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	Недоступно
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
ПК-A	Сетевой адаптер	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. Проверка сеанса связи по протоколу Telnet с помощью программы Wireshark

Часть 4. Проверка сеанса связи по протоколу SSH с помощью программы Wireshark

Часть 5. Настройка коммутатора для доступа по протоколу SSH

Часть 6. Настройка протокола SSH в интерфейсе командной строки коммутатора

Исходные данные/сценарий

Раньше для удалённой настройки сетевых устройств в основном применялся протокол Telnet. При этом протоколы типа Telnet не включают проверку подлинности и шифрование информации, передаваемой между клиентом и сервером, что позволяет сетевым средствам слежения перехватывать пароли и данные конфигурации.

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

Чтобы протокол SSH работал, на взаимодействующих сетевых устройствах должна быть настроена его поддержка. В ходе лабораторной работы вы активируете на маршрутизаторе SSH-сервер и подключитесь к маршрутизатору, используя ПК с клиентом SSH. В локальной сети подключение обычно устанавливается с помощью Ethernet и IP-адреса.

Кроме того, в ходе лабораторной работы вы настроите маршрутизатор для приёма подключений по протоколу SSH и воспользуетесь программой Wireshark для перехвата и просмотра сеансов Telnet и SSH. Это покажет, какую важную роль играет шифрование данных, осуществляемое протоколом SSH. И, наконец, вам придётся самостоятельно настроить коммутатор для подключения по протоколу SSH.

Примечание. Маршрутизаторы, используемые на практических занятиях CCNA: маршрутизаторы с интеграцией сервисов серии Cisco 1941 (ISR) установленной версии Cisco IOS 15.2(4) M3 (образ universalk9). Используемые коммутаторы: семейство коммутаторов Cisco Catalyst 2960 версии CISCO IOS 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии CISCO IOS. В зависимости от модели и версии Cisco IOS выполняемые доступные команды и выводы могут отличаться от данных, полученных в ходе лабораторных работ. Точные идентификаторы интерфейса см. в таблице сводной информации об интерфейсах маршрутизаторов в конце данной лабораторной работы.

Примечание. Убедитесь, что информация, имеющаяся на маршрутизаторе и коммутаторе, удалена и они не содержат файлов загрузочной конфигурации. Если вы не уверены, что сможете это сделать, обратитесь к инструктору.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с универсальным образом M3 версии CISCO IOS 15.2(4) или аналогичным)
- 1 коммутатор (серия Cisco 2960, с программным обеспечением Cisco IOS версии 15.0(2), образ lanbasek9 или аналогичный)
- Один ПК (Windows 7, Vista или XP с эмулятором терминала, например Tera Term, и установленной программой Wireshark)
- Консольные кабели для настройки устройств CISCO IOS через консольные порты
- Кабели Ethernet в соответствии с топологией

Часть 1: Основные настройки устройства

В части 1 потребуется настройка топологии сети и основных параметров, таких как IP-адреса интерфейсов, доступ к устройствам и пароли на маршрутизаторе.

Шаг 1: Создайте сеть в соответствии с изображенной на схеме топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Шаг 3: Настройте маршрутизатор.

a. Подключите консоль к маршрутизатору и активируйте привилегированный режим.

b. Войдите в режим конфигурации.

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

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

e. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.

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

g. Зашифруйте пароли.

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

i. Настройте и активируйте интерфейс маршрутизатора G0/1 с помощью сведений, содержащихся в таблице адресации.

j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 4: Настройте ПК-A.

a. Настройте на ПК-A IP-адрес и маску подсети.

b. Настройте на ПК-A шлюз по умолчанию.

Шаг 5: Проверьте подключение к сети.

Отправьте эхо-запрос с помощью команды ping с ПК-A 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 передаётся в виде открытого текста. Протокол SSH шифрует данные сессии и требует аутентификации устройств, поэтому для удалённых подключений рекомендуется использовать именно его. В части 2 вам нужно настроить маршрутизатор для приёма соединений по протоколу SSH по линиям VTY.

