Лабораторная работа № 16. Организация удаленного доступа к коммутатору по SSH

Протокол SSH обеспечивает безопасное соединение благодаря шифрованию передаваемых данных, включая пароли.

Как и в протоколе Telnet, в SSH-соединении участвуют две стороны: клиент и сервер. Чтобы подключиться к интерфейсу командной строки коммутатора по протоколу SSH, администратор запускает на рабочей станции SSH-клиент и вводит IP-адрес управления коммутатора. При этом рабочая станция должна находиться в той же подсети, что и коммутатор, если в сети не настроена маршрутизация.

В управляемых коммутаторах D-Link по умолчанию активирован протокол Telnet. Для управления коммутатором через SSH, администратор должен отключить Telnet и запустить SSH-сервер.

При подключении клиента SSH-сервер проверяет его подлинность с помощью одного из методов аутентификации:

- **Аутентификация по паролю**. Клиент отправляет сообщение, в котором содержится пароль в открытом виде. Это сообщение передаётся по зашифрованному каналу.
- **Аутентификация узла**. Выполняется аутентификация клиентского устройства, а не самого клиента. Этот метод работает, когда клиент отправляет подпись, созданную с помощью закрытого ключа узла. Таким образом, все пользователи, имеющие доступ к этому устройству, будут аутентифицированы.
- **Аутентификация с открытым ключом**. Клиент отправляет серверу сообщение, в котором содержится открытый ключ клиента. Сообщение подписывается закрытым ключом. Когда сервер его получает, он проверяет ключ и подпись клиента. Если ключ и подпись верны, аутентификация успешна.

В лабораторной работе рассмотрим аутентификацию с открытым ключом. В ОС Linux для генерации ключей и удалённого управления устройствами через SSH используется установленная по умолчанию утилита **OpenSSH**.

В ОС Windows для генерации ключей и доступа к интерфейсу командной строки коммутатора по SSH используется программа **PuTTY**.

Оборудование на 1 рабочее место:

Рабочая станция с ОС Linux или ОС Windows.....1 шт.
Коммутатор DGS-3120-24TC.....1 шт.
Кабель Ethernet.....1 шт.
Консольный кабель.....1 шт.

© 2018 D-Link

Используемое ПО для ОС Windows:
Программа эмуляции терминала PuTTY
Программа для генерации ключей PuTTYgen
Программа для хранения пароля для закрытого ключа Pageant
Анализатор трафика Wireshark
TFTP-сервер Tftpd

Используемое ПО для ОС Linux:
Программа эмуляции терминала Minicom
Утилита OpenSSH
Анализатор трафика Wireshark
TFTP-сервер Tftpd-hpa

Цель работы: изучить протокол SSH для удалённого управления коммутатором.

> **Примечание**
>
> Далее в лабораторной работе рассмотрены варианты подключения к интерфейсу командной строки коммутатора через SSH для рабочей станции с ОС Windows и ОС Linux. Выполните настройки в зависимости от используемой операционной системы.

© 2018 D-Link

16.1 Доступ к коммутатору по SSH с рабочей станции ОС Linux

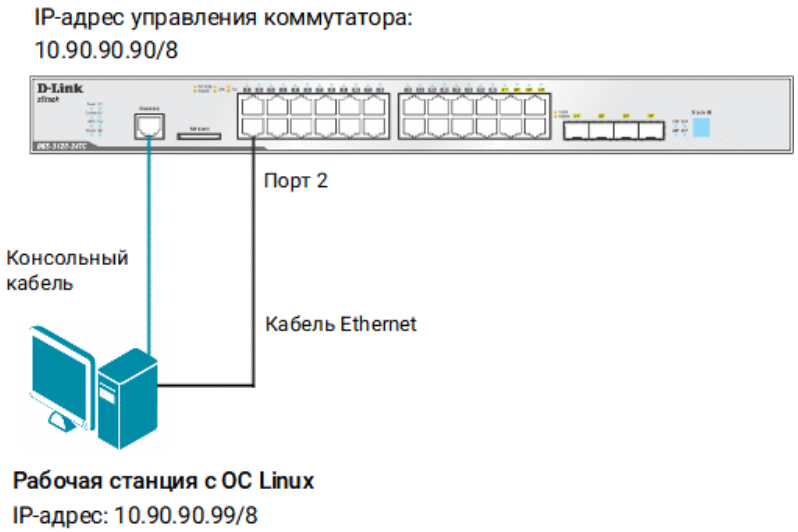

Рис. 16.1 Схема подключения

Настройка рабочей станции

1. Подключите рабочую станцию к коммутатору, как показано на рисунке 16.1.

