Отчёт по лабораторной работе 2

Предварительная настройка оборудования Cisco

Суннатилло Махмудов

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить основные навыки по начальному конфигурированию оборудования Cisco.

2 Теоретические сведения по работе

В современных компьютерных сетях важную роль играет правильная настройка и подключение сетевого оборудования. К основным устройствам, используемым при построении локальных сетей, относятся маршрутизаторы, коммутаторы и оконечные устройства пользователей. Их корректная конфигурация обеспечивает стабильную передачу данных, безопасность доступа и возможность удалённого администрирования.

2.1 Настройка сетевых устройств

Первоначальная настройка маршрутизаторов и коммутаторов выполняется через консольный доступ. В процессе конфигурации обычно задаются следующие параметры:

– имя устройства (hostname), позволяющее идентифицировать его в сети;
– IP-адреса интерфейсов, обеспечивающие сетевую доступность;
– пароль для привилегированного режима (`enable secret`);
– пароли для консольного и удалённого доступа (линии `console` и `vty`);
– создание локальных пользователей с правами доступа;
– включение шифрования паролей (`service password-encryption`);
– настройка доменного имени устройства;
– генерация криптографических ключей для работы защищённых протоколов;
– сохранение конфигурации в энергонезависимую память.

На коммутаторах дополнительно может настраиваться интерфейс управле-

ния (SVI), назначаться VLAN и указываться шлюз по умолчанию для удалённого администрирования.

2.2 Виды подключения к сетевому оборудованию

Существует несколько способов подключения к сетевым устройствам:

1. Консольное подключение

Используется для первичной настройки. Подключение осуществляется с помощью консольного кабеля напрямую от ПК к устройству. Такой способ не требует наличия сетевых настроек и работает даже при отсутствии IP-адреса на устройстве.

2. Подключение по Telnet

Позволяет управлять устройством удалённо по сети. Требует предварительной настройки IP-адреса и пароля. Недостатком является передача данных в незашифрованном виде.

3. Подключение по SSH

Является более безопасным вариантом удалённого доступа. Все передаваемые данные шифруются, что защищает логины и пароли от перехвата. Для работы требуется настроить доменное имя и сгенерировать RSA-ключи.

4. Подключение через AUX-порт

Используется реже и применяется для удалённого доступа через модем и телефонную линию.

3 Выполнение лабораторной работы

1. В логической рабочей области **Packet Tracer** была собрана тестовая сеть: размещены маршрутизатор **Cisco 2811** (*msk-donskaya-smahmudov-gw-1*), коммутатор **Cisco 2960-24TT** (*msk-donskaya-smahmudov-sw-1*) и два оконечных устройства **PC-PT** (*PC0-smahmudov* и *PC1-smahmudov*).

   Подключения выполнены согласно заданию:
   – **PC0** соединён с **маршрутизатором**;
   – **PC1** соединён с **коммутатором**.
   Для первоначальной настройки также использовались консольные подключения.

   Далее на ПК были настроены статические IPv4-адреса:
   – **PC0-smahmudov**: 192.168.1.10
   – **PC1-smahmudov**: 192.168.2.10
   Маска подсети для всех устройств: 255.255.255.0

