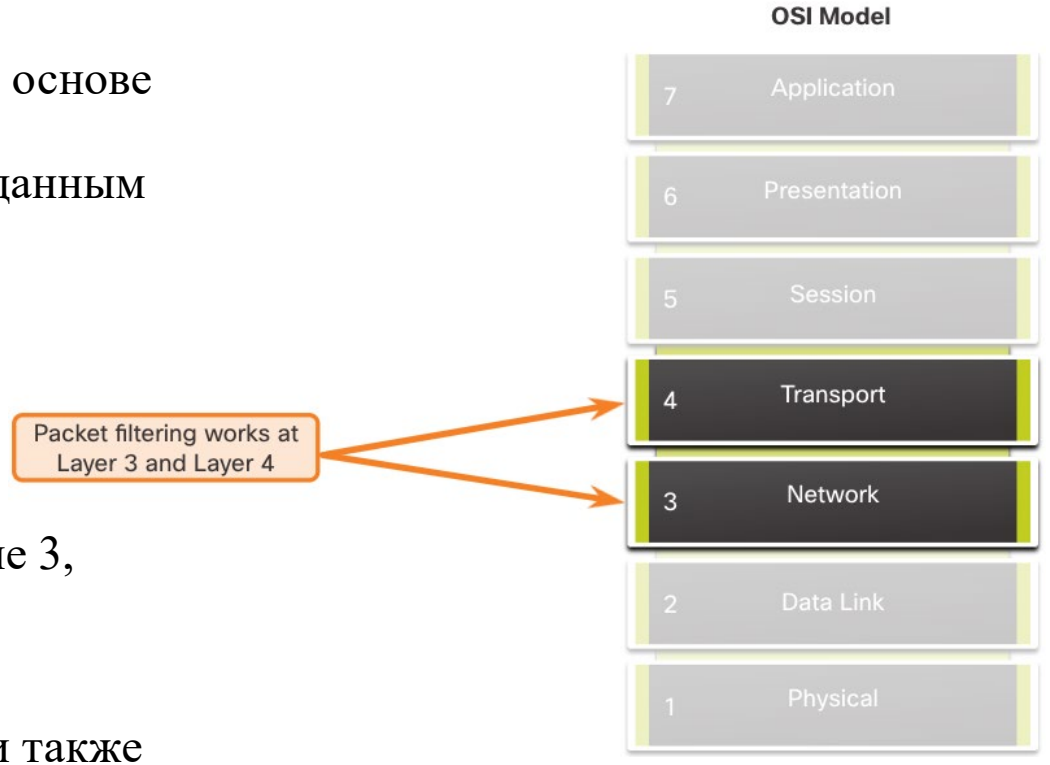
Проверка хостов в целях разрешения или запрета доступа к сетевым сервисам.

Предоставление приоритета определенным классам сетевого трафика

# 4.1 НАЗНАЧЕНИЕ ACL-СПИСКОВ
## 4.1.2 ФИЛЬТРАЦИЯ ПАКЕТОВ

Фильтрация пакетов обеспечивает контроль доступа к сети на основе анализа входящих и исходящих пакетов с последующей переадресацией или отбрасыванием этих пакетов согласно заданным критериям.

Фильтрация пакетов может выполняться на уровне 3 или 4.




Маршрутизаторы Cisco поддерживают два типа ACL:

**Стандартные списки ACL** - ACL фильтруют только на уровне 3, используя только адрес источника IPv4.

**Расширенные списки ACL** - фильтр ACL на уровне 3 с использованием адреса IPv4 источника и/или назначения. Они также могут фильтровать на уровне 4, используя порты TCP, UDP и дополнительную информацию о типе протокола для более точного управления.

# 4.1 НАЗНАЧЕНИЕ ACL-СПИСКОВ
## 4.1.3 ПРИНЦИПЫ 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 можно настроить для применения к входящему трафику и к исходящему трафику.

**Примечание:** Списки контроля доступа не применяются к пакетам, созданным маршрутизатором.

Входящий ACL фильтрует пакеты, приходящие на определенный интерфейс, до того, как они будут направлены на исходящий интерфейс. Входящий ACL-список эффективен, поскольку он сохраняет ресурсы на поиск маршрута, если пакет отбрасывается.

Исходящий ACL фильтрует пакеты после их маршрутизации — вне зависимости от входящего интерфейса.

# 4.1 НАЗНАЧЕНИЕ ACL-СПИСКОВ
## 4.1.3 ПРИНЦИПЫ РАБОТЫ ACL-СПИСКОВ

Когда ACL применяется к интерфейсу, он выполняет определенную рабочую процедуру. Ниже приведены действия, используемые при поступлении трафика в интерфейс маршрутизатора с настроенным входящим стандартным ACL IPv4.