2. Настройте на рабочей станции статический IP-адрес:

```
$ sudo ifconfig enp0s3 10.90.90.99/8
```

3. В отдельной вкладке терминала запустите анализатор трафика **Wireshark**. Выберите интерфейс локальной сети `enp0s3` для захвата трафика:

```
$ sudo wireshark
```

Генерация ключей RSA

Открытый и закрытый ключи генерируются с помощью программы **ssh-keygen**, которая входит в пакет **OpenSSH** для операционных систем Linux.

> **Примечание**
>
> В дистрибутиве Linux Ubuntu 18.04 утилита **OpenSSH** установлена по умолчанию. В лабораторной работе приведены команды для версии `OpenSSH_7.6p1 Ubuntu-4`. Для проверки версии введите команду:
>
> ```
> $ ssh -V
> ```


© 2018 D-Link

1. Для создания открытого и закрытого ключей откройте терминал и введите команду:

```
$ ssh-keygen -t rsa
```

Опция **-t** позволяет указать алгоритм для генерации ключа.

Не меняйте путь для сохранения ключей. После приглашения **Enter file in which to save the key** нажмите клавишу **Enter**. Зашифруйте закрытый ключ с помощью пароля. В запросе **Enter passphrase (empty for no password)** введите пароль **PassKey** и повторите его в приглашении **Enter same passphrase again**. Если вы забыли пароль, то восстановить его невозможно. Чтобы изменить пароль выполните команду:

```
$ ssh-keygen -p
```

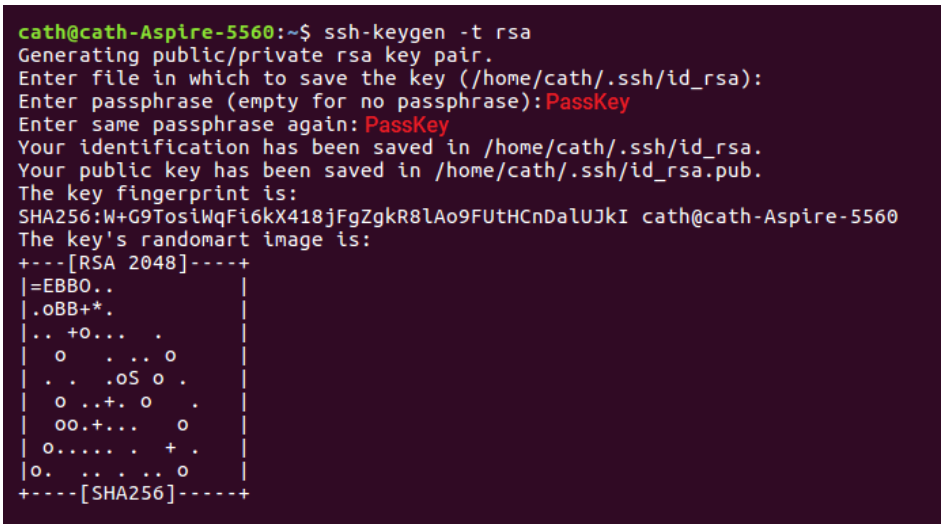

Рис. 16.2 Генерация RSA-ключей в Linux

По умолчанию закрытый ключ сохраняется в `~/.ssh/id_rsa`, а открытый ключ — в `~/.ssh/id_rsa.pub`. Закрытый ключ `id_rsa` следует держать в секрете. В случае его компрометации создайте новый ключ. Открытый ключ `id_rsa.pub` нужно загрузить на коммутатор.

При использовании закрытого ключа `id_rsa` необходимо каждый раз вводить пароль, которым он зашифрован. При частом подключении по SSH это неудобно. В этом случае можно доверить управление ключами программе **ssh-agent**, которая хэширует зашифрованные закрытые ключи и позволяет использовать их при подключении к SSH-серверу без повторного ввода пароля. Пароль, которым зашифрован закрытый ключ, вводится один раз при его добавлении в кэш **ssh-agent**. В Linux **ssh-agent** автоматически запускается при входе в систему. Для его запуска введите команду:

```
$ ssh-agent
```


© 2018 D-Link

2. Добавьте закрытый ключ `id_rsa` в **ssh-agent**:

```
$ ssh-add
```

Появится приглашение для ввода пароля, которым зашифрован закрытый ключ `id_rsa`. Введите **PassKey**. После этого закрытый ключ будет передан агенту.

