# Практическая работа №8
# Вариант 6

Кирилл Денисов ИВБО-02-19

29 января 2022 г.

*Таблица 1 — Таблица адресации*

| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** | **Шлюз по умолчанию** |
|---|---|---|---|---|
| R1_DENISOV | G0/1 | 192.168.1.6 | 255.255.255.0 | — |
| S1 | VLAN 1 | 192.168.1.16 | 255.255.255.0 | 192.168.1.6 |
| PC-A | NIC | 192.168.1.26 | 255.255.255.0 | 192.168.1.6 |

**Часть 1.** Настройка основных параметров устройств

**Шаг 1.1.** Создание сети согласно топологии

Создадим сеть для выполнения данного практического задания согласно топологии. (см. рисунок 1).

**Шаг 1.2.** Выполнение инициализации и перезагрузки маршрутизатора и коммутатора

Дождемся инициализации маршрутизатора и коммутатора S1 и выполним их перезагрузку.

**Шаг 1.3.** Настройка маршрутизатора

Подключимся к маршрутизатору R1_DENISOV и произведем его настройку в соответствии с заданием. Приведем текущую конфигурацию маршрутизатора.

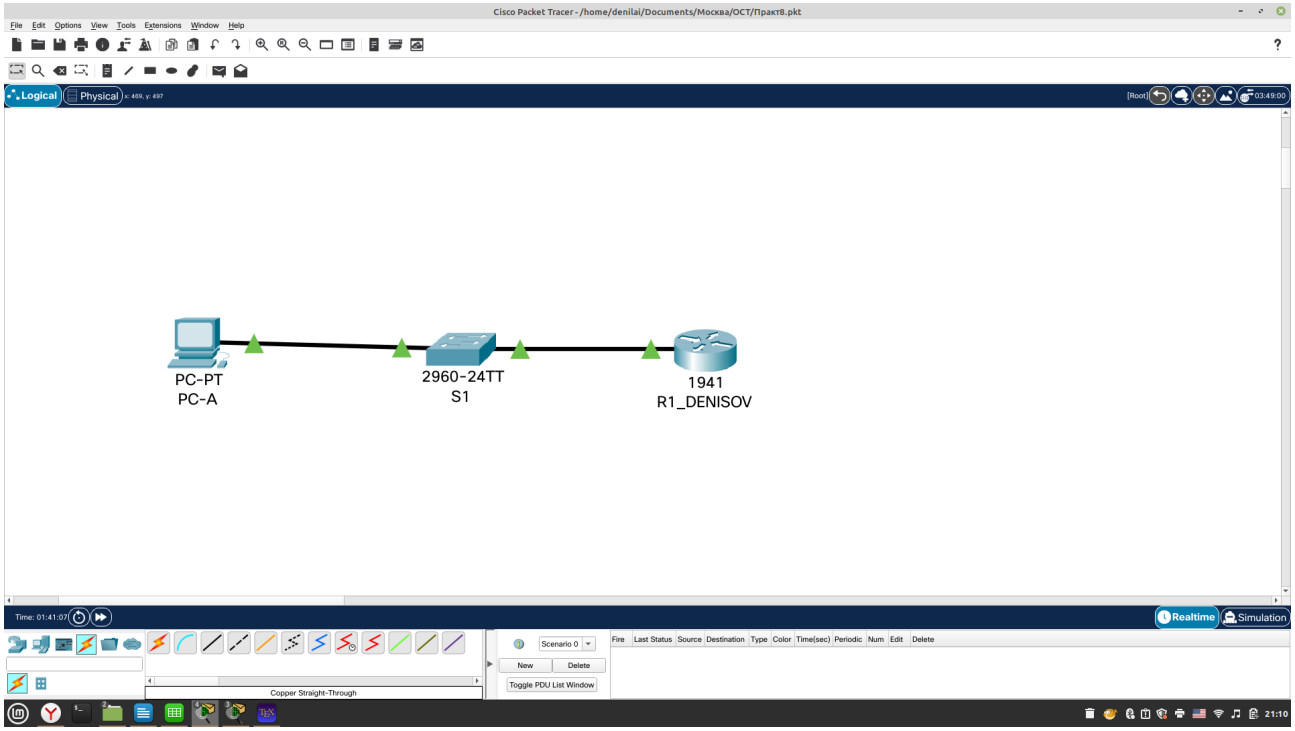


Рисунок 1 — Топология сети

```
R1_DENISOV#show running-config
Building configuration...

Current configuration : 1211 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 10
!
hostname R1_DENISOV
!
login block-for 30 attempts 2 within 120
!
enable secret 5 $1$mERr$5wXi8fVAu3dNc0gNCjvIQ1
!
ip cef
no ipv6 cef
!
username SSHadmin privilege 15 secret 5 $1$mERr$uMzC7If3IbCZVifeGQ3rg/
!
license udi pid CISCO1941/K9 sn FTX15244MJ5-
!
ip domain-name cisco-lab.ru
!
```

```
spanning-tree mode pvst
