Отчёт по лабораторной работе 2

Предварительная настройка оборудования Cisco

Авдадаев Джамал

Содержание

1 Введение

1.1 Цель работы

Получить основные навыки по начальному конфигурированию оборудования Cisco.

2 Ход выполнения

В логической рабочей области Packet Tracer был создан новый проект. В рабочее поле размещены маршрутизатор **2811**, коммутатор **2960-24TT** и два оконечных устройства типа **PC-PT**. Один компьютер подключён напрямую к маршрутизатору, второй — к коммутатору. Соединения выполнены медным прямым кабелем (Copper Straight-Through), как показано на схеме.

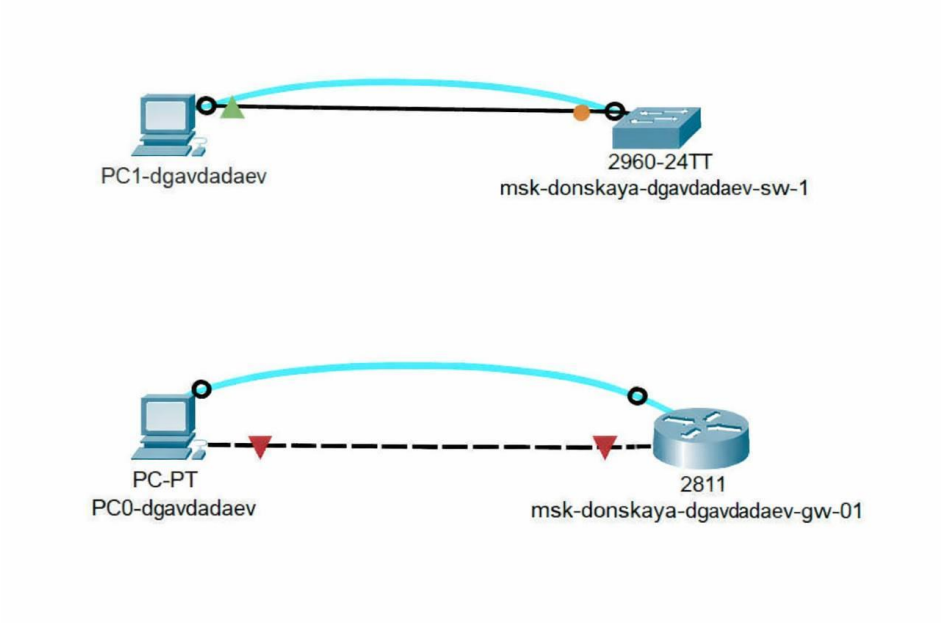

Рис. 1: Топология сети: ПК — коммутатор и ПК — маршрутизатор

На первом ПК (подключённом к коммутатору) был задан статический IP-адрес в сети 192.168.2.0/24: - PC1 — **192.168.2.10**
- Маска: **255.255.255.0**
- Основной шлюз: **192.168.2.1**