Если на маршрутизаторе настроен стандартный список контроля доступа (ACL) IPv4, то, получив пакет, такой маршрутизатор извлекает из заголовка пакета IPv4-адрес источника.

Далее маршрутизатор последовательно сравнивает адрес с адресом в каждой из записей в списке контроля доступа (ACL), начиная с первой записи.

Когда сопоставление установлено, маршрутизатор выполняет инструкцию, разрешающую или запрещающую пакет, а остальные ACE в ACL, если таковые имеются, не анализируются.

Если исходный IPv4-адрес не совпадает ни с одним ACE в ACL, пакет отбрасывается, поскольку существует неявный запрет ACE, автоматически применяемый ко всем ACL.

Последней записью ACL-списка всегда является косвенный отказ, блокирующий весь трафик. Он скрыт и не отображается в конфигурации.

**Примечание.** ACL должен иметь по крайней мере одну инструкцию разрешения, иначе весь трафик будет отклонен из-за неявного оператора deny ACE.

# 4.2 ШАБЛОННЫЕ МАСКИ В ACL-СПИСКАХ
## 4.2.1 ОБЗОР ШАБЛОННЫХ МАСОК ACL-СПИСКОВ

Шаблонная маска аналогична маске подсети в том, что она использует процесс логического И  для определения того, какие биты IPv4-адреса соответствуют. В отличии от маски подсети, в которой 1 определяет совпадение, а 0 определяет не совпадение в шаблонной маске - верно обратное.

IPv4 ACE использует 32-разрядную шаблонную маску, чтобы определить, какие биты адреса необходимо проверить на соответствие.

Для совпадения двоичных единиц и нулей шаблонные маски используют следующие правила:

**Бит 0 шаблонной маски** — совпадает с соответствующим значением бита в адресе.

**Бит 1 шаблонной маски** — игнорирует соответствующее значение бита в адресе.

# 4.2 ШАБЛОННЫЕ МАСКИ В ACL-СПИСКАХ
## 4.2.1 ОБЗОР ШАБЛОННЫХ МАСОК ACL-СПИСКОВ

| Групповая маска | Последний октет (в двоичном формате) | Значение (0 - совпадение, 1 - игнорирование) |
|---|---|---|
| **0.0.0.0** | **00000000** | Соответствие всем октетам. |
| **0.0.0.63** | **00111111** | Совпадение первых трех октетов<br>Сопоставление двух левых битов последнего октета<br>Игнорировать последние 6 бит адреса |
| **0.0.0.15** | **00001111** | Совпадение первых трех октетов<br>Совпадение четырех левых  бит последнего октета<br>Игнорировать последние 4 бита последнего октета |
| **0.0.0.248** | **11111100** | Совпадение первых трех октетов<br>Игнорировать шесть левых битов последнего октета<br>Совпадение последних двух битов |
| **0.0.0.255** | **11111111** | Совпадение первых трех октетов<br>Игнорировать последний октет |

# 4.2 ШАБЛОННЫЕ МАСКИ В ACL-СПИСКАХ
## 4.2.2 ТИПЫ ШАБЛОННЫХ МАСОК

**Шаблонные маски для соответствия хосту.**

Предположим, ACL 10 требуется ACE, который разрешает только узел с адресом IPv4 192.168.1.1. Напомним, что «0» равно совпадению, а «1» равно игнорированию. Для соответствия конкретному адресу IPv4 узла требуется шаблонная маска, состоящая из всех нулей (т.е. 0.0.0.0).

При обработке ACE шаблонная маска разрешает только адрес 192.168.1.1. ACE в ACL 10 будет **access-list 10 permit 192.168.1.1 0.0.0.0**.

| | Десятичные | Двоичные |
|---|---|---|
| адрес IPv4 | 192.168.1.1 | **11000000.10101000.00000001.00000001** |
| Шаблонная маска | 0.0.0.0 | **00000000.00000000.00000000.00000000** |
| Разрешенный IPv4 адрес | 192.168.1.1 | **11000000.10101000.00000001.00000001** |

# 4.2 ШАБЛОННЫЕ МАСКИ В ACL-СПИСКАХ
## 4.2.2 ТИПЫ ШАБЛОННЫХ МАСОК

**Расчет шаблонных масок для соответствия подсетям IPv4.**

ACL 10 требуется ACE, разрешающий все узлы в сети 192.168.1.0/24. Шаблонная маска 0.0.0.255 предусматривает, что первые три октета должны точно совпадать, а четвертый октет — нет.

