Лабораторная работа. Доступ к сетевым устройствам по протоколу SSH

# Топология



# Таблица адресации

| Устройство | Интерфейс | IP-адрес | Маска подсети | Шлюз по умолчанию |
| --- | --- | --- | --- | --- |
| R1 | G0/0/1 | 192.168.1.1 | 255.255.255.0 | — |
| S1 | VLAN 1 | 192.168.1.11 | 255.255.255.0 | 192.168.1.1 |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |

# Задачи

Часть 1. Настройка основных параметров устройства

Часть 2. Настройка маршрутизатора для доступа по протоколу SSH

Часть 3. Настройка коммутатора для доступа по протоколу SSH

Часть 4. SSH через интерфейс командной строки (CLI) коммутатора

## Настройка основных параметров устройств

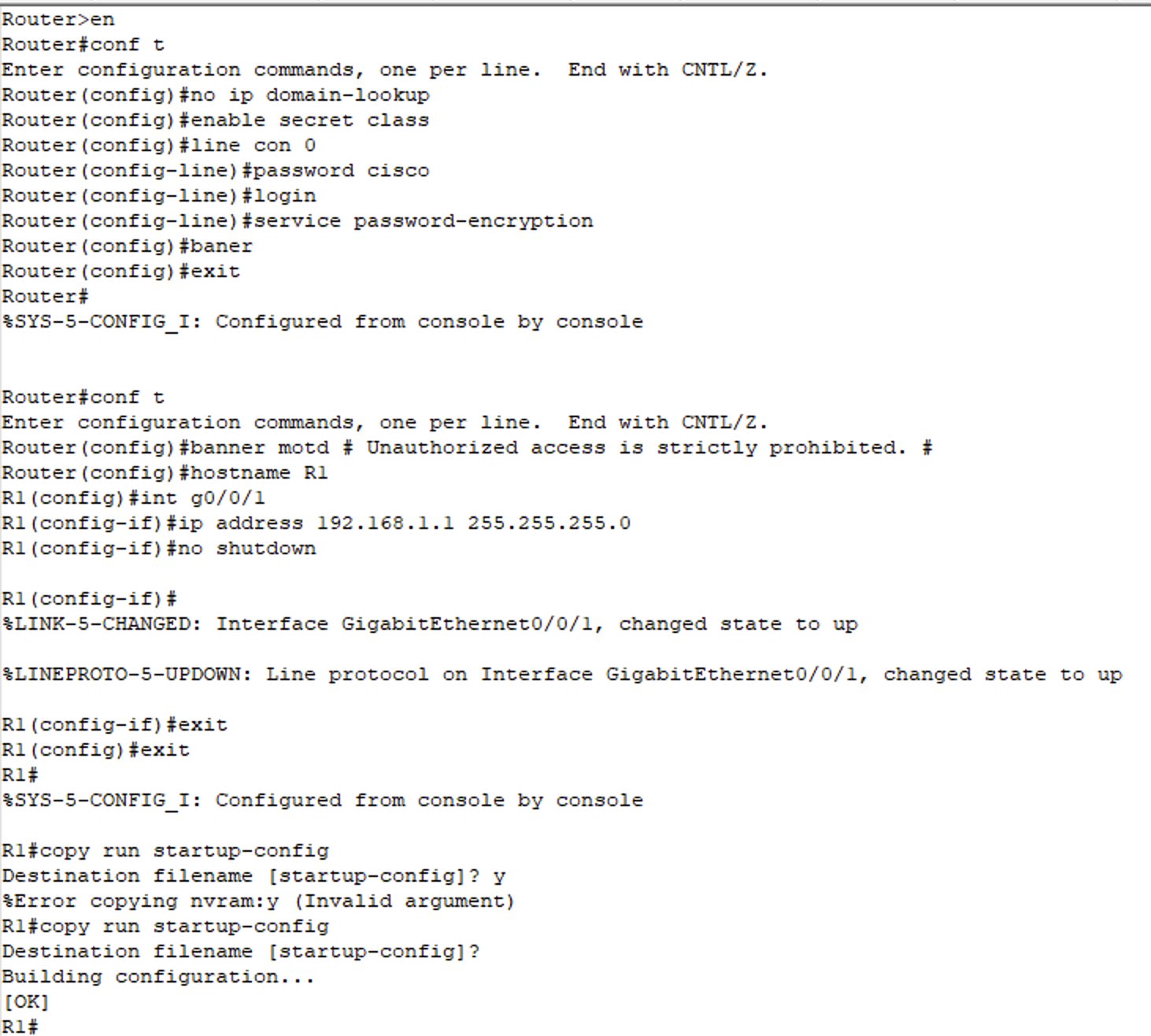
### Создайте сеть согласно топологии.

### Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

### Настройте маршрутизатор.

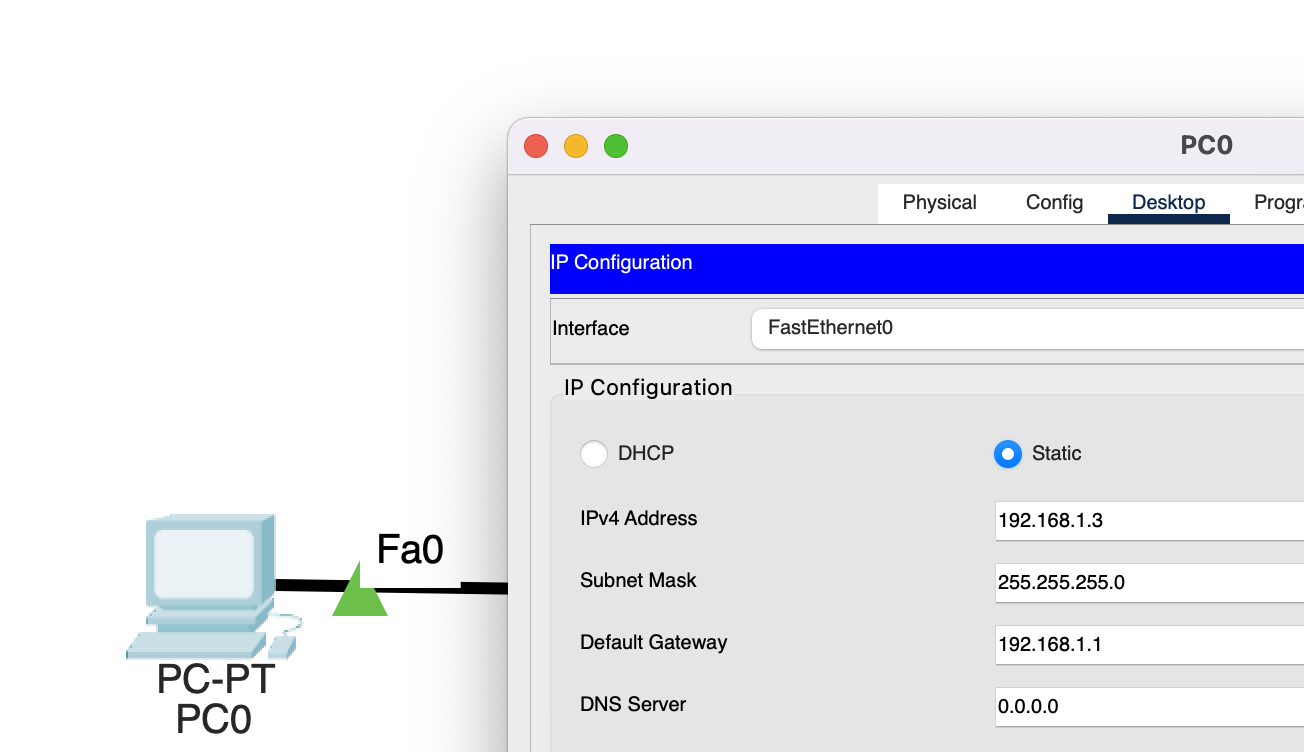
Откройте окно конфигурации

* + - 1. Подключитесь к маршрутизатору с помощью консоли и активируйте привилегированный режим EXEC.
      2. Войдите в режим конфигурации.
      3. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
      4. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
      5. Назначьте **cisco** в качестве пароля консоли и включите вход в систему по паролю.
