Лабораторная работа. Настройка и проверка ограничений VTY

Топология

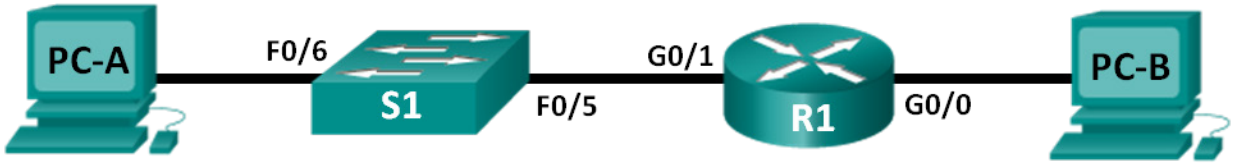

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Задачи

Часть 1. Настройка базовых параметров устройств

Часть 2. Настройка и применение списка контроля доступа на маршрутизаторе R1

Часть 3. Проверка списка контроля доступа с помощью Telnet

Часть 4. Задание повышенной сложности. Настройка и применение списка контроля доступа на коммутаторе S1

Исходные данные/Сценарий

Рекомендуется ограничивать доступ к интерфейсам управления маршрутизатором, например консольное соединение и каналы VTY. Список контроля доступа (ACL) можно использовать для разрешения доступа определённым IP-адресам, благодаря чему только компьютеры администраторов имеют доступ к маршрутизатору через telnet или SSH.

Примечание. В выходных данных устройства Cisco ACL-список обозначается, как access-list.

В этой лабораторной работе вам предстоит создать и применить стандартный именованный ACL-список, ограничивающий удалённый доступ к VTY-каналам маршрутизатора.

После создания и применения ACL-списка вам нужно проверить его функционирование путём получения доступа к маршрутизатору с различных IP-адресов посредством Telnet.

В этой лабораторной работе предоставлены все команды, необходимые для создания и применения ACL-списка.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9).
В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства

и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсе маршрутизатора в конце этой лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с универсальным образом M3 под управлением ОС Cisco IOS 15.2(4) или аналогичная модель);
- 1 коммутатор (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet, расположенные в соответствии с топологией.

Примечание. Интерфейсы Gigabit Ethernet на маршрутизаторах Cisco 1941 определяют скорость автоматически, поэтому между маршрутизатором и PC-B можно использовать прямой кабель Ethernet. При использовании маршрутизатора Cisco другой модели может потребоваться кроссовый кабель Ethernet.

Часть 1: Настройка базовых параметров устройств

В первой части лабораторной работы от вас потребуется создать топологию сети и настроить IP-адреса интерфейсов, доступ к устройствам и пароли на маршрутизаторе.

Шаг 1: Создайте сеть в соответствии со схемой топологии.

Шаг 2: Настройте сетевые параметры на узлах PC-A и PC-B в соответствии с таблицей адресации.

Шаг 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

a. Отключите поиск DNS.

b. Настройте имена устройств в соответствии со схемой топологии.

c. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.

d. Назначьте **cisco** в качестве пароля консоли и активируйте ведение журналов и вход.

e. Назначьте **cisco** в качестве пароля vty и активируйте ведение журналов и вход.

f. Зашифруйте пароли.

g. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.

h. Настройте IP-адреса на интерфейсах, указанных в таблице адресации.

i. Настройте шлюз по умолчанию для коммутатора.

j. Сохраните файл текущей конфигурации в файл загрузочной конфигурации.

Часть 2: Настройка и применение списка контроля доступа на маршрутизаторе R1

Во второй части необходимо настроить стандартный именованный ACL-список и применить его на каналах виртуального терминала маршрутизатора, чтобы ограничить удалённый доступ к маршрутизатору.