3. Запретите на рабочей станции аутентификацию по паролю при подключении через SSH. Откройте файл `/etc/ssh/ssh_config`. Уберите символ # напротив строки `PasswordAuthentication no`:

```
$ sudo gedit /etc/ssh/ssh_config

PasswordAuthentication no
```

Настройка TFTP-сервера в Linux

Открытый ключ загружается на коммутатор с помощью TFTP-сервера. При этом сервер TFTP должен находиться в той же IP-подсети, что и коммутатор. По умолчанию TFTP-сервер в Linux не установлен.

1. Проверьте статус TFTP-сервера:

```
$ sudo service tftpd-hpa status
```

2. Если TFTP-сервер не установлен, то введите команду:

```
$ sudo apt-get install tftpd-hpa
```

> **Примечание**
>
> После завершения установки TFTP-сервер запускается автоматически. Рабочая директория для загрузки файлов — `var/lib/tftpboot`.

3. Скопируйте открытый ключ в рабочую директорию TFTP-сервера:

```
$ sudo cp ~/.ssh/id_rsa.pub /var/lib/tftpboot/
```


© 2018 D-Link

Настройка коммутатора

1. На рабочей станции откройте отдельную вкладку в терминале и запустите утилиту **Minicom**:

```
$ sudo minicom
```

2. Сбросьте настройки коммутатора к заводским настройкам по умолчанию:

```
reset config
```

3. Создайте учётную запись администратора:

```
create account admin DlinkUser
```

4. Укажите пароль и подтверждение пароля администратора:

```
Enter a case-sensitive new password: DlinkPassword
Enter the new password again for confirmation: DlinkPassword
```

5. Проверьте настройки учётных записей пользователей:

```
show account
```

6. Выключите протокол Telnet:

```
disable telnet
```

7. Активируйте протокол SSH:

```
enable ssh
```

8. Настройте аутентификацию с открытым ключом и отключите аутентификацию по паролю и аутентификацию узла:

```
config ssh authmode publickey enable
config ssh authmode password disable
config ssh authmode hostbased disable
```


© 2018 D-Link

9. Проверьте выполненные настройки:

```
show ssh authmode
```

10. Установите метод аутентификации с открытым ключом для учётной записи пользователя **DlinkUser**:

```
config ssh user DlinkUser authmode publickey
```

11. Проверьте выполненные настройки:

```
show ssh user authmode
```

12. Настройте параметры SSH-сервера:

```
config ssh server maxsession 8 contimeout 120 authfail 2 rekey never
```

Описание опций:
maxsession — определяет количество одновременных подключений к SSH-серверу;
countimeout — указывает время в секундах, через которое SSH-подключение закроется при бездействии SSH-клиента;
authfail — указывает максимальное число неудачных попыток подключения;
rekey — указывает время в минутах, через которое повторно генерируются сессионные ключи.

13. Проверьте настройки SSH-сервера:

```
show ssh server
```

14. Загрузите открытый ключ `id_rsa.pub` на коммутатор:

```
download ssh client_pub_key 10.90.90.99 src_file id_rsa.pub
```

15. Посмотрите открытый ключ:

```
show ssh client_pub_key
```


© 2018 D-Link

Подключение к коммутатору по SSH

1. Подключитесь к командной строке управления коммутатора через SSH. Для этого откройте терминал и введите команду:

```
$ ssh DLinkUser@10.90.90.90
```

На экране появится сообщение: «Unable to negotiate whit 10.90.90.90 port 22: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1». Это говорит о том, что SSH-клиент и SSH-сервер не смогли согласовать алгоритм обмена ключами. Коммутатор поддерживает только алгоритм **diffie-hellman-group1-sha1**, в OpenSSH 7.0 этот алгоритм по умолчанию выключен.

2. Активируйте алгоритм **diffie-hellman-group1-sha1** в OpenSSH. Для этого укажите опцию `-oKexAlgorithms=+diffie-hellman-group1-sha1` (команда вводится в одну строку):

```
$ ssh -oKexAlgorithms=+diffie-hellman-group1-sha1
DLinkUser@10.90.90.90
```

3. В открывшемся окне командной строки коммутатора после приглашения **UserName** введите **DlinkUser**, после приглашения **PassWord** — **DlinkPassword**.