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/1
ip address 192.168.1.6 255.255.255.0
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
ip access-list extended sl_def_acl
deny tcp any any eq telnet
deny tcp any any eq www
deny tcp any any eq 22
permit tcp any any eq 22
!
banner motd ^CAuthorized users only!^C
!
line con 0
exec-timeout 5 0
password 7 0822455D0A16
login
!
line aux 0
!
line vty 0 4
exec-timeout 5 0
password 7 0822455D0A16
login local
transport input ssh
  !
end

```

После проведения настройки сохраним текущую конфигурацию в файл загрузочной конфигурации с помощью команды `copy running-config`

`startup-config`.

**Шаг 1.4.** Установка более надежных паролей

Согласно данным рекомендациям по лучшим практическим методикам надежные пароли, примеры которых приведены в этой лабораторной работе, необходимо всегда использовать в реальной работе. Однако для упрощения выполнения работы в остальных лабораторных работах данного курса используются пароли cisco и class.

Измените зашифрованный пароль привилегированного режима EXEC в соответствии с рекомендациями. Установите следующий пароль: **Enablep@55** с помощью команды `enable secret Enablep@55`.

Установим минимальную длину 10 символов для всех паролей с помощью команды `security passwords min-length 10`.

**Шаг 1.5.** Настройка компьютер PC-A Настроим для PC-A IP-адрес и маску подсети и шлюз по умолчанию в соответствии с заданием, приведенным в таблице 1 (см. рисунок 2).

