

Сетевые технологии

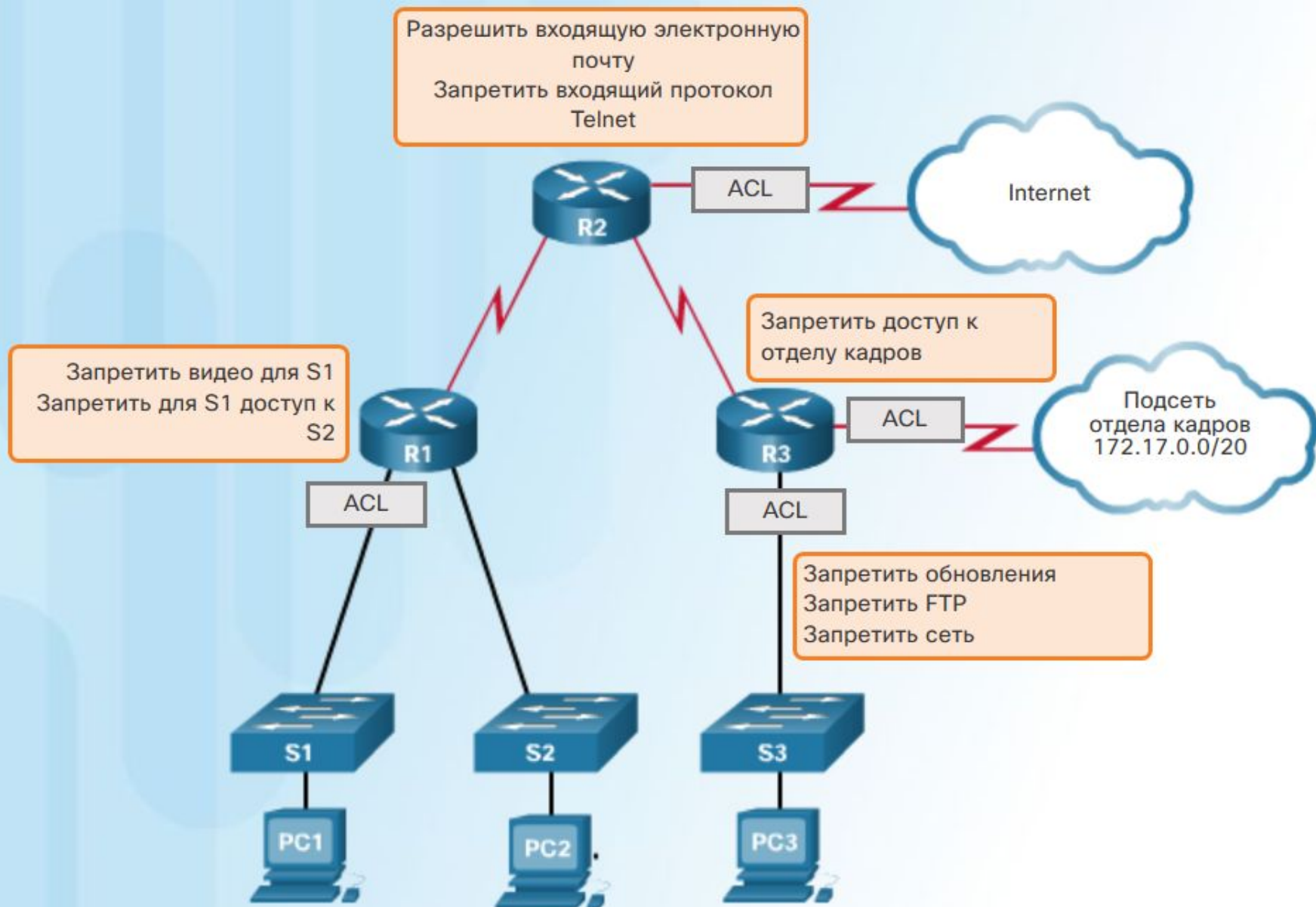
ACL
NAT

ACL-списки

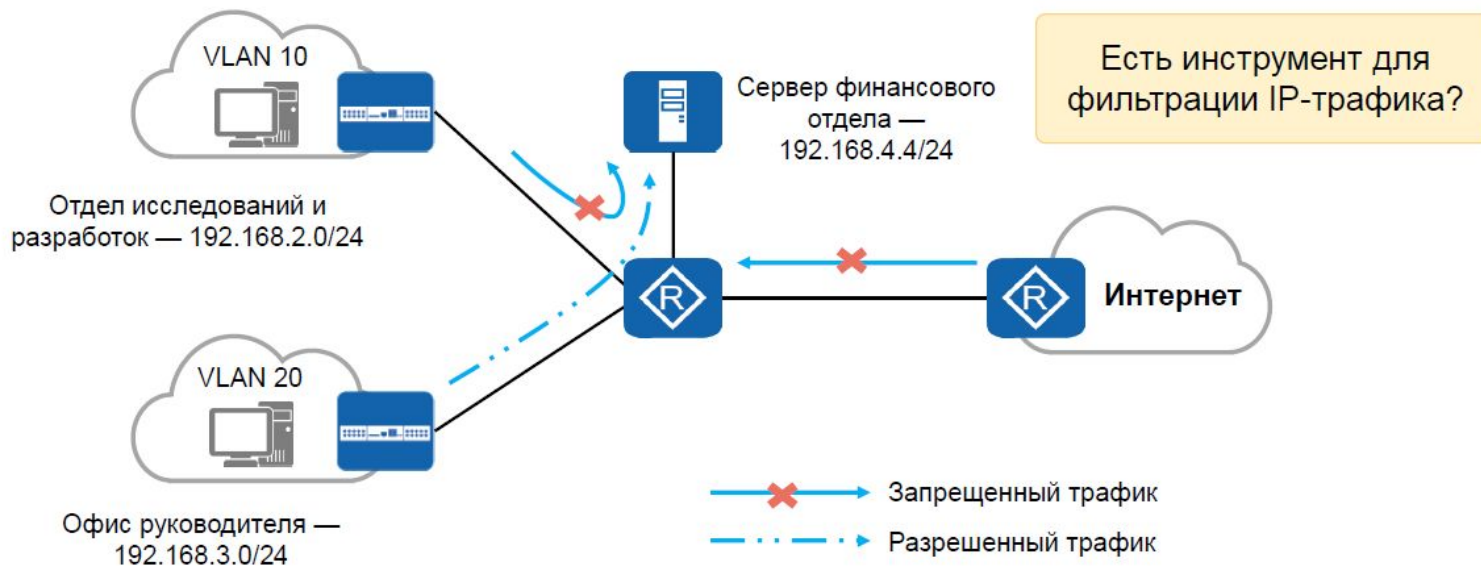


- ACL-список — это ряд команд IOS, определяющих, пересылает ли маршрутизатор пакеты или сбрасывает их, исходя из информации в заголовке пакета.
- Одна из наиболее используемых функций операционной системы Cisco IOS.
- Выполняют следующие задачи:
 - Ограничение сетевого трафика для повышения производительности сети.
 - Управление потоком трафика.
 - Обеспечивают базовый уровень безопасности в отношении доступа к сети
 - Осуществляют фильтрацию трафика на основе типа трафика.
- По умолчанию ACL-списки не сконфигурированы на маршрутизаторе, поэтому маршрутизатор не фильтрует трафик

ACL – списки в действии



ACL – списки в действии



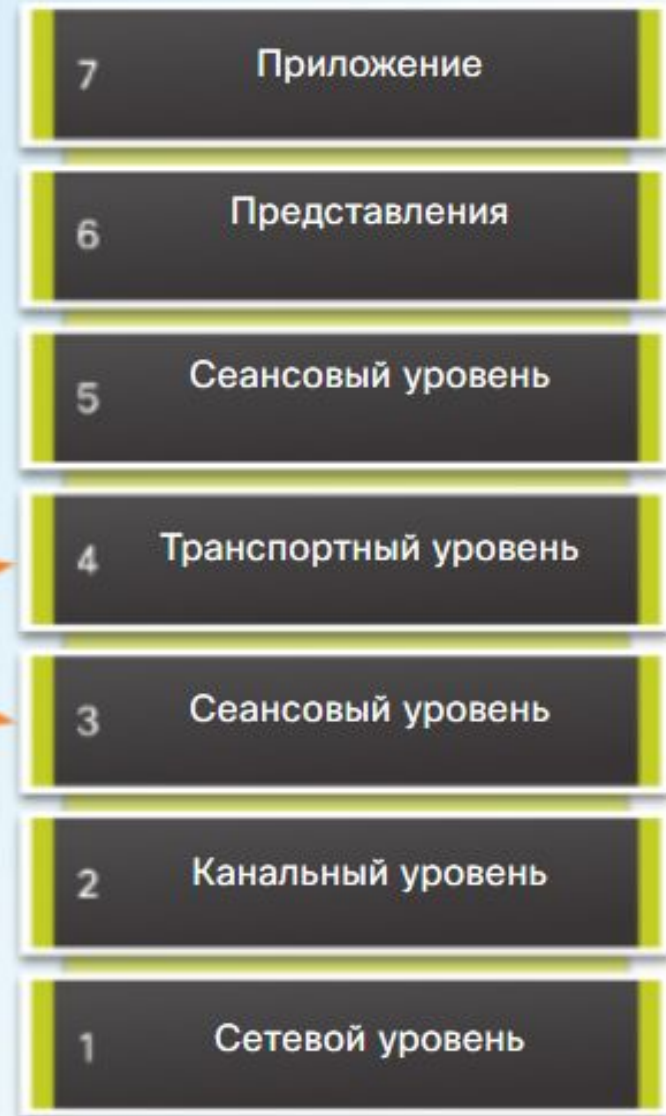
Чтобы обеспечить безопасность данных финансового отдела, предприятие запрещает доступ отделу исследований и разработок (R&D) к серверу финансового отдела, но разрешает доступ к серверу из офиса руководителя.