Шаг 1: Настройте аутентификацию устройств.

При генерации ключа шифрования используются имя устройства и домен. Это значит, что эти имена необходимо указать перед вводом команды **crypto key**.

a. Укажите имя устройства.

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

b. Укажите 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 учётных записей.

```
R1(config)# username admin privilege 15 secret adminpass
R1(config)#
*Feb  6 23:24:43.971: End->Password:QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjT1HbmYxZigc
R1(config)#
```

Примечание. Пятнадцатый уровень привилегий предоставляет 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 — выберите проверку пользователей по локальной базе учётных 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#
```

Часть 3: Проверка сеанса связи по протоколу Telnet с помощью программы Wireshark

В части 3 вы воспользуетесь программой Wireshark для перехвата и просмотра данных, передаваемых во время сеанса связи маршрутизатора по протоколу Telnet. С помощью программы Tera Term вы подключитесь к маршрутизатору R1 по протоколу Telnet, войдёте в систему и запустите на маршрутизаторе команду show run.

Примечание. Если на вашем компьютере нет программного обеспечения клиента Telnet/SSH, его необходимо установить. Чаще всего для работы с протоколами Telnet и SSH используются программы Tera Term (http://download.cnet.com/Tera-Term/3000-20432_4-75766675.html) и PuTTy (www.putty.org).

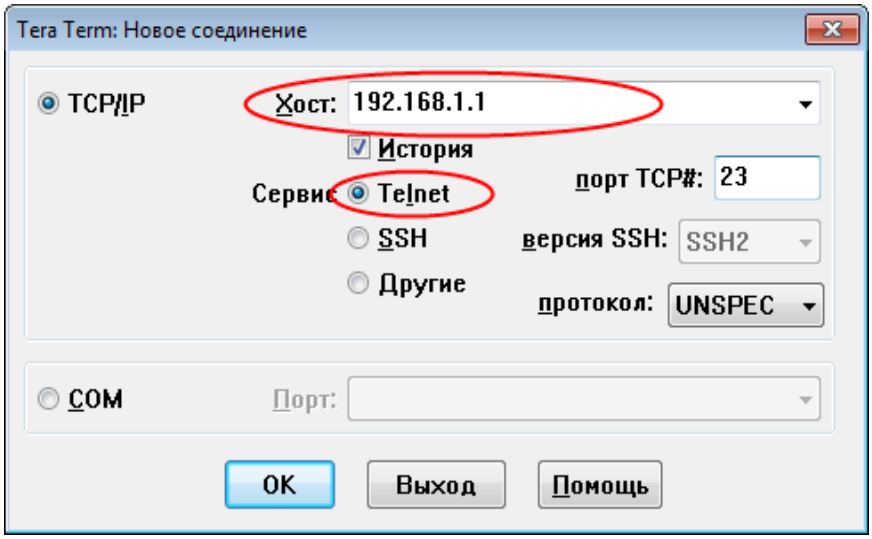
Примечание. По умолчанию доступ к Telnet из командной строки вWindows 7 отключён. Чтобы активировать подключение по протоколу Telnet из окна командной строки, нажмите кнопку **Пуск** >**Панель управления**>**Программы**>**Программы и компоненты**>**Включение или отключение компонентов Windows**. Установите флажок рядом с компонентом **Клиент Telnet** и нажмите кнопку **OK**.

Шаг 1: Откройте Wireshark и начните сбор данных в интерфейсе локальной сети.

Примечание. Если перехват данных в интерфейсе локальной сети запустить не удаётся, попробуйте открыть программу Wireshark с помощью параметра **Запуск от имени администратора**.

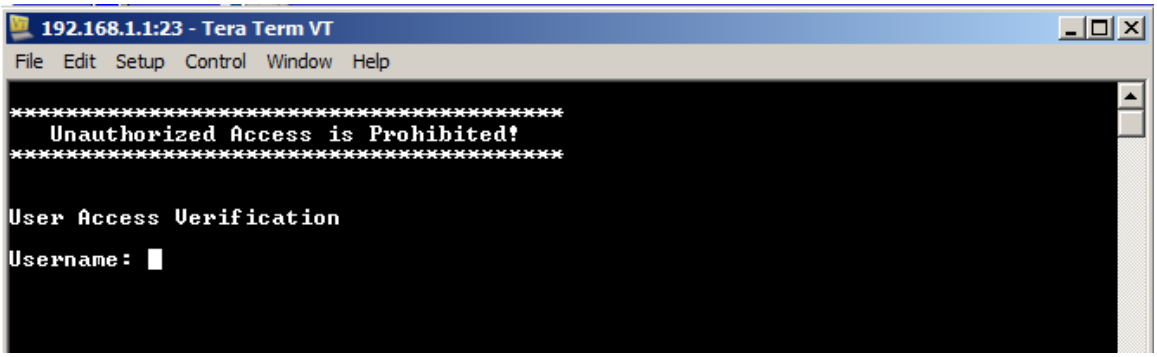
Шаг 2: Начните сеанс подключения к маршрутизатору по протоколу Telnet.

a. Запустите программу Tera Term, установите переключатель сервиса **Telnet**, а в поле «Host» введите **192.168.1.1**.



Какой порт TCP используется для сеансов Telnet по умолчанию?

b. В окне командной строки после приглашения Username: (Имя пользователя) введите **admin**, а после Password: (Пароль) — **adminpass**. Эти запросы появляются потому, что командой **login local** вы настроили линии VTY на использование локальной базы учётных записей.



c. Введите команду **show run**.

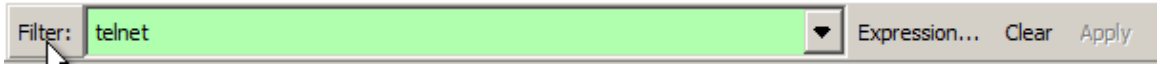
```
R1# show run
```

d. Введите команду **exit**, чтобы завершить сеанс работы с протоколом Telnet и выйти из программы Tera Term.