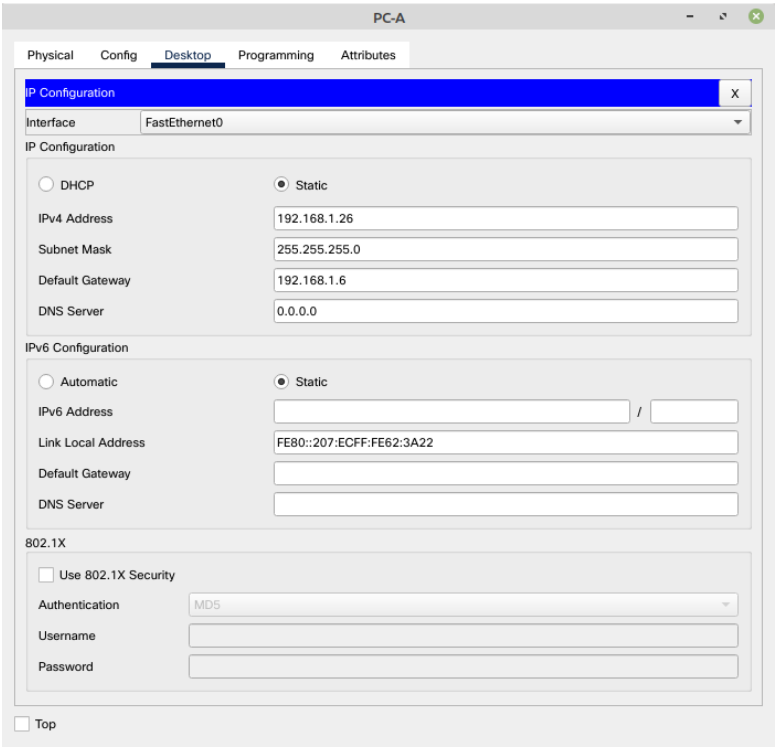


Рисунок 2

**Шаг 1.6.** Проверка подключения к сети

Пошлем с PC-A эхо-запрос на маршрутизатор R1_DENISOV . Убедимся, что эхо-запрос выполнен успешно (см. рисунок 3).

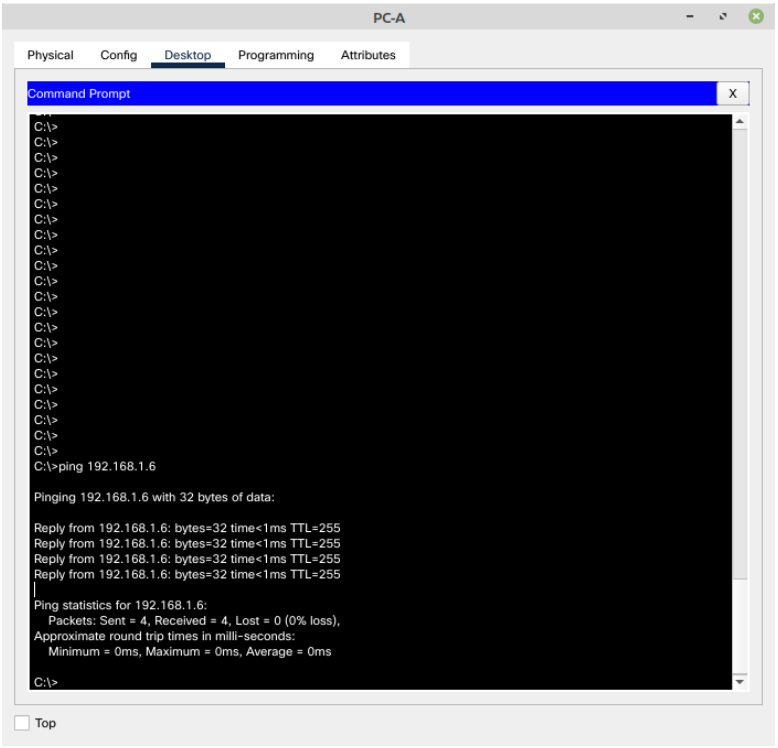


Рисунок 3 — Эхо запрос на маршрутизатор R1_DENISOV

**Часть 2.** Настройка маршрутизатора для доступа по протоколу SSH и обеспечение базовых мер безопасности

**Шаг 2.1.** Настройка аутентификации устройств

Перейдем в режим глобальной конфигурации. Зададим имя для маршрутизатора с помощью команды `hostname R1_DENISOV` . Зададим домен для устройства с помощью команды `ip domain-name cisco-lab.ru`

**Шаг 2.2.** Создание ключа шифрования с указанием его длины

Перейдем в режим глобальной конфигурации. Создадми ключ шифрования с помощью команды `crypto key generate rsa modulus 1024.`

**Шаг 2.3.** Создание пользователя в локальной базе учетных записей

Перейдем в режим глобальной конфигурации. Создадим пользователя с помощью команды `username SSHadmin privilege 15 secret Admin1p@55`.

**Шаг 2.4.** Активация протокола SSH на линиях VTY

Перейдем в режим конфигурации линии с помощью команды `line vty 0 4`.

Активируем протокол SHH с помощью команды `transport input telnet ssh`.

Изменим способ входа в систему таким образом, чтобы использовалась проверка пользователей по локальной базе учетных записей с помощью команды `login local`.