   Шлюзы по умолчанию:
   – PC0: 192.168.1.254
   – PC1: 192.168.2.1

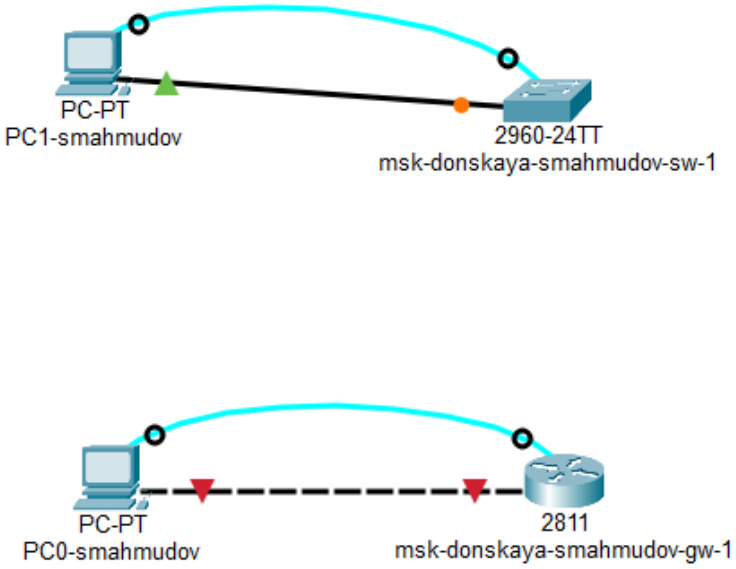

Рис. 3.1: Топология сети: PC–Router и PC–Switch

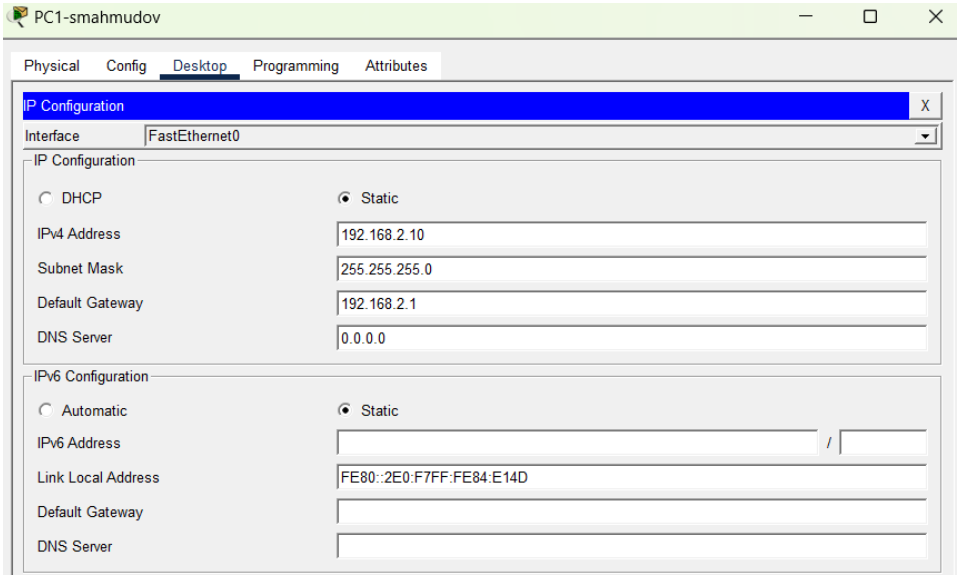

Рис. 3.2: Настройка IPv4 на PC1-smahmudov

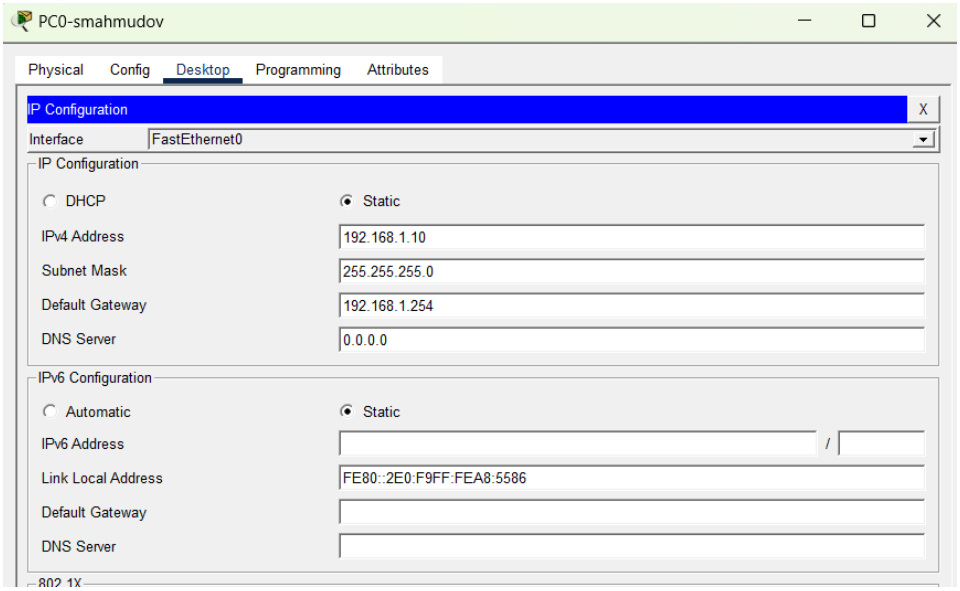

Рис. 3.3: Настройка IPv4 на PC0-smahmudov

2. Выполнена настройка маршрутизатора **msk-donskaya-smahmudov-gw-1** через интерфейс командной строки.

