

# Лабораторная работа № 2.

Предварительная настройка оборудования Cisco

Козлов Всеволод Павлович

## Содержание

Цель работы .....	1
Задание .....	1
Выполнение лабораторной работы.....	2
Ответы на контрольные вопросы .....	6
Выводы .....	7
Список литературы.....	7

## Список иллюстраций

Коммутатор и оконечное устройство.....	2
Конфигурация коммутатора .....	3
Работоспособность соединений.....	3
Удаленное подключение к коммутатору .....	4
Маршрутизатор и оконечное устройство .....	4
Конфигурация маршрутизатора .....	5
Работоспособность соединений.....	5
Удаленное подключение к маршрутизатору.....	6

## Список таблиц

**Элементы списка иллюстраций не найдены.**

## Цель работы

Получить основные навыки по начальному конфигурированию оборудования Cisco.

## Задание

1. Сделать предварительную настройку маршрутизатора: – задать имя в виде «город-территория-учётная\_записьтип\_оборудования-номер» (см. пункт 2.5), например, msk-donskaya-osbender-gw-1; – задать интерфейсу Fast Ethernet с номером 0 ip-адрес 192.168.1.254 и маску 255.255.255.0, затем поднять интерфейс; – задать пароль для доступа к привилегированному режиму (сначала в открытом виде, затем — в зашифрованном); – настроить доступ к оборудованию сначала через telnet, затем — через ssh (используя в качестве

имени домена `donskaya.rudn.edu`); – сохранить и экспортировать конфигурацию в отдельный файл.

2. Сделать предварительную настройку коммутатора: – задать имя в виде «город-территория-учётная\_записьтип\_оборудования-номер» (см. пункт 2.5), например `msk-donskaya-osbender-sw-1`; – задать интерфейсу `vlan 2` `ip`-адрес `192.168.2.1` и маску `255.255.255.0`, затем поднять интерфейс; – привязать интерфейс `Fast Ethernet` с номером 1 к `vlan 2`; – задать в качестве адреса шлюза по умолчанию адрес `192.168.2.254`; – задать пароль для доступа к привилегированному режиму (сначала в открытом виде, затем — в зашифрованном); – настроить доступ к оборудованию сначала через `telnet`, затем — через `ssh` (используя в качестве имени домена `donskaya.rudn.edu`); – для пользователя `admin` задать доступ 1-го уровня по паролю; – сохранить и экспортировать конфигурацию в отдельный файл.

## Выполнение лабораторной работы

Разместил коммутатор и оконечное устройство, соединил их и настроил `ip`-адрес `PC0` (рис. 1).

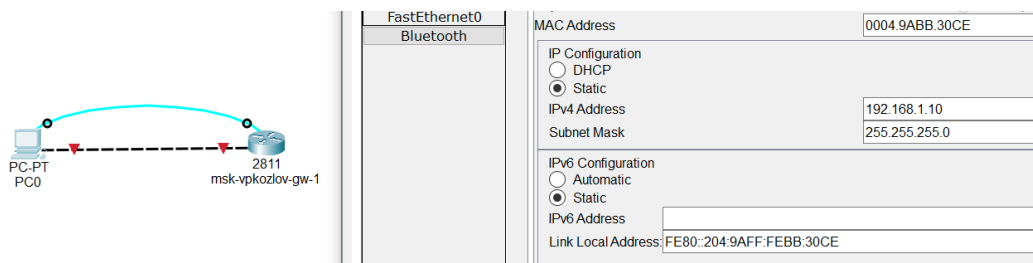


Рис. 1. Коммутатор и оконечное устройство

Изменил конфигурацию коммутатора (рис. 2).

