Лабораторная работа

Доступ к интерфейсу командной строки по протоколу SSH

Топология

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Основной шлюз
R1	G0/0/1	192.168.1.1	255.255.255.0	—
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	Сетевой адаптер	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

Часть 1. Настройка основных параметров устройств

Часть 2. Настройка доступа к интерфейсу командной строки по протоколу SSH на маршрутизаторе

Часть 3. Настройка доступа к интерфейсу командной строки по протоколу SSH на коммутаторе

Часть 4. Установка соединения с интерфейса командной строки (CLI) по протоколу SSH

Общие сведения

При использовании протокола Telnet для удаленного доступа к интерфейсу командной строки сетевых устройств не выполняется шифрование передаваемой информации, что позволяет сетевым анализаторам кадров перехватывать пароли и данные конфигурации.

Сетевой протокол Secure SHell (SSH) устанавливает безопасное соединение с интерфейсом командной строки удаленного устройства. Протокол SSH шифрует все данные, передаваемые по среде передачи, и обеспечивает аутентификацию удаленного узла. Протокол SSH все чаще используется вместо Telnet для удаленного доступа к устройствам.

Чтобы протокол SSH можно было использовать на сетевых устройствах, необходимо включить поддержку протокола SSH. В данной лабораторной работе необходимо включить SSH-сервер на маршрутизаторе и коммутаторе, а затем подключиться к интерфейсу командной строки маршрутизатора и коммутатора, используя компьютер с установленным SSH-клиентом.

Примечание. В зависимости от модели маршрутизатора или коммутатора и версии Cisco IOS, ***доступные идентификаторы интерфейса, команды и результаты их выполнения могут***

отличаться от тех, которые приведены в лабораторной работе.

Примечание. Проверьте, что на всех устройствах удалена начальная конфигурация.

Необходимые ресурсы

• 1 Маршрутизатор Cisco с универсальным образом Cisco IOS

• 1 коммутатор Cisco с Cisco IOS

• 1 компьютер с ОС Windows с установленной программой эмуляции терминала

• Консольные кабели для подключения к устройствам Cisco через консольные порты.

• Кабели Ethernet для создания сети согласно Топологии

Часть 1. Настройка основных параметров устройств

В первой части необходимо создать топологию сети и настроить основные параметры, такие как IP-адреса интерфейсов, доступ к устройству и пароли на маршрутизаторе.

Шаг 1. Создайте конфигурацию сети согласно Топологии.

Шаг 2. Перезагрузите маршрутизатор и коммутатор.

Шаг 3. Настройте маршрутизатор.

a. Подключитесь к консольному порту маршрутизатора с помощью консольного кабеля.

b. Войдите в привилегированный режим.

c. Войдите в режим глобальной конфигурации.

d. Отключите поиск DNS, чтобы запретить маршрутизатору преобразовывать в имена узлов неверно введенные пользователем команды.

e. Установите **`class`** в качестве зашифрованного пароля привилегированного режима.

f. Установите **`cisco`** в качестве пароля для консольного подключения и включите вход в систему по паролю.

g. Установите **`cisco`** в качестве пароля для линий VTY и включите вход в систему по паролю.

h. Зашифруйте все пароли.

i. Создайте баннер, предупреждающий о том, что несанкционированный доступ запрещен.

j. Настройте и включите интерфейс G0/0/1 на маршрутизаторе, используя информацию из **Таблицы адресации**.

Шаг 4. Настройте компьютер PC-A.

a. Настройте на компьютере PC-A IP-адрес, маску подсети и IP-адрес основного шлюза.

Шаг 5. Проверьте подключение.

В окне командной строки компьютера PC-A с помощью команды **ping** отправьте эхо-запрос на IP-адрес интерфейса G0/0/1 маршрутизатора R1. Найдите и устраните неполадки подключения в случае необходимости.

Часть 2. Настройка доступа к интерфейсу командной строки по протоколу SSH на маршрутизаторе

Во второй части небходимо настроить маршрутизатор для приема соединений по линиям VTY, с использованием протокола SSH.

Шаг 1. Настройте аутентификацию устройств.

Имя устройства и домен используются для генерации ключа шифрования. Поэтому эти настройки необходимо выполнить в первую очередь.

a. Назначьте имя устройства **в соответствии с вашим вариантом**.

b. Назначьте домен для устройства.

Шаг 2. Сгенерируйте ключ шифрования, указав его длину.

Шаг 3. Создайте пользователя в локальной базе учетных записей.

Создайте пользователя, используя **`admin`** в качестве имени пользователя и **`Adm1nP@55`** в качестве пароля.