Применение ACL

- Соответствие IP-трафика
- Политики фильтрации трафика
- Трансляция сетевых адресов (NAT)
- Политики маршрутизации
- Политики межсетевого экрана
- Настройка политик QoS
- Прочее

ACL – список с позиции модели OSI

Модель OSI




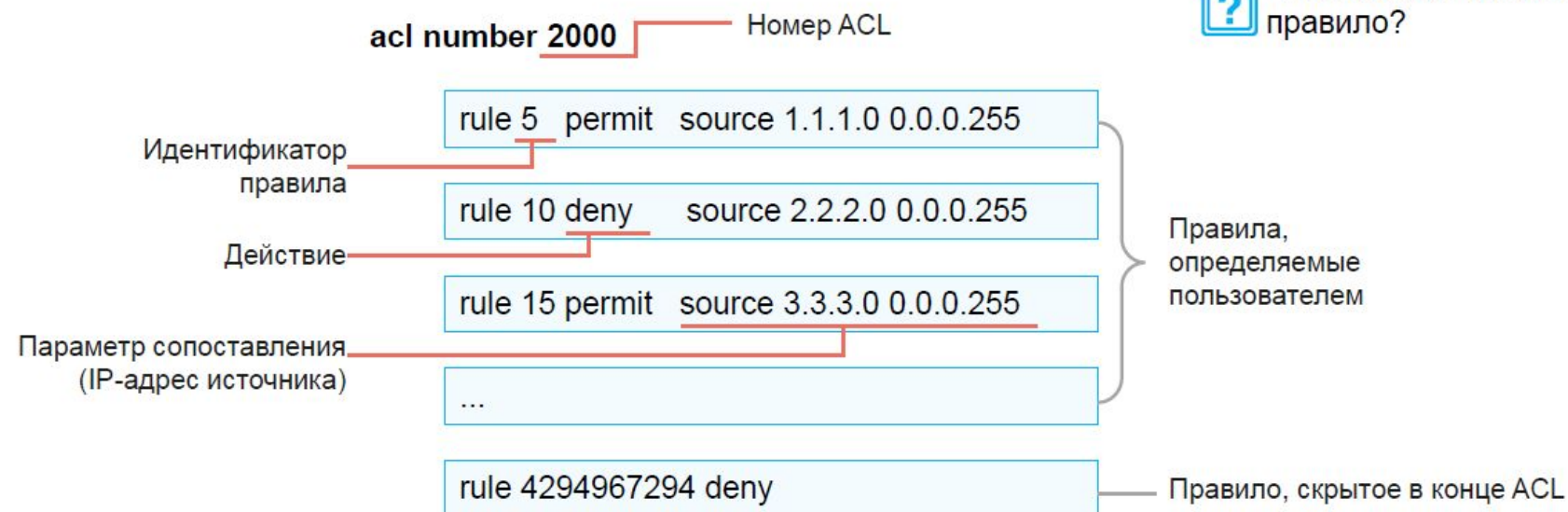
Фильтрация пакетов осуществляется на уровне 3 и уровне 4

Состоит из ACE записей (Access Control Entry)

Состав ACL

- ACL состоит из нескольких правил. Оператор permit/deny в каждой строке является действием, соответствующим правилу.

 Что означает каждое правило?



□ В конце – неявный запрет


Идентификатор правила

```
acl number 2000
```

Идентификатор
правила

```
rule 5 deny source 10.1.1.1 0
rule 10 deny source 10.1.1.2 0
rule 15 permit source 10.1.1.0 0.0.0.255
```

Шаг = 5

 Как добавить правило?

```
rule 11 deny source 10.1.1.3 0
```

```
acl number 2000
```

```
rule 5 deny source 10.1.1.1 0
rule 10 deny source 10.1.1.2 0
rule 11 deny source 10.1.1.3 0
rule 15 permit source 10.1.1.0 0.0.0.255
```

Идентификатор правила и шаг

- **Идентификатор правила**
Каждое правило в ACL имеет идентификатор (ID).
- **Шаг**
Шаг — это приращение идентификаторов соседних правил, автоматически назначаемых системой. Шаг по умолчанию — 5. Установка значения шага упрощает вставку правила между существующими правилами ACL.
- **Назначение идентификатора правила**
Если правило добавляется в пустой ACL, но для правила вручную не указан идентификатор, система выделяет значение шага (например, 5) в качестве идентификатора правила. Если ACL содержит правила с идентификаторами, указанными вручную, и добавляется правило без указанного вручную идентификатора, система выделяет этому правилу идентификатор, который больше, чем самый большой идентификатор правила в ACL, и является наименьшим целым числом, кратным значению шага.

Подстановочная маска (инверсная, шаблонная)

```
acl number 2000
rule 5      deny  source 10.1.1.1 0
rule 10     deny  source 10.1.1.2 0
rule 15     permit source 10.1.1.0 0.0.0.255
```

Подстановочный
знак

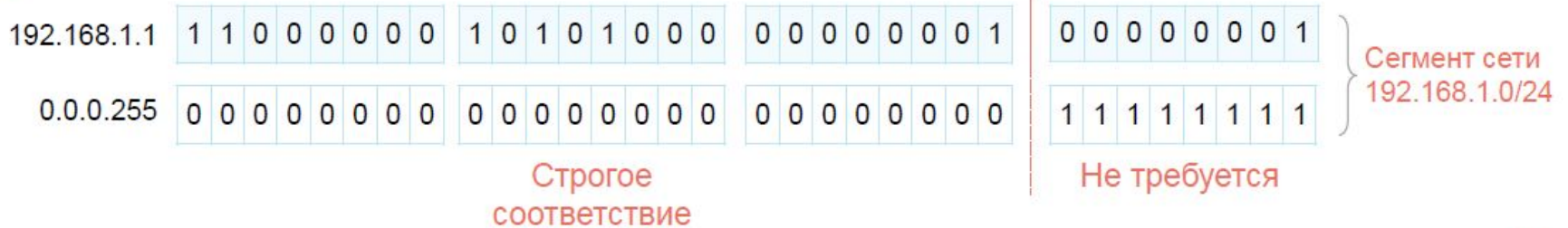
Подстановочная маска

- Подстановочная маска— это 32-битное число, которое указывает, какие биты в IP-адресе строго фиксированные, а какие нет.
- Подстановочная маска обычно представляется в виде десятичного числа с разделительными точками, так же, как и маска сети. Однако их значения различаются.

- Правило сопоставления

0: строгое соответствие; 1: не требуется

? Как сопоставить адрес сегмента сети, соответствующий 192.168.1.1/24?



0 и 1 могут быть в ЛЮБОМ месте

0 и 1 могут быть в ЛЮБОМ

месте

- Подстановочная маска может использоваться для сопоставления нечетных IP-адресов в сегменте сети 192.168.1.0/24, например 192.168.1.1, 192.168.1.3 и 192.168.1.5.

Строгое соответствие

Не требуется

Строгое соответствие

192.168.1	1							
192.168.1	0	0	0	0	0	0	0	1



192.168.1.1 0.0.0.254



Значения 1 или 0 в подстановочной маске могут быть непоследовательным.

192.168.1	3							
192.168.1	0	0	0	0	0	0	1	1

192.168.1	5							
192.168.1	0	0	0	0	0	1	0	1

Подстановочный знак

...

0.0.0.	1	1	1	1	1	1	1	0
--------	---	---	---	---	---	---	---	---

Специальная подстановочная маска

- Точно соответствует IP-адресу 192.168.1.1.
 $192.168.1.1 \text{ } 0.0.0.0 = 192.168.1.1 \text{ } 0$
- Соответствие всем IP-адресам.
 $0.0.0.0 \text{ } 255.255.255 = \text{any}$

Примеры применения шаблонной маски

IP-адрес 192.168.1.1 1100000.10101000.00000001.00000001

Wildcard Mask 0.0.0.0 0000000.00000000.00000000.00000000

Результат 192.168.1.1 1100000.10101000.00000001.00000001

- каждый бит в IPv4-адресе 192.168.1.1 должен точно совпадать

IP-адрес 192.168.1.1 1100000.10101000.00000001.00000001

WM 255.255.255.255 11111111.11111111.11111111.11111111

Результат 0.0.0.0 0000000.00000000.00000000.00000000

- Игнорировать все биты

Примеры применения шаблонной маски

IP-адрес 192.168.1.1 1100000.10101000.00000001.00000001

WMask 0.0.0.255 0000000.00000000.00000000.11111111

Результат 192.168.1.1 1100000.10101000.00000001.00000000

▣ любой узел в сети 192.168.1.0/24 будет совпадать

IP-адрес 192.168.16.0 1100000.10101000.00010000.00000000

WMask 0.0.15.255 0000000.00000000.00001111.11111111

Результат от 192.168.16.0 1100000.10101000.00010000.00000000
до 192.168.31.255 1100000.10101000.00011111.11111111

