**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.**

1. Подключитесь к консольному порту маршрутизатора с помощью

консольного кабеля.

1. Войдите в привилегированный режим.
2. Войдите в режим глобальной конфигурации.
3. Отключите поиск DNS, чтобы запретить маршрутизатору преобразовывать в имена узлов неверно введенные пользователем команды.
4. Установите **class** в качестве зашифрованного пароля

привилегированного режима.

1. Установите **cisco** в качестве пароля для консольного подключения

и включите вход в систему по паролю.

1. Установите **cisco** в качестве пароля для линий VTY и включите

вход в систему по паролю.

1. Зашифруйте все пароли.
2. Создайте баннер, предупреждающий о том, что несанкционированный доступ запрещен.
3. 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.

1. Назначьте имя устройства **в соответствии с вашим вариантом**.
2. 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.**

1. Включите использование протоколов Telnet и SSH на входящих

линиях VTY с помощью команды **transport input**.

1. 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.**

1. Запустите программу эмуляции терминала на компьютере PC-A.
2. 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.**

1. Подключитесь к консольному порту коммутатора с помощью

консольного кабеля.

1. Перейдите привилегированный режим.
2. Перейдите в режим глобальной конфигурации.
3. Отключите поиск DNS, чтобы запретить коммутатору преобразовывать в имена узлов неверно введенные пользователем команды.
4. Установите **class** в качестве зашифрованного пароля

привилегированного режима.

1. Установите **cisco** в качестве пароля для консольного подключения

и включите вход в систему по паролю.

1. Установите **cisco** в качестве пароля для линий VTY и включите

вход в систему по паролю.

1. Зашифруйте все пароли.
2. Создайте баннер, предупреждающий о том, что несанкционированный доступ запрещен.
3. 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.

1. Назначьте имя устройства.
2. Назначьте домен для устройства.
3. Сгенерируйте ключ шифрования, указав его длину.
4. Создайте пользователя в локальной базе учетных записей.
5. Включите использование протоколов Telnet и SSH на линиях VTY.
6. 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?

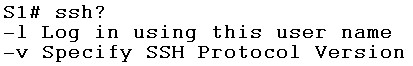
|  |
| --- |
| Да |

**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.**

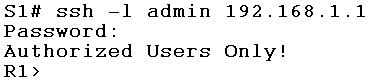
Посмотрите возможные параметры для команды **ssh**, используя справку:



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

1. 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**



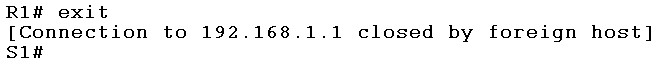
1. Чтобы вернуться в командную строку коммутатора S1, не закрывая SSH-сеанс с маршрутизатором R1, нажмите на клавиатуре комбинацию Ctrl+Shift+6. Отпустите Ctrl+Shift+6 и нажмите x.



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



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



Какие версии протокола SSH поддерживаются Cisco IOS?

|  |
| --- |
| 2 |

**Вопрос для повторения**

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

|  |
| --- |
| Создаем учетные записи для пользователей в необходимом устройстве, настроить подключение ssh через локальные записи (login local). Пользователям предстоит подключаться через SSH. |