Шаг 1: Настройте и примените стандартный именованный ACL-список.

a. Подключитесь к маршрутизатору R1 с помощью консольного подключения и активируйте привилегированный режим.

b. В режиме глобальной конфигурации посмотрите параметры команды **ip access-list**, используя пробел и знак вопроса.

```
R1(config)# ip access-list ?
  extended    Extended Access List
  helper      Access List acts on helper-address
  log-update  Control access list log updates
  logging     Control access list logging
  resequence  Resequence Access List
  standard    Standard Access List
```

c. Посмотрите параметры команды **ip access-list standard**, используя пробел и знак вопроса.

```
R1(config)# ip access-list standard ?
  <1-99>       Standard IP access-list number
  <1300-1999>  Standard IP access-list number (expanded range)
  WORD         Access-list name
```

d. Добавьте **ADMIN-MGT** в конец команды **ip access-list standard** и нажмите клавишу Enter. Теперь вы находитесь в режиме конфигурации стандартного именованного списка доступа (config-std-nacl).

```
R1(config)# ip access-list standard ADMIN-MGT
R1(config-std-nacl)#
```

e. Построчно введите записи разрешения (permit) или запрета (deny), которые также называют правилами ACL-списка (записи ACE). Помните, что в конце ACL-списка стоит скрытая запись **deny any**, которая запрещает весь трафик. Введите знак вопроса, чтобы просмотреть параметры команды.

```
R1(config-std-nacl)# ?
Standard Access List configuration commands:
  <1-2147483647>  Sequence Number
  default         Set a command to its defaults
  deny            Specify packets to reject
  exit            Exit from access-list configuration mode
  no              Negate a command or set its defaults
  permit          Specify packets to forward
  remark          Access list entry comment
```

f. Создайте разрешающую запись ACE для администраторского узла PC-A в сети 192.168.1.3, а также дополнительную запись ACE, разрешающую доступ другим зарезервированным административным IP-адресам от 192.168.1.4 до 192.168.1.7. Обратите внимание, как с помощью ключевого слова **host** первая запись ACE разрешает доступ одному узлу. Вместо этого можно было бы использовать запись ACE **permit 192.168.1.3 0.0.0.0**. Вторая разрешающая запись ACE

обеспечивает доступ узлам от 192.168.1.4 до 192.168.1.7 с помощью шаблонной маски 0.0.0.3, которая является обратной маской маски подсети 255.255.255.252.

```
R1(config-std-nacl)# permit host 192.168.1.3
R1(config-std-nacl)# permit 192.168.1.4 0.0.0.3
R1(config-std-nacl)# exit
```

Создание запрещающей записи не требуется, поскольку в конце любого ACL-списка имеется косвенная запись **deny any**.

g. Теперь, когда вы создали именованный список ACL, примените его на каналах vty.

```
R1(config)# line vty 0 4
R1(config-line)# access-class ADMIN-MGT in
R1(config-line)# exit
```

Часть 3: Проверка списка контроля доступа с помощью Telnet

В третьей части лабораторной работы вам предстоит использовать Telnet для доступа к маршрутизатору с целью проверки корректности функционирования именованного ACL-списка.

Примечание. SSH является более безопасным протоколом, чем Telnet; однако для использования SSH сетевое устройство должно быть настроено на приём SSH-подключений. Для удобства в данной лабораторной работе используется Telnet.

a. Откройте командную строку на компьютере PC-A и проверьте подключение к маршрутизатору с помощью команды **ping**.

```
C:\Users\user1> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=5ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms
C:\Users\user1>
```

b. С помощью командной строки на PC-A запустите клиентскую программу Telnet, чтобы настроить подключение к маршрутизатору по протоколу telnet. Введите логин и пароли привилегированного режима. После этого вы должны войти, увидеть баннерное сообщение и оказаться в консольном режиме маршрутизатора R1.

```
C:\Users\user1> telnet 192.168.1.1

Unauthorized access is prohibited!

User Access Verification

Password:
R1>enable
Password:
```

```
R1#
```

Удалось ли настроить подключение по протоколу Telnet?

c. В командной строке введите **exit** и затем нажмите клавишу Enter, чтобы закрыть сеанс Telnet.

d. Измените IP-адрес, чтобы убедиться, что именованный ACL-список блокирует неразрешённые IP-адреса. Измените IPv4-адрес PC-A на 192.168.1.100.

e. Снова попытайтесь подключиться по telnet к маршрутизатору R1 по адресу 192.168.1.1. Сеанс Telnet прошёл успешно?