   В процессе конфигурации были выполнены следующие действия:

   – Переход в привилегированный режим и режим глобальной конфигурации;

   – Задано имя устройства (hostname);

   – Настроен интерфейс **FastEthernet0/0**: выполнено включение (`no shutdown`) и назначен IP-адрес 192.168.1.254 с маской 255.255.255.0;

   – Настроены линии удалённого доступа **VTY 0–4** с паролем `cisco` и разрешением входа;

   – Настроен доступ через консоль (`line console 0`, пароль `cisco`, `login`);

   – Задан привилегированный пароль `enable secret cisco`;

   – Включено шифрование паролей (`service password-encryption`);

   – Создан локальный пользователь `admin` с паролем `cisco`;

   – Указано доменное имя `donskaya.rudn.edu`;

   – Сгенерированы RSA-ключи для удалённого доступа;

   – Разрешён вход по SSH на линиях VTY (`transport input ssh`);

– Конфигурация сохранена в память устройства (`write memory`).

В процессе генерации ключей длиной 512 бит система сообщила о невозможности использования SSH версии 2, поэтому был автоматически включён SSH 1.5.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname msk-donskaya-smahmudov-gw-1
msk-donskaya-smahmudov-gw-1(config)#interface f0/0
msk-donskaya-smahmudov-gw-1(config-if)#no shutdown

msk-donskaya-smahmudov-gw-1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

msk-donskaya-smahmudov-gw-1(config-if)#ip address 192.168.1.254 255.255.255.0
msk-donskaya-smahmudov-gw-1(config-if)#line vty 0 4
msk-donskaya-smahmudov-gw-1(config-line)#password cisco
msk-donskaya-smahmudov-gw-1(config-line)#login
msk-donskaya-smahmudov-gw-1(config-line)#line console 0
msk-donskaya-smahmudov-gw-1(config-line)#password cisco
msk-donskaya-smahmudov-gw-1(config-line)#login
msk-donskaya-smahmudov-gw-1(config-line)#enable secret cisco
msk-donskaya-smahmudov-gw-1(config)#service password-encryption
msk-donskaya-smahmudov-gw-1(config)#username admin privilege 1 secret cisco
msk-donskaya-smahmudov-gw-1(config)#ip domain-name donskaya.rudn.edu
msk-donskaya-smahmudov-gw-1(config)#crypto key generate rsa
The name for the keys will be: msk-donskaya-smahmudov-gw-1.donskaya.rudn.edu
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

msk-donskaya-smahmudov-gw-1(config)#line vty 0 4
*Mar 1 0:6:19.511: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:6:19.511: %SSH-5-ENABLED: SSH 1.5 has been enabled
msk-donskaya-smahmudov-gw-1(config-line)#transport input ssh
msk-donskaya-smahmudov-gw-1(config-line)#exit
msk-donskaya-smahmudov-gw-1(config)#exit
msk-donskaya-smahmudov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-smahmudov-gw-1#write memory
Building configuration...
[OK]
msk-donskaya-smahmudov-gw-1#
```

Рис. 3.4: Фрагмент конфигурации маршрутизатора

3. Выполнена настройка коммутатора **msk-donskaya-smahmudov-sw-1**.

   В ходе настройки были выполнены следующие действия:

   – Задано имя устройства (hostname);

   – Настроен интерфейс управления **Vlan2**, назначен IP-адрес 192.168.2.1 с маской 255.255.255.0 и выполнено включение интерфейса;

   – Пользовательский порт **FastEthernet0/1** переведён в режим access и привязан к VLAN 2;

– Настроен шлюз по умолчанию для удалённого управления: 192.168.2.254;

– Настроены линии **VTY 0–4** с паролем `cisco` и разрешением входа;

– Настроен доступ через консоль (`line console 0`);

– Задан привилегированный пароль `enable secret cisco`;

– Включено шифрование паролей;

– Создан локальный пользователь `admin`;

– Указано доменное имя `donskaya.rudn.edu`;

– Сгенерированы RSA-ключи и включён доступ по SSH (`transport input ssh`).

При длине ключа 512 бит также было выведено предупреждение о невозможности использования SSH версии 2, после чего был активирован SSH 1.5.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname msk-donskaya-smahmudov-sw-1
msk-donskaya-smahmudov-sw-1(config)#interface vlan2
msk-donskaya-smahmudov-sw-1(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

msk-donskaya-smahmudov-sw-1(config-if)#no shutdown
msk-donskaya-smahmudov-sw-1(config-if)#ip address 192.168.2.1 255.255.255.0
msk-donskaya-smahmudov-sw-1(config-if)#interface f0/1
msk-donskaya-smahmudov-sw-1(config-if)#switchport mode access
msk-donskaya-smahmudov-sw-1(config-if)#switchport access vlan 2
msk-donskaya-smahmudov-sw-1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up

msk-donskaya-smahmudov-sw-1(config-if)#ip default-gateway 192.168.2.254
msk-donskaya-smahmudov-sw-1(config)#line vty 0 4
msk-donskaya-smahmudov-sw-1(config-line)#password cisco
msk-donskaya-smahmudov-sw-1(config-line)#login
msk-donskaya-smahmudov-sw-1(config-line)#line console 0
msk-donskaya-smahmudov-sw-1(config-line)#password cisco
msk-donskaya-smahmudov-sw-1(config-line)#login
msk-donskaya-smahmudov-sw-1(config-line)#enable secret cisco
msk-donskaya-smahmudov-sw-1(config)#service password-encryption
msk-donskaya-smahmudov-sw-1(config)#username admin privilege 1 secret cisco
msk-donskaya-smahmudov-sw-1(config)#ip domain-name donskaya.rudn.edu
msk-donskaya-smahmudov-sw-1(config)#crypto key generate rsa
The name for the keys will be: msk-donskaya-smahmudov-sw-1.donskaya.rudn.edu
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

msk-donskaya-smahmudov-sw-1(config)#line vty 0 4
*Mar 1 0:11:2.898: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:11:2.898: %SSH-5-ENABLED: SSH 1.5 has been enabled
msk-donskaya-smahmudov-sw-1(config-line)#transport input ssh
msk-donskaya-smahmudov-sw-1(config-line)#
```