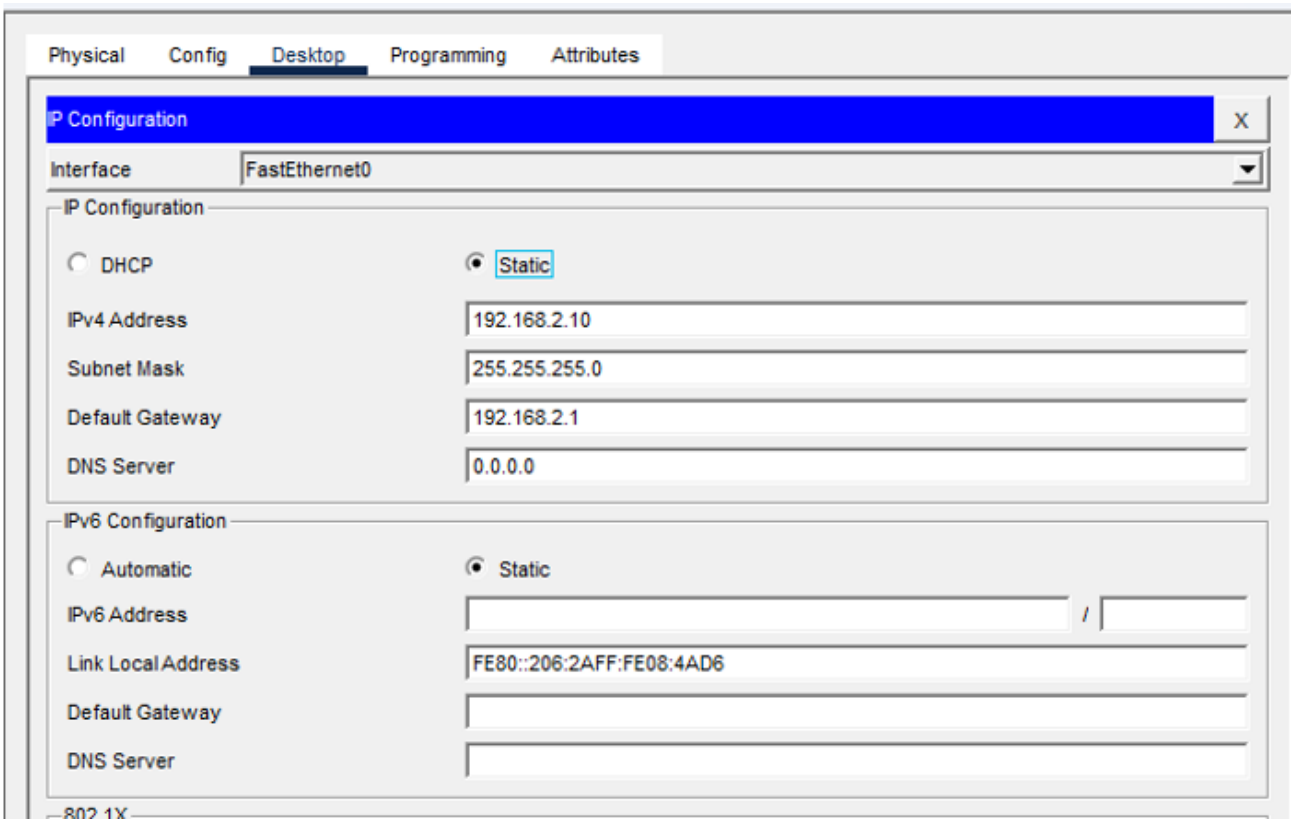

Рис. 2: Настройка IP на PC1

На втором ПК (подключённом к маршрутизатору) была настроена адресация сети 192.168.1.0/24: - PC0 — **192.168.1.1**
- Маска: **255.255.255.0**
- Основной шлюз: **192.168.1.254**

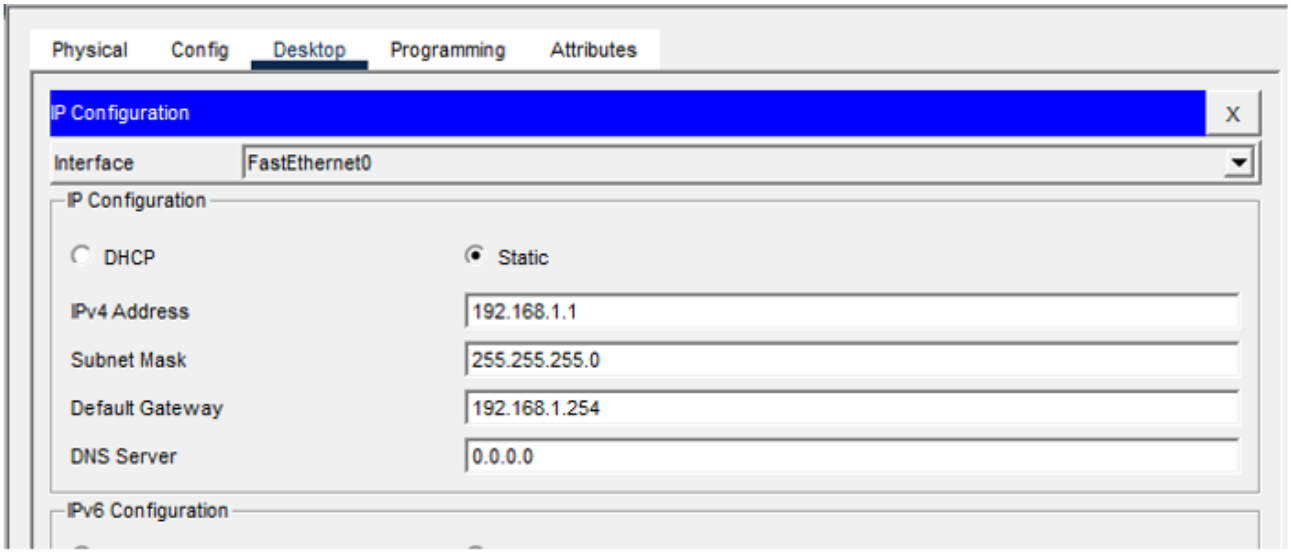

Рис. 3: Настройка IP на PC0

На коммутаторе выполнена базовая конфигурация. Установлено имя устройства, создан интерфейс управления VLAN 2 и назначен IP-адрес **192.168.2.1/24**, который используется для удалённого администрирования. Порт FastEthernet0/1 переведён в режим access и привязан к VLAN 2. Также задан шлюз по умолчанию **192.168.2.254**.