При обработке шаблонная  маска 0.0.0.255 разрешает все узлы в сети 192.168.1.0/24. ACE в ACL 10 будет **access-list 10 permit 192.168.1.0 0.0.0.255**.

| | Десятичные | Двоичные |
|---|---|---|
| адрес IPv4 | 192.168.1.1 | **11000000.10101000.00000001.00000001** |
| Групповая маска | 0.0.0.255 | **00000000.00000000.00000000.11111111** |
| Разрешенный IPv4 адрес | 192.168.1.0/24 | **11000000.10101000.00000001.00000000** |

# 4.2 ШАБЛОННЫЕ МАСКИ В ACL-СПИСКАХ
## 4.2.2 ТИПЫ ШАБЛОННЫХ МАСОК

**Шаблонная маски для соответствия диапазону адресов IPv4.**

ACL 10 требуется ACE, разрешающий все узлы в сетях 192.168.16.0/24, 192.168.17.0/24,..., 192.168.31.0/24.

При обработке шаблонной маски 0.0.15.255 разрешает все узлы в сетях 192.168.16.0/24 до 192.168.31.0/24. ACE в ACL 10 будет **access-list 10 permit 192.168.16.0 0.0.15.255**.

| | Десятичные | Двоичные |
|---|---|---|
| адрес IPv4 | 192.168.16.0 | **11000000.10101000.00010000.00000000** |
| Групповая маска | 0.0.15.255 | **00000000.00000000.00001111.11111111** |
| Разрешенный IPv4 адрес | 192.168.16.0/24<br>…<br>192.168.31.0/24 | **11000000.10101000.00010000.00000000**<br><br>**11000000.10101000.00011111.00000000** |

# 4.2 ШАБЛОННЫЕ МАСКИ В ACL-СПИСКАХ
## 4.2.3 ВЫЧИСЛЕНИЕ ШАБЛОННЫХ МАСОК

Вычисление шаблонных масок может быть сопряжено с определенными сложностями. Простым способом является вычитание маски подсети из значения 255.255.255.255.

**Несколько примеров:**

Предположим, вы хотели, чтобы ACE в ACL 10 разрешил доступ всем пользователям в сети 192.168.3.0/24. Чтобы вычислить маску подсети, вычитайте маску подсети (255.255.255.0) из 255.255.255.255. В результате получается шаблонная маска 0.0.0.255. ACE **access-list 10 permit 192.168.3.0 0.0.255**.

Предположим, что вы хотели, чтобы ACE в ACL 10 разрешил сетевой доступ для 14 пользователей в подсети 192.168.3.32/28. Вычтите подсеть (например, 255.255.255.240) из 255.255.255.255.255. В результате получается шаблонная маска 0.0.0.15. ACE будет **access-list 10 permit 192.168.3.32 0.0.0.15**.

Предположим, что требуется ACE в ACL 10, чтобы разрешить только сети 192.168.10.0 и 192.168.11.0. Эти две сети можно суммировать как 192.168.10.0/23, которая представляет собой маску подсети 255.255.254.0. Вычесть маску подсети 255.255.254.0 из 255.255.255.255. В результате получается шаблонная маска 0.0.1.255. ACE будет **access-list 10 permit 192.168.10.0 0.0.1.255**.

# 4.2 ШАБЛОННЫЕ МАСКИ В ACL-СПИСКАХ
## 4.2.4 КЛЮЧЕВЫЕ СЛОВА ДЛЯ ШАБЛОННЫХ МАСОК

Cisco IOS предоставляет два ключевых слова для определения наиболее распространенных видов применения шаблонных масок.

Два ключевых слова:

**host** - применяется для маски 0.0.0.0. Эта маска подразумевает соответствие всех битов IPv4-адреса. Таким образом, фильтруется единственный адрес хоста.