Рис. 3.5: Фрагмент конфигурации коммутатора

4. Выполнена проверка сетевой связности с помощью команды **ping**.

С компьютера **PC1-smahmudov** был отправлен запрос на IP-адрес интерфейса управления коммутатора **192.168.2.1**. В ответ получены ICMP-ответы, что подтверждает корректность настройки IP-адресации и работоспособность соединения. Первый пакет был потерян, что связано с процессом ARP-резолвинга.

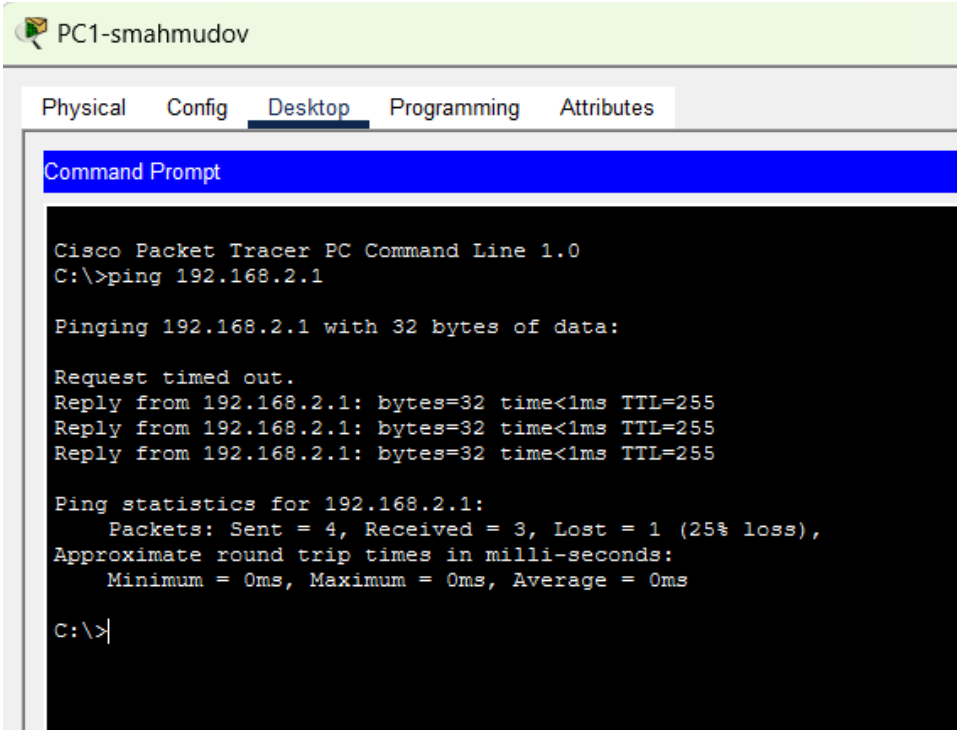

Рис. 3.6: Проверка соединения PC1 с коммутатором

С компьютера **PC0-smahmudov** был выполнен ping до интерфейса маршрутизатора **192.168.1.254**. Все пакеты успешно доставлены, потерь не зафиксировано, что подтверждает корректную настройку интерфейса маршрутизатора и сетевого подключения.