Дополнительно настроены параметры доступа: - пароль на консоль и VTY-линии — **cisco**; - включено шифрование паролей; - создан пользователь **admin**; - задан домен; - сгенерированы RSA-ключи; - разрешён доступ по протоколу **SSH**.

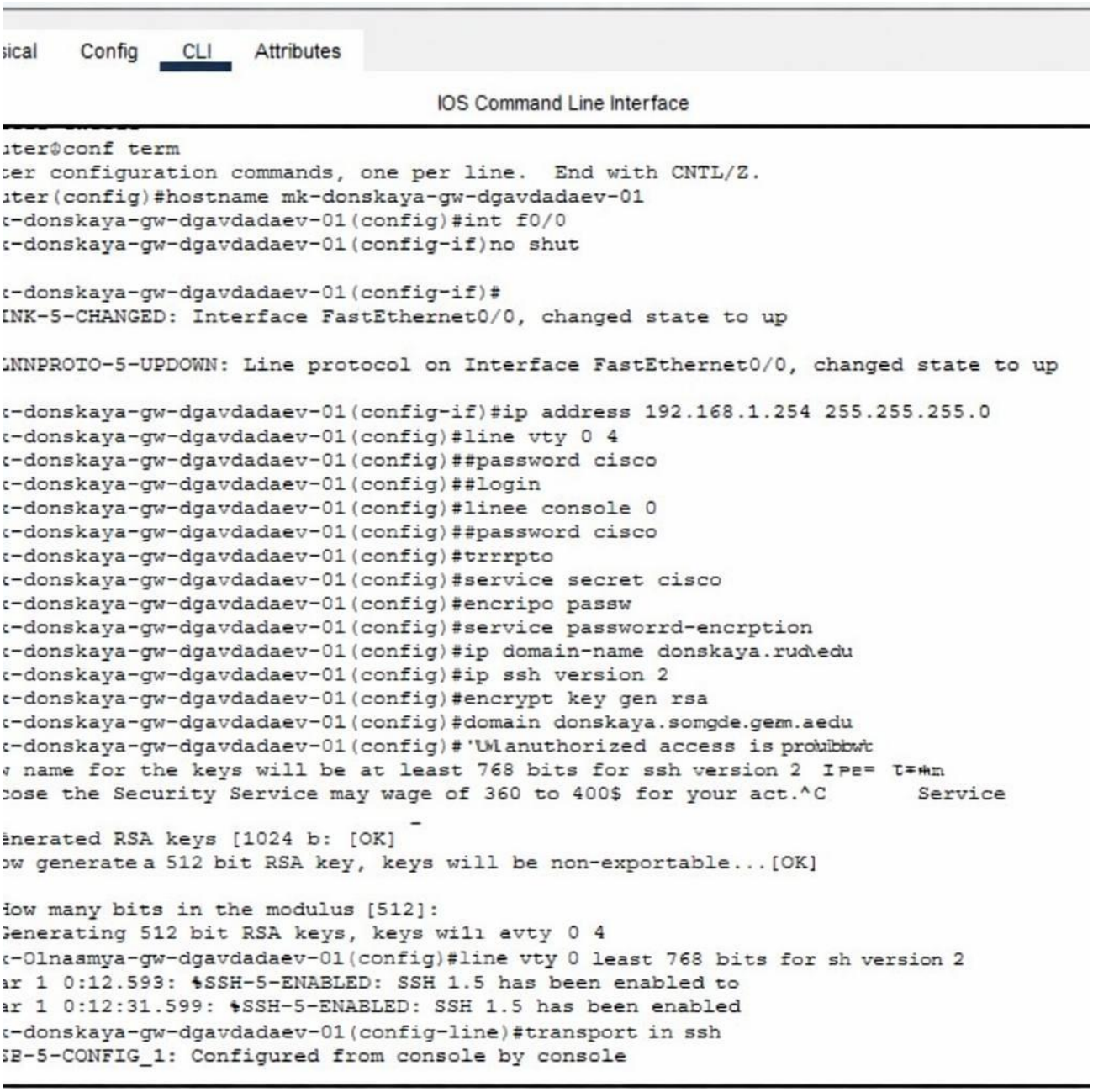

Рис. 4: Конфигурация коммутатора через CLI

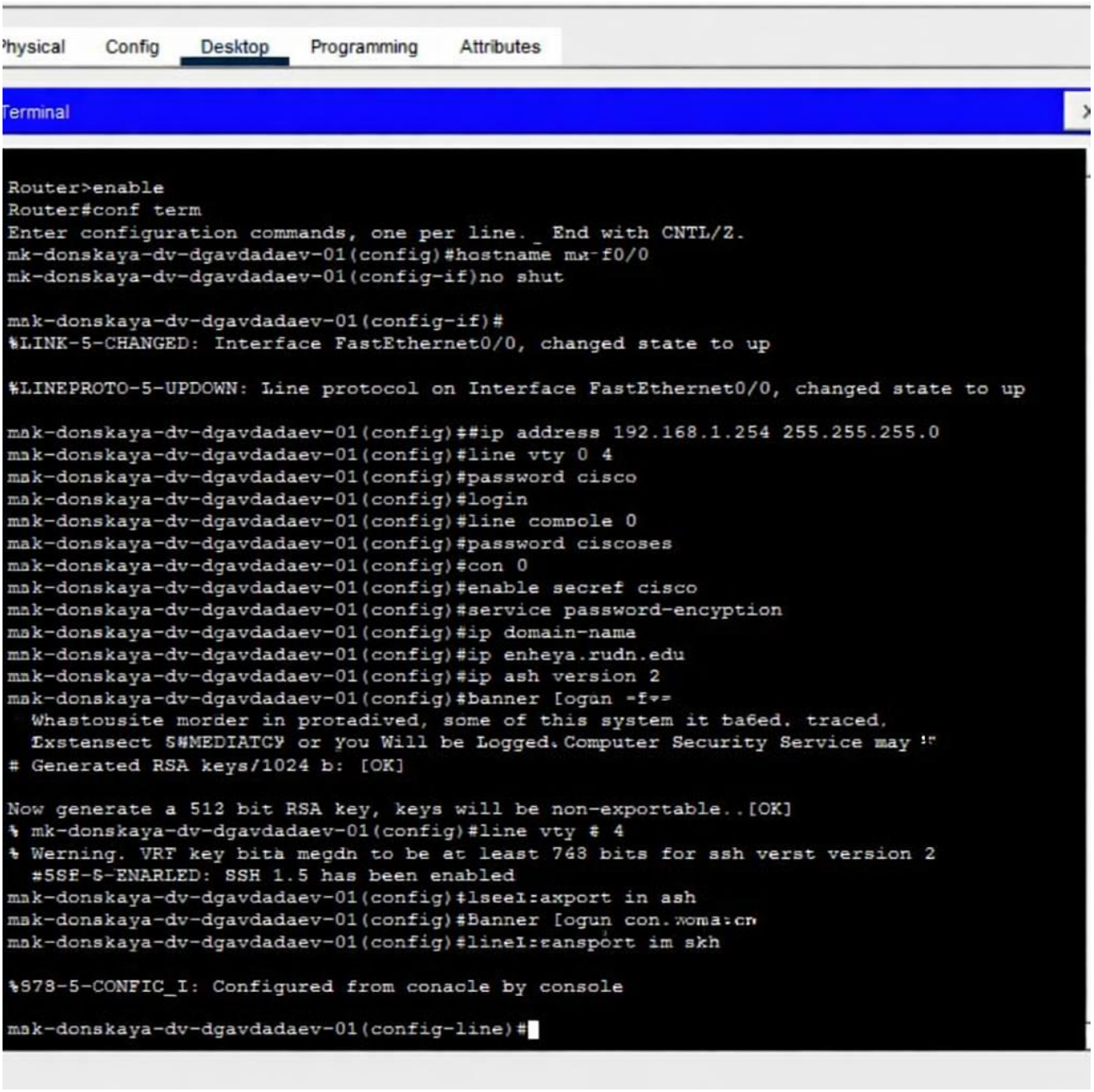

Рис. 5: Завершение настройки SSH на коммутаторе

На маршрутизаторе настроен интерфейс FastEthernet0/0 с адресом **192.168.1.254/24**, который используется в качестве шлюза для подключённого ПК. Интерфейс активирован командой **no shutdown**.

Также выполнены настройки удалённого доступа: - заданы пароли на консоль и VTY-линии; - включено шифрование паролей; - создан пользователь **admin**; - указан домен; - сгенерированы RSA-ключи; - разрешено подключение по **SSH**.

