Лабораторная работа. Настройка параметров безопасности коммутатора

Топология

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	172.16.99.1	255.255.255.0	N/A
S1	VLAN 99	172.16.99.11	255.255.255.0	172.16.99.1
PC-A	NIC	172.16.99.3	255.255.255.0	172.16.99.1

Задачи

Часть 1. Настройка топологии и установка исходного состояния устройства

Часть 2. Настройка базовых параметров устройств и проверка подключения

Часть 3. Настройка и проверка доступа с помощью протокола SSH к коммутатору S1

- Настройте доступ по протоколу SSH.
- Измените параметры SSH.
- Проверьте конфигурацию SSH.

Часть 4. Настройка и проверка параметров безопасности для S1

- Настройте и проверьте общие функции безопасности.
- Настройте и проверьте функцию безопасности порта.

Исходные данные/Сценарий

На компьютерах и серверах следует ограничивать доступ, устанавливая качественную систему безопасности. На ваших устройствах сетевой инфраструктуры, например коммутаторах и маршрутизаторах, тоже важно настраивать функции безопасности.

В ходе данной лабораторной работе вам нужно настроить функции безопасности на коммутаторах LAN в соответствии с практическими рекомендациями. Вам следует разрешить только сеансы протокола SSH и безопасного протокола HTTPS. Кроме того, вам предстоит настроить и проверить работу функции безопасности порта, направленную на блокировку любого устройства с MAC-адресом, который неизвестен коммутатору.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторных работах используется коммутатор Cisco Catalyst 2960 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 интерфейсах маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что информация из маршрутизаторов и коммутаторов удалена, и они не содержат файлов загрузочной конфигурации. Если вы не уверены, обратитесь к преподавателю или вернитесь к процедурам инициализации и перезагрузки устройств, описанных в предыдущей лабораторной работе.

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);
- 1 ПК (под управлением 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.

Часть 1. Настройка топологии и инициализация устройств

В первой части вам предстоит создать топологию сети и при необходимости удалить все конфигурации.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Если ранее на маршрутизаторе или коммутаторе были сохранены конфигурационные файлы, выполните инициализацию и перезагрузку устройств, чтобы восстановить базовые настройки.

Часть 2. Настройка базовых параметров устройств и проверка подключения

Во второй части лабораторной работы вам предстоит настроить базовые параметры маршрутизатора, коммутатора и ПК. Имена и адреса устройств можно найти в топологии и таблице адресации в начале этой лабораторной работы.

Шаг 1: Настройте IP-адрес на PC-A.

Шаг 2: Настройте базовые параметры на маршрутизаторе R1.

a. Задайте имя устройства.

b. Отключите поиск DNS.

c. Настройте IP-адрес интерфейса в соответствии с таблицей адресации.

d. Назначьте **class** в качестве пароля привилегированного режима EXEC.

e. Назначьте **cisco** в качестве пароля консоли и виртуального терминала VTY и активируйте вход.

f. Зашифруйте все незашифрованные пароли.

g. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 3: Выполните базовую настройку коммутатора S1.

Не рекомендуется назначать административный IP-адрес коммутатора для сети VLAN 1 (или любой другой VLAN с конечными пользователями). На данном этапе вам предстоит создать VLAN 99 на коммутаторе и назначить этой сети IP-адрес.

a. Задайте имя устройства.

b. Отключите поиск DNS.

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

d. Назначьте **cisco** в качестве пароля консоли и виртуального терминала VTY и активируйте вход.

e. Настройте шлюз по умолчанию для коммутатора S1 с помощью IP-адреса маршрутизатора R1.

f. Зашифруйте все незашифрованные пароли.

g. Сохраните текущую конфигурацию в загрузочную конфигурацию.

h. Создайте на коммутаторе сеть VLAN 99 и назовите её **Management**.

```
S1(config)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# exit
S1(config)#
```

i. Настройте IP-адрес интерфейса административной сети VLAN 99 в соответствии с таблицей адресации и включите интерфейс.

```
S1(config)# interface vlan 99
S1(config-if)# ip address 172.16.99.11 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
S1#
```

j. Выполните команду **show vlan** на коммутаторе S1. В каком состоянии находится сеть VLAN 99?

k. Выполните команду **show ip interface brief** на коммутаторе S1. В каком состоянии интерфейс VLAN 99 и протокол?