**Шаг 2.5.** Сохраните текущую конфигурацию в файл загрузочной конфигурации

Для сохранения конфигурации выполним комнаду `opy running-config startup-config`.

**Шаг 2.6.** Установка соединения с маршрутизатором по протоколу SSH Установим соединение с маршрутизатором R1_DENISOV из командной строки компьютера PC-A (см. рисунок 4).

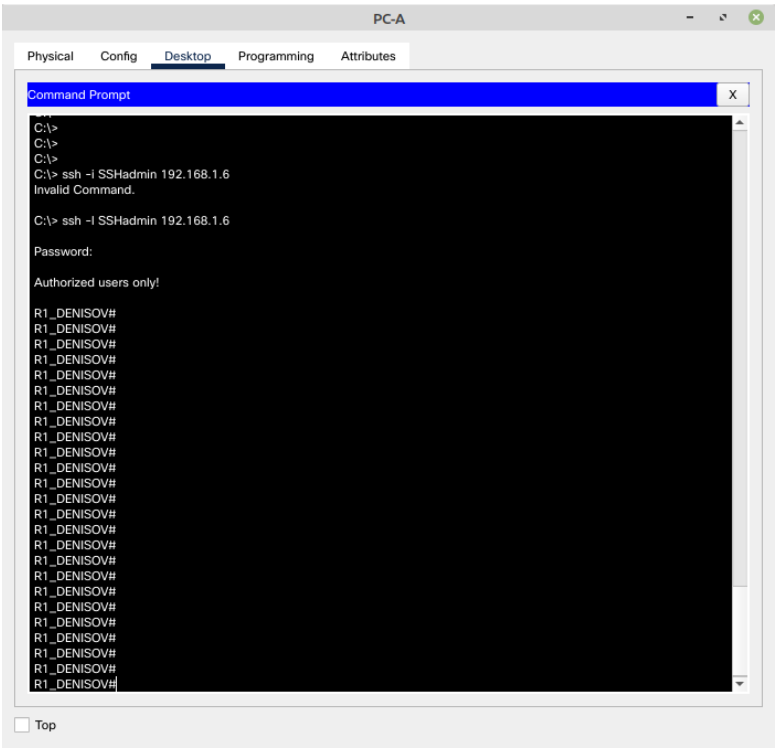


Рисунок 4 — Авторизация на маршрутизаторе R1_DENISOV по SHH

После совершения аутентификации видим приглашение для ввода привилегированного режима.

**Шаг 2.7.** Проверка соблюдения требований безопасности

**Вопрос:** Подключитесь к маршрутизатору R1_DENISOV по протоколу Telnet. Разрешает ли R1_DENISOV подключение по протоколу Telnet? Дайте пояснение.

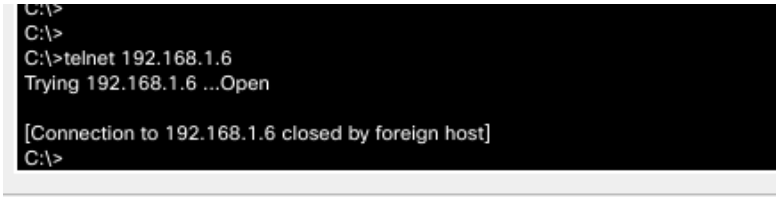


Рисунок 5 — Отклонение подключения к R1_DENISOV по протоколу telnet

**Ответ:** *Подключение отклонено, потому что мы установили только SSH в качестве протокола соединения с маршрутизатором (см. рисунок 5).*

**Вопрос:** Подключитесь к маршрутизатору R1_DENISOV по протоколу SSH. Разрешает ли R1_DENISOV подключение по протоколу SSH?

**Ответ:** *Да, подключение выполнено успешно (см. рисунок 4).*

**Вопрос:** Намеренно укажите неверное имя пользователя и пароль, чтобы проверить, будет ли заблокирован доступ к системе после двух неудачных попыток. Что произошло после ввода неправильных данных для входа в систему во второй раз?