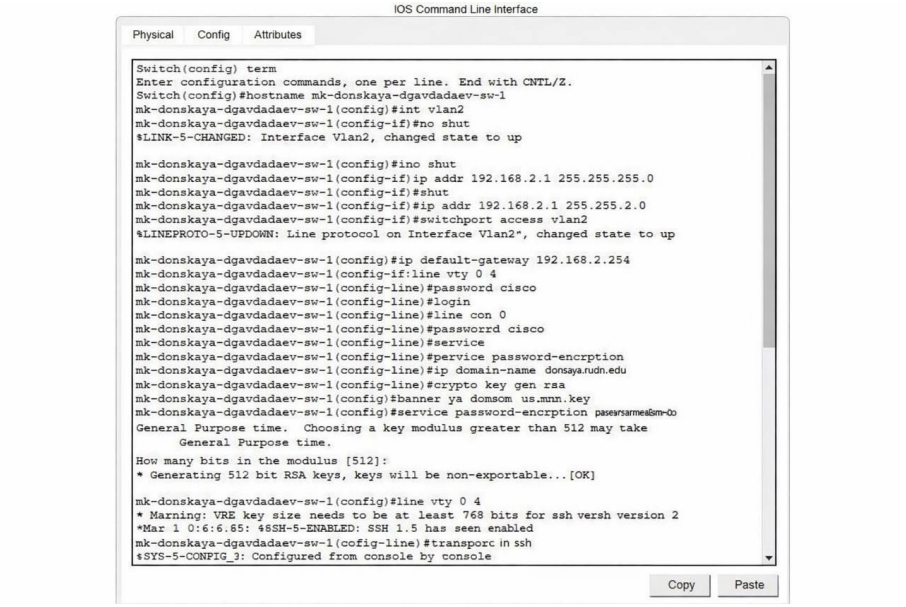

Рис. 6: Конфигурация маршрутизатора через CLI

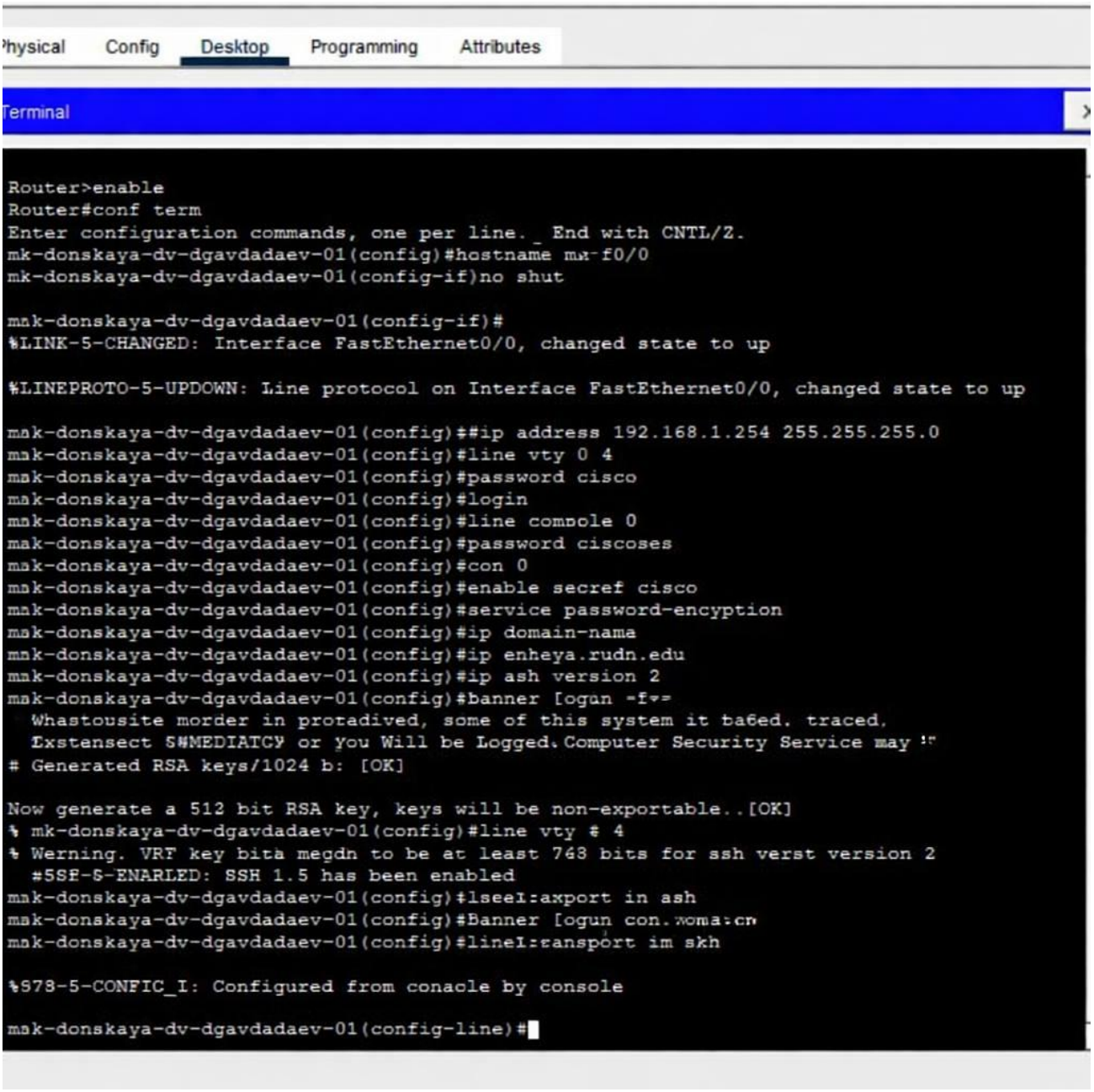

Рис. 7: Настройка параметров удалённого доступа на маршрутизаторе

После завершения настройки была выполнена проверка доступности устройств с помощью команды **ping**.

С ПК, подключённого к коммутатору, была проверена доступность IP-адреса коммутатора **192.168.2.1**. Ответы получены, что подтверждает корректную настройку сети.

Далее была выполнена попытка удалённого подключения: - по **telnet** — соединение устанавливается, но закрывается; - по **SSH** — выполнен успешный вход под пользователем **admin**.