**any** - замещает маску 255.255.255.255 Эта маска указывает игнорировать весь IPv4-адрес или принять любой адрес.

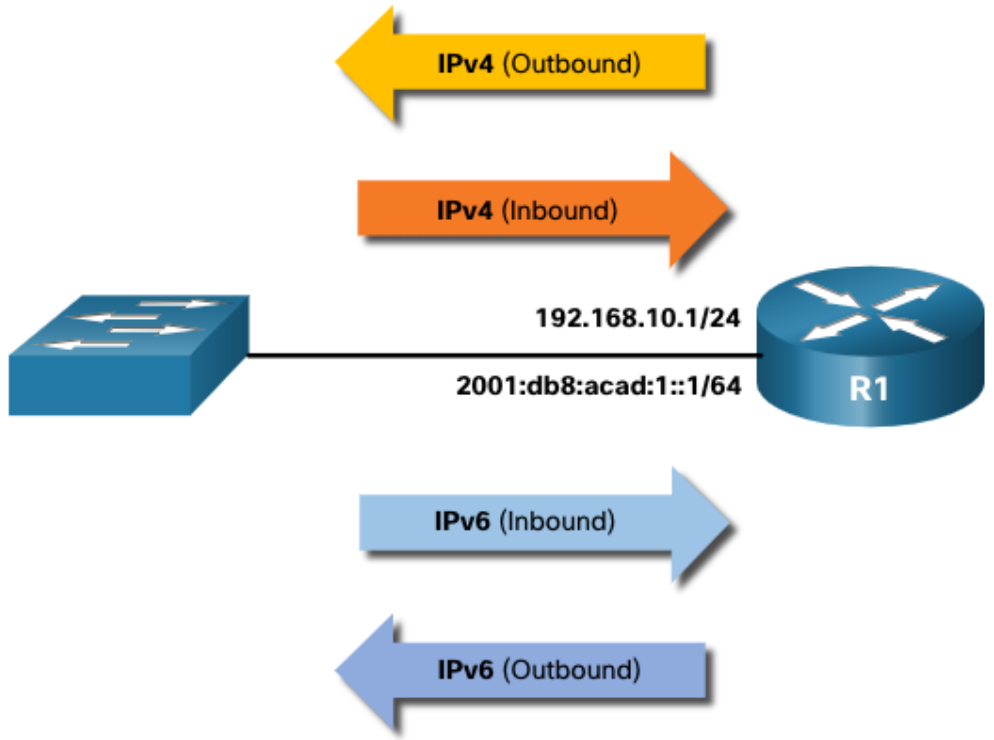
# 4.3 РЕКОМЕНДАЦИИ ПО СОЗДАНИЮ СПИСКОВ ACL

## 4.3.1 ОГРАНИЧЕННОЕ ЧИСЛО СПИСКОВ ACL НА ИНТЕРФЕЙСЕ

Существует ограничение на количество списков ACL, которые могут быть применены к интерфейсу маршрутизатора. Например, интерфейс с двойным стеком маршрутизатора (например, IPv4 и IPv6) может иметь до четырех ACL, как показано на рисунке.

В частности, интерфейс маршрутизатора может иметь:

- один исходящий список ACL IPv4
- один входящий список ACL IPv4
- один входящий список ACL IPv6
- один исходящий список ACL IPv6




**Примечание.** Списки контроля доступа не требуется конфигурировать на оба направления. Количество списков ACL и их направление, применяемое к интерфейсу, будут зависеть от политики безопасности организации.

# 4.3 РЕКОМЕНДАЦИИ ПО СОЗДАНИЮ СПИСКОВ ACL

## 4.3.2 ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ

Создание ACL-списков требует внимания к деталям и повышенной осторожности. Ошибки могут привести к серьезным последствиям и дополнительным затратам, связанным с простоями, поиском и устранением неполадок, а также некорректной работой сетевых служб. Перед настройкой ACL-списка необходимо создать базовый план реализации.

| Рекомендации | Преимущество |
|---|---|
| Создавайте ACL-списки, исходя из корпоративной политики обеспечения информационной безопасности. | Соблюдение рекомендации обеспечивает соответствие требованиям информационной безопасности компании. |
| Напишите, что вы хотите, чтобы ACL сделал. | 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. |
| Документируйте списки ACL с помощью команды **remark** . | Это поможет вам (и другим) понять цель ACE. |
| Проверьте работу ACL-списков в пробной сети перед внедрением в реальную действующую сеть. | Соблюдение рекомендации поможет избежать дорогостоящих ошибок. |

# 4.4 ТИПЫ ACL IPV4

## 4.4.1 СТАНДАРТНЫЕ И РАСШИРЕННЫЕ СПИСКИ КОНТРОЛЯ ДОСТУПА

Типы списков контроля доступа для IPv4:

**Стандартные списки ACL** — разрешают или запрещают пакеты, основанные только на исходном IPv4-адресе.

**Расширенные списки ACL** — разрешают или запрещают пакеты, основанные на адресе IPv4 источника и адресе назначения IPv4, типе протокола, TCP-или UDP-портах источника и назначения и т. д.