4. Отключите приглашение ввода имени пользователя и пароля для учётных записей пользователей, которые при подключении по SSH используют метод аутентификации с открытым ключом. Введите в командной строке коммутатора:

```
config ssh publickey bypass_login_screen state enable
```

5. Отключитесь от коммутатора. В командной строке введите:

```
logout или ~.
```

6. Чтобы каждый раз при подключении по SSH не вводить опцию `-oKexAlgorithms=+diffie-hellman-group1-sha1`, добавьте в файл `~/.ssh/config` строку `KexAlgorithms=diffie-hellman-group1-sha1`:

```
$ sudo gedit ~/.ssh/config
KexAlgorithms=diffie-hellman-group1-sha1
```


© 2018 D-Link

7. Повторно подключитесь к коммутатору по SSH:

```
$ ssh DLinkUser@10.90.90.90
```

Появилось приглашение для ввода имени пользователя и пароля? _____

После загрузки открытого ключа на коммутатор, ему присваивается идентификатор Key ID, начиная с 1. Администратор может привязать учётную запись пользователя к открытому ключу по идентификатору. Если открытый ключ относится к учётной записи пользователя, то только этот пользователь получит доступ к коммутатору по SSH. Открытый ключ можно привязать к нескольким учётным записям. Открытый ключ, который не связан с учётной записью пользователя, будет использоваться всеми пользователями.

8. Проверьте, какой идентификатор назначен открытому ключу:

```
show ssh client_pub_key
```

9. Привяжите учётную запись **DlinkUser** к открытому ключу:

```
config ssh client_pubkey_owner key_id 1 add user DlinkUser
```

10. Проверьте выполненные настройки:

```
show ssh client_pub_key
```

11. Создайте ещё одну учётную запись администратора:

```
create account admin Dlink1
```

12. Укажите пароль и подтверждение пароля администратора:

```
Enter a case-sensitive new password: Dlink1
Enter the new password again for confirmation: Dlink1
```

13. Проверьте настройки учётных записей пользователей:

```
show account
```


© 2018 D-Link

14. Установите метод аутентификации с открытым ключом для учётной записи пользователя **Dlink1**:

```
config ssh user Dlink1 authmode publickey
```

15. Проверьте выполненные настройки:

```
show ssh user authmode
```

16. Подключитесь к коммутатору через SSH, используя учётные данные **Dlink1**:

```
$ ssh DLink1@10.90.90.90
```

Что наблюдаете?_____

17. Подключитесь к коммутатору через SSH, используя учётные данные **DlinkUser**.

18. Привяжите учётную запись **Dlink1** к открытому ключу:

```
config ssh client_pubkey_owner key_id 1 add user Dlink1
```

19. Проверьте выполненные настройки:

```
show ssh client_pub_key
```

20. Подключитесь к коммутатору через SSH, используя учётные данные **Dlink1**.

Получилось подключиться? _____

Какой можете сделать вывод?_____

21. Включите приглашение ввода имени пользователя и пароля для учётных записей пользователей, которые используют метод аутентификации с открытым ключом. Введите в командной строке коммутатора:

```
config ssh publickey bypass_login_screen state disable
```


© 2018 D-Link

Анализ захваченного трафика

1. На рабочей станции остановите захват трафика в программе **Wireshark**. Установите фильтр для отображения пакетов протокола SSH.

2. Выберите любой пакет SSH, щелкните по нему правой кнопкой мыши и выберите **Follow → TCP Stream**.