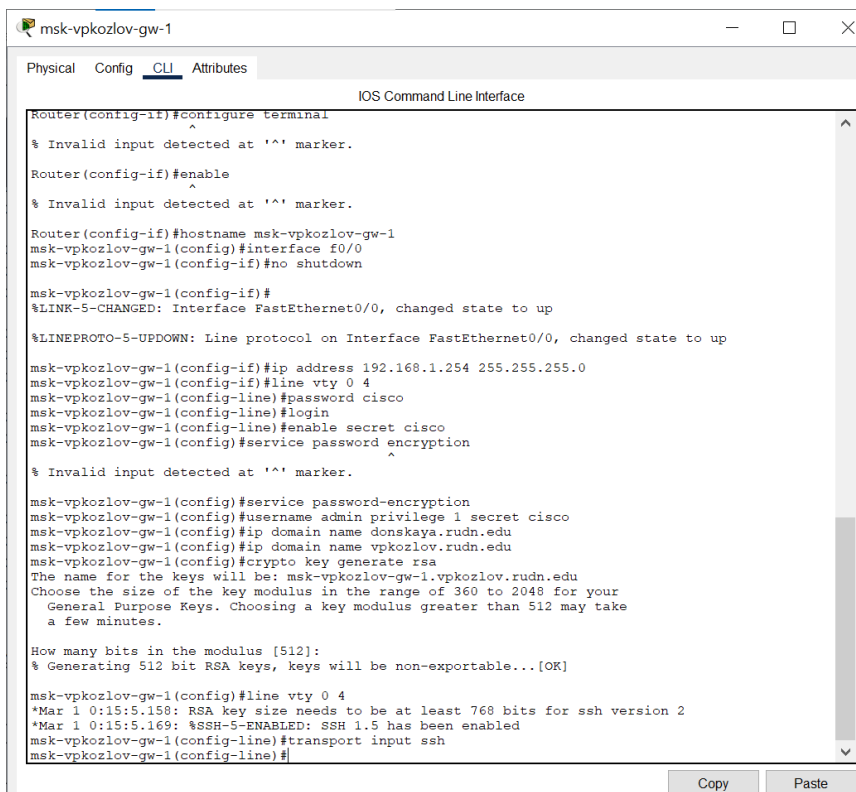


Рис. 2. Конфигурация коммутатора

Проверил работоспособность соединений с помощью команды ping (рис. 3).

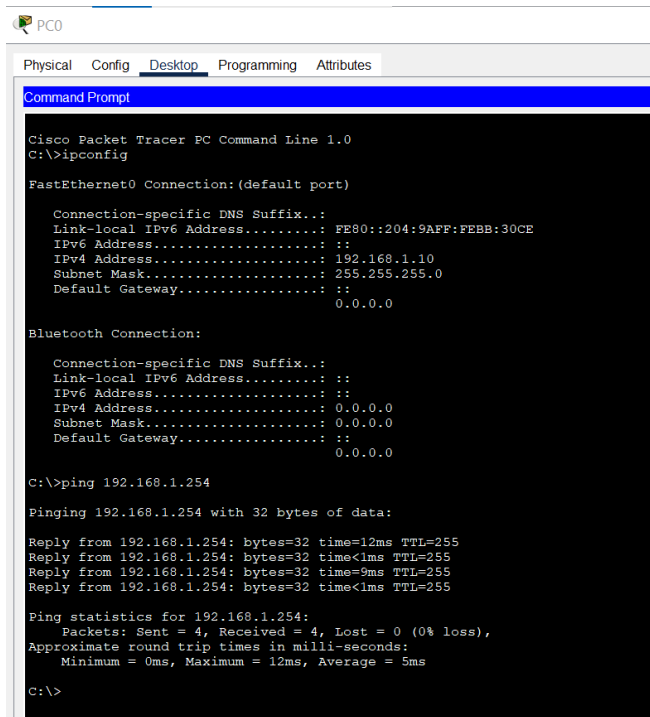


Рис. 3. Работоспособность соединений

Попробовал подключиться к коммутатору по протоколу удалённого доступа (telnet, ssh) (рис. 4).

```
C:\>
C:\>telnet 192.168.2.1
Trying 192.168.2.1 ...Open

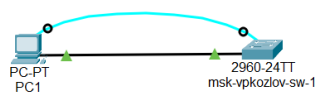
[Connection to 192.168.2.1 closed by foreign host]
C:\>ssh -l admin 192.168.2.1
Password: |

msk-vpkozlov-sw-1>en
Password:
msk-vpkozlov-sw-1#exit

[Connection to 192.168.2.1 closed by foreign host]
C:\>
```

*Рис. 4. Удаленное подключение к коммутатору*

Разместил маршрутизатор и оконечное устройство, соединил их и настроил ip-адрес PC1 (рис. 5).



*Рис. 5. Маршрутизатор и оконечное устройство*

Изменил конфигурацию маршрутизатора (рис. 6).