# 4.4 ТИПЫ ACL IPV4
## 4.4.2 ИМЕНОВАННЫЕ И НУМЕРОВАННЫЕ СПИСКИ КОНТРОЛЯ ДОСТУПА

**Нумерованный список контроля доступа (ACL)**

ACL, пронумерованные 1-99 или 1300-1999, являются стандартными ACL, в то время как ACL, пронумерованные 100-199 или 2000-2699, являются расширенными ACL.

```
R1(config)# access-list ?
 <1-99> IP standard access list
 <100-199> IP extended access list
 <1100-1199>Расширенный список доступа к 48-битным MAC-адресам
 <1300-1999> IP standard access list (expanded range)
 <200-299> Protocol type-code access list
 <2000-2699> IP extended access list (expanded range)
 <700-799> 48-bit MAC address access list
 rate-limit Simple rate-limit specific access list
 template Enable IP template acls
Router(config)# access-list
```

# 4.4 ТИПЫ ACL IPV4
## 4.4.2 ИМЕНОВАННЫЕ И НУМЕРОВАННЫЕ СПИСКИ КОНТРОЛЯ ДОСТУПА

**Именованные списки контроля доступа**

Именованные списки ACL являются предпочтительным методом для использования при настройке списков ACL. В частности, стандартные и расширенные списки ACL могут быть названы для предоставления сведений о назначении ACL. Например, именование расширенного ACL FTP-FILTER намного лучше, чем присвоение нумерованного ACL 100.

Команда глобальной конфигурации **ip access-list** используется для создания именованного списка ACL, как показано в следующем примере.

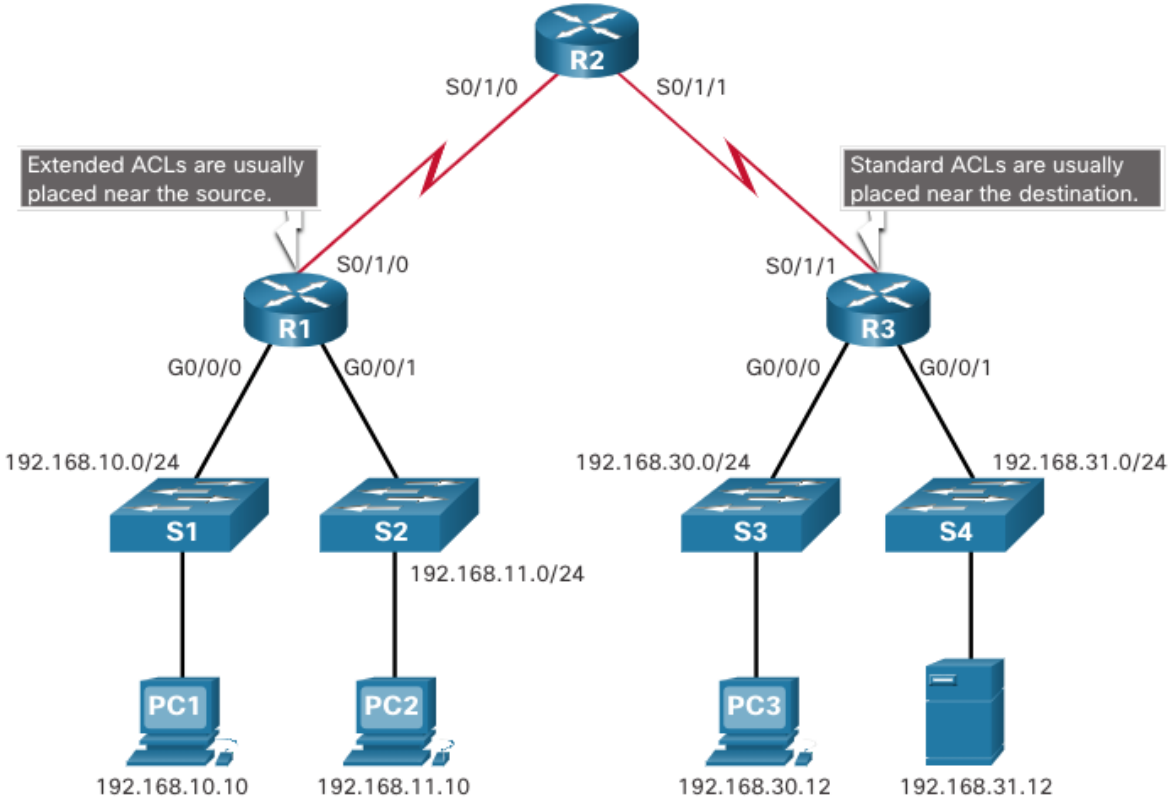
```
R1(config)# ip access-list extended FTP-FILTER
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq ftp
R1 (config-ext-nacl) # разрешить tcp 192.168.10.0 0.0.255 любые eq ftp-
данные R1 (config-ext-nacl) #
```

# 4.4 ТИПЫ ACL IPV4
## 4.4.3 ГДЕ РАЗМЕСТИТЬ СПИСКИ КОНТРОЛЯ ДОСТУПА

Каждый список контроля доступа (ACL) должен быть размещен там, где он может демонстрировать максимальную эффективность.