Зашифрован трафик, передаваемый между рабочей станцией и коммутатором? _____

© 2018 D-Link

16.2 Доступ к коммутатору по SSH с рабочей станции ОС Windows

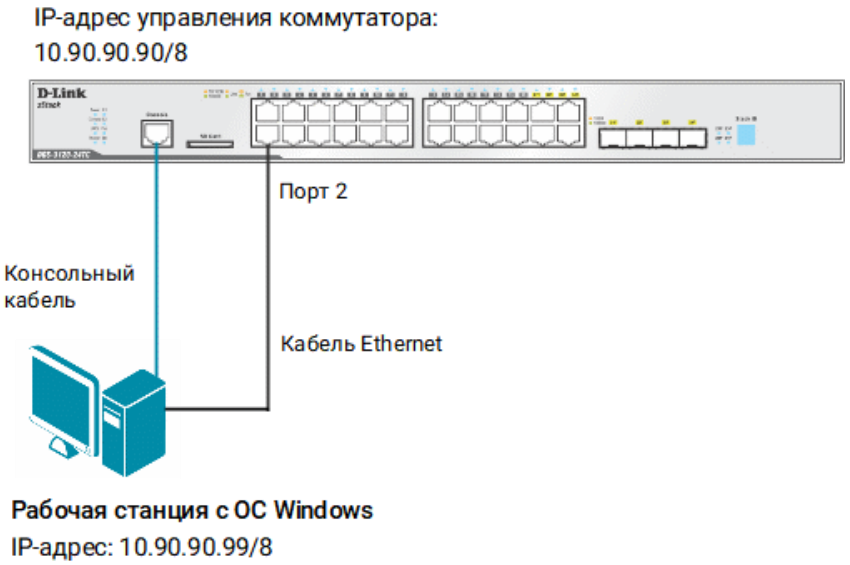

Рис. 16.3 Схема подключения

Настройка рабочей станции

1. Подключите рабочую станцию к коммутатору и настройте статический IP-адрес, как показано на рисунке 16.3.

2. Запустите анализатор трафика **Wireshark**. Выберите интерфейс локальной сети для захвата трафика.

Генерация ключей RSA

1. Запустите программу **PuTTYgen**. В открывшемся окне установите переключатель **RSA**, в поле **Number of bits in a generated key** введите **2048**, затем нажмите кнопку **Generate**. Хаотично перемещайте мышку в пределах окна программы до окончания генерации ключей.

© 2018 D-Link

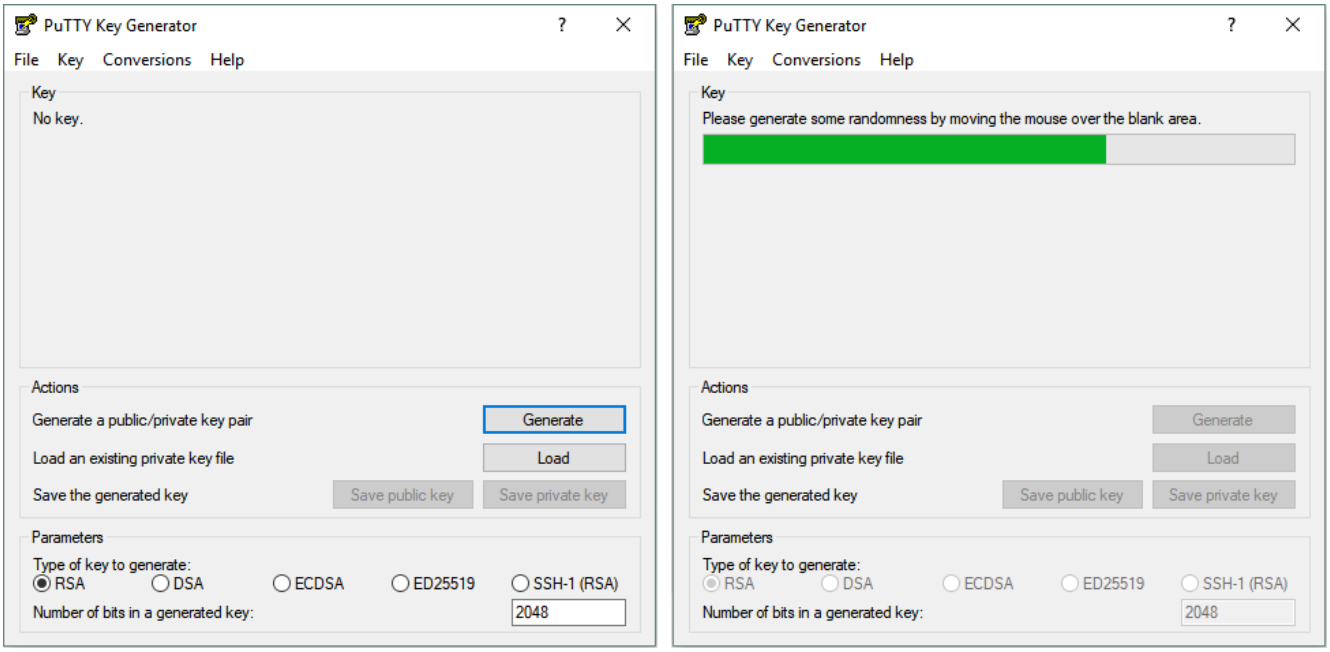

Рис. 16.4 Генерация ключей RSA

2. Зашифруйте закрытый ключ с помощью пароля. В поле **Key passphrase** введите пароль **PassKey** и повторите его в поле **Confirm passphrase**.