```
R1# exit
```

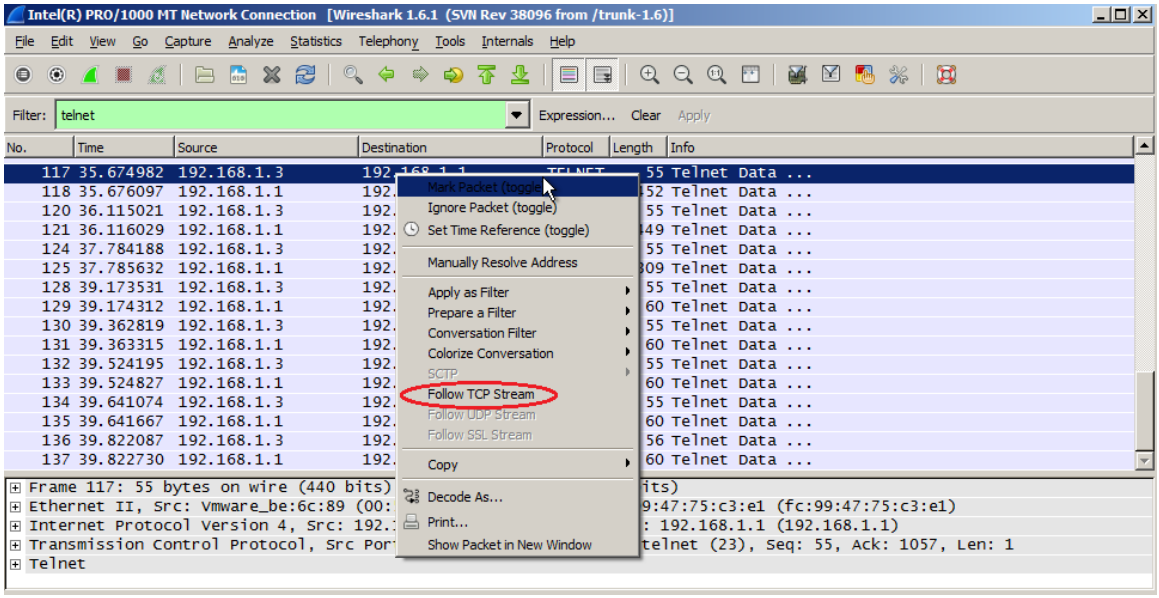
Шаг 3: Остановите сбор данных программой Wireshark.

Шаг 4: Примените один из фильтров Telnet для данных, собираемых программой Wireshark.

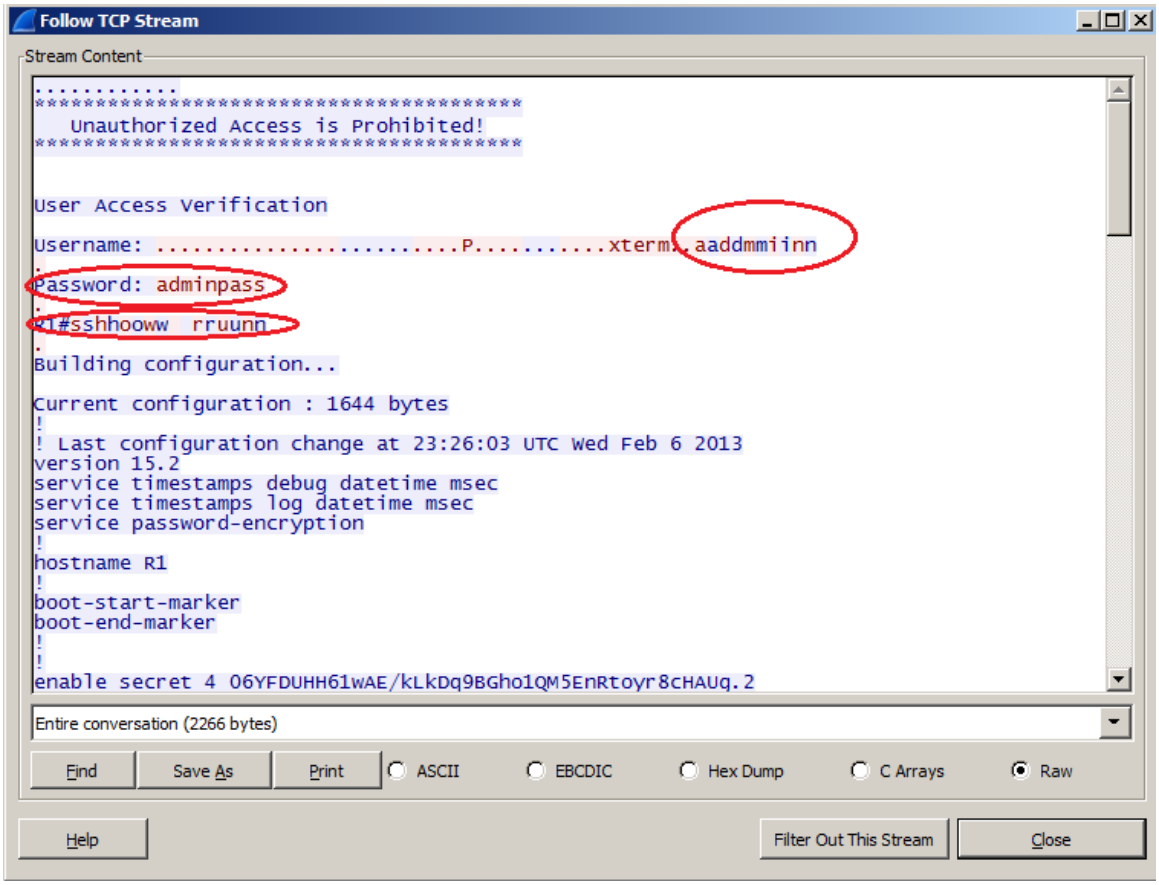


Шаг 5: Используйте функцию TCP в Wireshark для просмотра сеанса Telnet.

a. Нажмите правой кнопкой мыши на одну из строк **Telnet** в разделе **Packet list** (Список пакетов) программы Wireshark и выберите в раскрывающемся списке пункт **Follow TCP Stream** (Следить за TCP-потоком).



b. В окне Follow TCP Stream (Следить за TCP-потоком) отображаются данные о текущем сеансе подключения к маршрутизатору по протоколу Telnet. Весь сеанс связи (включая