Расширенные списки контроля доступа следует располагать как можно ближе к источнику фильтруемого трафика.

Стандартные списки контроля доступа следует размещать как можно ближе к месту назначения.



# 4.4 ТИПЫ ACL IPV4
## 4.4.3 ГДЕ РАЗМЕСТИТЬ СПИСКИ КОНТРОЛЯ ДОСТУПА

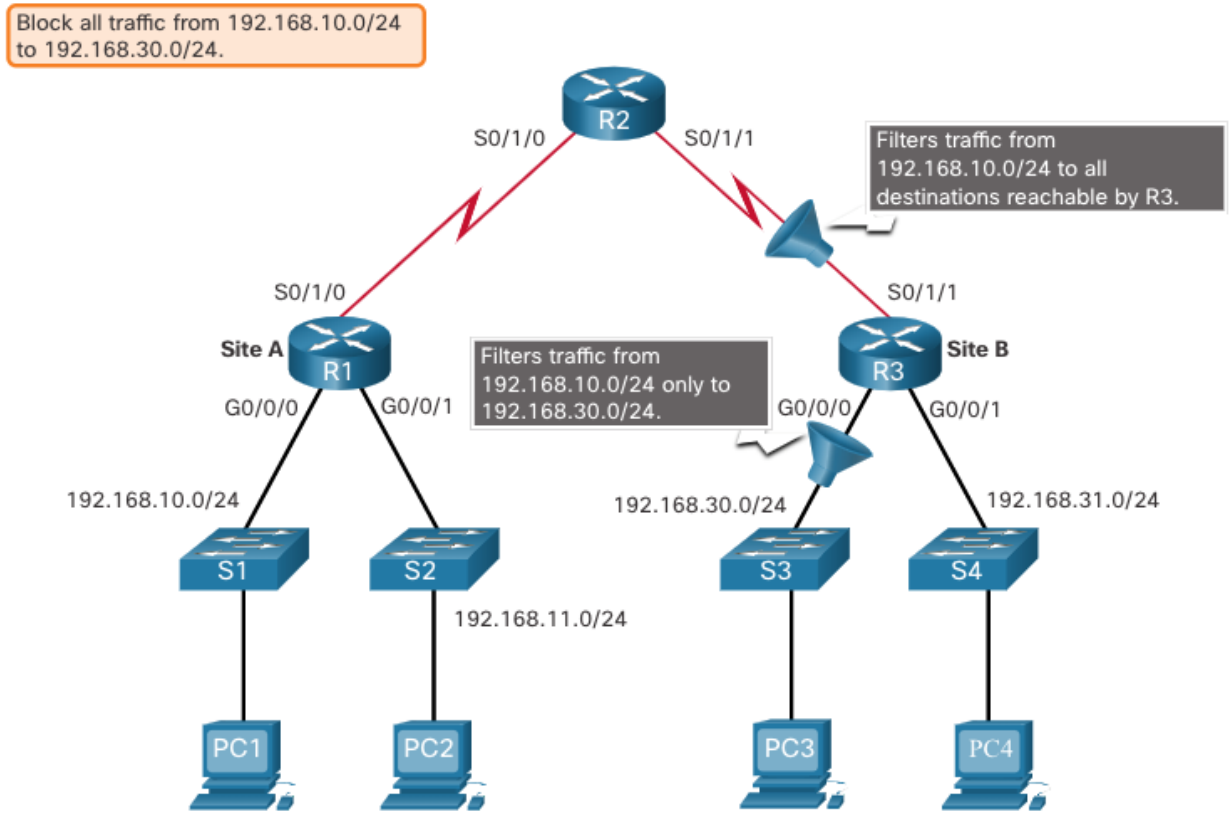
| Факторы, влияющие на размещение ACL | Описание |
|---|---|
| **Степень контроля сетей данной организации** | Размещение ACL может зависеть от того, контролирует ли организация сеть источника и сеть назначения. |
| **Пропускная способность участвующих сетей** | Возможно, желательно отфильтровать нежелательный трафик у источника, чтобы предотвратить передачу трафика, потребляющего пропускную способность. |
| **Простота настройки конфигурации** | Возможно, проще реализовать ACL в месте назначения, но трафик будет использовать полосу пропускания без необходимости.<br>Расширенный ACL-список можно применить на каждом маршрутизаторе, с которого идет трафик. Это позволит сохранить пропускную способность при помощи фильтрации трафика на источнике, но для этого требуется создание расширенных ACL-списков на нескольких маршрутизаторах. |

