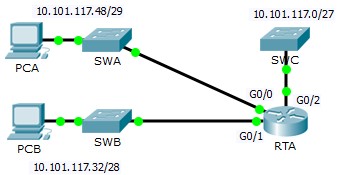
**Packet Tracer. Настройка расширенных списков контроля доступа (ACL). Сценарий 2**

# Топология



# Таблица адресации



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** | **Шлюз по умолчанию** |
| RTA | G0/0 | 10.101.117.49 | 255.255.255.248 | Н/П |
| G0/1 | 10.101.117.33 | 255.255.255.240 | Н/П |
| G0/2 | 10.101.117.1 | 255.255.255.224 | Н/П |
| PCA | NIC | 10.101.117.51 | 255.255.255.248 | 10.101.117.49 |
| PCB | NIC | 10.101.117.35 | 255.255.255.240 | 10.101.117.33 |
| SWA | VLAN 1 | 10.101.117.50 | 255.255.255.248 | 10.101.117.49 |
| SWB | VLAN 1 | 10.101.117.34 | 255.255.255.240 | 10.101.117.33 |
| SWC | VLAN 1 | 10.101.117.2 | 255.255.255.224 | 10.101.117.1 |

# Задачи

**Часть 1. Настройка, применение и проверка расширенного нумерованного списка ACL**

**Часть 2. Вопросы для повторения**

# Исходные данные/сценарий

В этом сценарии устройствам в одной локальной сети разрешен удаленный доступ к устройствам в другой локальной сети по протоколу SSH. Весь трафик из других сетей, кроме ICMP, отклоняется.

На коммутаторах и маршрутизаторе также были предварительно настроены следующие параметры.

* Пароль привилегированного доступа: **ciscoenpa55**
* Пароль консоли: **ciscoconpa55**
* Имя локального пользователя и пароль: **Admin**/**Adminpa55**

# Часть 1: Настройка, применение и проверка расширенного нумерованного списка ACL

Настройте, примените и проверьте список ACL в соответствии со следующей политикой.

* Разрешен трафик SSH с устройств в сети 10.101.117.32/28 к устройствам в сетях 10.101.117.0/27.

©

**Packet Tracer. Настройка расширенных списков контроля доступа (ACL). Сценарий 2**

* Разрешен трафик ICMP от любого источника к любому месту назначения.
* Весь прочий трафик, направляющийся в сети 10.101.117.0/27, блокируется..

**Шаг 1: Настройте расширенный список ACL.**

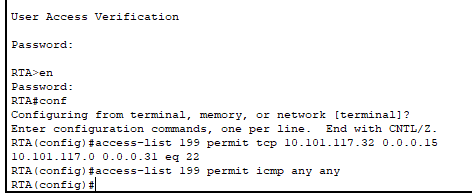
1. В соответствующем режиме настройки на маршрутизаторе RTA используйте последний допустимый номер расширенного списка контроля доступа для настройки ACL. Создайте первый оператор ACL согласно следующим инструкциям.
   1. Последний номер расширенного списка – 199.
   2. Протокол – TCP.
   3. Сеть источника – 10.101.117.32.
   4. Чтобы определить шаблонную маску, можно вычесть 255.255.255.240 из 255.255.255.255.
   5. Сеть назначения – 10.101.117.0.
   6. Чтобы определить шаблонную маску, можно вычесть 255.255.255.224 из 255.255.255.255.
   7. Протокол – SSH (порт 22).

Каков первый оператор ACL?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Трафик ICMP разрешен, требуется второй оператор ACL. Используйте тот же номер списка контроля доступа для разрешения всего трафика ICMP, независимо от адресов источника и назначения. Каков второй оператор ACL? (Подсказка. Используйте ключевые слова **any**.)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Весь прочий IP-трафик отклоняется по умолчанию.
2. 

**Шаг 2: Примените расширенный список ACL.**

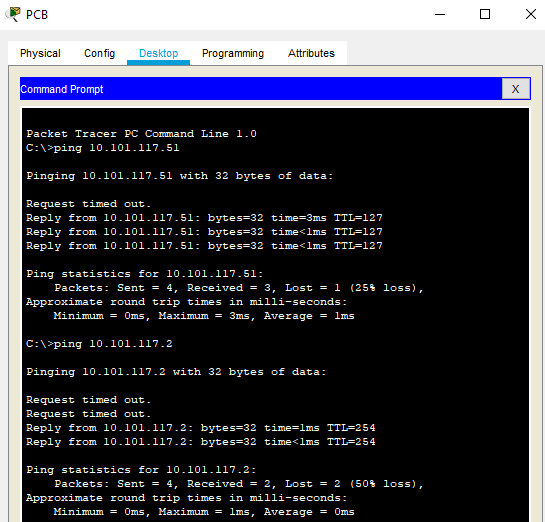
Как правило, расширенные списки ACL размещаются рядом с источником. Но поскольку список доступа 199 затрагивает трафик, поступающий из сетей 10.101.117.48/29 и 10.101.117.32/28, лучше всего разместить этот список ACL на интерфейсе Gigabit Ethernet 0/2 в исходящем направлении. Какая команда позволяет применить ACL 199 к интерфейсу Gigabit Ethernet 0/2?



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Шаг 3: Проверьте реализацию расширенного списка ACL.**

1. Отправьте эхо-запрос с компьютера **PCB** на все прочие IP-адреса в сети. Если эхо-запросы завершаются неудачно, проверьте IP-адреса, прежде чем продолжить.