пароль) отображается открытым текстом. Обратите внимание на то, что введённые имя пользователя и команда **show run** отображаются с повторяющимися символами. Это связано с настройкой отображения в Telnet, которая позволяет выводить на экран символы, набираемые на клавиатуре.



c. Закончив просмотр сеанса Telnet в окне **Follow TCP Stream** (Следить за TCP-потоком), нажмите кнопку **Close** (Закрыть).

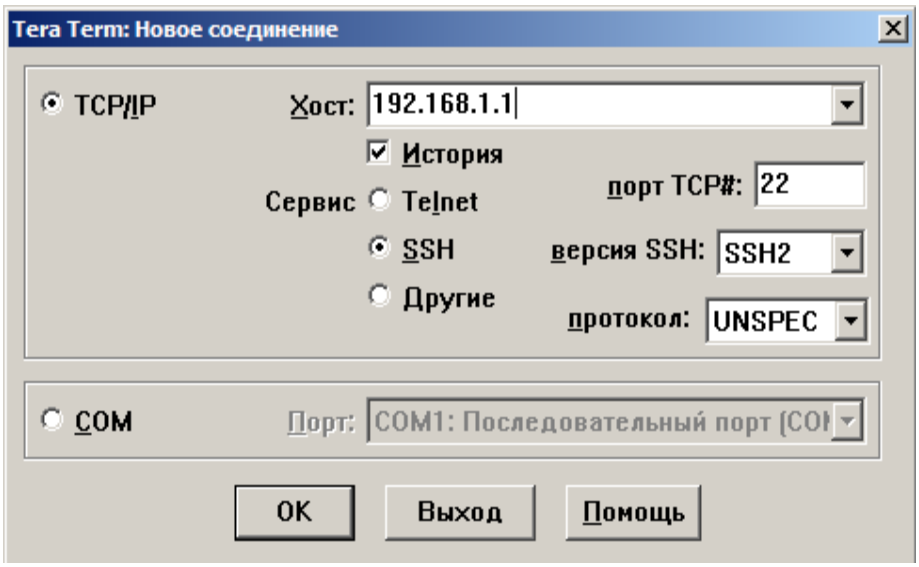
Часть 4: Проверка сеанса связи по протоколу SSH с помощью программы Wireshark

В части 4 вам нужно будет с помощью программы Tera Term установить сеанс подключения к маршрутизатору по протоколу SSH. Программа Wireshark будет использоваться для перехвата и просмотра данных этого сеанса.