**Ответ:** *Возможность подключения заблокирована на 30 секунд после того, как в течение 120 секунд неправильные данные были введены больше 2 раз.*

**Вопрос:** Из сеанса подключения к маршрутизатору с помощью консоли отправьте команду `show login`, чтобы проверить состояние входа в систему.

**Ответ:**

**Вопрос:** По истечении 30 секунд повторите попытку подключения к R1_DENISOV по протоколу SSH и войдите в систему, используя имя SSHadmin и пароль Admin1p@55. Что отобразилось после успешного входа в систему?

**Ответ:** *По истечении 30 секунд попытка авторизации на маршрутизаторе R1_DENISOV прошла успешно. Таймаут истек. После совершения аутентификации видим приглашение для ввода привилегированного режима.*

**Вопрос:** Войдите в привилегированный режим EXEC и введите в качестве пароля Enablep@55. Если вы неправильно вводите пароль, прерывается ли сеанс SSH после двух неудачных попыток в течение 120 секунд? Дайте пояснение.

**Часть 3.** Настройка коммутатора для доступа по протоколу SSH и обеспечение базовых мер безопасности

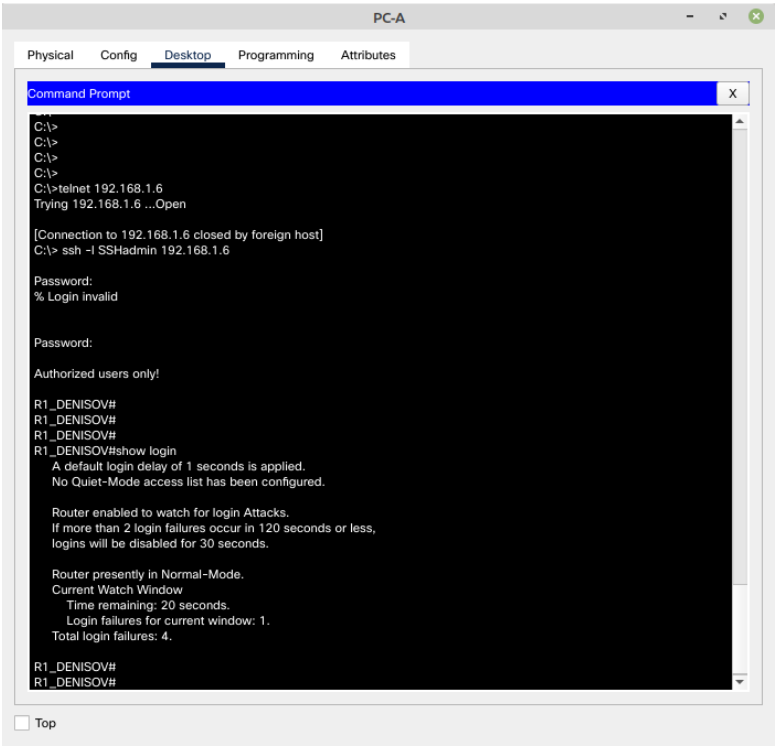


Рисунок 6 — Результат работы команды show login на маршрутизаторе R1_DENISOV

**Шаг 3.1.** Настройте основные параметры коммутатора

По аналогии с маршрутизатором R1_DENISOV , настроим коммутатор S1 . Приведем его конфигурацию.

```
S1#show running-config
Building configuration...

Current configuration : 1711 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$5wXi8fVAu3dNc0gNCjvIQ1
!
no ip domain-lookup
ip domain-name cisco-lab.ru
!
username SSHadmin secret 5 $1$mERr$uMzC7If3IbCZVifeGQ3rg/
!
spanning-tree mode pvst
```

```
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
shutdown
!
interface FastEthernet0/3
shutdown
!
interface FastEthernet0/4
shutdown
!
interface FastEthernet0/5
shutdown
!
interface FastEthernet0/6
shutdown
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
```

```
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
