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

**Шаг 1.     Отправьте ping-запросы по локальной сети, чтобы проверить подключение.**

a)     Из командной строки **PC1** отправьте ping-запрос на **PC2**.

б)    Из командной строки **PC1** отправьте ping-запрос на **PC3**.

Почему ping-запросы прошли успешно?

Поскольку уровни с 1 по 3 полностью функциональны, и нет ничего, что фильтровало бы сообщения ICMP между двумя локальными сетями.

**Шаг 2.     Отправьте ping-запросы в удаленные сети, чтобы протестировать работу списка контроля доступа.**

a)     Из командной строки **PC1** отправьте ping-запрос на **PC4**.

б)    Из командной строки узла **PC1** отправьте ping-запрос на **DNS-сервер**.

Почему возникает сбой при отправке ping-запросов? (Подсказка. Для анализа используйте режим моделирования или просмотрите конфигурации маршрутизатора.)

Сбои эхо-запросов не выполняются, поскольку R1 настроен с ACL, чтобы запретить любому эхо-тесту выход из Serial 0/0/0.

**Часть 2.     Удаление списка контроля доступа и повторное тестирование**

**Шаг 1.     Используйте команды show, чтобы проверить конфигурацию списка контроля доступа.**

а)     Используйте команды**show run** и**show access-lists**, чтобы просмотреть текущие списки контроля доступа. 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

Имя ACL-списка СЛОВО

<cr>

Если вы знаете номер или имя ACL-списка, вы можете дополнительно отфильтровать выходные данные команды**show**. Однако на маршрутизаторе **R1**применен только один ACL-список, поэтому будет достаточно команды **show access-lists**.

R1#**show access-lists**

Standard IP access list 11

10 deny 192.168.10.0 0.0.0.255

20 permit any

Первая строка списка контроля доступа запрещает все пакеты из сети **192.168.10.0/24**, в том числе эхо-запросы по протоколу ICMP (ping-запросы). Вторая строка списка контроля доступа разрешает прохождение через маршрутизатор всего остального трафика по протоколу IP (**ip)** от любого источника (**any**) источника.

б)    Чтобы список контроля доступа влиял на работу маршрутизатора, его необходимо применить к интерфейсу в определенном направлении. В этом сценарии список контроля доступа используется для фильтрации исходящего трафика на интерфейсе. Поэтому весь трафик, покидающий указанный интерфейс на маршрутизаторе R1, будет проверяться на соответствие списку ACL 11.

Несмотря на возможность просмотра сведений об IP с помощью команды **show ip interface**, в некоторых случаях эффективнее использовать команду **show run**.

С помощью обеих или одной из этих команд определите, к какому интерфейсу и в каком направлении применяется список контроля доступа?

Serial 0/0/0, исходящий трафик

**Шаг 2.     Удаление списка контроля доступа 11 из конфигурации**

ACL-списки можно удалить из конфигурации, применив команду **no access list** [*номер ACL-списка*]. Команда **no access-list** удаляет все списки контроля доступа, настроенные на маршрутизаторе. Команда **no access-list** [*номер ACL-списка*] удаляет только указанный список контроля доступа.

а)     В интерфейсе Serial0/0/0 удалите список контроля доступа 11, который был применен к этому интерфейсу в качестве **исходящего** фильтра:

R1(config)# **int se0/0/0**

R1(config-if)#**no ip access-group 11 out**

б)    В режиме глобальной настройки удалите список контроля доступа, применив следующую команду:

R1(config)# **no access-list 11**

в)     Убедитесь, что теперь ping-запросы от компьютера **PC1** успешно достигают **DNS-сервера** и **PC4**.