Какое сообщение вы получили?

f. Измените IP-адрес на PC-A, чтобы убедиться, что именованный ACL-список разрешает узлу с IP-адресом в диапазоне от 192.168.1.4 до 192.168.1.7 подключаться к маршрутизатору по telnet. После изменения IP-адреса на PC-A откройте командную строку Windows и попытайтесь подключиться к маршрутизатору R1 по telnet.

Сеанс Telnet прошёл успешно?

g. В привилегированном режиме на R1 введите команду **show ip access-lists** и нажмите клавишу Enter. В выходных данных команды обратите внимание, как устройство Cisco IOS автоматически назначает номера строк записям доступа ACL-списка с шагом 10 и показывает количество успешных совпадений для каждого разрешающего правила (в скобках).

```
R1# show ip access-lists
Standard IP access list ADMIN-MGT
    10 permit 192.168.1.3 (2 matches)
    20 permit 192.168.1.4, wildcard bits 0.0.0.3 (2 matches)
```

Поскольку вам удалось установить два успешных подключения по Telnet с маршрутизатором, и каждый сеанс Telnet был инициирован с IP-адреса, который совпадает с одной из разрешающих записей ACE, существуют совпадения для каждой разрешающей записи ACE.

Как вы думаете, почему для каждой разрешающей записи ACE есть два совпадения, в то время как с каждого IP-адреса было создано только одно соединение?

Как бы вы определили, в какой момент протокол Telnet создаёт два совпадения во время подключения Telnet?

h. Войдите в режим глобальной конфигурации на маршрутизаторе R1.

i. Войдите в режим конфигурации списка доступа под именем ADMIN-MGT и добавьте запись **deny any** в конец ACL-списка.

```
R1(config)# ip access-list standard ADMIN-MGT
R1(config-std-nacl)# deny any
R1(config-std-nacl)# exit
```

Примечание. Поскольку в конце каждого ACL-списка содержится скрытая запись **deny any**, добавление явной записи **deny any** не требуется, хотя она может быть полезной в отношении регистрации событий или проверки количества совпадений с записью **deny any** в ACL-списке.

j. Попробуйте подключиться от PC-B к маршрутизатору R1 по telnet. Это создаёт совпадения с записью **deny any** в списке доступа под именем ADMIN-MGT.

k. В привилегированном режиме введите команду **show ip access-lists** и нажмите клавишу Enter. Вы должны увидеть несколько совпадений с записями **deny any**.

```
R1# show ip access-lists
Standard IP access list ADMIN-MGT
    10 permit 192.168.1.3 (2 matches)
    20 permit 192.168.1.4, wildcard bits 0.0.0.3 (2 matches)
    30 deny any (3 matches)
```

Ошибка подключения Telnet создаёт больше совпадений с явной записью запрета, чем успешное подключение. Как вы думаете, почему?

Часть 4: Задание повышенной сложности. Настройка и применение списка контроля доступа на коммутаторе S1

Шаг 1: Настройте и примените стандартный именованный ACL-список для каналов VTY на коммутаторе S1.

a. Не обращаясь к командам конфигурации маршрутизатора R1, попробуйте настроить ACL-список на коммутаторе S1, разрешая доступ только для IP-адреса узла PC-A.

b. Примените ACL-список на каналах VTY коммутатора S1. Помните, что на коммутаторе больше каналов vty, чем на маршрутизаторе.

Шаг 2: Проверьте ACL-список для VTY на коммутаторе S1.

Настройте подключение по Telnet от каждого ПК, чтобы проверить корректность работы ACL-списка для vty. Подключение по telnet к коммутатору S1 должно быть успешным от узла PC-A, но не от узла PC-B.

Вопросы на закрепление

1. Как видно из удалённого доступа к vty, списки ACL — это мощный инструмент фильтрации, который можно применить не только на входящих и исходящих сетевых интерфейсах. Как ещё можно использовать списки контроля доступа (ACL)?

2. Может ли ACL-список, применённый на интерфейсе удалённого управления VTY, повысить безопасность подключения по Telnet? Делает ли это протокол Telnet более целесообразным инструментом управления удалённым доступом?

3. Почему следует применять ACL-список к каналам vty, а не к конкретным интерфейсам?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet №1**	**Интерфейс Ethernet №2**	**Последовательный интерфейс №1**	**Последовательный интерфейс №2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.