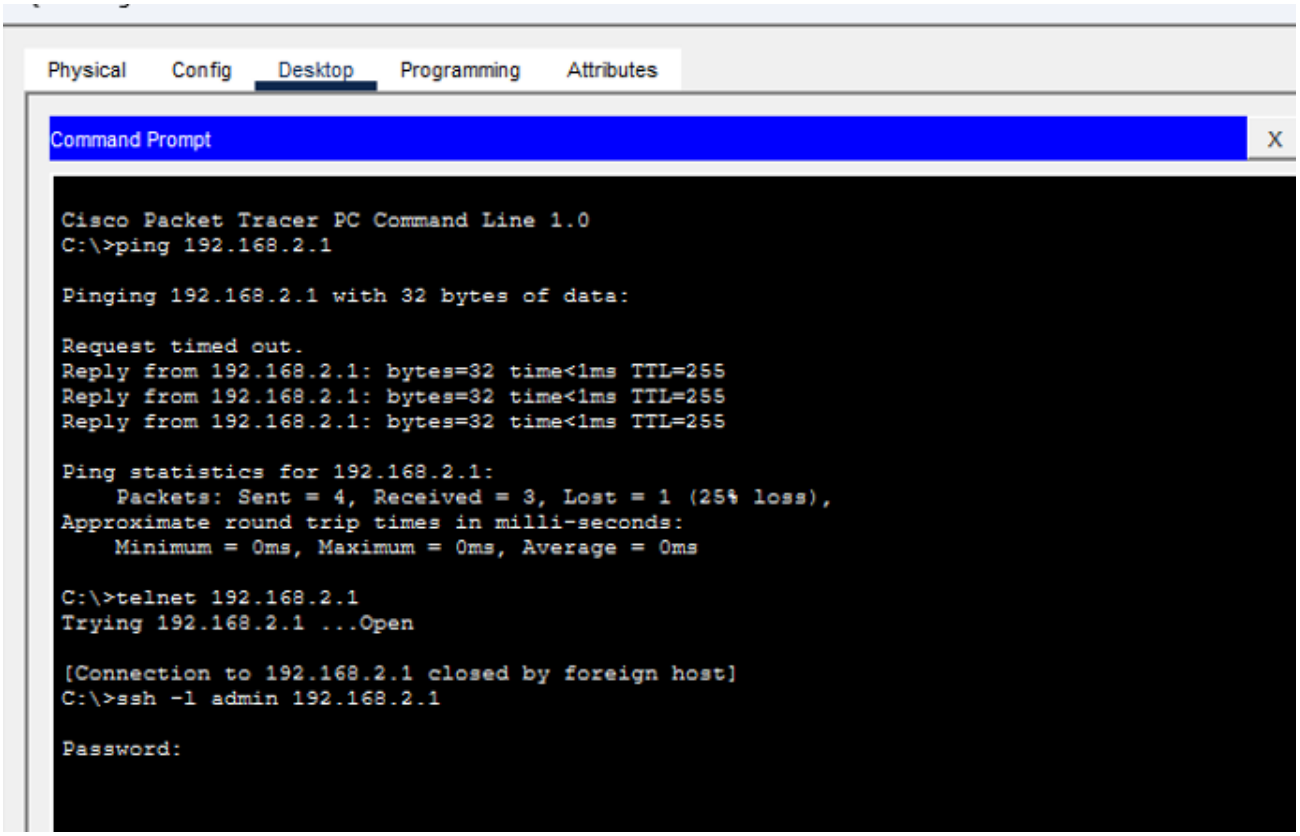

Рис. 8: Проверка ping и подключение по SSH к коммутатору

Аналогичная проверка была выполнена с ПК, подключённого к маршрутизатору. Выполнен ping до адреса **192.168.1.254**, получены ответы без потерь пакетов. Затем выполнено подключение по SSH, подтверждающее корректную настройку удалённого администрирования.