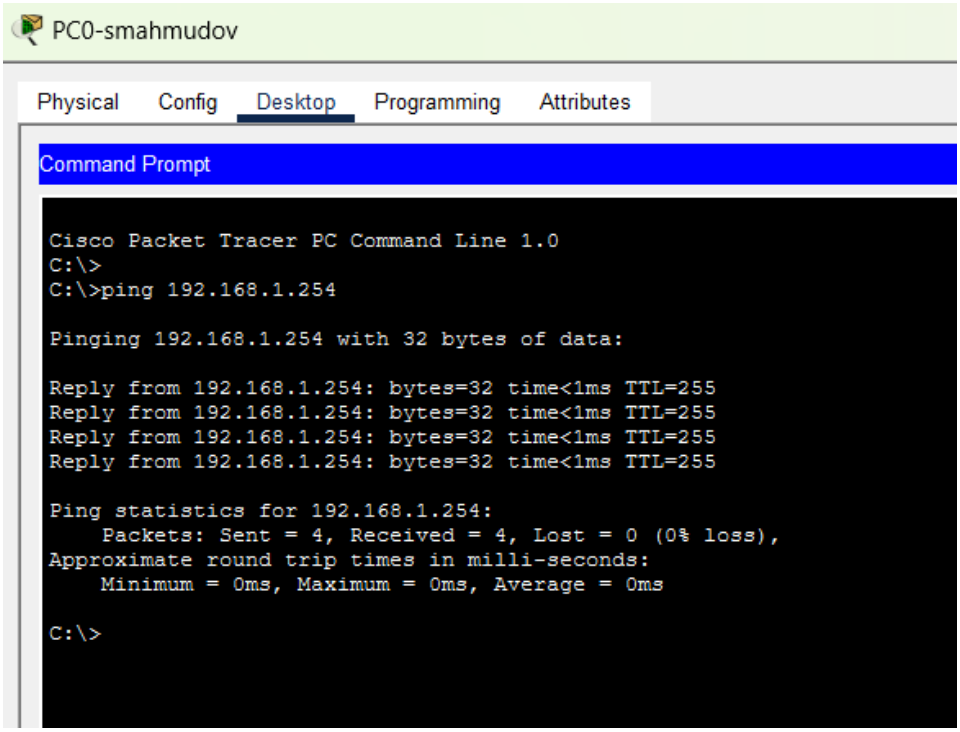

Рис. 3.7: Проверка соединения PC0 с маршрутизатором

5. Выполнено подключение к коммутатору и маршрутизатору различными способами удалённого доступа.

   Сначала было выполнено подключение через **консольный кабель**, после чего произведена настройка параметров доступа, включая создание пользователя, настройку паролей и генерацию RSA-ключей для использования SSH.