      6. Назначьте **cisco** в качестве пароля VTY и включите вход в систему по паролю.
      7. Зашифруйте открытые пароли.
      8. Создайте баннер, который предупреждает о запрете несанкционированного доступа.
      9. Настройте и активируйте на маршрутизаторе интерфейс G0/0/1, используя информацию, приведенную в таблице адресации.
      10. Сохраните текущую конфигурацию в файл загрузочной конфигурации.



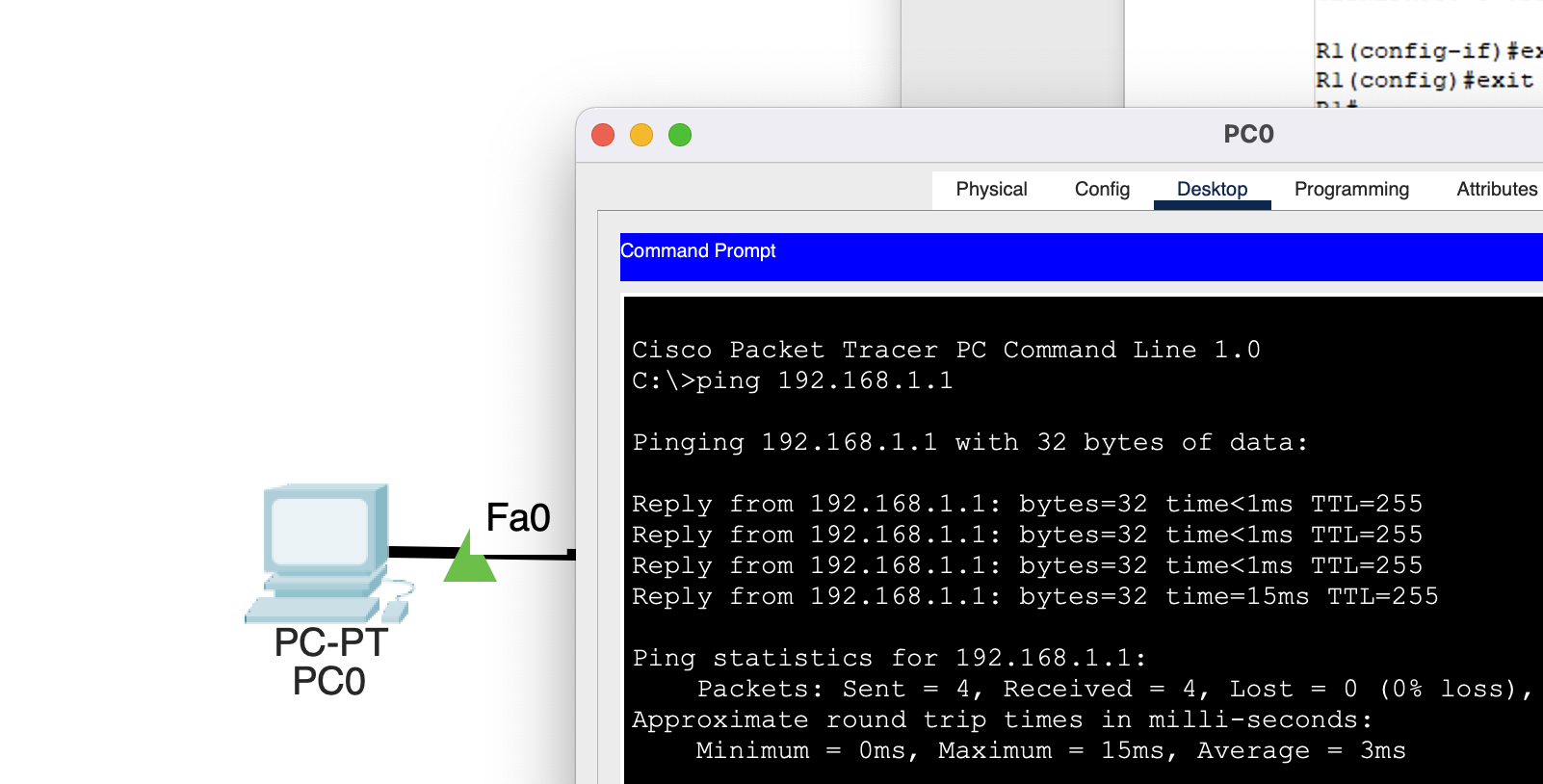
### Настройте компьютер PC-A.