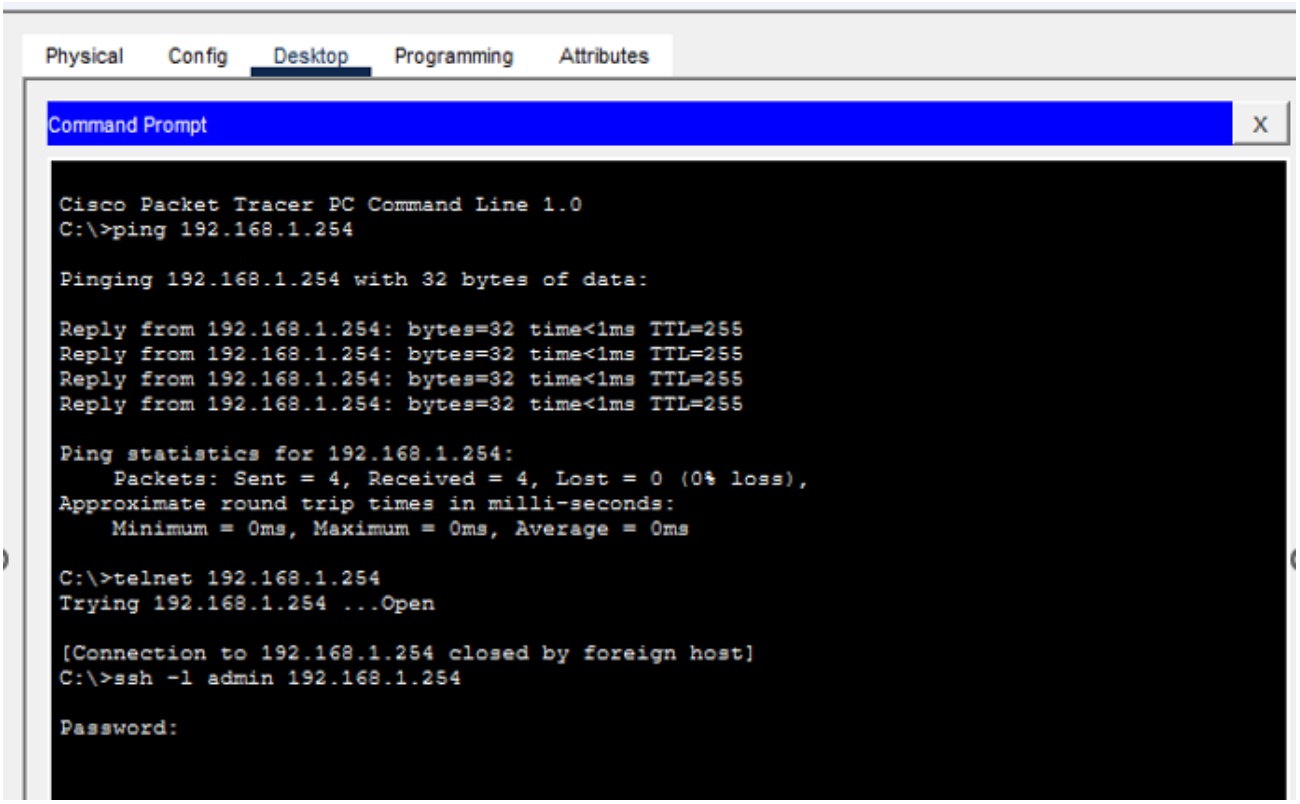

Рис. 9: Проверка связи и подключение по SSH к маршрутизатору

В результате выполнения работы была создана и настроена простая сеть с использованием маршрутизатора и коммутатора. Проведена базовая конфигурация устройств, назначены IP-адреса, настроены параметры удалённого доступа и выполнена проверка связности с помощью ICMP-пакетов и протокола SSH.