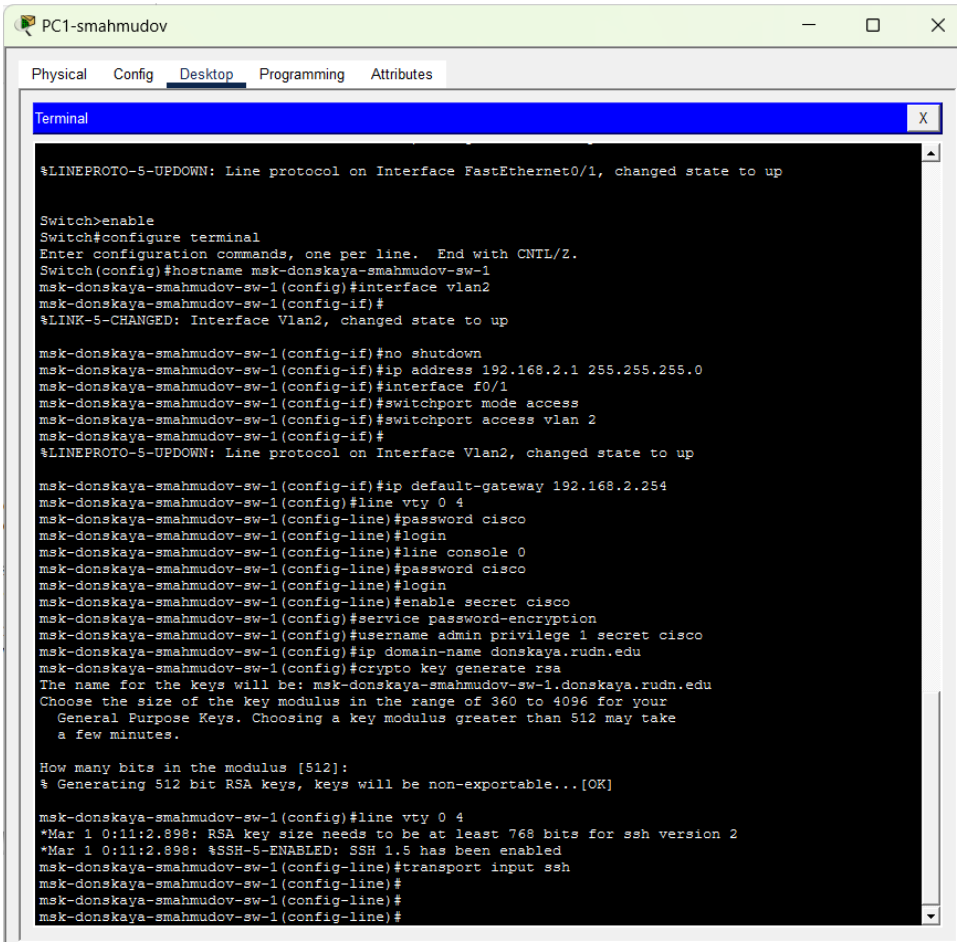

Рис. 3.8: Консольная настройка коммутатора

Далее с компьютера **PC1-smahmudov** выполнена попытка подключения к коммутатору:

– при использовании **telnet** соединение устанавливается, но сразу завершается;

– при использовании **SSH** выполнен вход под пользователем `admin`, после чего получен доступ к командной строке устройства.

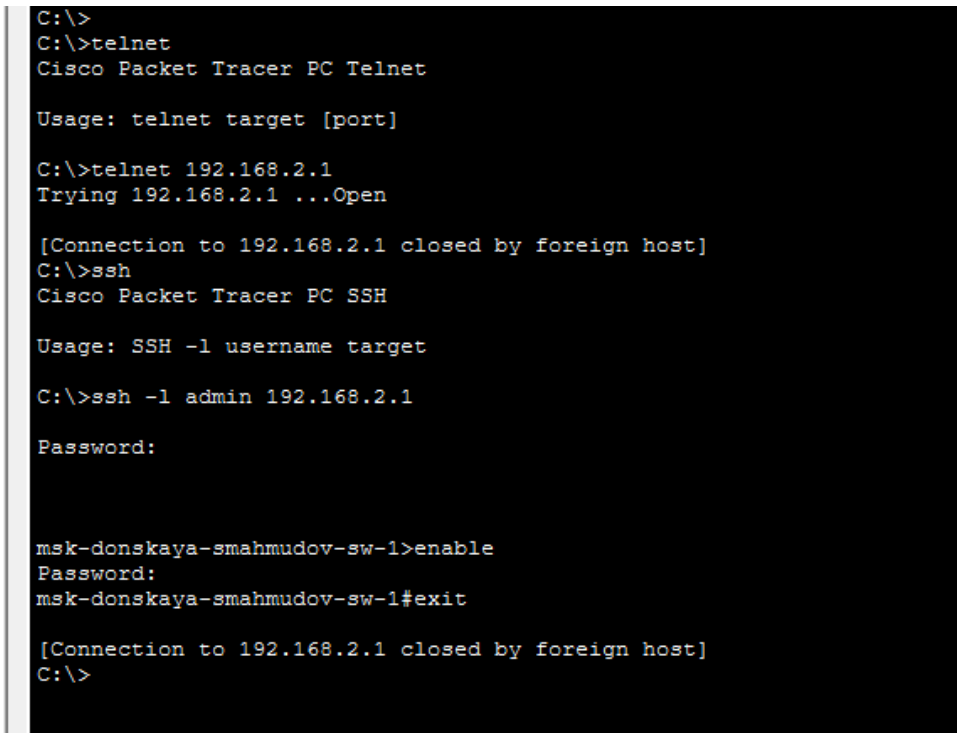

Рис. 3.9: Подключение к коммутатору по SSH

Аналогичные действия были выполнены для маршрутизатора. Через консоль произведена его настройка и включён доступ по SSH.