* + - 1. Настройте для PC-A IP-адрес и маску подсети.
      2. Настройте для PC-A шлюз по умолчанию.



### Проверьте подключение к сети.

Пошлите с PC-A команду Ping на маршрутизатор R1. Если эхо-запрос с помощью команды ping не проходит, найдите и устраните неполадки подключения.



Закройте окно настройки.

## Настройка маршрутизатора для доступа по протоколу SSH

### Настройте аутентификацию устройств.

При генерации ключа шифрования в качестве его части используются имя устройства и домен. Поэтому эти имена необходимо указать перед вводом команды **crypto key**.

Откройте окно конфигурации

* + - 1. Задайте домен для устройства.

R1(config)#ip domain-name otus.domain

### Создайте ключ шифрования с указанием его длины.

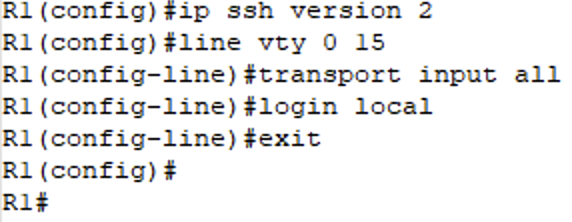
### Создайте имя пользователя в локальной базе учетных записей.

Настройте имя пользователя, используя **admin** в качестве имени пользователя и **Adm1nP @55** в качестве пароля.

R1(config)#username admin privilege 15 secret Adm1nP @55

### Активируйте протокол SSH на линиях VTY.

* + - 1. Активируйте протоколы Telnet и SSH на входящих линиях VTY с помощью команды **transport input**.
      2. Измените способ входа в систему таким образом, чтобы использовалась проверка пользователей по локальной базе учетных записей.



### Сохраните текущую конфигурацию в файл загрузочной конфигурации.

R1#copy run startup-config

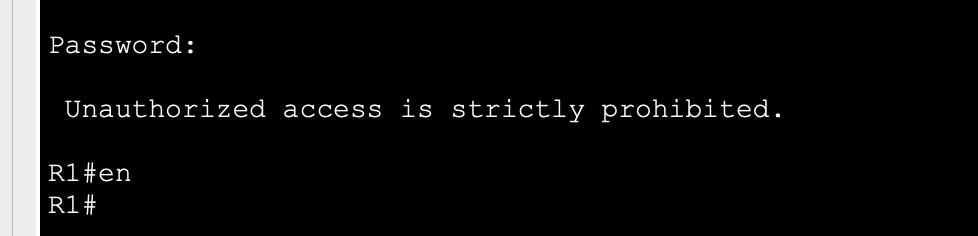
Destination filename [startup-config]?

Building configuration...