▣ диапазон адресов от 192.168.16.0 до 192.168.31.0

Примеры применения шаблонной маски

IP-адрес 192.168.1.0 1100000.10101000.00000001.00000000

WMask 0.0.254.255 0000000.00000000.11111110.11111111

Результат 192.168.1.0 1100000.10101000.00000001.00000000

- все узлы из нечетных подсетей основной сети 192.168.0.0

Расчет шаблонной маски

- маску для соответствия сетям 192.168.10.0 и 192.168.11.0

IP-адрес 192.168.10.0 11000000.10101000.00001010.00000000

IP-адрес 192.168.11.0 11000000.10101000.00001011.00000000

Маска 255.255.254.0 11111111.11111111.11111110.00000000

255.255.255.255 11111111.11111111.11111111.11111111

255.255.254.000 11111111.11111111.11111110.00000000

000.000.001.255 00000000.00000000.00000001.11111111

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

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

R1(config)# access-list 10 permit 192.168.10.0
0.0.1.255

Расчет шаблонной маски

- Разрешить сети 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
```

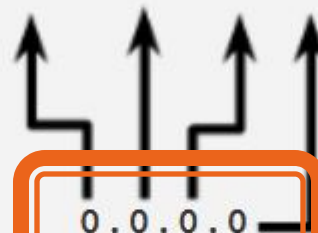
```
R1(config)# access-list 10 permit 192.168.16.0 0.0.15.255
```

Ключевые слова шаблонной маски

- 192.168.10.10 0.0.0.0 сопоставляет все биты адреса
- Шаблонную маску подсети можно сократить, указав ключевое слово `host` (`host 192.168.10.10`) перед IP-адресом

Шаблонная маска:

192.168.10.10



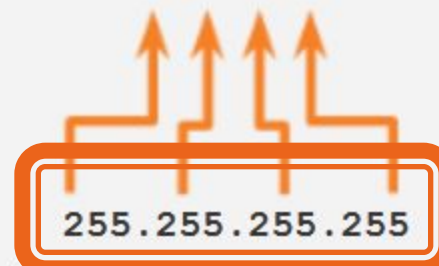
host

```
R1(config)# access-list 1 permit 192.168.10.10 0.0.0.0
R1(config)# access-list 1 permit host 192.168.10.10
```

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

Шаблонная маска:

0.0.0.0

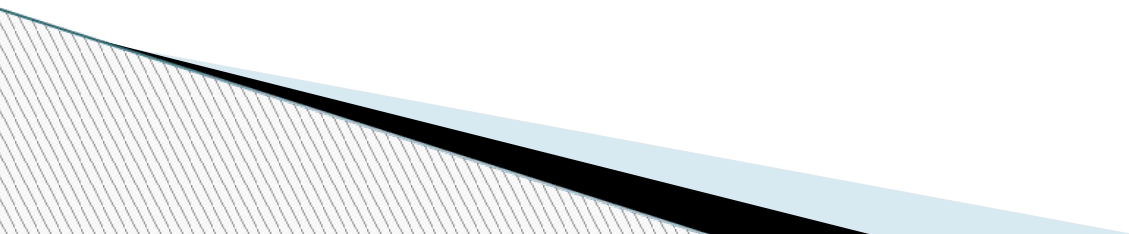


any

(Игнорировать все биты)