Шаг 4. Включите использование протокола SSH на линиях VTY.

a. Включите использование протоколов Telnet и SSH на входящих линиях VTY с помощью команды **`transport input`**.

b. Задайте проверку пользователей по локальной базе учетных записей при входе в интерфейс командной строки.

Шаг 5. Установите соединение с интерфейсом командной строки маршрутизатора по протоколу SSH.

a. Запустите программу эмуляции терминала на компьютере PC-A.

b. Установите SSH-соединение с интерфейсом командной строки маршрутизатора R1, используя имя пользователя **`admin`** и пароль **`Adm1nP@55`**.

Часть 3. Настройка доступа к интерфейсу командной строки по протоколу SSH на коммутаторе

В части 3 необходимо настроить коммутатор для приема соединений по протоколу SSH, а затем установить SSH-соединение с помощью программы эмуляции терминала.

Шаг 1. Настройте основные параметры коммутатора.

a. Подключитесь к консольному порту коммутатора с помощью консольного кабеля.

b. Перейдите привилегированный режим.

c. Перейдите в режим глобальной конфигурации.

d. Отключите поиск DNS, чтобы запретить коммутатору преобразовывать в имена узлов неверно введенные пользователем команды.

e. Установите **`class`** в качестве зашифрованного пароля привилегированного режима.

f. Установите **`cisco`** в качестве пароля для консольного подключения и включите вход в систему по паролю.

g. Установите **`cisco`** в качестве пароля для линий VTY и включите вход в систему по паролю.

h. Зашифруйте все пароли.

i. Создайте баннер, предупреждающий о том, что несанкционированный доступ запрещен.

j. Настройте и включите на коммутаторе виртуальный интерфейс VLAN 1, используя информацию из **Таблице адресации**.

Шаг 2. Настройте коммутатор для соединения по протоколу SSH.

Для настройки протокола SSH на коммутаторе используйте те же команды, что применялись для аналогичной настройки маршрутизатора в части 2.

a. Назначьте имя устройства.

b. Назначьте домен для устройства.

c. Сгенерируйте ключ шифрования, указав его длину.

d. Создайте пользователя в локальной базе учетных записей.

e. Включите использование протоколов Telnet и SSH на линиях VTY.

f. Задайте проверку пользователей по локальной базе учетных записей при входе в интерфейс командной строки.

Шаг 3. Установите соединение с интерфейсом командной строки коммутатора по протоколу SSH.

Запустите программу эмуляции терминала на компьютере PC-A, затем установите соединение по протоколу SSH с интерфейсом командной строки коммутатора S1.

Получилось установить SSH-соединение с коммутатором?

Часть 4. Установка соединения по протоколу SSH из интерфейса командной строки (CLI) коммутатора

Клиент SSH встроен в ОС Cisco IOS и может быть запущен из интерфейса командной строки. В части 4 необходимо установить соединение с маршрутизатором по протоколу SSH, используя интерфейс командной строки коммутатора.

Шаг 1. Посмотрите доступные параметры для клиента SSH в Cisco IOS.

Посмотрите возможные параметры для команды **ssh**, используя справку:

```
S1# ssh?
-l Log in using this user name
-v Specify SSH Protocol Version
```

Шаг 2. Установите соединение по протоколу SSH от коммутатора S1 к маршрутизатору R1.

a. Введите команду **ssh -l admin** чтобы подключиться под именем пользователя **admin** к интерфейсу командной строки маршрутизатора R1 по протоколу SSH. После приглашения введите пароль **Adm1nP@55**

```
S1# ssh -l admin 192.168.1.1
Password:
Authorized Users Only!
R1>
```

b. Чтобы вернуться в командную строку коммутатора S1, не закрывая SSH-сеанс с маршрутизатором R1, нажмите на клавиатуре комбинацию Ctrl+Shift+6. Отпустите Ctrl+Shift+6 и нажмите x.

```
R1>
S1#
```

c. Чтобы вернуться в командную строку маршрутизатора R1, в строке интерфейса командной строки коммутатора S1 дважды нажмите на клавиатуре **Ввод**.

```
S1#
[Resuming connection 1 to 192.168.1.1 ... ]
R1>
```

d. Для завершения SSH-сеанса на маршрутизаторе R1, в командной строке маршрутизатора введите команду **exit**.

```
R1# exit
[Connection to 192.168.1.1 closed by foreign host]
S1#
```

Какие версии протокола SSH поддерживаются Cisco IOS?

Вопрос для повторения

Как предоставить удаленный доступ к интерфейсу командной строки сетевого устройства нескольким пользователям, которые имеют собственное имя и пароль?