[OK]

### Установите соединение с маршрутизатором по протоколу SSH.

* + - 1. Запустите Tera Term с PC-A.
      2. Установите SSH-подключение к R1. Use the username **admin** and password **Adm1nP@55**. У вас должно получиться установить SSH-подключение к R1.



Закройте окно настройки.

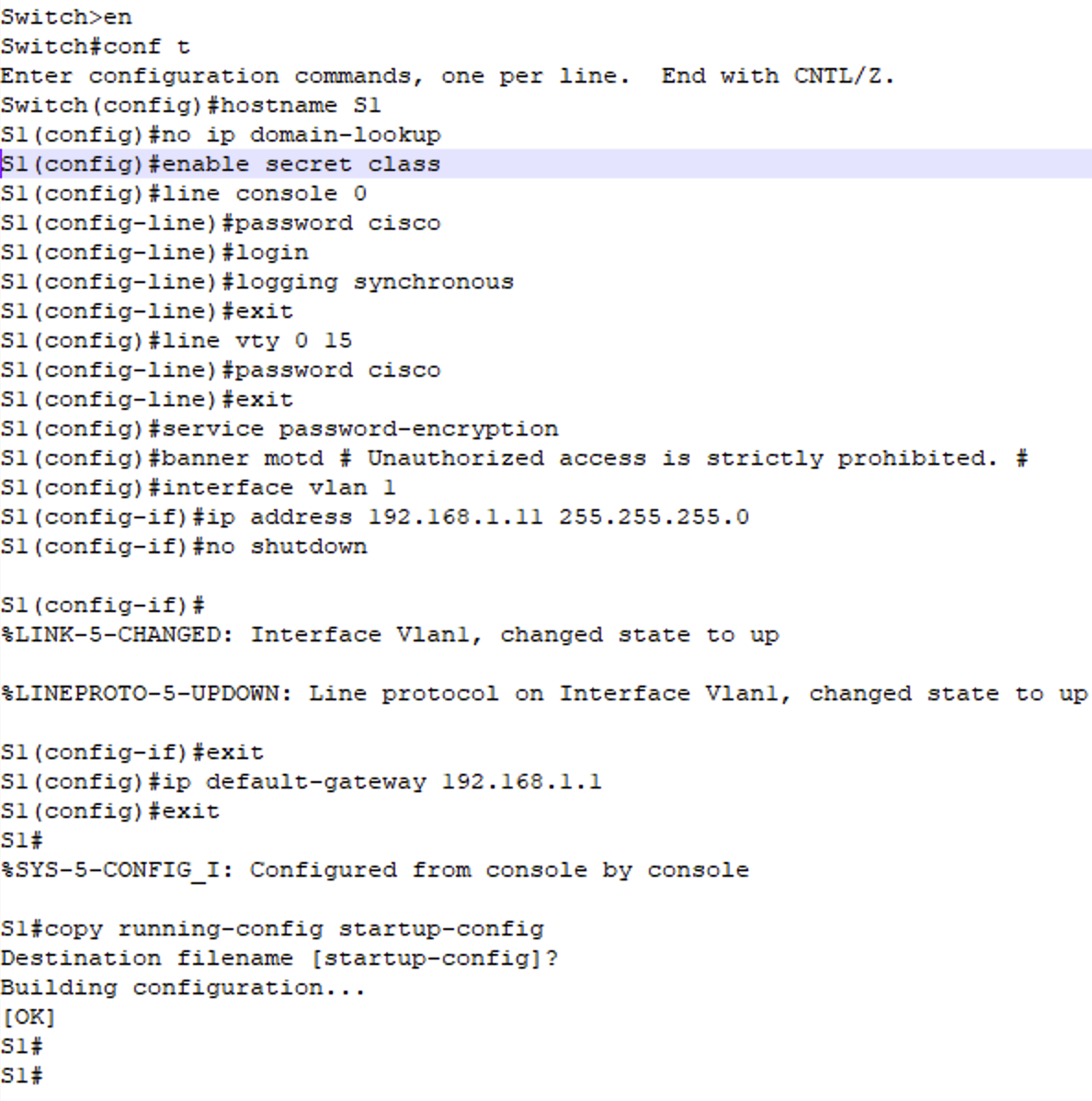
## Настройка коммутатора для доступа по протоколу SSH

В части 3 вам предстоит настроить коммутатор для приема подключений по протоколу SSH, а затем установить SSH-подключение с помощью программы Tera Term.

