

Packet Tracer. Настройка протокола SSH

Топология

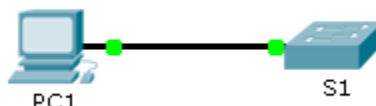


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0

Задачи

Часть 1. Настройка шифрования паролей

Часть 2. Шифрование передачи данных

Часть 3. Проверка реализации SSH

Исходные данные

Для безопасного управления удалёнными подключениями рекомендуется заменить протокол Telnet на протокол SSH. В Telnet используется открытый незашифрованный текстовый обмен. Протокол SSH обеспечивает безопасность удалённых подключений, предоставляя надёжное шифрование всех данных, передаваемых между устройствами. В этом упражнении необходимо обеспечить безопасность удалённого коммутатора с использованием зашифрованного пароля и протокола SSH.

Часть 1. Настройка шифрования паролей

- С помощью командной строки на узле **PC1**, подключитесь к коммутатору **S1** через Telnet. Пароль для пользовательского и привилегированного доступа — **cisco**.
 - Сохраните текущую конфигурацию, чтобы любые допущенные вами ошибки можно было отменить, отключив питание коммутатора **S1**.
 - Отобразите текущую конфигурацию и обратите внимание на то, что пароли написаны в виде открытого текста. Введите команду, позволяющую шифровать незашифрованные пароли:
-
- Убедитесь, что пароли зашифрованы.

Часть 2. Обеспечение защищенной коммуникации

Шаг 1: Настройте имя домена IP и создайте ключи шифрования.

В принципе, использование Telnet небезопасно, поскольку текстовые данные передаются в незашифрованном виде. Поэтому рекомендуется по возможности использовать протокол SSH.

- Присвойте домену имя **netacad.pka**.

- b. Для шифрования данных требуются ключи шифрования. Создайте RSA ключи длиной 1024 бит.

Шаг 2: Создайте пользователя SSH и перенастройте линии VTY на доступ только по протоколу SSH.

- a. Создайте пользователя-администратора (**administrator**) с паролем **cisco**.
- b. Настройте линии VTY для проверки регистрационных данных в локальных базах данных имён пользователей, а также для разрешения удалённого доступа только по протоколу SSH. Удалите существующий пароль линии VTY.

Часть 3. Проверка реализации протокола SSH

- a. Завершите сеанс работы Telnet и попробуйте снова войти в систему через Telnet. Попытка должна завершиться неудачей.
- b. Попробуйте войти в систему через протокол SSH. Введите **ssh** и нажмите **ВВОД**, не добавляя какие-либо параметры, чтобы отобразить инструкции использования команды. Совет. Параметр **-1** — это буква «L», а не цифра 1.
- c. После успешного входа перейдите в режим привилегированного доступа EXEC и сохраните конфигурацию. Если вам не удалось получить доступ к коммутатору **S1**, отключите питание и повторите шаги, описанные в части 1.