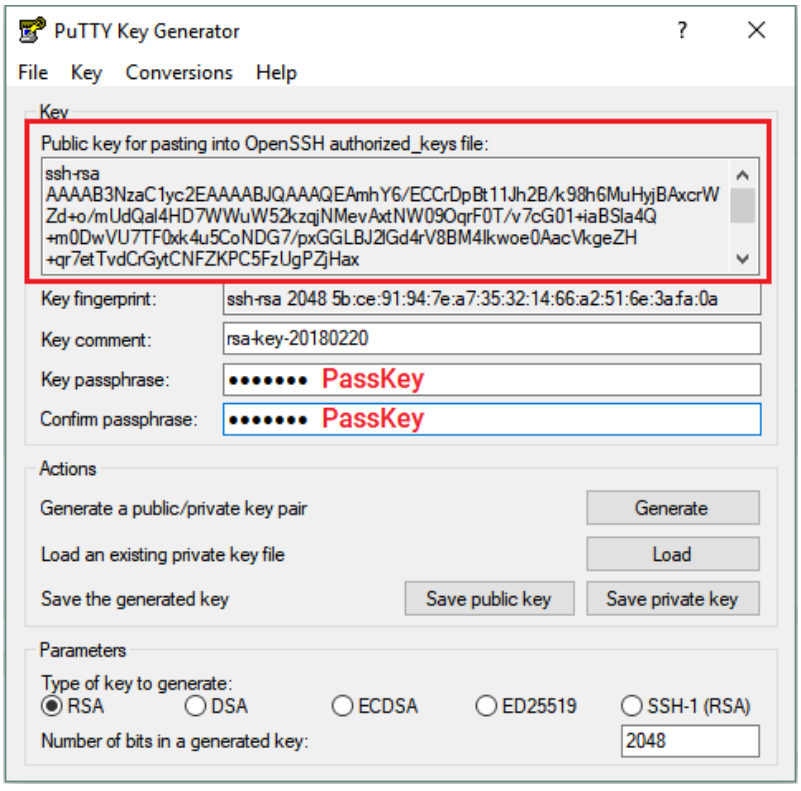

Рис. 16.5 Открытый ключ и шифрование закрытого ключа

В текстовом поле **Public key for pasting into OpenSSH authorized_keys file** содержится открытый ключ, который нужно будет загрузить на коммутатор.

© 2018 D-Link

> **Примечание**
>
> Форматы открытых ключей, сгенерированных в PuTTY и OpenSSH, отличаются. Открытый ключ PuTTY начинается с **—— BEGIN SSH2 PUBLIC KEY**. Если сохранить открытый ключ PuTTY с помощью кнопки **Save public key**, а затем загрузить его в коммутатор, то появится сообщение о неизвестном формате ключа. Для доступа к коммутатору через SSH требуется открытый ключ формата OpenSSH, который начинается с **ssh-rsa AAAA**. Поэтому для подключения к коммутатору по открытому ключу, сгенерированному в PuTTY, сохраняйте его в формате OpenSSH.

3. Сохраните открытый ключ в формате OpenSSH. Нажмите правой кнопкой мыши в текстовом поле **Public key for pasting into OpenSSH authorized_keys file** и выберите **Выделить все**. Скопируйте открытый ключ и вставьте его в текстовый файл. Сохраните файл с именем `id_rsa.pub`.

4. Сохраните закрытый ключ. Нажмите **Save private key**. В открывшемся окне введите имя файла `id_rsa.ppk`. Закрытый ключ следует держать в секрете.

При использовании закрытого ключа `id_rsa.ppk` необходимо каждый раз вводить пароль, которым он зашифрован. При частом подключении по SSH это неудобно, поэтому для хранения паролей будем использовать программу **Pageant**.

5. Запустите программу **Pageant**. После запуска появится иконка  в правом нижнем углу панели задач. Нажмите на иконку правой кнопкой мыши и выберите **Add Key**. Выберите закрытый ключ `id_rsa.ppk`. В приглашении для ввода пароля введите **PassKey**.

