Лабораторная работа. Доступ к сетевым устройствам по протоколу SSH

Топология

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	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	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

Часть 1. Настройка основных параметров устройства

Часть 2. Настройка маршрутизатора для доступа по протоколу SSH

Часть 3. Настройка коммутатора для доступа по протоколу SSH

Часть 4. SSH через интерфейс командной строки (CLI) коммутатора

Общие сведения/сценарий

Раньше для удаленной настройки сетевых устройств в основном применялся протокол Telnet. Однако он не обеспечивает шифрование информации, передаваемой между клиентом и сервером, что позволяет анализаторам сетевых пакетов перехватывать пароли и данные конфигурации.

Secure Shell (SSH) — это сетевой протокол, устанавливающий безопасное подключение с эмуляцией терминала к маршрутизатору или иному сетевому устройству. Протокол SSH шифрует все сведения, которые поступают по сетевому каналу, и предусматривает аутентификацию удаленного компьютера. Протокол SSH все больше заменяет Telnet — именно его выбирают сетевые специалисты в качестве средства удаленного входа в систему. Чаще всего протокол SSH применяется для входа в удаленное устройство и выполнения команд, но может также передавать файлы по связанным протоколам SFTP или SCP.

Чтобы протокол SSH мог работать, на сетевых устройствах, взаимодействующих между собой, должна быть настроена поддержка SSH. В этой лабораторной работе необходимо включить SSH-сервер на маршрутизаторе, после чего подключиться к этому маршрутизатору, используя ПК с установленным клиентом SSH. В локальной сети подключение обычно устанавливается с помощью Ethernet и IP.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сервисами Cisco 1941 (ISR) под управлением Cisco IOS версии 15.2(4) M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Точные идентификаторы интерфейсов см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что у всех маршрутизаторов и коммутаторов была удалена начальная конфигурация. Если вы не уверены, обратитесь к инструктору.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с операционной системой Cisco IOS 15.2(4)M3 (универсальный образ) или аналогичная модель)
- 1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.0(2) с образом lanbasek9 или аналогичная модель)
- 1 ПК (Windows 7 или 8 с программой эмуляции терминала, например, Tera Term, и установленной программой Wireshark)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- Кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Настройка основных параметров устройств

В части 1 потребуется настроить топологию сети и основные параметры, такие как IP-адреса интерфейсов, доступ к устройствам и пароли на маршрутизаторе.

Шаг 1: Создайте сеть согласно топологии.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Шаг 3: Настройте маршрутизатор.

a. Подключитесь к маршрутизатору с помощью консоли и активируйте привилегированный режим EXEC.

b. Войдите в режим конфигурации.

c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

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

e. Назначьте **cisco** в качестве пароля консоли и включите режим входа в систему по паролю.

f. Назначьте **cisco** в качестве пароля VTY и включите вход по паролю.

g. Зашифруйте открытые пароли.

h. Создайте баннер, который предупреждает о запрете несанкционированного доступа.

i. Настройте и активируйте на маршрутизаторе интерфейс G0/1, используя информацию, приведенную в таблице адресации.

j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 4: Настройте компьютер PC-A.

a. Настройте для PC-A IP-адрес и маску подсети.

b. Настройте для PC-A шлюз по умолчанию.

Шаг 5: Проверьте подключение к сети.

Пошлите с PC-A команду Ping на маршрутизатор R1. Если эхо-запрос с помощью команды ping не проходит, найдите и устраните неполадки подключения.

Часть 2: Настройка маршрутизатора для доступа по протоколу SSH

Подключение к сетевым устройствам по протоколу Telnet сопряжено с риском для безопасности, поскольку вся информация передается в виде открытого текста. Протокол SSH шифрует данные сеанса и обеспечивает аутентификацию устройств, поэтому для удаленных подключений рекомендуется использовать именно этот протокол. В части 2 вам нужно настроить маршрутизатор для приема соединений SSH по линиям VTY.

Шаг 1: Настройте аутентификацию устройств.

При генерации ключа шифрования в качестве его части используются имя устройства и домен. Поэтому эти имена необходимо указать перед вводом команды **crypto key**.

a. Задайте имя устройства.

```
Router(config)# hostname R1
```

b. Задайте домен для устройства.

```
R1(config)# ip domain-name ccna-lab.com
```

Шаг 2: Создайте ключ шифрования с указанием его длины.

```
R1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

R1(config)#
*Jan 28 21:09:29.867: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Шаг 3: Создайте имя пользователя в локальной базе учетных записей.

```
R1(config)# username admin privilege 15 secret adminpass
```

Примечание. Уровень привилегий 15 дает пользователю права администратора.

Шаг 4: Активируйте протокол SSH на линиях VTY.

a. Активируйте протоколы Telnet и SSH на входящих линиях VTY с помощью команды **transport input**.

