Packet Tracer. Настройка стандартных ACL-списков

Топология

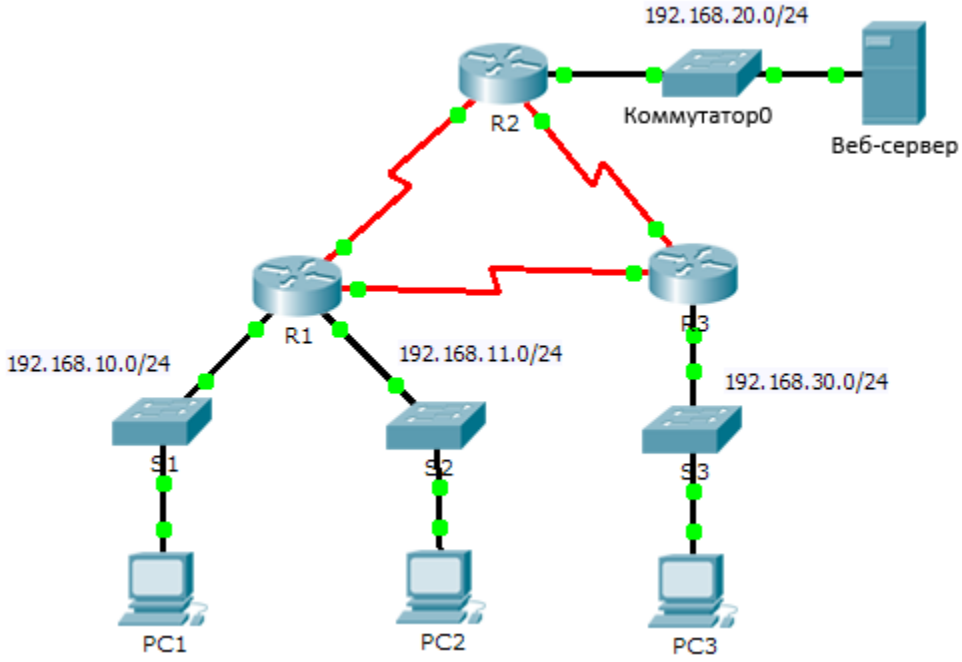

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	F0/0	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	F0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.3.3.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
WebServer	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Задачи

Часть 1. Планирование реализации ACL-списка

Часть 2. Настройка, применение и проверка стандартных ACL-списков

Исходные данные/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).

Часть 1. Планирование реализации ACL-списка

Шаг 1: Изучите текущую конфигурацию сети.

Перед применением каких-либо ACL-списков к сети важно убедиться в наличии полного подключения. Убедитесь в том, что обеспечено полное подключение сети, выбрав ПК и отправив с него эхо-запросы на другие устройства в этой сети. Эхо-запросы на каждое устройство должны быть успешными.

Шаг 2: Исследуйте правила сетевой безопасности и разработайте план реализации ACL-списка.

a. На маршрутизаторе **R2** реализованы следующие правила сетевой безопасности:

- Для сети 192.168.11.0/24 запрещён доступ к **веб-серверу** в сети 192.168.20.0/24.
- Другие виды доступа разрешены.

Чтобы ограничить доступ из сети 192.168.11.0/24 к **веб-серверу** в сети 192.168.20.254 без нарушения передачи остального трафика, на маршрутизаторе **R2** следует создать и применить ACL-список. Список доступа должен быть размещён на исходящем интерфейсе по направлению к **веб-серверу**. Чтобы разрешить остальной трафик, на маршрутизаторе R2 следует создать второе правило.

b. На маршрутизаторе **R3** реализованы следующие правила сетевой безопасности:

- Сеть 192.168.10.0/24 не может обмениваться данными с сетью 192.168.30.0/24.
- Другие виды доступа разрешены.

Чтобы ограничить доступ из сети 192.168.10.0/24 к сети 192.168.30/24 без нарушения передачи остального трафика, на маршрутизаторе **R3** следует создать и применить ACL-список. ACL-список должен быть размещён на исходящем интерфейсе по направлению к узлу **PC3**. Чтобы разрешить остальной трафик, на маршрутизаторе **R3** следует создать второе правило.

Часть 2. Настройка, применение и проверка стандартных ACL-списков

Шаг 1: Настройте и примените нумерованный стандартный ACL-список на маршрутизаторе R2.

a. Создайте ACL-список с номером 1 на маршрутизаторе **R2**, установив запрет доступа к сети 192.168.20.0/24 от сети 192.168.11.0/24.

```
R2(config)# access-list 1 deny 192.168.11.0 0.0.0.255
```

b. По умолчанию список доступа отклоняет трафик, не соответствующий заданному правилу. Чтобы разрешить другой трафик, задайте следующее правило:

```
R2(config)# access-list 1 permit any
```

c. Чтобы ACL-список осуществлял фильтрацию трафика, он должен быть применён на каком-либо маршрутизаторе. Примените ACL-список, разместив его для исходящего трафика интерфейса Gigabit Ethernet 0/0.

```
R2(config)# interface GigabitEthernet0/0
R2(config-if)# ip access-group 1 out
```

Шаг 2: Настройте и примените нумерованный стандартный ACL-список на маршрутизаторе R3.

a. Создайте ACL-список под номером 1 на маршрутизаторе **R3**, установив запрет доступа к сети 192.168.30.0/24 от сети узла **PC1** (192.168.10.0/24).

```
R3(config)# access-list 1 deny 192.168.10.0 0.0.0.255
```

b. По умолчанию список доступа отклоняет трафик, не соответствующий заданному правилу. Чтобы разрешить остальной трафик, создайте второе правило для списка ACL 1.

```
R3(config)# access-list 1 permit any
```

c. Примените ACL-список, разместив его для исходящего трафика интерфейса Gigabit Ethernet 0/0.

```
R3(config)# interface GigabitEthernet0/0
R3(config-if)# ip access-group 1 out
```

Шаг 3: Проверьте конфигурацию и работоспособность списка ACL.

a. На маршрутизаторах **R2** и **R3** введите команду **show access-list**, чтобы проверить конфигурации ACL-списков. Введите команду **show run** или **show ip interface gigabitethernet 0/0**, чтобы проверить размещения ACL-списков.

b. При размещении двух ACL-списков сетевой трафик фильтруется в соответствии с правилами, описанными в части 1. Для проверки реализаций ACL-списков выполните следующие проверки:

- Эхо-запрос с 192.168.10.10 к 192.168.11.10 прошёл успешно.
- Эхо-запрос с 192.168.10.10 к 192.168.20.254 прошёл успешно.
- Сбой эхо-запроса с 192.168.11.10 к 192.168.20.254.
- Сбой эхо-запроса с 192.168.10.10 к 192.168.30.10.
- Эхо-запрос с 192.168.11.10 к 192.168.30.10 прошёл успешно.
- Эхо-запрос с 192.168.30.10 к 192.168.20.254 прошёл успешно.