```
R1(config)# access-list 1 permit 0.0.0.0 255.255.255.255
R1(config)# access-list 1 permit any
```

Тест



Классификация и идентификация

Классификация ACL на основе методов определения правил ACL

Категория	Диапазон номеров	Описание
Базовый ACL	От 2000 до 2999	Определяет правила на основе IPv4-адресов источника, информации о фрагментации и эффективных временных диапазонов.
Расширенный	От 3000 до 3999	Определяет правила на основе адресов IPv4 источника и назначения, типов протокола IPv4, типов ICMP, номеров портов источника/назначения TCP, номеров портов источника/назначения UDP и эффективных временных диапазонов.
ACL 2-ого уровня	От 4000 до 4999	Определяет правила на основе информации в заголовках пакетов Ethernet, такой как MAC-адреса источника и назначения и типы протоколов 2-ого уровня.
ACL, определяемый пользователем	От 5000 до 5999	Определяет правила на основе заголовков пакетов, сдвигов, масок строк символов и строк символов, определяемых пользователем.
ACL пользователя	От 6000 до 6999	Определяет правила на основе IPv4-адресов источника или групп списка управления пользователем (UCL), IPv4-адресов или UCL-групп назначения, типов протокола IPv4, типов ICMP, номеров портов источника/назначения TCP и номеров портов источника/назначения UDP.

Классификация ACL на основе методов идентификации ACL

Категория	Описание
Нумерованный ACL	Традиционный метод идентификации ACL. Идентификация нумерованного ACL осуществляется по номеру.
Именованный ACL	Идентификация именованного ACL осуществляется по имени.

Нумерованные и именованные ACL-списки

- Нумерованный: номер присваивается в зависимости от того, какой протокол будет фильтроваться
 - Cisco 1 -99 и 1300-1999 стандартный ACL IPv4
 - Cisco 100 -199 и 2000-2699 расширенный ACL

Types	Value Ranges	Parameters
Basic	2000-2999	Source IP
Advanced	3000-3999	Source & Destination IP, Protocol, Source & Destination Port
Layer 2 ACL	4000-4999	MAC Address

- Именованный: имя присваивается для определения ACL
 - Буквенно-цифровые символы
 - Рекомендуются заглавные символы
 - Без пробелов и знаков препинания

Базовые (Стандартные) и расширенные ACL-списки

- Базовый ACL

Диапазон номеров:
от 2000 до 2999

IP-адрес источника		Заголовок IP	Заголовок TCP/UDP	Данные
acl number 2000				
rule	5	deny	source 10.1.1.1 0	
rule	10	deny	source 10.1.1.2 0	
rule	15	permit	source 10.1.1.0 0.0.0.255	

- Только по IP источника

- Расширенный ACL

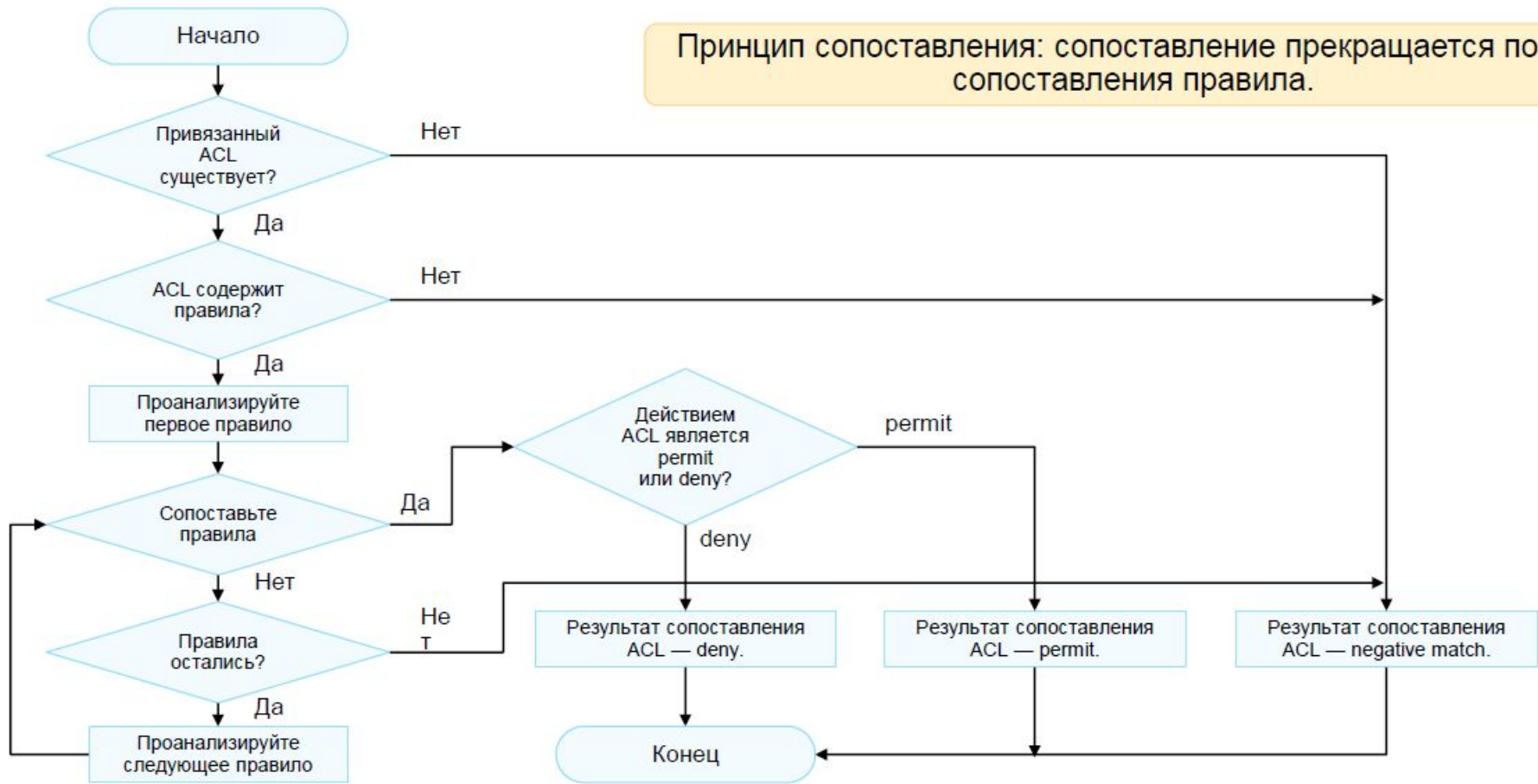
Диапазон номеров:
3000-3999

IP-адрес источника, IP-адрес назначения и тип протокола		Номера портов источника и назначения		Заголовок IP	Заголовок TCP/UDP	Данные
acl number 3000						
rule	5	permit	ip	source 10.1.1.0 0.0.0.255	destination 10.1.3.0 0.0.0.255	
rule	10	permit	tcp	source 10.1.2.0 0.0.0.255	destination 10.1.3.0 0.0.0.255	destination-port eq 21

- IP источника
- IP назначения
- Порт источника
- Порт назначения
- Тип (номер) протокола (IP, ICMP, UDP,...)

Механизм сопоставления ACL

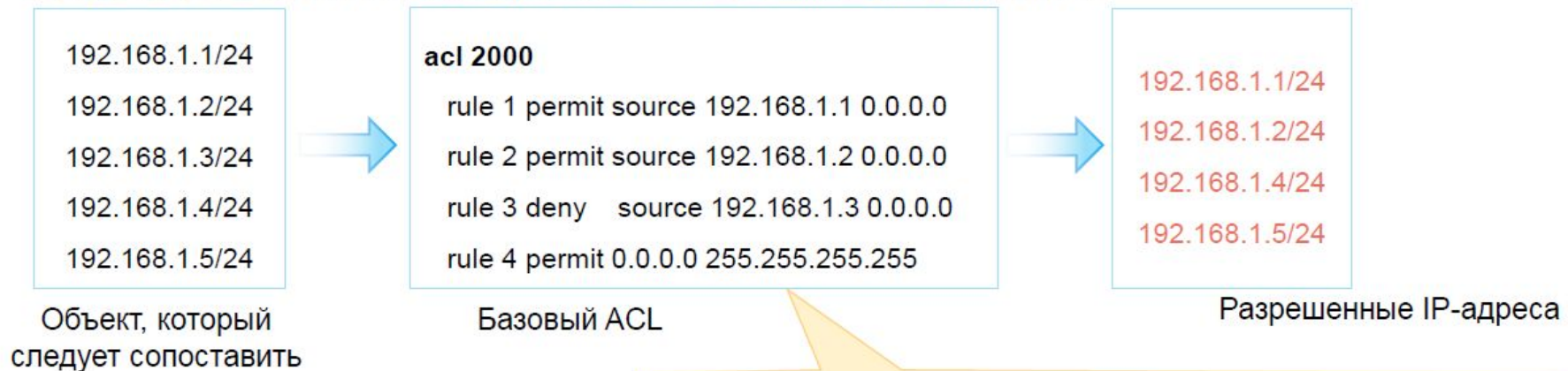
Принцип сопоставления: сопоставление прекращается после сопоставления правила.