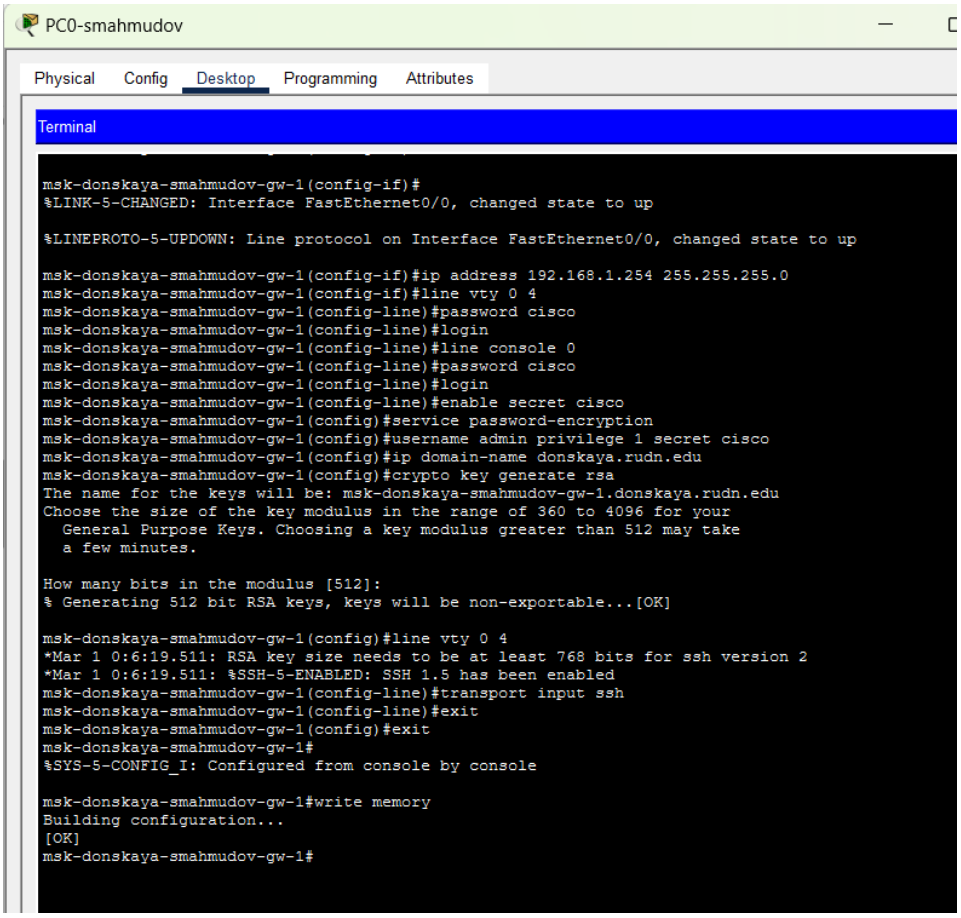

Рис. 3.10: Консольная настройка маршрутизатора

С компьютера **PC0-smahmudov** выполнено удалённое подключение к маршрутизатору:

– telnet-сессия устанавливается, но закрывается удалённой стороной;

– при подключении по **SSH** выполнена авторизация пользователя `admin`, после чего получен доступ к интерфейсу командной строки устройства.