Шаг 1: Откройте Wireshark и начните сбор данных в интерфейсе локальной сети.

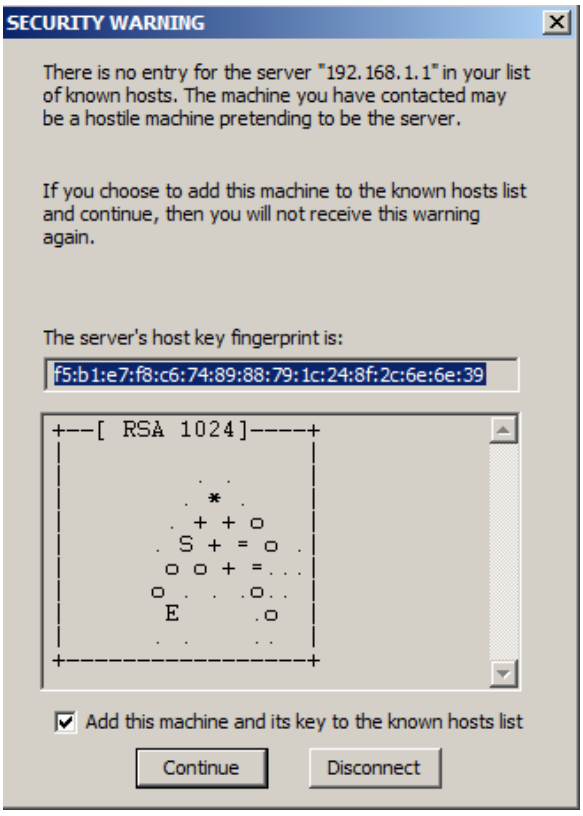
Шаг 2: Запустите на маршрутизаторе сеанс связи по протоколу SSH.

a. Откройте программу Tera Term и введите в поле «Host» окна «Tera Term: Новое соединение» IP-адрес интерфейса G0/1 маршрутизатора R1. Убедитесь в том, что переключатель **SSH** установлен, и нажмите кнопку **OK** для подключения к маршрутизатору.

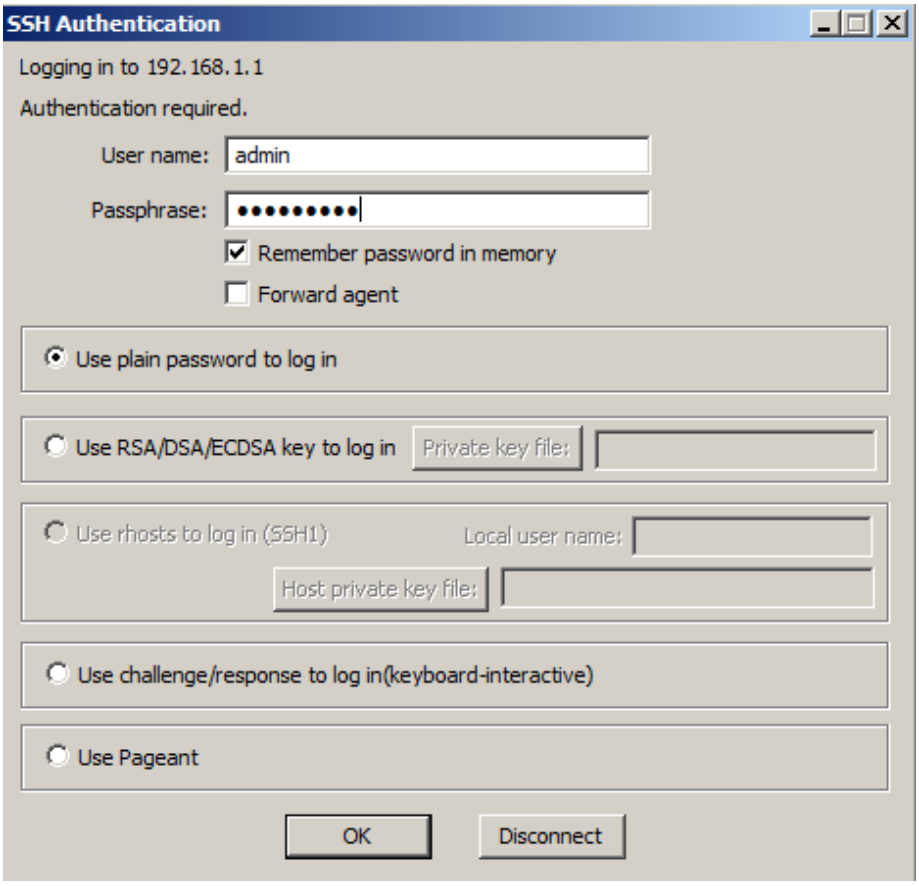


Какой порт TCP используется для сеансов SSH по умолчанию?

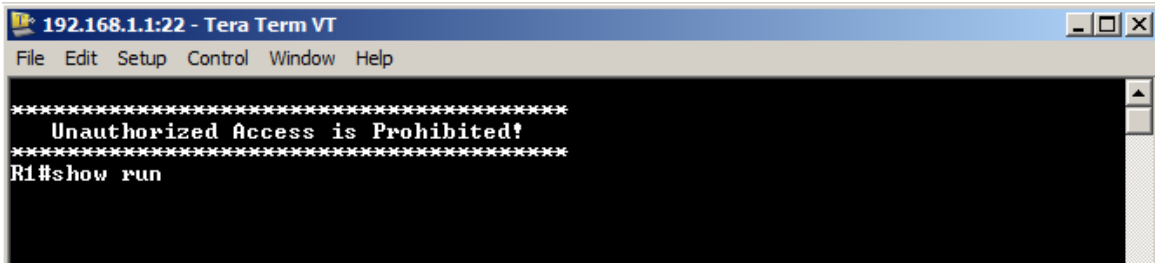
b. После первой установки подключения к устройству по протоколу SSH откроется окно **SECURITY WARNING** (Предупреждение безопасности), которое означает, что вы ещё не подключались к этому устройству. Это сообщение является частью процесса аутентификации. Прочтите текст предупреждения безопасности и нажмите кнопку **Continue** (Продолжить).



c. В окне SSH Authentication (Аутентификация SSH) в качестве имени пользователя укажите **admin**, а в качестве пароля — **adminpass**. Нажмите кнопку **OK**, чтобы войти в систему маршрутизатора.



d. Вы установили сеанс SSH на маршрутизаторе. Окно программы Tera Term очень похоже на окно командной строки. После приглашения введите команду **show run**.



e. Чтобы завершить сеанс SSH и выйти из программы Tera Term, введите команду **exit**.