Порядок и результат взаимодействия ACL

- Порядок конфигурации (режим config)

- Система сопоставляет пакеты с правилами ACL в порядке возрастания идентификатора правила. То есть в первую очередь обрабатывается правило с наименьшим идентификатором.

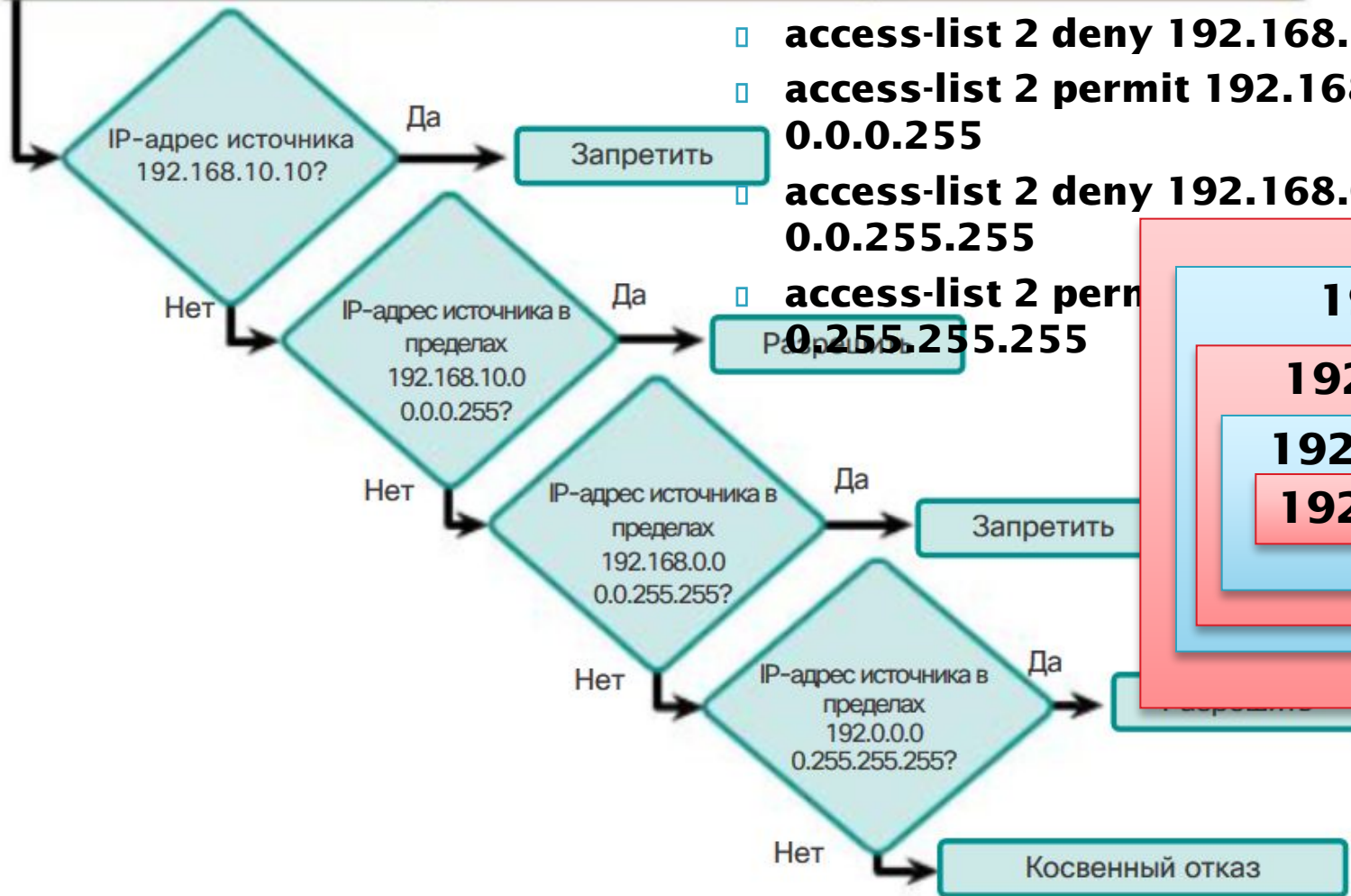
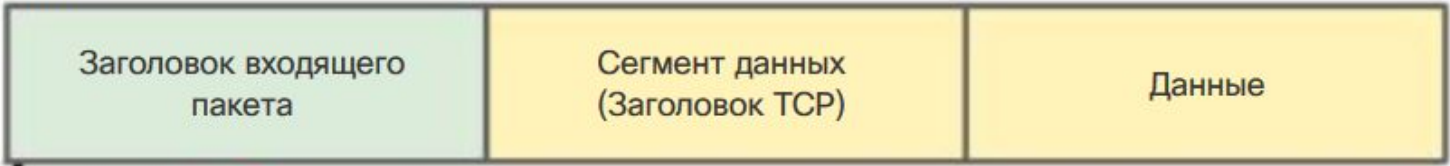


Означает ли permit, что трафик разрешен?

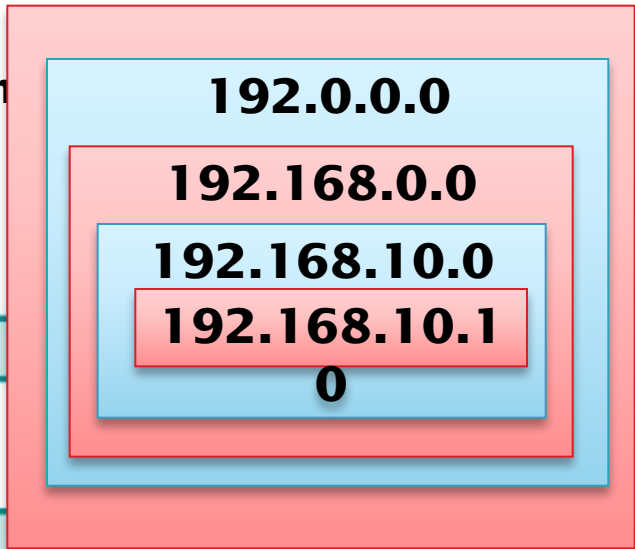
Правило 1: разрешает пакеты с IP-адресом источника 192.168.1.1.
Правило 2: разрешает пакеты с IP-адресом источника 192.168.1.2.
Правило 3: отклоняет пакеты с IP-адресом источника 192.168.1.3.
Правило 4: разрешает пакеты со всех остальных IP-адресов.

Порядок записей списка

G0/0

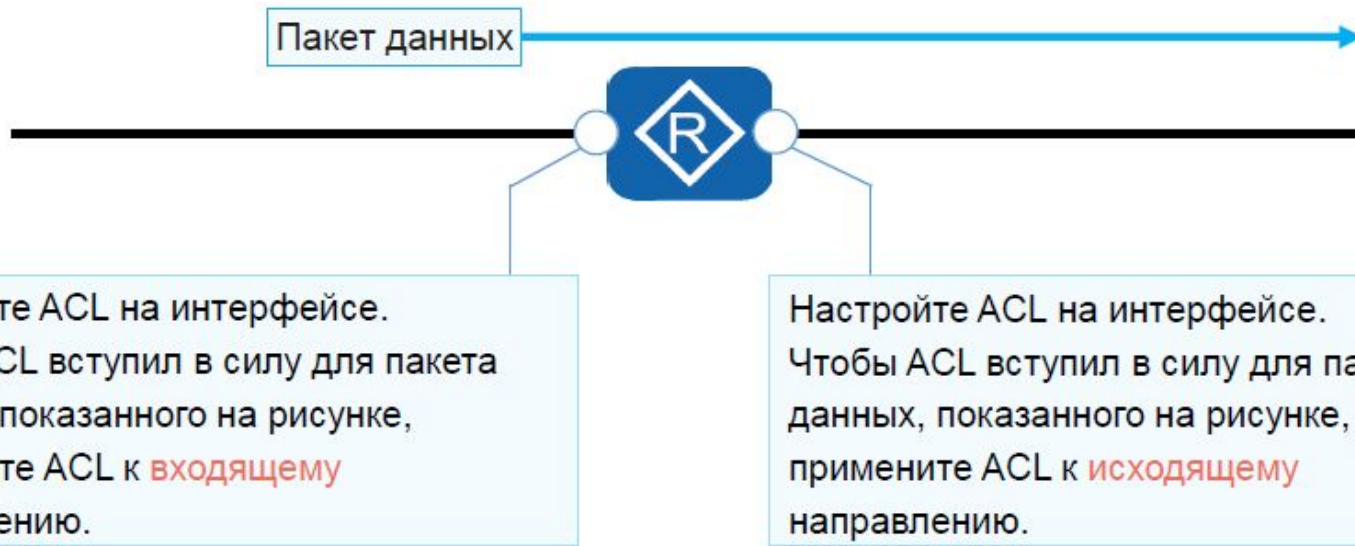
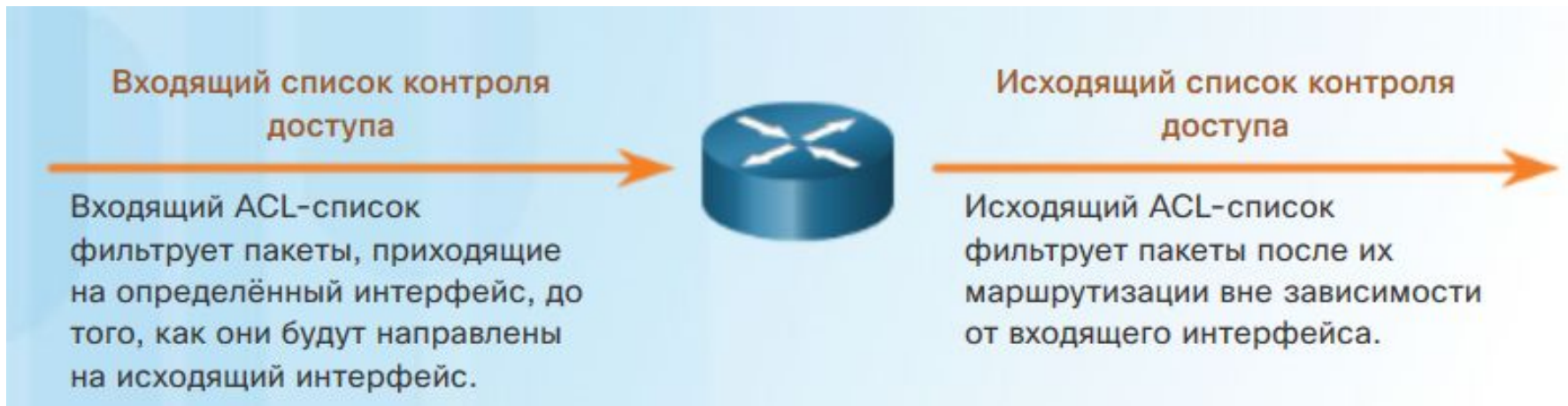


- ❑ **access-list 2 deny 192.168.10.10 0.0.0.0**
- ❑ **access-list 2 permit 192.168.10.0 0.0.0.255**
- ❑ **access-list 2 deny 192.168.0.0 0.0.255.255**
- ❑ **access-list 2 permit 192.0.0.0 0.255.255.255**



Возможно изменение порядка?

Входящий и исходящий ACL-списки

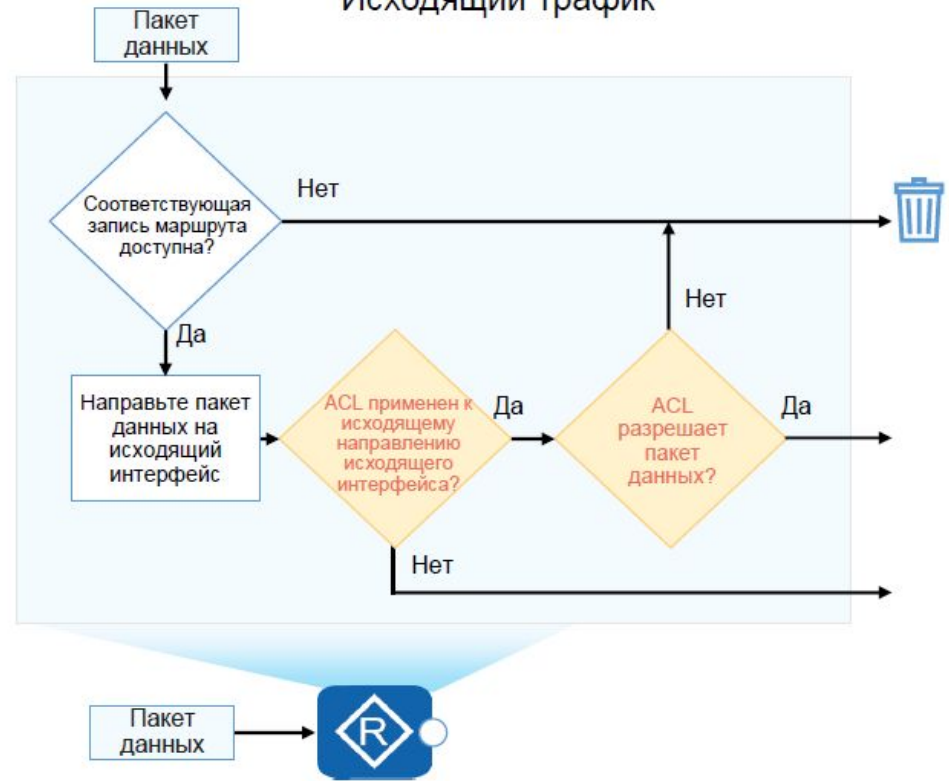


Входящий и исходящий трафик

Входящий трафик



Исходящий трафик



Рекомендации по применению: три правила



По одному списку для интерфейса, направления и протокола

Имея два интерфейса и два работающих протокола, этот маршрутизатор в целом мог бы иметь восемь отдельных ACL-списков.

Правила применения списков ACL

У вас может быть только один ACL-список на один протокол, интерфейс и направление:

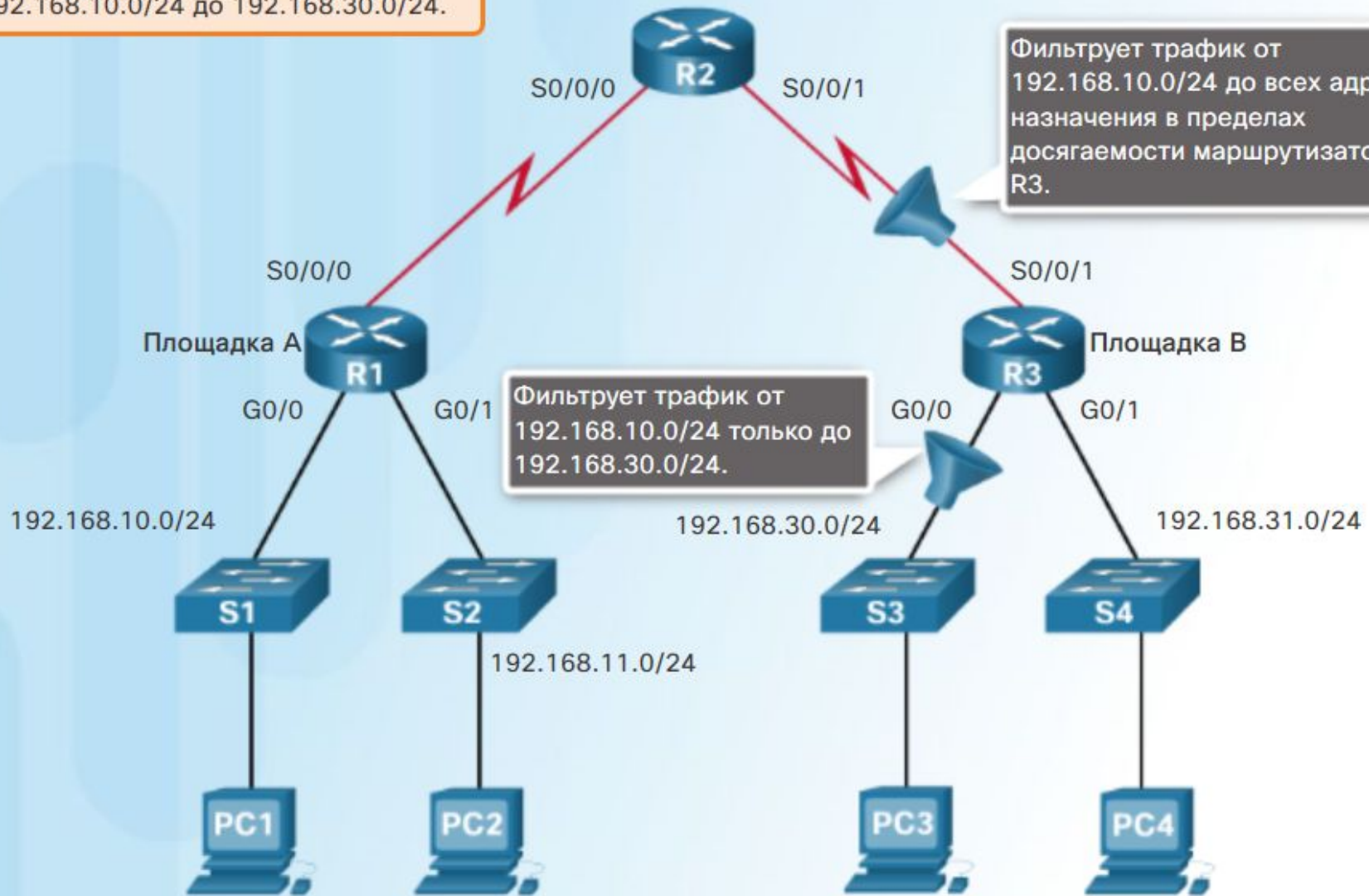
- Один ACL-список для одного протокола (например IPv4 или IPv6)
- Один ACL-список для одного направления (например IN или OUT)
- Один ACL-список для одного интерфейса (например, GigabitEthernet0/0)

Рекомендации по созданию

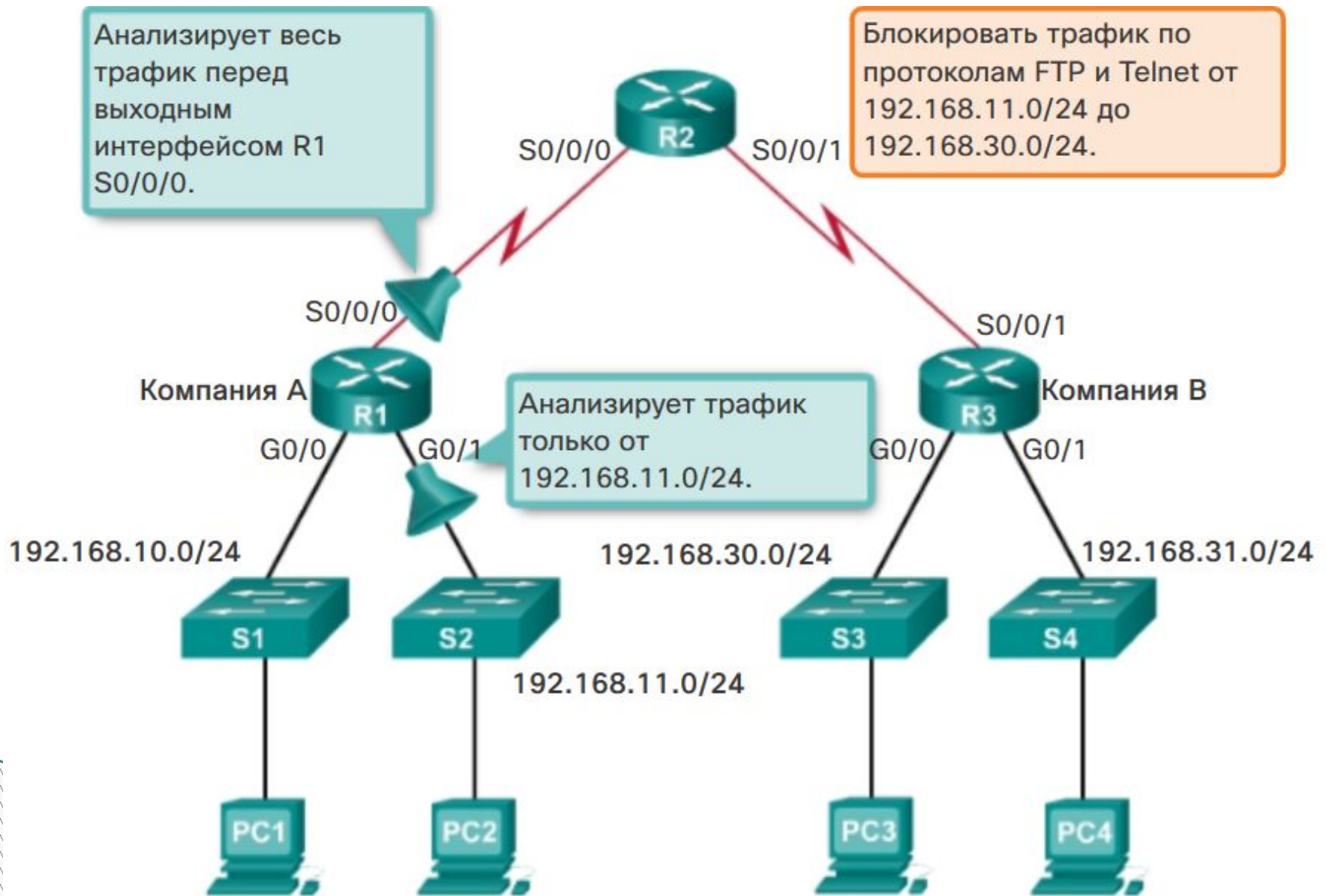
Рекомендации	Преимущество
Создавайте ACL-списки, исходя из корпоративной политики обеспечения информационной безопасности.	Соблюдение рекомендации обеспечивает соответствие требованиям информационной безопасности компании.
Подготовьте описание обязательных действий ваших ACL-списков.	Соблюдение рекомендации 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.

Размещение стандартного ACL

Блокировать весь трафик от 192.168.10.0/24 до 192.168.30.0/24.



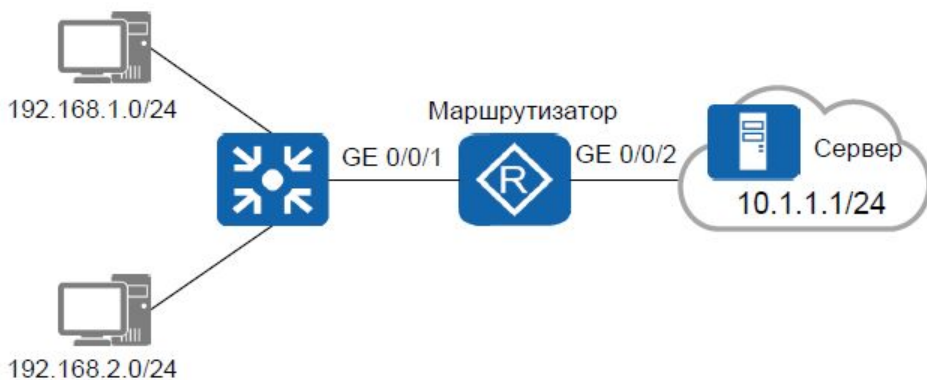
Размещение расширенного ACL



Размещение списков доступа

- И размещение и тип списка доступа может зависеть от :
- Сферы контроля сетевого администратора
- Пропускной способности задействованных сетей

Пример базового ACL



- Требования:

Чтобы предотвратить доступ хоста пользователя в сегменте 192.168.1.0/24 к сети, в которой находится сервер, настройте базовый ACL на маршрутизаторе. ACL должен запретить пакеты, IP-адреса источника которых находятся в сегменте сети 192.168.1.0/24, и разрешит другие пакеты.

1. Настройте IP-адреса и маршруты на маршрутизаторе.

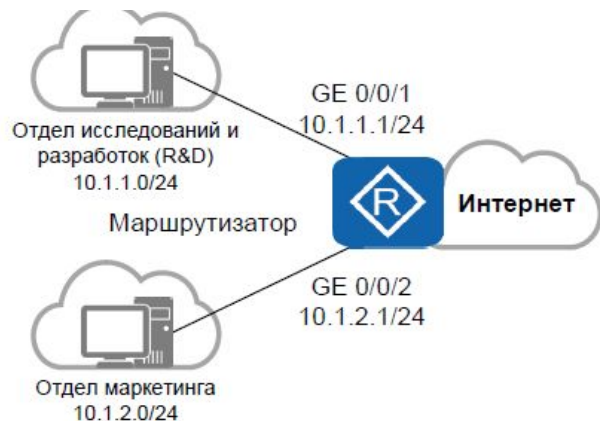
2. Настройте **базовый ACL** на маршрутизаторе, таким образом, что запретить доступ из сетевого сегмента 192.168.1.0/24 к сети, в которой находится сервер.