Почему протокол выключен несмотря на то, что вы выполнили команду **no shutdown** для интерфейса VLAN 99?

l. Назначьте порты F0/5 и F0/6 для сети VLAN 99 на коммутаторе.

```
S1# config t
S1(config)# interface f0/5
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# end
```

m. Выполните команду **show ip interface brief** на коммутаторе S1. В каком состоянии интерфейс VLAN 99 и протокол?

Примечание. При сходимости состояний портов может произойти небольшая задержка.

Шаг 4: Проверьте наличие подключения между всеми устройствами.

a. От компьютера PC-A отправьте эхо-запрос на шлюз по умолчанию маршрутизатора R1. Успешно ли выполнены эхо-запросы?

b. От компьютера PC-A отправьте эхо-запрос на адрес управления коммутатора S1. Успешно ли выполнены эхо-запросы?

c. От коммутатора S1 отправьте эхо-запрос на шлюз по умолчанию маршрутизатора R1. Успешно ли выполнены эхо-запросы?

d. В компьютере PC-A откройте веб-браузер и перейдите по адресу http://172.16.99.11. Если появится запрос на ввод имени пользователя пароля, оставьте имя пользователя пустым, а в качестве пароля введите **class**. Если появится запрос о защищённом подключении, ответьте **No.** Удалось ли вам получить доступ к веб-интерфейсу на коммутаторе S1?

e. Закройте сеанс браузера на компьютере PC-A.

Примечание. Незащищённый веб-интерфейс (сервер HTTP) коммутатора Cisco 2960 включён по умолчанию. Для обеспечения безопасности рекомендуется отключить данную службу, как описано в части 4.

Часть 3. Настройка и проверка доступа с помощью протокола SSH к коммутатору S1

Шаг 1: Настройте доступ к протоколу SSH на коммутаторе S1.

a. Включите SSH на S1. В режиме глобальной конфигурации создайте имя домена **CCNA-Lab.com**.

```
S1(config)# ip domain-name CCNA-Lab.com
```

b. Создайте запись локальной базы данных пользователей, которую вы будете использовать для подключения к коммутатору через SSH. Пользователь должен обладать правами доступа администратора.

Примечание. Используемый пароль не является надёжным. Он используется исключительно в рамках лабораторной работы.

```
S1(config)# username admin privilege 15 secret sshadmin
```

c. Настройте вход транспортировки таким образом, чтобы в каналах VTY были разрешены только подключения по протоколу SSH. Для аутентификации используйте локальную базу данных.

```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
```

d. Создайте ключ шифрования RSA с использованием модуля 1024 бит.

```
S1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: S1.CCNA-Lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
```

```
[OK] (elapsed time was 3 seconds)

S1(config)#
S1(config)# end
```

e. Проверьте конфигурацию протокола SSH и ответьте на следующие вопросы.

```
S1# show ip ssh
```

Какую версию SSH использует коммутатор?

Сколько попыток аутентификации разрешает SSH?

На какое значение настроен лимит времени по умолчанию для SSH?

Шаг 2: Измените конфигурацию SSH на коммутаторе S1.

Измените конфигурацию SSH по умолчанию.

```
S1# config t
S1(config)# ip ssh time-out 75
S1(config)# ip ssh authentication-retries 2
```

Сколько попыток аутентификации разрешает SSH?

На какое значение настроен лимит времени для протокола SSH?

Шаг 3: Проверьте конфигурацию SSH на коммутаторе S1.

a. С помощью клиентского программного обеспечения SSH на компьютере PC-A (например Tera Term), настройте SSH-подключение к коммутатору S1. Если в вашей клиентской программе SSH появилось сообщение о ключе узла, примите его. Войдите в систему, используя **admin** в качестве имени пользователя, и **cisco** в качестве пароля.