### Настройте основные параметры коммутатора.

Откройте окно конфигурации

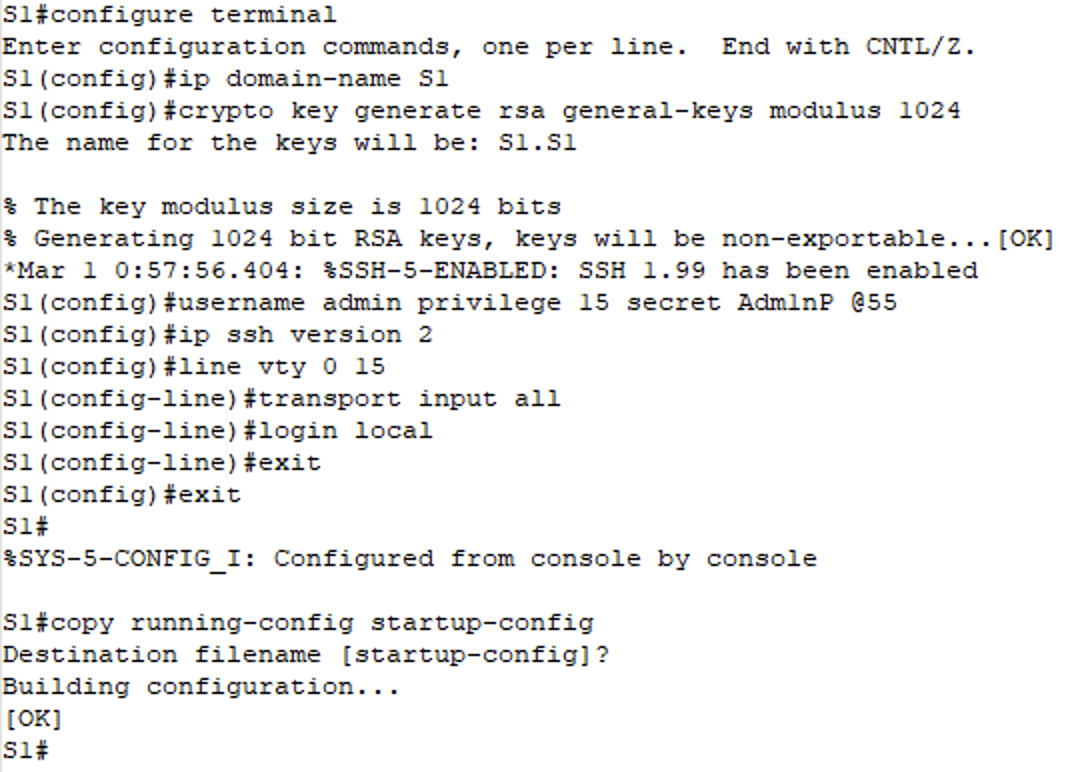
* + - 1. Подключитесь к коммутатору с помощью консольного подключения и активируйте привилегированный режим EXEC.
      2. Войдите в режим конфигурации.
      3. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
      4. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
      5. Назначьте **cisco** в качестве пароля консоли и включите вход в систему по паролю.
      6. Назначьте **cisco** в качестве пароля VTY и включите вход в систему по паролю.
      7. Зашифруйте открытые пароли.
      8. Создайте баннер, который предупреждает о запрете несанкционированного доступа.
      9. Настройте и активируйте на коммутаторе интерфейс VLAN 1, используя информацию, приведенную в таблице адресации.
      10. Сохраните текущую конфигурацию в файл загрузочной конфигурации.