ip address 192.168.1.16 255.255.255.0
!
banner motd ^CAuthorized users only!^C
!
!
!
line con 0
password 7 0822455D0A16
login
exec-timeout 5 0
!
line vty 0 4
exec-timeout 5 0
password 7 0822455D0A16
login local
transport input ssh
line vty 5 15
```

```
 exec-timeout 5 0
118 password 7 0822455D0A16
 login local
120 transport input ssh
 !
122 end
```

**Шаг 3.2.** Настройка коммутатора для соединения по протоколу SSH

По аналогии с маршрутизатором R1_DENISOV произведем настройку коммутатора S1 для соединения по протоколу SSH.

Перейдем в режим глобальной конфигурации. Зададим имя для маршрутизатора с помощью команды `hostname R1_DENISOV` . Зададим домен для устройства с помощью команды `ip domain-name cisco-lab.ru`.

Создадми ключ шифрования с помощью команды `crypto key generate rsa modulus 1024` .

Создадим пользователя с помощью команды `username admin privilege 15 secret Enablep@55`.

Перейдем в режим конфигурации линии с помощью команды `line vty 0 4`.

Активируем протокол SHH с помощью команды `transport input telnet ssh`.

Изменим способ входа в систему таким образом, чтобы использовалась проверка пользователей по локальной базе учетных записей с помощью команды `login local`.

**Шаг 3.3.** Отключение неиспользуемых портов

Перейдем в режим глобальной конфигурации, затем в режим конфигурации множества интерфейсов с помощью команды `interface range FastEthernet0/2 - 24` и выключим их с помощью команды `shutdown`. После этого, все неиспользуемые порты будут отключены.

**Шаг 3.4.** Установка соединение с коммутатором по протоколу SSH

С компьютера PC-A установим подключение по протоколу SSH к интерфейсу SVI коммутатора S1. Подключение проведено успешно (см. рисунок 7), причем соединение по протоколу telnet отклоняется по соображениям безопасности.

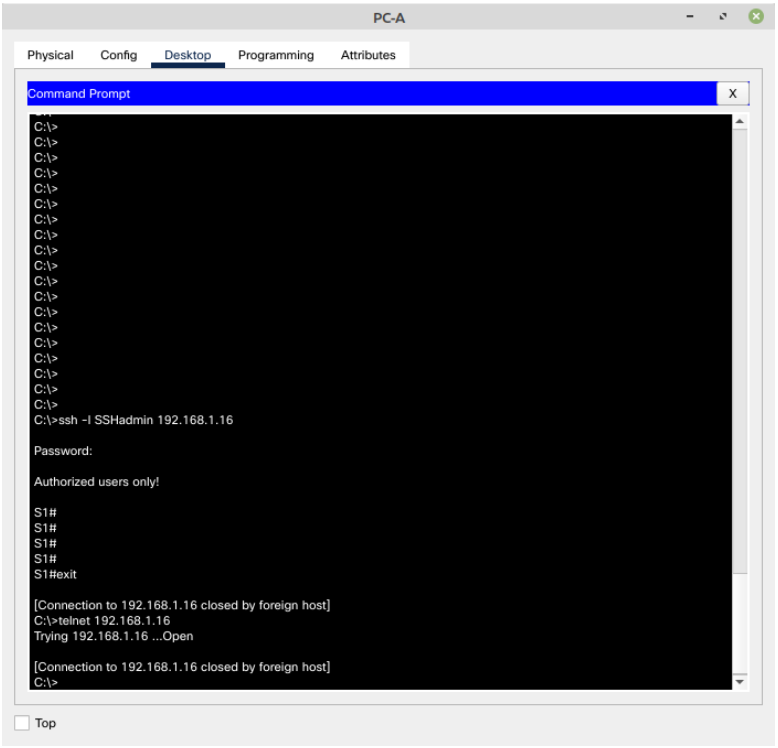


Рисунок 7 — Соединение с коммутатором S1 по протоколу SSH

**Шаг 3.5.** Проверка мер безопасности

Убедимся что протокол Telnet на коммутаторе отключен.