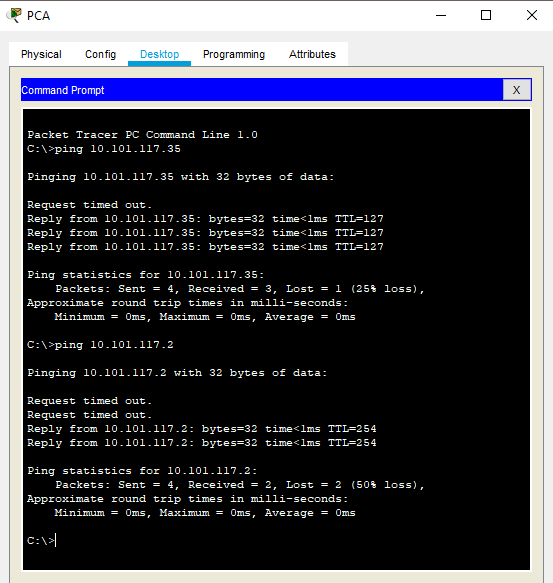


1. Установите SSH-подключение с компьютера **PCB** к коммутатору **SWC**. Имя пользователя – **Admin**, пароль – **Adminpa55**.

PC> **ssh -l Admin 10.101.117.2**



1. Выйдите из SSH-сеанса с коммутатором SWC.
2. Отправьте эхо-запрос с компьютера **PCA** на все прочие IP-адреса в сети. Если эхо-запросы завершаются неудачно, проверьте IP-адреса, прежде чем продолжить.

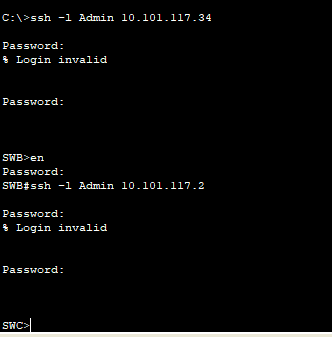


1. Установите SSH-подключение с компьютера **PCA** к коммутатору **SWC**. В соответствии со списком контроля доступа маршрутизатор отклоняет подключение.



1. Установите SSH-подключение с компьютера **PCA** к коммутатору **SWB**. Список контроля доступа размещен на интерфейсе **G0/2** и не влияет на это подключение. Имя пользователя – **Admin**, пароль – **Adminpa55**.
2. Войдите на коммутатор **SWB** иневыходите из системы. Установите SSH-подключение к коммутатору **SWC** в привилегированном режиме.

SWB# **ssh -l Admin 10.101.117.2**



©

**Packet Tracer. Настройка расширенных списков контроля доступа (ACL). Сценарий 2**

# Часть 2: Вопросы для повторения

1. Каким образом компьютер PCA смог обойти список контроля доступа 199 и установить SSH-подключение к коммутатору SWC?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Так, пінг успішний і так, поведінка правильна. Політика безпеки, що діє в R3, блокує трафік, що надходить з Інтернету, що надходить у зони INSIDE або CONFROOM. Поки R3 розглядає пакети ICMP, генеровані PC-A, як трафік, що походить з Інтернету, пакети ICMP націлені на власний IP-адресу R3, призначений G0 / 1. Усі власні IP-адреси R3 (10.2.2.1, 192.168.33.1 та 192.168.3.1) вважаються частиною зони Я. Оскільки для самозони явно не налаштовано жодних політик, R3 дотримується поведінки за замовчуванням і дозволяє пакети.

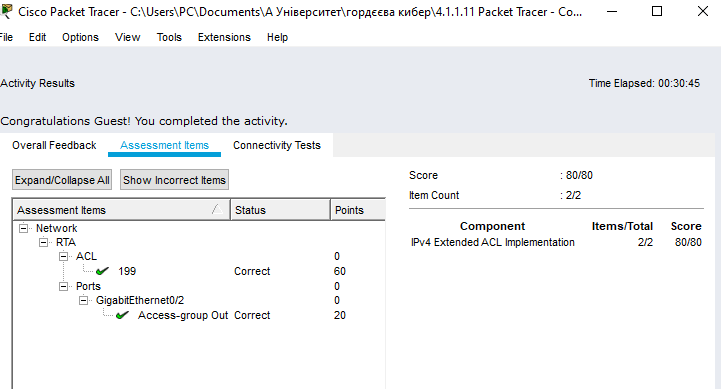
1. Как можно было бы предотвратить косвенный доступ PCA к коммутатору SWC, при этом разрешив SSH-доступ компьютера PCB к SWC?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Так, пінг успішний і так, поведінка правильна. Політика безпеки, що застосовується в R3, блокує трафік, що надходить у зону ВНУТРІ. Поки R3 розглядає пакети ICMP, генеровані PC-C, як трафік, що походить від ConfRoom, пакети ICMP націлені на власний IP-адресу R3, призначений G0 / 1. Усі власні IP-адреси R3 (10.2.2.1, 192.168.33.1 та 192.168.3.1) вважаються частиною зони Я. Оскільки для самозони явно не налаштовано жодних політик, R3 дотримується поведінки за замовчуванням і дозволяє пакети.



**Предлагаемый способ подсчета баллов**

|  |  |  |  |
| --- | --- | --- | --- |
| **Раздел задания** | **Расположение вопроса** | **Возможное количество баллов** | **Заработанные баллы** |
| Часть 1. Настройка, применение и проверка расширенного нумерованного списка ACL | Шаг 1a | 4 |  |
| Шаг 1b | 4 |  |
| Шаг 2 | 4 |  |
| **Всего по части 1** | | 12 |  |
| Часть 2. Вопросы для повторения | Вопрос 1 | 4 |  |
| Вопрос 2 | 4 |  |
| **Всего по части 2** | | 8 |  |
| **Баллы по Packet Tracer** | | 80 |  |
| **Общее число баллов** | | 100 |  |

©