3 Вывод

В ходе выполнения работы была создана и настроена простая сеть в Cisco Packet Tracer с использованием маршрутизатора, коммутатора и двух оконечных устройств. Выполнена базовая конфигурация сетевого оборудования: назначены IP-адреса интерфейсам, настроены параметры управления коммутатором через VLAN, задан шлюз по умолчанию и активированы интерфейсы. Были отработаны навыки настройки удалённого доступа к сетевым устройствам. Настроены линии console и VTY, включено шифрование паролей, создан локальный пользователь, сгенерированы RSA-ключи и выполнена настройка подключения по протоколу SSH. Проведена проверка доступности устройств с помощью команды ping, что подтвердило корректность выполненной адресации и соединений. Также была выполнена попытка подключения к маршрутизатору и коммутатору различными способами: через консольный кабель, а также по протоколам удалённого доступа telnet и SSH. Установлено, что защищённое подключение по SSH обеспечивает успешный удалённый вход на устройства и позволяет управлять ими по сети.

3.1 Контрольные вопросы

3.1.1 1. Укажите возможные способы подключения к сетевому оборудованию.

Существует несколько способов подключения к сетевым устройствам для их настройки и администрирования:

- **Консольное подключение** — прямое соединение компьютера с устройством через консольный кабель. Используется для первоначальной настройки.
- **Telnet** — удалённое подключение по сети с передачей данных в открытом виде.
- **SSH** — удалённое защищённое подключение с шифрованием данных.
- **Web-интерфейс** — доступ через браузер (если поддерживается устройством).
- **Через вспомогательный (AUX) порт** — используется реже, обычно для удалённого доступа через модем.

3.1.2 2. Каким типом сетевого кабеля следует подключать оконечное оборудование пользователя к маршрутизатору и почему?

Оконечное оборудование подключается к маршрутизатору с помощью **прямого медного кабеля (Copper Straight-Through)**.

Это связано с тем, что соединяются устройства разного типа: - компьютер (оконечное устройство); - маршрутизатор (сетевое устройство).

У таких устройств используются разные схемы передачи и приёма сигналов, поэтому прямой кабель обеспечивает корректное соединение.

3.1.3 3. Каким типом сетевого кабеля следует подключать оконечное оборудование пользователя к коммутатору и почему?

Для подключения ПК к коммутатору также используется **прямой медный кабель (Copper Straight-Through)**.

Коммутатор является промежуточным сетевым устройством, а компьютер — оконечным. Поскольку соединяются разные типы устройств, применяется прямой кабель, обеспечивающий правильное соответствие контактов передачи и приёма.

3.1.4 4. Каким типом сетевого кабеля следует подключать коммутатор к коммутатору и почему?

Для соединения двух коммутаторов традиционно используется **перекрёстный кабель (Copper Cross-Over)**.

Это объясняется тем, что соединяются однотипные устройства. У них одинаковое расположение линий передачи и приёма, поэтому требуется перекрёстное соединение контактов для корректной передачи данных. В современных устройствах часто применяется технология Auto-MDIX, которая позволяет использовать и прямой кабель.

3.1.5 5. Укажите возможные способы настройки доступа к сетевому оборудованию по паролю.

Доступ к сетевому оборудованию можно защитить несколькими способами:

- установка пароля на **console line** — для локального доступа через консоль;
- установка пароля на **VTY-линии** — для удалённых подключений;
- использование команды **enable secret** — для защиты привилегированного режима;
- создание локального пользователя с именем и паролем;
- включение шифрования паролей с помощью service password-encryption.

3.1.6 6. Укажите возможные способы настройки удалённого доступа к сетевому оборудованию. Какой из способов предпочтительнее и почему?

Удалённый доступ можно настроить следующими способами:

- **Telnet** — простой способ удалённого подключения по сети;
- **SSH** — защищённое подключение с использованием шифрования.

Предпочтительным является **SSH**, так как он шифрует передаваемые данные, включая логины и пароли. В отличие от Telnet, который передаёт информацию в открытом виде, SSH обеспечивает более высокий уровень безопасности и защиты от перехвата данных.