# 4.4 ТИПЫ ACL IPV4

## 4.4.4 ПРИМЕР РАЗМЕЩЕНИЯ СТАНДАРТНОГО СПИСКА КОНТРОЛЯ ДОСТУПА

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

Следуя основным рекомендациям по размещению, администратор разместил стандартный список ACL на маршрутизаторе R3.



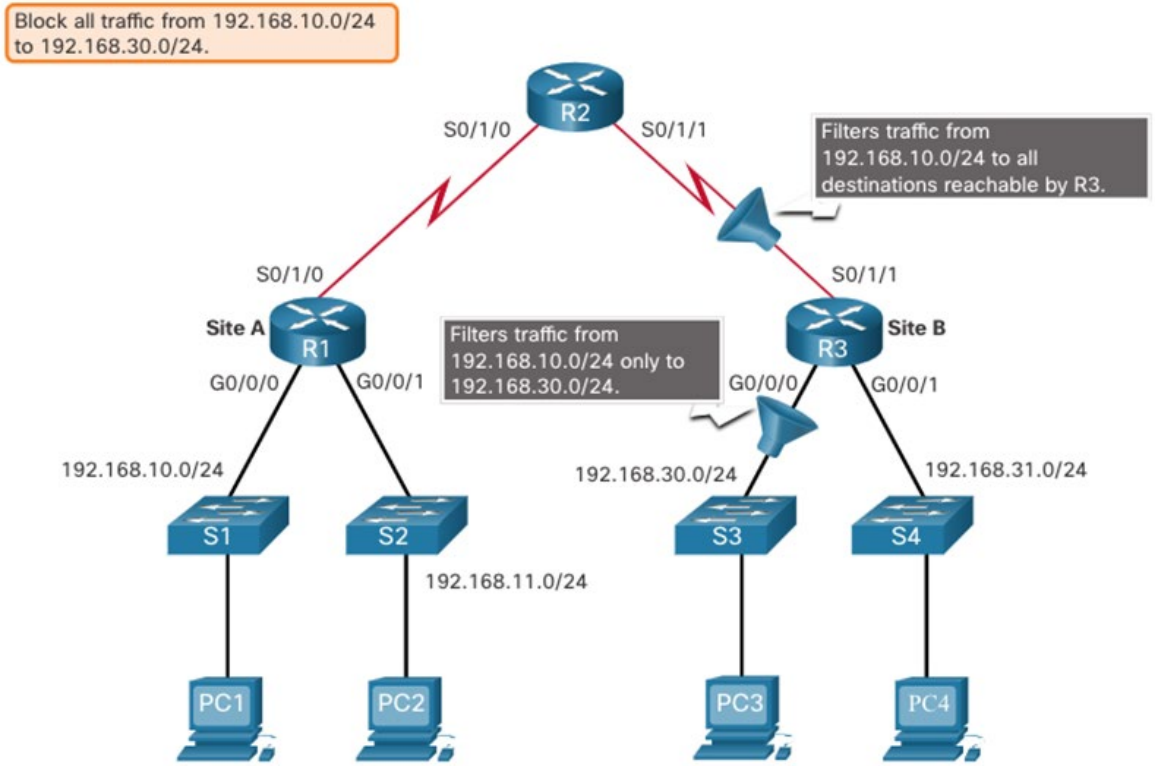
# 4.4 ТИПЫ ACL IPV4

## 4.4.4 ПРИМЕР РАЗМЕЩЕНИЯ СТАНДАРТНОГО СПИСКА КОНТРОЛЯ ДОСТУПА

Существует два возможных интерфейса на R3 для применения стандартного ACL:

**Интерфейс R3 S0/1/1 (входящий)** — стандартный ACL может применяться для входящего трафика на интерфейсе R3 S0/1/1 для запрета трафика из сети .10. Однако он также фильтрует трафик .10 в сеть 192.168.31.0/24 (в данном примере .31). Поэтому стандартный ACL не должен применяться к этому интерфейсу.

**Интерфейс R3 G0/0 (исходящий)** — стандартный ACL может быть применен для исходящего трафика на интерфейсе R3 G0/0/0. Применение данного списка не повлияет на другие сети, доступные для R3. Пакеты из сети .10 все равно смогут добраться до сети .31. Это лучший интерфейс для размещения стандартного списка ACL в соответствии с требованиями трафика.