```
R1# exit
```

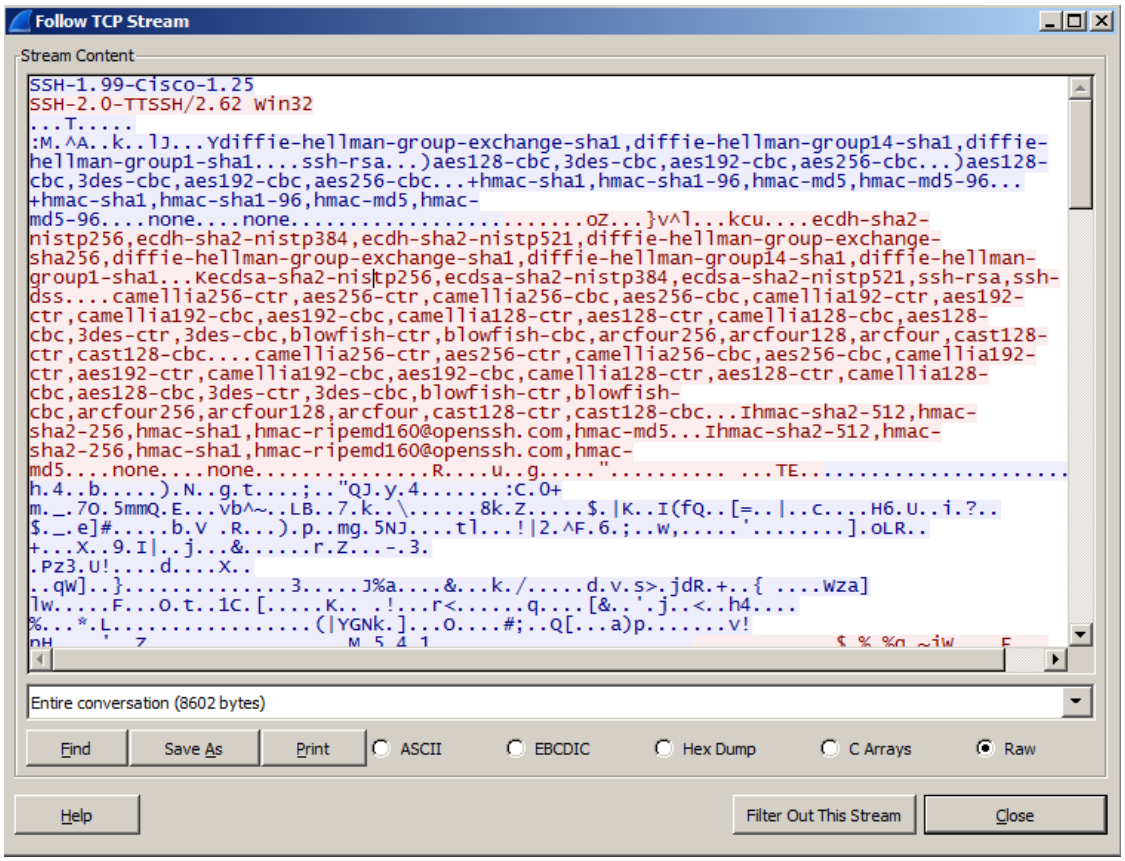
Шаг 3: Остановите сбор данных программой Wireshark.

Шаг 4: Примените один из фильтров SSH для данных, собираемых программой Wireshark.

Шаг 5: Используйте функцию TCP в Wireshark для просмотра сеанса Telnet.

a. Нажмите правой кнопкой мыши на одну из строк **SSHv2** в разделе **Packet list** (Список пакетов) программы Wireshark и выберите в раскрывающемся списке пункт **Follow TCP Stream** (Следить за TCP-потоком).

b. Изучите окно **Follow TCP Stream** (Следить за TCP-потоком) сеанса SSH. Данные зашифрованы и не доступны для прочтения. Сравните данные сеанса SSH с данными сеанса Telnet.



Почему для удалённых подключений протокол SSH является более предпочтительным, чем протокол Telnet?

c. Завершив изучение сеанса SSH, нажмите кнопку **Close** (Закрыть).

d. Закройте программу Wireshark.

Часть 5: Настройка коммутатора для доступа по протоколу SSH

В части 5 вы настроите коммутатор в топологии для приёма подключений по протоколу SSH, а затем установите сеанс SSH с помощью программы Tera Term.

Шаг 1: Настройте базовые параметры коммутатора.

Шаг 2: Настройте коммутатор для доступа по протоколу SSH.

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

Шаг 3: Установите подключение к коммутатору по протоколу SSH.

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

Шаг 4: При необходимости устраните неполадки.

Удалось ли вам установить сеанс SSH с коммутатором?

Часть 6: Настройка протокола SSH в интерфейсе командной строки коммутатора

Клиент SSH интегрирован в операционную систему Cisco IOS и может запускаться из интерфейса командной строки. В части 6 вы установите подключение к маршрутизатору по протоколу SSH из интерфейса командной строки коммутатора.

Шаг 1: Посмотрите, какие параметры доступны для клиента SSH в Cisco IOS.

