Пример настройки удаленного доступа к коммутатору по SSH

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

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 передается 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.

Задача

Нужно 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.

Примечание к настройке

Рассматриваемый пример настройки подходит для следующих серий коммутаторов: DGS-1250, DGS-1510, DGS-1520, DGS-3130, DGS-3630, DXS-3610.

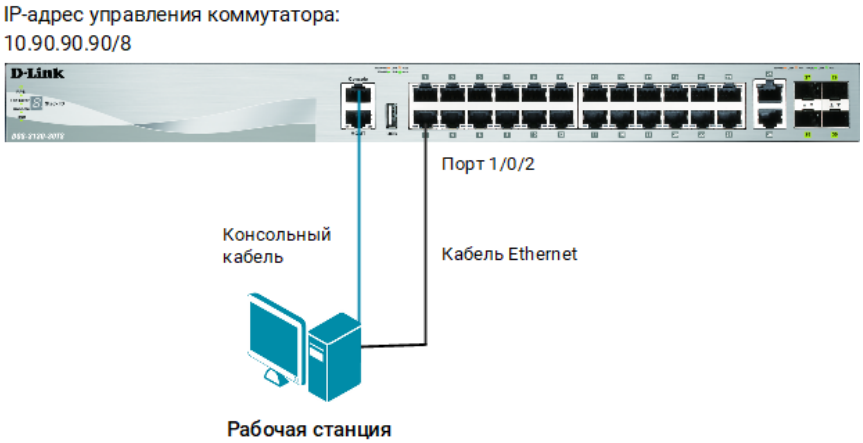

Рисунок 1. Схема подключения

Настройка коммутатора

1. Создайте учётную запись администратора (DlinkUser) и пароль для неё (DlinkPassword):

```
Switch#configure terminal
Switch(config)#username DlinkUser privilege 15 password 0 DlinkPassword
Switch(config)#end
```

> **Примечание**
>
> В этом примере **DlinkUser** – это имя учетной записи, **DlinkPassword** – пароль. Учетной записи DlinkUser назначается максимальный уровень привилегий – 15.

2. Создайте пару ключей (открытый/закрытый), которые будут использоваться коммутатором для шифрования и расшифрования трафика при передаче по SSH-соединению:

```
Switch#crypto key generate rsa modulus 1024
```

3. Активируйте доступ к коммутатору по SSH:

```
Switch#configure terminal
Switch(config)#line ssh
Switch(config-ssh)#login local
Switch(config-ssh)#exit
```

4. Выключите протокол Telnet:

```
Switch(config)#no ip telnet server
```

5. Активируйте протокол SSH:

```
Switch(config)#ip ssh server
```

6. При необходимости настройте параметры SSH-сервера:

```
Switch(config)#ip ssh timeout 120
Switch(config)#ip ssh authentication-retries 2
```

> **Примечание**
>
> Параметры SSH-сервера:
> **timeout** — указывает время в секундах, через которое SSH-подключение закроется при бездействии SSH-клиента;
> **authentication-retries** — указывает максимальное число неудачных попыток подключения.

Настройка рабочей станции с ОС Windows

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**.

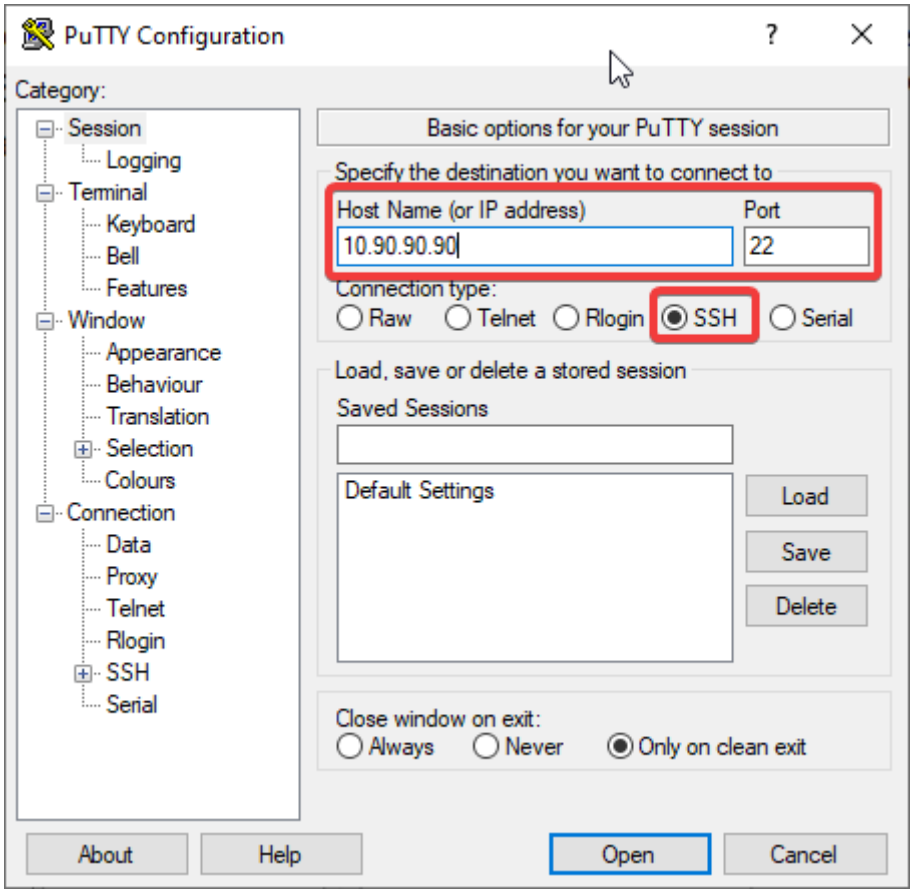

Рисунок 2. Окно настройки и подключения Putty

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

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