Удалось ли настроить связь?

Какой запрос был отображён на коммутаторе S1? Почему?

b. Чтобы завершить сеанс SSH на коммутаторе S1, введите **exit**.

Часть 4. Настройка и проверка параметров безопасности для S1

В четвёртой части лабораторной работы вам предстоит закрыть неиспользуемые порты, выключить определённые сервисы, работающие на коммутаторе, и настроить функцию безопасности порта на основе MAC-адресов. Коммутаторы могут быть подвержены переполнению таблицы MAC-адресов, спуфинг-атакам и попыткам неавторизованных подключений к портам коммутатора. Вам нужно будет настроить функцию порта безопасности, чтобы ограничить количество MAC-адресов, которые могут быть получены портом коммутатора, а также отключить порт при превышении этого количества.

Шаг 1: Настройка общих функций безопасности на коммутаторе S1.

a. Настройте баннер MOTD (сообщение дня) для коммутатора S1 в виде соответствующего предупреждения.

b. Выполните команду **show ip interface brief** на коммутаторе S1. Какие физические порты включены?

c. Выключите все неиспользуемые физические порты коммутатора. Используйте команду **interface range**.

```
S1(config)# interface range f0/1 – 4
S1(config-if-range)# shutdown
S1(config-if-range)# interface range f0/7 – 24
S1(config-if-range)# shutdown
S1(config-if-range)# interface range g0/1 – 2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

d. Выполните команду **show ip interface brief** на коммутаторе S1. В каком состоянии находятся порты от F0/1 до F0/4?

e. Введите команду **show ip http server status**.

В каком состоянии находится сервер HTTP?

Какой порт сервера он использует?

В каком состоянии находится защищённый сервер HTTP?

Какой порт сервера он использует?

f. Сеансы HTTP отправляют все данные в незашифрованном виде. Вам нужно отключить сервис HTTP, который работает на коммутаторе S1.

```
S1(config)# no ip http server
```

g. В компьютере PC-A откройте веб-браузер и перейдите по адресу http://172.16.99.11. Что у вас получилось?

h. В компьютере PC-A откройте защищённый сеанс веб-браузера по адресу https://172.16.99.11. Примите сертификат. Войдите в систему без имени пользователя, используйте пароль **class**. Что у вас получилось?

i. Закройте сеанс браузера на компьютере PC-A.

Шаг 2: Настройка и проверка работы функции безопасности порта на коммутаторе S1.

a. Запишите MAC-адрес интерфейса G0/1 маршрутизатора R1. В интерфейсе командной строки маршрутизатора R1 выполните команду **show interface g0/1** и запишите MAC-адрес интерфейса.

```
R1# show interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is 30f7.0da3.1821 (bia
3047.0da3.1821)
```

Каков MAC-адрес интерфейса G0/1 маршрутизатора R1?

b. В интерфейсе командной строки S1 выполните команду **show mac address-table** в привилегированном режиме. Найдите динамические записи для портов F0/5 и F0/6. Запишите их ниже.

MAC-адрес интерфейса F0/5:

MAC-адрес интерфейса F0/6:

c. Настройка базовой безопасности порта.

Примечание. Как правило, эту процедуру выполняют на всех портах доступа коммутатора. Интерфейс F0/5 представлен в качестве примера.

1) Из интерфейса командной строки коммутатора S1 войдите в режим конфигурации интерфейса для порта, который подключается к R1.

```
S1(config)# interface f0/5
```

2) Выключите порт.

```
S1(config-if)# shutdown
```

3) Включите функцию безопасности порта на интерфейсе F0/5.

```
S1(config-if)# switchport port-security
```

Примечание. Выполнение команды **switchport port-security** позволит установить максимальное количество MAC-адресов на значение 1. При попытке нарушения безопасности порт будет выключен. Команды **switchport port-security maximum** и **switchport port-security violation** можно использовать для того, чтобы изменить настройки по умолчанию.

4) Настройте статическую запись для MAC-адреса интерфейса G0/1 маршрутизатора R1, записанного на шаге 2a.