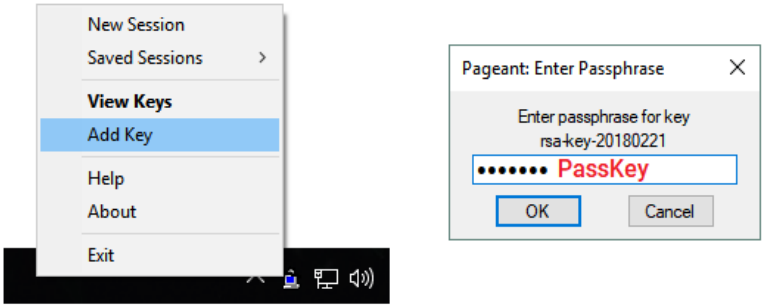

Рис. 16.6 Добавление закрытого ключа в Pageant

© 2018 D-Link

Настройка TFTP-сервера

1. Запустите на рабочей станции TFTP-сервер **tftpd**. В поле **Current Directory** установите рабочую директорию для загрузки файлов.

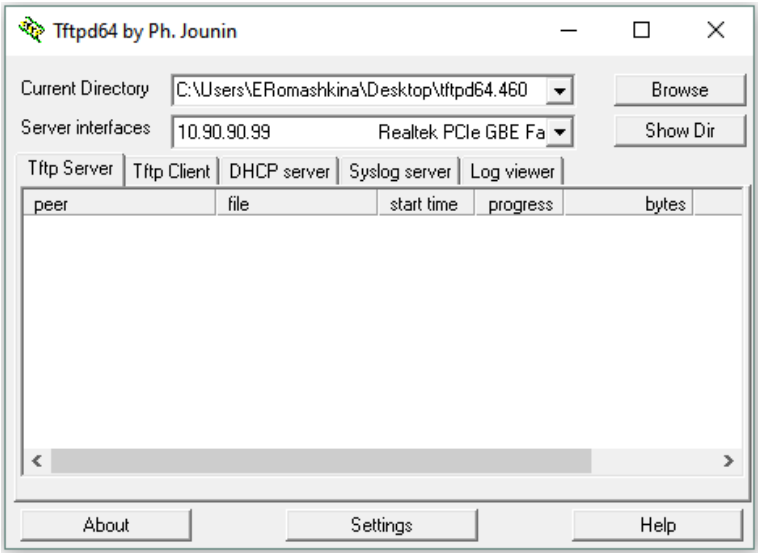

Рис. 16.7 Выбор рабочей директории TFTP-сервера

2. Скопируйте открытый ключ `id_rsa.pub` в рабочую директорию TFTP-сервера.

Настройка коммутатора

1. Подключитесь к интерфейсу командной строки коммутатора. На рабочей станции запустите программу эмуляции терминала **PuTTY**.

2. Сбросьте настройки коммутатора к заводским настройкам по умолчанию:

```
reset config
```

3. Создайте учётную запись администратора:

```
create account admin DlinkUser
```

4. Укажите пароль и подтверждение пароля администратора:

```
Enter a case-sensitive new password: DlinkPassword
Enter the new password again for confirmation: DlinkPassword
```


© 2018 D-Link

5. Проверьте настройки учётных записей пользователей:

```
show account
```

6. Выключите протокол Telnet:

```
disable telnet
```

7. Активируйте протокол SSH:

```
enable ssh
```

8. Настройте аутентификацию с открытым ключом и отключите аутентификацию по паролю и аутентификацию узла:

```
config ssh authmode publickey enable
config ssh authmode password disable
config ssh authmode hostbased disable
```

9. Проверьте выполненные настройки:

```
show ssh authmode
```

10. Установите метод аутентификации с открытым ключом для учётной записи пользователя **DlinkUser**:

```
config ssh user DlinkUser authmode publickey
```

11. Проверьте выполненные настройки:

```
show ssh user authmode
```

12. Настройте параметры SSH-сервера:

```
config ssh server maxsession 8 contimeout 120 authfail 2 rekey never
```


© 2018 D-Link

Описание опций:
maxsession — определяет количество одновременных подключений к SSH-серверу;
countimeout — указывает время в секундах, через которое SSH-подключение закроется при бездействии SSH-клиента;
authfail — указывает максимальное число неудачных попыток подключения;
rekey — указывает время в минутах, через которое повторно генерируются сессионные ключи.