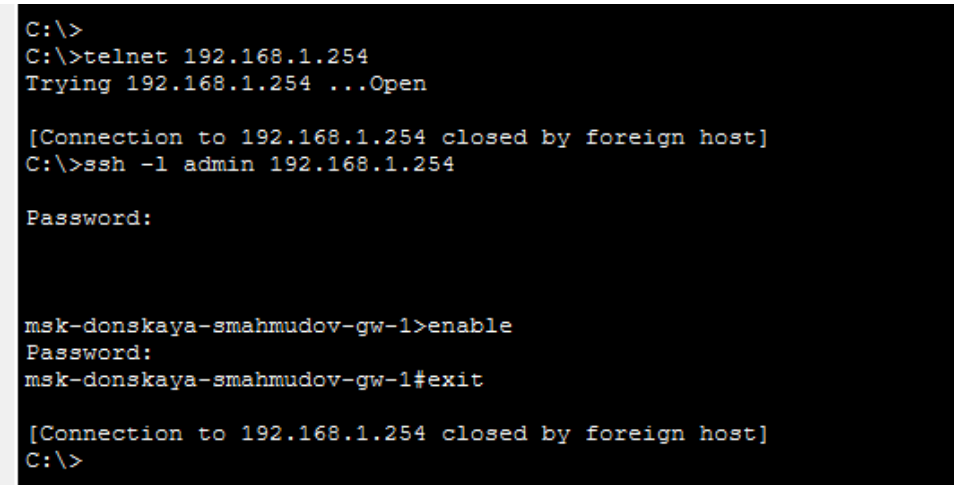

Рис. 3.11: Подключение к маршрутизатору по SSH

4 Вывод

В ходе лабораторной работы была собрана и настроена простая сеть в среде Cisco Packet Tracer с использованием маршрутизатора, коммутатора и двух оконечных устройств. Были выполнены базовые настройки сетевых устройств: назначены IP-адреса интерфейсам, настроены параметры VLAN на коммутаторе, заданы пароли доступа, создан пользователь для удалённого администрирования и сгенерированы RSA-ключи для использования SSH. Проведена проверка работоспособности соединений с помощью команды ping, что подтвердило корректность настройки сетевой адресации и доступность устройств. Также были опробованы различные способы подключения к коммутатору и маршрутизатору: через консольный кабель, а также по протоколам удалённого доступа telnet и SSH. В результате была подтверждена возможность безопасного удалённого управления сетевыми устройствами.

5 Контрольные вопросы

1. **Укажите возможные способы подключения к сетевому оборудованию.**

   Подключение к сетевому оборудованию может выполняться следующими способами:
   – через консольный кабель (Console) — используется для первоначальной настройки устройства при прямом физическом подключении;
   – через Telnet — удалённый доступ по сети с передачей данных в открытом виде;
   – через SSH — удалённый доступ по сети с шифрованием данных;
   – через веб-интерфейс (если поддерживается устройством) — управление через браузер по HTTP/HTTPS;
   – через вспомогательный порт AUX — используется для удалённого подключения через модем.

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

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

   Это связано с тем, что соединяются устройства разных типов:
   – компьютер (конечное устройство);
   – маршрутизатор (сетевое устройство).

   У них различная логика работы портов (MDI ↔ MDI-X), поэтому используется прямой кабель для корректной передачи сигналов.

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

   ПК подключается к коммутатору также с помощью **прямого кабеля (Copper Straight-Through)**.

   Это объясняется тем, что соединяются устройства разных типов:
   – конечное устройство (ПК);
   – коммутатор (сетевое устройство канального уровня).

   В этом случае передающие и принимающие пары проводов должны соединяться напрямую, что и обеспечивает прямой кабель.

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

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

   Это связано с тем, что соединяются устройства одного типа. Перекрёстный кабель меняет местами передающие и принимающие линии, обеспечивая корректный обмен данными между однотипными портами.

   В современных устройствах с поддержкой Auto-MDI/MDI-X тип кабеля может определяться автоматически, однако классическим решением является использование перекрёстного кабеля.

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

   Основные способы настройки парольной защиты:
   – установка пароля на привилегированный режим: `enable password` или `enable secret`;
   – установка пароля на консольный доступ: настройка `line console 0`, команды `password` и `login`;
   – установка пароля на удалённый доступ: настройка `line vty 0 4`, команды

`password` и `login`;

– создание локальных пользователей с именем и паролем: `username <имя> secret <пароль>`;

– включение шифрования паролей в конфигурации: `service password-encryption`.

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 — защищённый способ удалённого доступа с использованием шифрования;

   – Web-доступ (HTTP/HTTPS) — при наличии встроенного веб-интерфейса.

   Предпочтительным способом является **SSH**, так как он обеспечивает шифрование передаваемых данных, включая логины и пароли. В отличие от Telnet, который передаёт информацию в открытом виде, SSH защищает соединение от перехвата и несанкционированного доступа.

6 Список литературы

1. 802.1D-2004 - IEEE Standard for Local and Metropolitan Area Networks. Media Access Control (MAC) Bridges : тех. отч. / IEEE. — 2004. — С. 1—277. — DOI: 10.1109/IEEESTD.2004.94569. — URL: http://ieeexplore.ieee.org/servlet/opac?punumber=9155

2. 802.1Q - Virtual LANs. — URL: http://www.ieee802.org/1/pages/802.1Q.html.

3. A J. Packet Tracer Network Simulator. — Packt Publishing, 2014. — ISBN 9781782170426. — URL: https://books.google.com/books?id=eVOcAgAAQBAJ&dq=cisco+packet

4. Cotton M., Vegoda L. Special Use IPv4 Addresses : RFC / RFC Editor. — 01.2010. — С. 1—11. — № 5735. — DOI: 10.17487/rfc5735. — URL: https://www.rfc-editor.org/info/rfc5735.

5. Droms R. Dynamic Host Configuration Protocol : RFC / RFC Editor. — 03.1997. — С. 1—45. — № 2136. — DOI: 10.17487/rfc2131. — URL: https://www.ietf.org/rfc/rfc2131.txt%20https://www.rfc-editor.org/info/rfc2131.