```
[Router] acl 2000
[Router-acl-basic-2000] rule deny source 192.168.1.0 0.0.0.255
[Router-acl-basic-2000] rule permit source any
```

3. Настройте фильтрацию трафика **во входящем направлении** GE 0/0/1.

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] traffic-filter inbound acl 2000
[Router-GigabitEthernet0/0/1] quit
```

Пример расширенного ACL-1



1. Настройте IP-адреса и маршруты на маршрутизаторе.
2. Создайте ACL 3001 и настройте правила для ACL, чтобы запретить трафик из отдела исследований и разработок в отдел маркетинга.

```
[Router] acl 3001
[Router-acl-adv-3001] rule deny ip source 10.1.1.0 0.0.0.255
destination 10.1.2.0 0.0.0.255
[Router-acl-adv-3001] quit rule permit ip any any
```

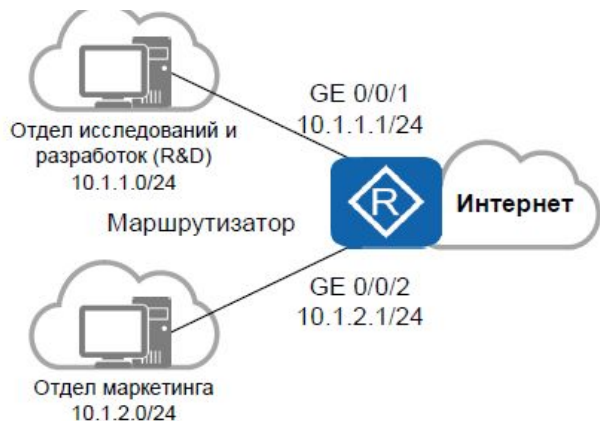
3. Создайте ACL 3002 и настройте правила для ACL, чтобы отклонять пакеты из отдела маркетинга в отдел исследований и разработок.

```
[Router] acl 3002
[Router-acl-adv-3002] rule deny ip source 10.1.2.0 0.0.0.255
destination 10.1.1.0 0.0.0.255
[Router-acl-adv-3002] quit rule permit ip any any
```

Требования:

- Отделы компании связаны через маршрутизатор. Чтобы упростить управление сетью, администратор выделяет IP-адреса различных сегментов сети отделу исследований и разработок и отделу маркетинга.
- Компания требует, чтобы маршрутизатор не допускал обмен данными между пользовательскими хостами в разных сегментах сети для обеспечения информационной безопасности.