### Настройте коммутатор для соединения по протоколу SSH.

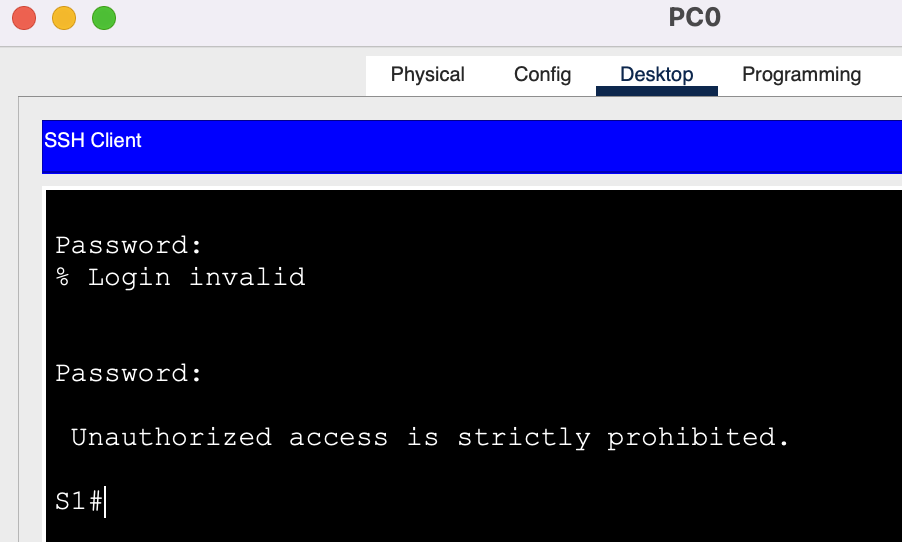
Для настройки протокола SSH на коммутаторе используйте те же команды, которые применялись для аналогичной настройки маршрутизатора в части 2.

* + - 1. Настройте имя устройства, как указано в таблице адресации.
      2. Задайте домен для устройства.
      3. Создайте ключ шифрования с указанием его длины.
      4. Создайте имя пользователя в локальной базе учетных записей.
      5. Активируйте протоколы Telnet и SSH на линиях VTY.
      6. Измените способ входа в систему таким образом, чтобы использовалась проверка пользователей по локальной базе учетных записей.



### Установите соединение с коммутатором по протоколу SSH.

Установлено SSH-соединение с коммутатором



Закройте окно настройки.

## Настройка протокола SSH с использованием интерфейса командной строки (CLI) коммутатора

### Посмотрите доступные параметры для клиента SSH в Cisco IOS.

Откройте окно конфигурации

Используйте вопросительный знак (**?**), чтобы отобразить варианты параметров для команды **ssh**.

S1# **ssh?**

-c Select encryption algorithm

-l Log in using this user name

-m Select HMAC algorithm

-o Specify options

-p Connect to this port

-v Specify SSH Protocol Version

-vrf Specify vrf name

WORD IP-адрес или имя хоста удаленной системы

### Установите с коммутатора S1 соединение с маршрутизатором R1 по протоколу SSH.

* + - 1. Чтобы подключиться к маршрутизатору R1 по протоколу SSH, введите команду **–l admin**. Это позволит вам войти в систему под именем **admin**. При появлении приглашения введите в качестве пароля **Adm1nP@55**

S1# **ssh -l admin 192.168.1.1**

Password:

Unauthorized access is strictly prohibited.

R1>

#### Вопрос:

Какие версии протокола SSH поддерживаются при использовании интерфейса командной строки?

SSH v1 и V2

#### Закройте окно настройки. SSH v1 и V2

# Вопрос для повторения

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

Нужно cоздать пользователя и задать пароль каждого пользователя в локальную базу данных с помощью команды username.