```
R1(config)# line vty 0 4
R1(config-line)# transport input telnet ssh
```


b. Измените способ входа в систему таким образом, чтобы использовалась проверка пользователей по локальной базе учетных записей.

```
R1(config-line)# login local
R1(config-line)# end
R1#
```

Шаг 5: Сохраните текущую конфигурацию в файл загрузочной конфигурации.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Шаг 6: Установите соединение с маршрутизатором по протоколу SSH.

a. Запустите Tera Term с PC-A.

b. Установите SSH-подключение к R1. Используйте имя пользователя **admin** и пароль **adminpass**. У вас должно получиться установить SSH-подключение к R1.

Часть 3: Настройка коммутатора для доступа по протоколу SSH

В части 3 вам предстоит настроить коммутатор в топологии для приема подключений по протоколу SSH, а затем установить SSH-подключение с помощью программы Tera Term.

Шаг 1: Настройте основные параметры коммутатора.

a. Подключитесь к коммутатору с помощью консольного подключения и активируйте привилегированный режим EXEC.

b. Войдите в режим конфигурации.

c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

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

e. Назначьте **cisco** в качестве пароля консоли и включите режим входа в систему по паролю.

f. Назначьте **cisco** в качестве пароля VTY и включите вход по паролю.

g. Зашифруйте открытые пароли.

h. Создайте баннер, который предупреждает о запрете несанкционированного доступа.

i. Настройте и активируйте на коммутаторе интерфейс VLAN 1, используя информацию, приведенную в таблице адресации.

j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 2: Настройте коммутатор для соединения по протоколу SSH.

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

a. Настройте имя устройства, как указано в таблице адресации.

b. Задайте домен для устройства.

```
S1(config)# ip domain-name ccna-lab.com
```


c. Создайте ключ шифрования с указанием его длины.

```
S1(config)# crypto key generate rsa modulus 1024
```

d. Создайте имя пользователя в локальной базе учетных записей.

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

e. Активируйте протоколы Telnet и SSH на линиях VTY.

```
S1(config)# line vty 0 15
S1(config-line)# transport input telnet ssh
```

f. Измените способ входа в систему таким образом, чтобы использовалась проверка пользователей по локальной базе учетных записей.

```
S1(config-line)# login local
S1(config-line)# end
```

Шаг 3: Установите соединение с коммутатором по протоколу SSH.

Запустите программу Tera Term на PC-A, затем установите подключение по протоколу SSH к интерфейсу SVI коммутатора S1.

Удалось ли вам установить SSH-соединение с коммутатором?

Часть 4: Настройка протокола SSH с использованием интерфейса командной строки (CLI) коммутатора

Клиент SSH встроен в операционную систему Cisco IOS и может запускаться из интерфейса командной строки. В части 4 вам предстоит установить соединение с маршрутизатором по протоколу SSH, используя интерфейс командной строки коммутатора.

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

Используйте вопросительный знак (**?**), чтобы отобразить варианты параметров для команды **ssh**.

```
S1# ssh ?
  -c    Select encryption algorithm
  -l    Log in using this user name
  -m    Select HMAC algorithm
  -o    Specify options
  -p    Connect to this port
  -v    Specify SSH Protocol Version
  -vrf  Specify vrf name
  WORD  IP address or hostname of a remote system
```

Шаг 2: Установите с коммутатора S1 соединение с маршрутизатором R1 по протоколу SSH.

a. Чтобы подключиться к маршрутизатору R1 по протоколу SSH, введите команду **–l admin**. Это позволит вам войти в систему под именем **admin**. При появлении приглашения введите в качестве пароля **adminpass**

```
S1# ssh -l admin 192.168.1.1
Password:
```



```
**********************************************
  Warning: Unauthorized Access is Prohibited!
**********************************************


R1#
```

b. Чтобы вернуться к коммутатору S1, не закрывая сеанс SSH с маршрутизатором R1, нажмите комбинацию клавиш **Ctrl**+**Shift**+**6**. Отпустите клавиши **Ctrl**+**Shift**+**6** и нажмите **x**. Отображается приглашение привилегированного режима EXEC коммутатора.

```
R1#
S1#
```

c. Чтобы вернуться к сеансу SSH на R1, нажмите клавишу Enter в пустой строке интерфейса командной строки. Чтобы увидеть окно командной строки маршрутизатора, нажмите клавишу Enter еще раз.

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


R1#
```

d. Чтобы завершить сеанс SSH на маршрутизаторе R1, введите в командной строке маршрутизатора команду **exit**.

```
R1# exit


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

Какие версии протокола SSH поддерживаются при использовании интерфейса командной строки?

Вопросы для повторения

Как предоставить доступ к сетевому устройству нескольким пользователям, у каждого из которых есть собственное имя пользователя?

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам 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 определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве. Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах Cisco IOS для обозначения интерфейса.

