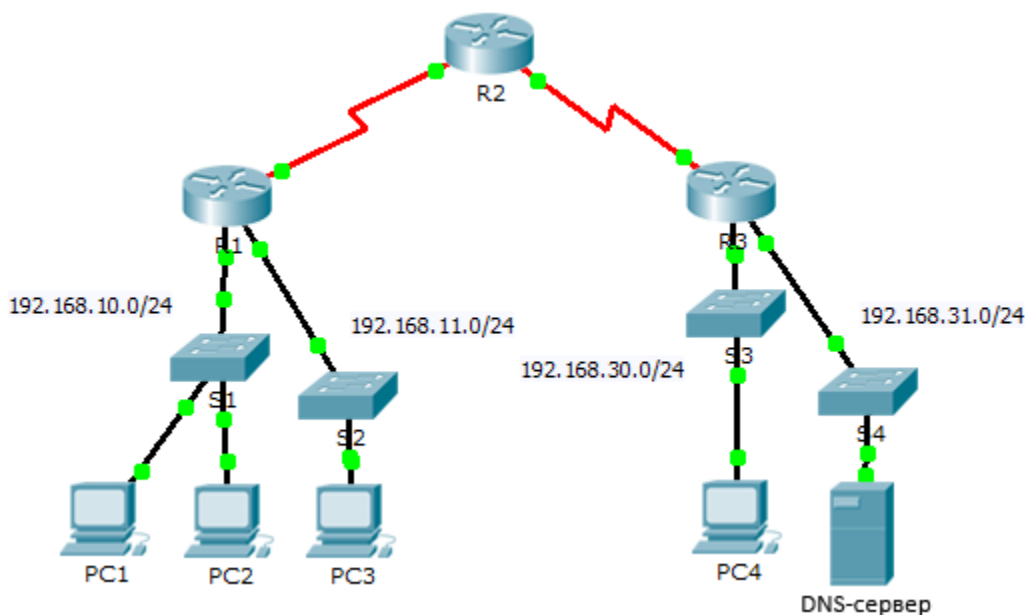


Packet Tracer. Наглядное представление работы ACL-списка

Топология



Задачи

Часть 1. Проверка локального подключения и тестирование работы списка контроля доступа

Часть 2. Удаление списка контроля доступа и повторное тестирование

Исходные данные

В рамках этого задания вы получите представление о том, как можно использовать список контроля доступа (ACL) для запрещения эхо-запросов, отправленных на узлы удалённых сетей. После удаления ACL-списка из конфигурации эхо-запросы будут успешными.

Часть 1. Проверка локального подключения и тестирование списка контроля доступа

Шаг 1: Отправьте эхо-запросы по локальной сети, чтобы проверить подключение.

- Из командной строки узла **PC1** отправьте эхо-запрос на **PC2**.
- Из командной строки узла **PC1** отправьте эхо-запрос на **PC3**.

Почему эхо-запросы прошли успешно?

Шаг 2: Отправьте эхо-запросы в удалённые сети, чтобы протестировать работу ACL-списка.

- a. Из командной строки узла **PC1** отправьте эхо-запрос на **PC4**.
- b. Из командной строки узла **PC1** отправьте эхо-запрос на **DNS-сервер**.

Почему эхо-запросы были выполнены неудачно? (Совет. Чтобы узнать источник проблемы, используйте режим моделирования или просмотрите конфигурации маршрутизатора).

Часть 2. Удаление ACL-списка и повторное тестирование

Шаг 1: Используйте команды show, чтобы проверить конфигурацию ACL-списка.

- a. Используйте команды **show run** и **show access-lists**, чтобы просмотреть текущие ACL-списки. Для быстрого просмотра текущих ACL-списков используйте команду **show access-lists**. Введите команду **show access-lists**, после которой нажмите ПРОБЕЛ и поставьте вопросительный знак (?), чтобы просмотреть доступные параметры:

```
R1#show access-lists ?
  <1-199>  ACL number
  WORD     ACL name
  <cr>
```

Если вы знаете номер или имя ACL-списка, вы можете дополнительно отфильтровать выходные данные команды **show**. Однако, маршрутизатор **R1** обладает только одним списком контроля доступа; поэтому команды **show access-lists** будет достаточно.

```
R1#show access-lists
Extended IP access list 101
  deny icmp any any echo
  permit ip any any
```

Первая строка ACL-списка запрещает передачу эхо-запросов ICMP из **любого** источника к **любому** месту назначения. Вторая строка списка пропускает остальной IP-трафик, направленный от **любого** источника к **любому** месту назначения (ip any any).

- b. Для работы ACL-списка на маршрутизаторе, его необходимо применить. В этом сценарии ACL-список используется для фильтрации трафика на интерфейсе. Несмотря на возможность просматривать сведения об IP с помощью команды **show ip interface**, в некоторых случаях эффективнее использовать команду **show run**. К какому интерфейсу применяется ACL-список при использовании одной или обеих команд? _____

Шаг 2: Удаление списка доступа 101 из конфигурации

ACL-список можно удалить из конфигурации, применив команду **no access list [номер списка ACL]**. В то время как применение команды **no access-list** приводит к удалению всех ACL-списков, настроенных на маршрутизаторе, команда **no access-list [номер списка контроля доступа]** позволяет удалить конкретный список контроля доступа.

- a. В режиме глобальной конфигурации удалите ACL-список посредством следующей команды:

```
R1(config)# no access-list 101
```

- b. Убедитесь, что теперь узел **PC1** может отправить эхо-запрос на **DNS-сервер**.

Предлагаемый способ подсчёта баллов

Пункт, содержащий вопрос	Возможное количество баллов	Количество заработанных баллов
Часть 1, шаг 1b.	50	
Часть 1, шаг 2b.	40	
Часть 2, шаг 2b.	10	
Общее количество баллов	100	