```
S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx
```

(Настоящий MAC-адрес интерфейса G0/1 маршрутизатора имеет формат xxxx.xxxx.xxxx).

Примечание. При желании вы можете использовать команду **switchport port-security mac-address**, чтобы добавить в текущую конфигурацию коммутатора защищённые MAC-адреса, которые были динамически получены на порте (до заданного максимального значения).

5) Включите порт коммутатора.

```
S1(config-if)# no shutdown
S1(config-if)# end
```

d. Проверьте функцию безопасности порта на интерфейсе F0/5 коммутатора S1 с помощью команды **show port-security interface**.

```
S1# show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

В каком состоянии находится порт F0/5?

e. Из командной строки маршрутизатора R1 отправьте эхо-запрос на компьютер PC-A, чтобы проверить подключение.

```
R1# ping 172.16.99.3
```

f. Далее, изменив MAC-адрес интерфейса маршрутизатора, вы нарушите систему безопасности. Войдите в режим конфигурации интерфейса для G0/1 и выключите его.

```
R1# config t
R1(config)# interface g0/1
R1(config-if)# shutdown
```

g. Настройте новый MAC-адрес для интерфейса, используя **aaaa.bbbb.cccc** в качестве адреса.

```
R1(config-if)# mac-address aaaa.bbbb.cccc
```

h. По возможности, одновременно с этим шагом установите консольное подключение на коммутаторе S1. В консольном подключении к коммутатору S1 вы увидите различные сообщения о нарушении системы безопасности. Включите интерфейс G0/1 маршрутизатора R1.

```
R1(config-if)# no shutdown
```

i. Из привилегированного режима коммутатора R1 отправьте эхо-запрос на компьютер PC-A. Успешно ли выполнен эхо-запрос? Поясните свой ответ.

j. На коммутаторе проверьте функцию безопасности порта с помощью команд, указанных ниже.

```
S1# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
---------------------------------------------------------------------
      Fa0/5            1           1                1         Shutdown
---------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :0
Max Addresses limit in System (excluding one mac per port) :8192

S1# show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : aaaa.bbbb.cccc:99
Security Violation Count   : 1

S1# show interface f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

```
<output omitted>

S1# show port-security address
                Secure Mac Address Table
------------------------------------------------------------------------
Vlan     Mac Address       Type                  Ports      Remaining Age
                                                             (mins)
----     -----------       ----                  -----   -------------
  99     30f7.0da3.1821    SecureConfigured      Fa0/5        -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :0
Max Addresses limit in System (excluding one mac per port) :8192
```

k. На маршрутизаторе выключите интерфейс G0/1, удалите жёстко запрограммированный MAC-адрес из маршрутизатора и повторно включите интерфейс G0/1.

```
R1(config-if)# shutdown
R1(config-if)# no mac-address aaaa.bbbb.cccc
R1(config-if)# no shutdown
R1(config-if)# end
```

l. Из маршрутизатора R1 повторите эхо-запрос на компьютер PC-A по адресу 172.16.99.3. Успешно ли выполнен эхо-запрос?

m. Чтобы определить причину неудачи эхо-запроса, выполните команду **show interface f0/5**. Запишите полученные результаты.

n. Очистите состояние выключения порта F0/5 в результате сбоя S1.

```
S1# config t
S1(config)# interface f0/5
S1(config-if)# shutdown
S1(config-if)# no shutdown
```

Примечание. При сходимости состояний портов может произойти небольшая задержка.

o. Чтобы убедиться, что порт F0/5 вышел из состояния выключения в результате сбоя, на коммутаторе S1 выполните команду **show interface f0/5**.

```
S1# show interface f0/5
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

p. Из командной строки маршрутизатора R1 повторите эхо-запрос на компьютер PC-A. Эхо-запрос должен пройти успешно.

Вопросы на закрепление

1. Зачем нужно включать функцию безопасности порта на коммутаторе?

2. Зачем нужно отключать неиспользуемые порты коммутатора?

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.