13. Проверьте настройки SSH-сервера:

```
show ssh server
```

14. Загрузите открытый ключ `id_rsa.pub` на коммутатор:

```
download ssh client_pub_key 10.90.90.99 src_file id_rsa.pub
```

15. Посмотрите открытый ключ:

```
show ssh client_pub_key
```

Подключение к коммутатору по SSH

1. На рабочей станции запустите программу **PuTTY**.

2. В открывшемся окне установите галочку **SSH**, в поле **Host Name (or IP address)** введите **10.90.90.90**, в поле **Port** — **22**.

3. В левой части окна выберите **Connection** → **SSH** → **Auth** установите галочку напротив **Attempt authentication using Pageant** и укажите путь к закрытому ключу в графе **Private key file for authentication**.

4. Сохраните настройки. В левой части окна выберите **Session**, в поле **Saved Session** введите **SSH**, затем нажмите **Save**.

5. Нажмите кнопку **Open**.

6. В приглашении **login as** введите **DlinkUser**.

© 2018 D-Link

7. В открывшемся окне командной строки коммутатора после приглашения **UserName** введите **DlinkUser**, после приглашения **PassWord** — **DlinkPassword**.

8. Отключите приглашение ввода имени пользователя и пароля для учётных записей пользователей, которые при подключении по SSH используют метод аутентификации с открытым ключом. Введите в командной строке коммутатора:

```
config ssh publickey bypass_login_screen state enable
```

9. Отключитесь от коммутатора. В командной строке введите:

```
logout
```

10. Повторно подключитесь к коммутатору через SSH.

Появилось приглашение для ввода имени пользователя и пароля? _____

После загрузки открытого ключа на коммутатор, ему присваивается идентификатор Key ID, начиная с 1. Администратор может привязать учётную запись пользователя к открытому ключу по идентификатору. Если открытый ключ относится к учётной записи пользователя, то только этот пользователь получит доступ к коммутатору по SSH. Открытый ключ можно привязать к нескольким учётным записям. Открытый ключ, который не связан с учётной записью пользователя, будет использоваться всеми пользователями.

11. Проверьте, какой идентификатор назначен открытому ключу:

```
show ssh client_pub_key
```

12. Привяжите учётную запись **DlinkUser** к открытому ключу:

```
config ssh client_pubkey_owner key_id 1 add user DlinkUser
```

13. Проверьте выполненные настройки:

```
show ssh client_pub_key
```

14. Создайте ещё одну учётную запись администратора:

```
create account admin Dlink1
```


© 2018 D-Link

15. Укажите пароль и подтверждение пароля администратора:

```
Enter a case-sensitive new password: Dlink1
Enter the new password again for confirmation: Dlink1
```

16. Проверьте настройки учётных записей пользователей:

```
show account
```

17. Установите метод аутентификации с открытым ключом для учётной записи пользователя **Dlink1**:

```
config ssh user Dlink1 authmode publickey
```

18. Проверьте выполненные настройки:

```
show ssh user authmode
```

19. Подключитесь к коммутатору по SSH, используя учётные данные **Dlink1**.

Получилось подключиться? _____

20. Подключитесь к коммутатору через SSH, используя учётные данные **DlinkUser**.

21. Привяжите учётную запись пользователя **Dlink1** к открытому ключу:

```
config ssh client_pubkey_owner key_id 1 add user Dlink1
```

22. Проверьте привязку учётных записей к открытому ключу:

```
show ssh client_pub_key
```

23. Подключитесь к коммутатору через SSH, используя учётные данные **Dlink1**.

Получилось подключиться? _____

Какой можно сделать вывод? _____

© 2018 D-Link

24. Включите приглашение ввода имени пользователя и пароля для учётных записей пользователей, которые используют метод аутентификации с открытым ключом. Введите в командной строке коммутатора:

```
config ssh publickey bypass_login_screen state disable
```

Анализ захваченного трафика

1. На рабочей станции остановите захват трафика в программе **Wireshark**. Установите фильтр для отображения пакетов **SSH**.

2. Выберите любой пакет SSH, щелкните по нему правой кнопкой мыши и выберите **Follow → TCP Stream**.

Зашифрован трафик, передаваемый между рабочей станцией и коммутатором? _____

© 2018 D-Link