Подключимся к коммутатору по протоколу SSH и намеренно укажем неверное имя пользователя и пароль, чтобы проверить, будет ли заблокирован доступ к системе.

По истечении 30 секунд повторим попытку подключения к R1_DENISOV по протоколу SSH и войдем в систему, используя имя пользователя **SSHadmin** и пароль **Admin1p@55**.

**Часть 4.** Настройка протокола SSH с использованием интерфейса командной строки (CLI) коммутатора

**Шаг 4.1.** Параметры для клиента SSH в Cisco IOS

Воспользуемся подсказкой «?» для команды `ssh` (см. рисунок 8).


Рисунок 8 — Параметры команды ssh в Cisco IOS

**Шаг 4.2.** Установка соединения с маршрутизатором R1_DENISOV по протоколу SSH с коммутатора S1

Чтобы подключиться к маршрутизатору R1_DENISOV по протоколу SSH, введем команду `ssh -l SSHadmin 192.168.1.6`. Это позволит нам войти в систему под именем SSHadmin. При появлении приглашения введите в качестве пароля **Admin1p@55** (см. рисунок 9).

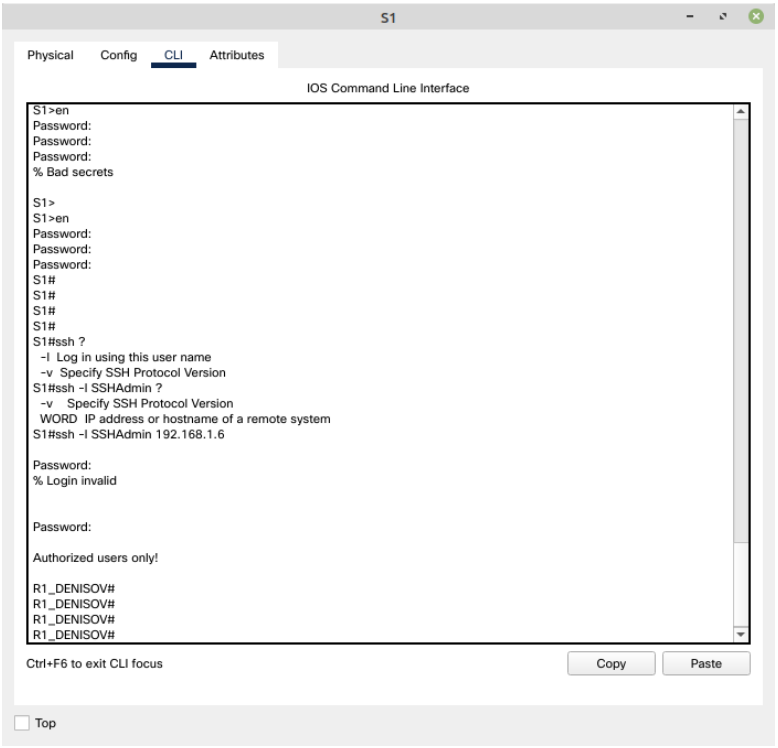


Рисунок 9 — Установка соединения с маршрутизатором R1_DENISOV по протоколу SSH с коммутатора S1

**Часть 5.** Защита лабораторной работы (ответ контрольные вопросы и вопросы преподавателя)

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

**Ответ:** *Нужно настроить доступ по SSH и создать несколько пользователей на узле при помощи команды* `username`.

**Вопрос:** Какие версии протокола SSH поддерживаются при использовании интерфейса командной строки?

**Ответ:** *Существует две версии SSH, SSH версии 1 и SSH версии 2. Второй обеспечивает более высокий уровень безопасности.*