Пример расширенного ACL-2



4. Настройте фильтрацию трафика во входящем направлении GE 0/0/1 и GE 0/0/2.

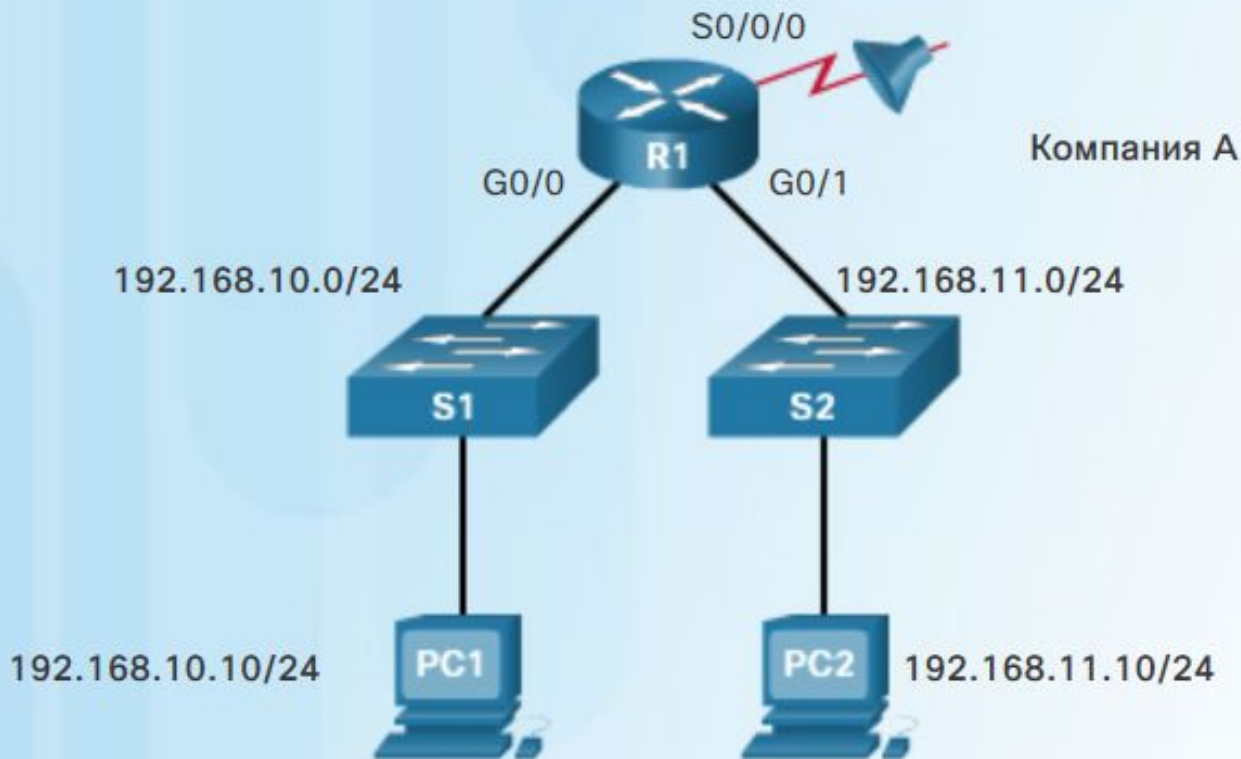
```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] traffic-filter inbound acl 3001
[Router-GigabitEthernet0/0/1] quit

[Router] interface GigabitEthernet 0/0/2
[Router-GigabitEthernet0/0/2] traffic-filter inbound acl 3002
[Router-GigabitEthernet0/0/2] quit
```

Требования:

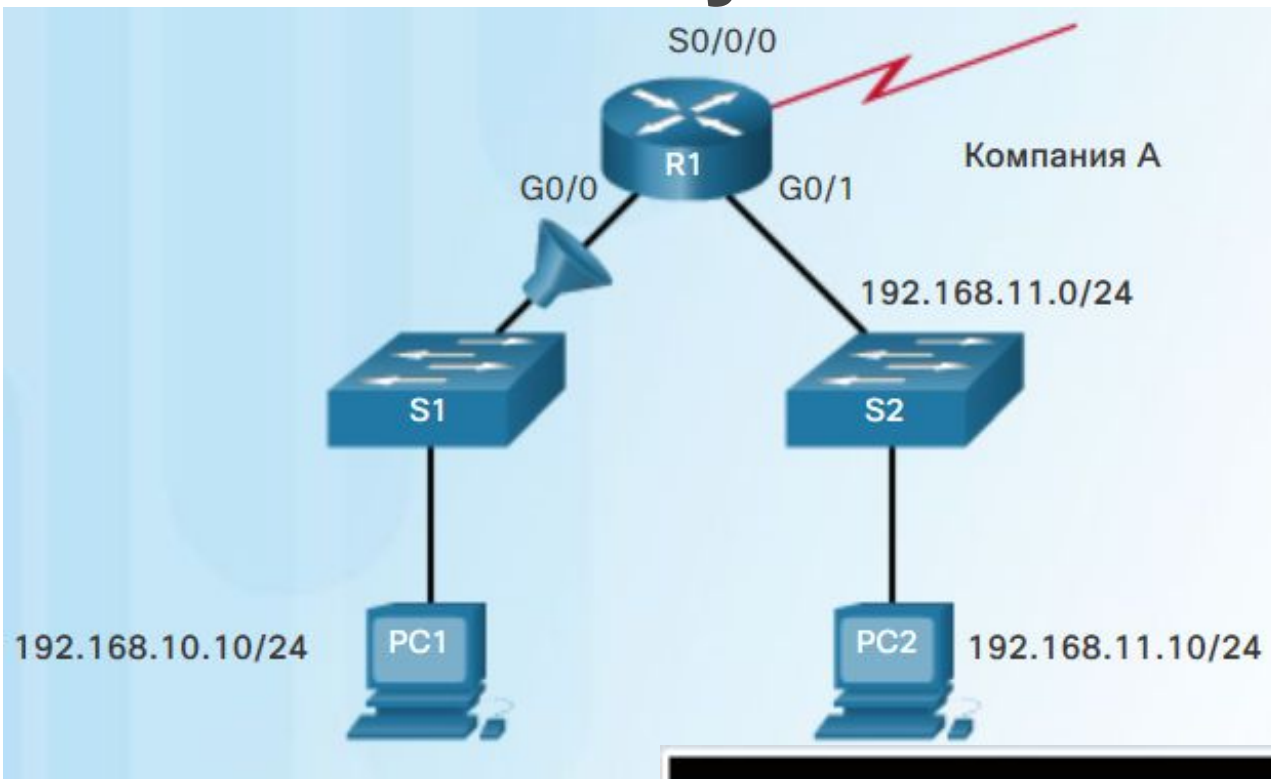
- Отделы компании связаны через маршрутизатор. Чтобы упростить управление сетью, администратор выделяет IP-адреса различных сегментов сети отделу исследований и разработок и отделу маркетинга.
- Компания требует, чтобы маршрутизатор не допускал обмен данными между пользовательскими хостами в разных сегментах сети для обеспечения информационной безопасности.