Введите 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 подключение коммутатора S1 к маршрутизатору R1 по протоколу SSH.

a. Чтобы подключиться к маршрутизатору R1 по протоколу SSH, введите команду **–ladmin**. Это позволит вам войти в систему под именем **admin**. При появлении запроса в качестве пароля введите **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 подключения к маршрутизатору R1 по протоколу SSH, нажмите клавиши **Ctrl**+**Shift**+**6**. Отпустите клавиши **Ctrl**+**Shift**+**6** и нажмите **x**. Откроется окно командной строки коммутатора с привилегированным режимом.

```
R1#
S1#
```

c. Чтобы вернуться к сеансу SSH на маршрутизаторе R1, нажмите клавишу ВВОД в пустом поле интерфейса командной строки. Чтобы открыть окно командной строки маршрутизатора, нажмите клавишу ВВОД ещё раз.

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

R1#
```

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

```
R1# exit

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

Какие версии протокола SSH поддерживаются интерфейсом командной строки?

Вопросы на закрепление

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

Сводная таблица интерфейса маршрутизатора

Общие сведения 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 для определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Не существует эффективного способа перечислить все комбинации настроек для каждого класса маршрутизаторов. Эта таблица включает в себя идентификаторы возможных сочетаний Ethernet и последовательных интерфейсов в устройстве. В таблицу интерфейсов не включены иные типы интерфейсов, даже если они присутствуют на каком-либо определённом маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое может использоваться в командах IOS для представления интерфейса.