



## Пример настройки 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.

### Примечание к настройке

Рассматриваемый пример настройки подходит для коммутаторов с D-Link-like CLI.

### Задача

Необходимо обеспечить безопасный удалённый доступ к интерфейсу командной строки (CLI) коммутатора. Для этой цели настроим доступ к CLI коммутатора по протоколу SSH с аутентификацией по паролю.

IP-адрес управления коммутатора:  
10.90.90.90/8

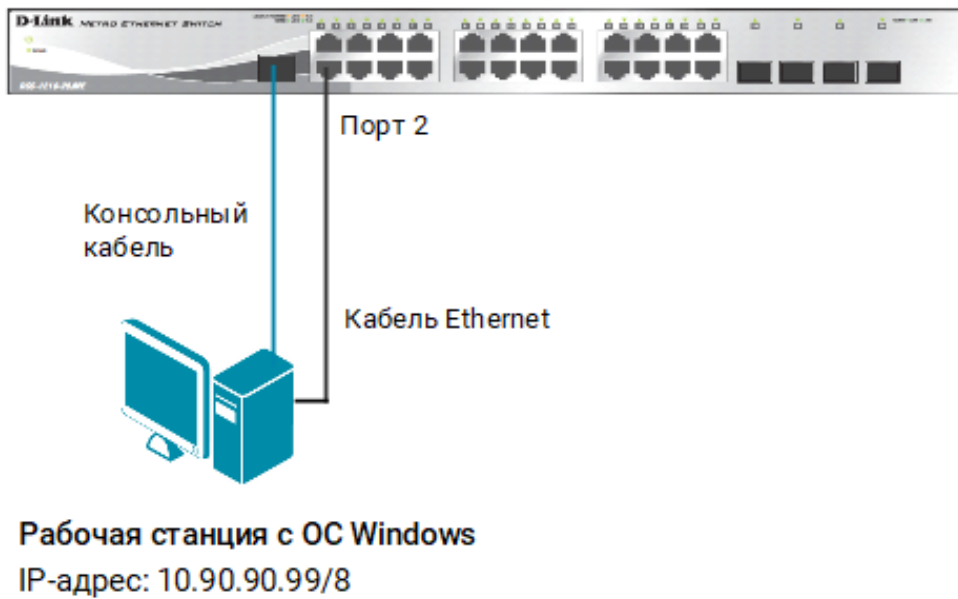


Рис. 1 Схема подключения

## Настройка коммутатора

1. Создайте учётную запись администратора:

```
create account admin DlinkUser
```

2. Укажите пароль и подтверждение пароля администратора:

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

3. Выключите протокол Telnet:

```
disable telnet
```

4. Активируйте протокол SSH:

```
enable ssh
```

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

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

6. Проверьте выполненные настройки:

```
show ssh authmode
```

7. Установите метод аутентификации по паролю для учётной записи пользователя **DlinkUser**:

```
config ssh user DlinkUser authmode password
```

8. Проверьте выполненные настройки:

```
show ssh user authmode
```

9. Настройте параметры SSH-сервера:

```
config ssh server maxsession 8 countimeout 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.

10. Проверьте настройки SSH-сервера:

```
show ssh server
```

## Подключение к коммутатору по SSH

1. Подключите рабочую станцию к коммутатору и настройте статический IP-адрес, как показано на рисунке 1.
2. На рабочей станции запустите программу PuTTY.
3. На экране появится панель входа приложения Putty. В строке **Connection type** выберите **SSH**, в строке **Host Name (or IP address)** введите **10.90.90.90**, в поле **Port** – **22**. Нажмите кнопку **Open**.

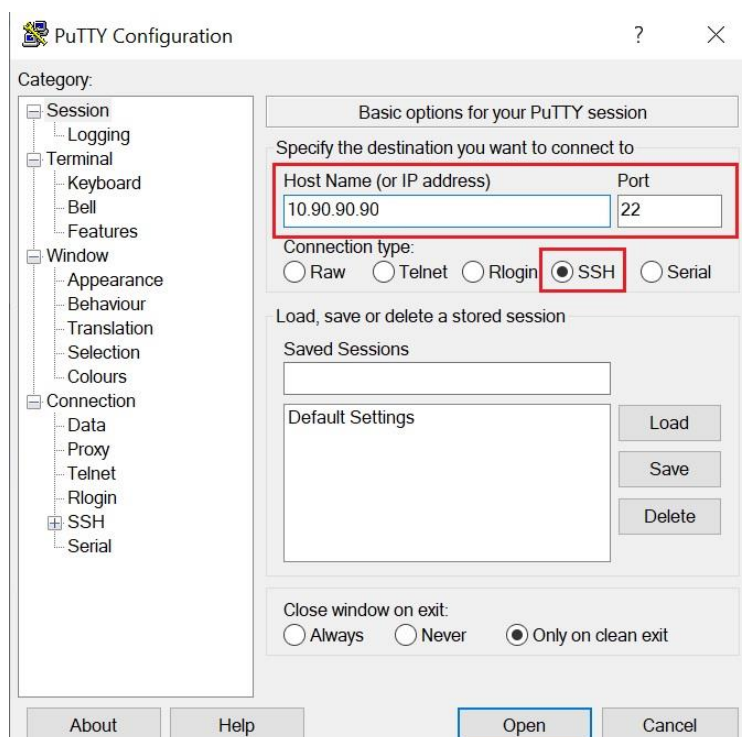


Рис. 2 Окно настройки и подключения Putty

4. В приглашении **login as** введите **DlinkUser**.
5. В открывшемся окне командной строки коммутатора после приглашения **UserName** введите **DlinkUser**, после приглашения **PassWord** – **DlinkPassword**.