Применение нумерованного списка доступа Cisco



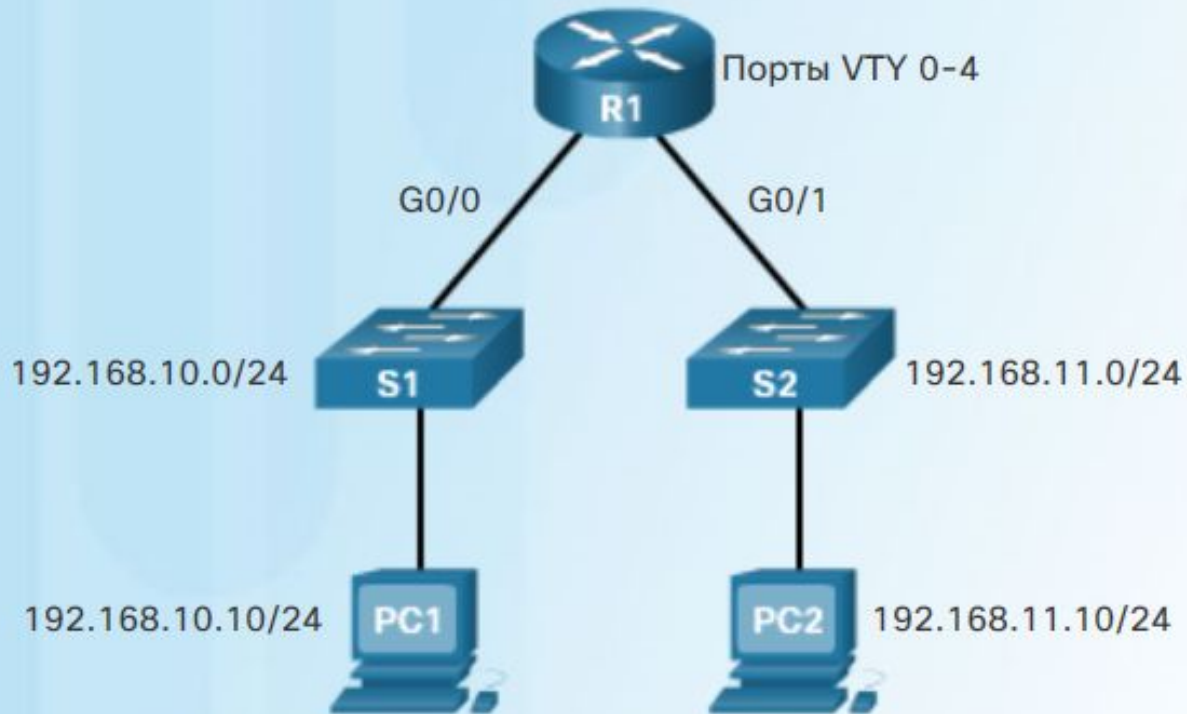
```
R1(config)# no access-list 1
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 1 out
```

Применение именованного списка доступа Cisco



```
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
```

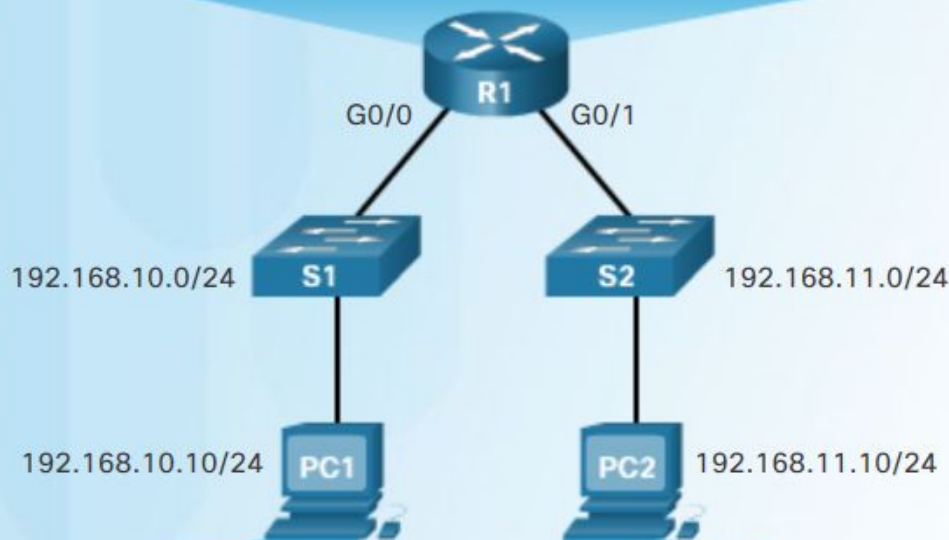
Команда access-class Cisco



```
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
```

Проверка настройки безопасности vty Cisco

```
R1# show access-lists
Standard IP access list 21
 10 permit 192.168.10.0, wildcard bits 0.0.0.255 (2 matches)
 20 deny any (1 match)
R1#
```



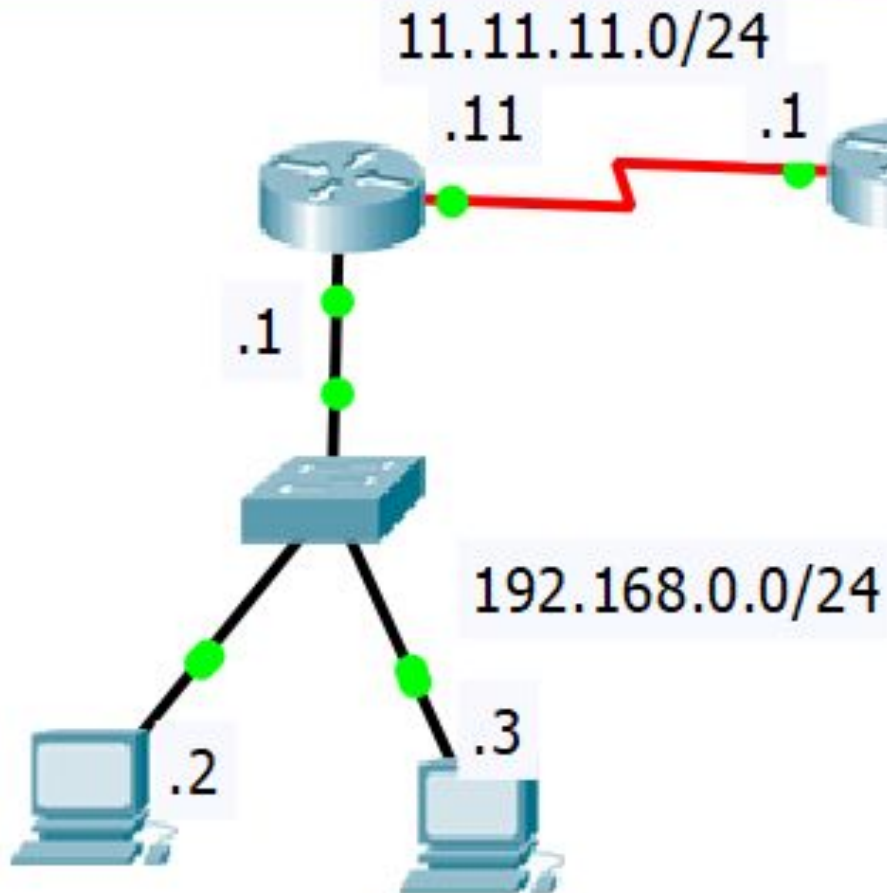
```
PC1>ssh 192.168.10.1
```

```
Login as: admin
Password: ****
R1>
```

```
PC2>ssh 192.168.11.1
ssh connect to host 192.168.11.1 port
22: Connection refused
```

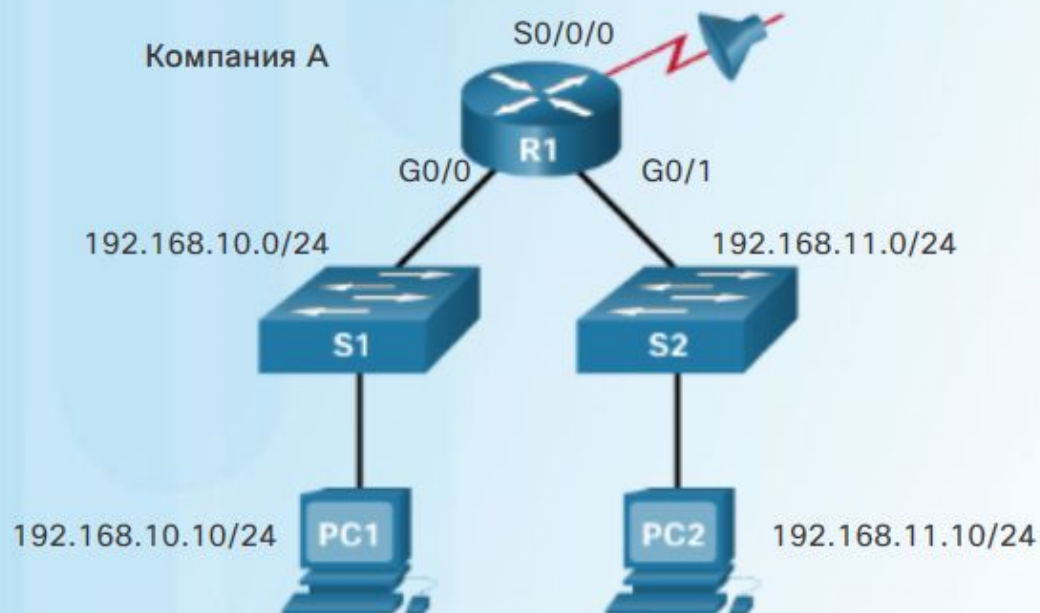
```
PC2>
```

Пример по 8 лабораторной работе



- R1(config)# ip access-list standard ADMIN-MGT
 - R1(config-std-nacl)# permit host 192.168.0.3
 - R1(config-std-nacl)# exit
- Примените список доступа на каналах vty.
- R1(config)# line vty 0 15
 - R1(config-line)# access-class ADMIN-MGT in
 - R1(config-line)# exit
 - R1# show ip access-lists
 - Standard IP access list ADMIN-MGT
 - 10 permit 192.168.0.3 (2 matches)

Последняя запись списка



□ Последняя запись deny

ACL-список 1

```
R1(config)# access-list 1 permit ip 192.168.10.0 0.0.0.255
```

ACL-список 2

```
R1(config)# access-list 2 permit ip 192.168.10.0 0.0.0.255  
R1(config)# access-list 2 deny any
```

ACL-списки для IPv6

- 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.
- Отсутствие шаблонных масок
- К `deny ipv6 any any IPv6` также включает два других косвенных условия по умолчанию:
 - `permit icmp any any nd-na`
 - `permit icmp any any nd-ns`