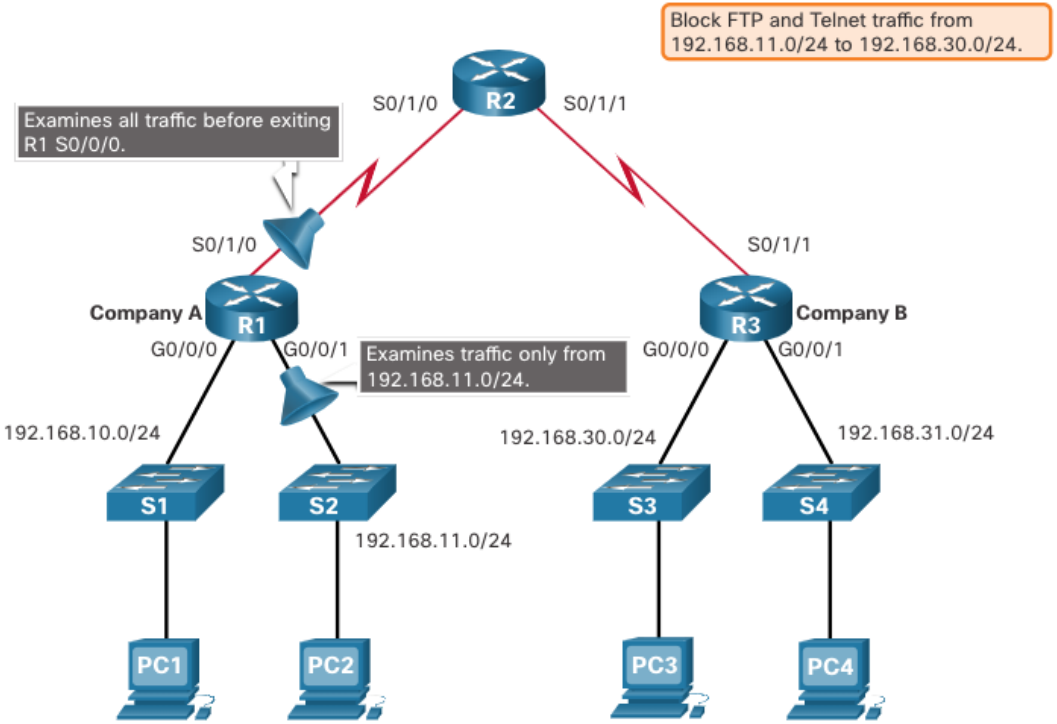
# 4.4 ТИПЫ ACL IPV4

## 4.4.5 ПРИМЕР РАЗМЕЩЕНИЯ РАСШИРЕННОГО СПИСКА КОНТРОЛЯ ДОСТУПА

Расширенный ACL должен быть расположен как можно ближе к источнику.

Однако организация может размещать списки ACL только на устройствах, которые она контролируют. Поэтому место размещения определяется, исходя из пределов сферы контроля сетевого администратора.

На рисунке, например, компания A хочет запретить трафик Telnet и FTP в сеть 192.168.30.0/24 компании B из их сети 192.168.11.0/24, разрешая при этом весь другой трафик.



# 4.4 ТИПЫ ACL IPV4

## 4.4.5 ПРИМЕР РАЗМЕЩЕНИЯ РАСШИРЕННОГО СПИСКА КОНТРОЛЯ ДОСТУПА

Расширенный ACL на R3  выполнил бы эту задачу, но администратор не контролирует R3. При этом нежелательный трафик сможет проходить через всю сеть только для того, чтобы оказаться заблокированным по достижении места назначения.

Решение - поместить расширенный список ACL на R1, который определяет адреса источника и назначения.

Рисунок показывает два интерфейса R1, на которых возможно применение расширенного ACL.

**Интерфейс R1 S0/1/0 (исходящий)** - Расширенный ACL может быть применен исходящий на интерфейсе S0/1/0. Это решение будет обрабатывать все пакеты, оставляющие R1, включая пакеты из 192.168.10.0/24.

**Интерфейс R1 G0/0/1 (входящий)** - расширенный ACL может применяться во входящем направлении на G0/0/1, и только пакеты из сети 192.168.11.0/24 подлежат обработке ACL на R1. Поскольку фильтр ограничивается только пакетами, покидающими сеть 192.168.11.0/24, применение расширенного списка контроля доступа на G0/1 — оптимальное решение.