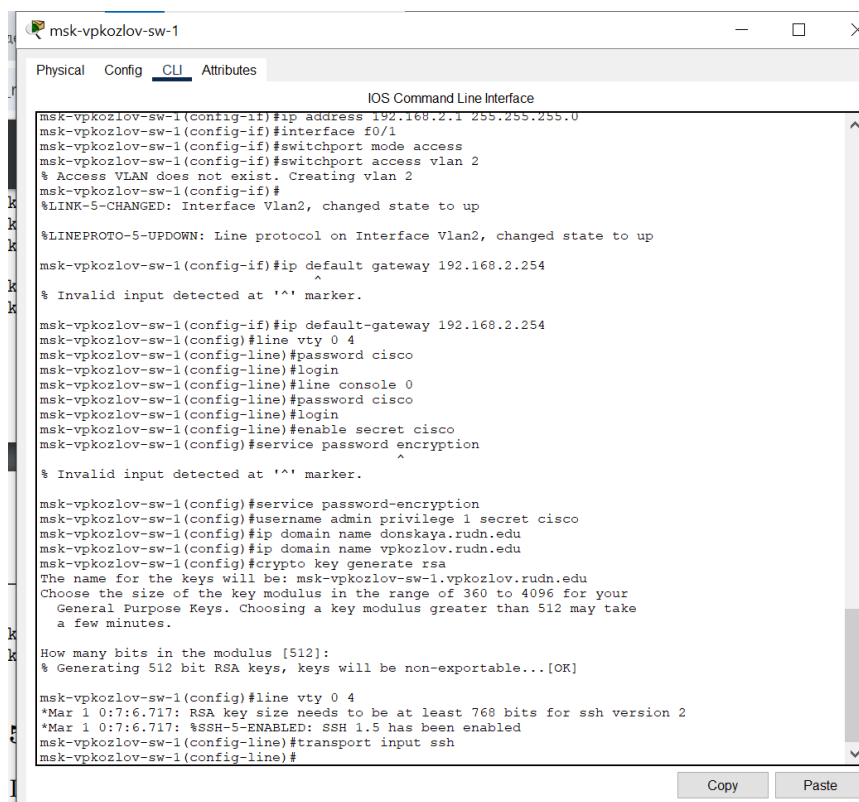


Рис. 6. Конфигурация маршрутизатора

Проверил работоспособность соединений с помощью команды ping (рис. 7).

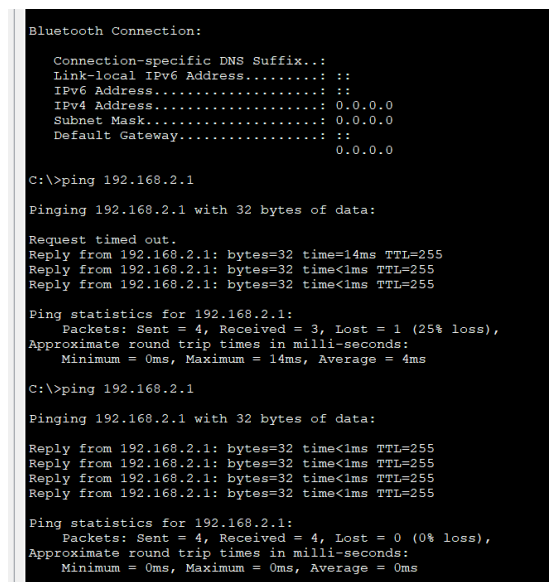


Рис. 7. Работоспособность соединений

Попробовал подключиться к маршрутизатору по протоколу удалённого доступа (telnet, ssh) (рис. 8).

```
C:\>telnet 192.168.1.254
Trying 192.168.1.254 ...Open

[Connection to 192.168.1.254 closed by foreign host]
C:\>ssh -l admin 192.168.1.254

Password:
Password:

msk-vpkozlov-gw-1>en
Password:
msk-vpkozlov-gw-1#exit

[Connection to 192.168.1.254 closed by foreign host]
C:\>
```

*Рис. 8. Удаленное подключение к маршрутизатору*

## Ответы на контрольные вопросы

1. Какие существуют способы подключения к сетевому оборудованию?
  - Подключение через консольный порт (локально).
  - Подключение по сети через SSH (Secure Shell).
  - Подключение по сети через Telnet (менее безопасный вариант).
  - Подключение через веб-интерфейс (HTTP/HTTPS).
  - Подключение через SNMP (Simple Network Management Protocol) для мониторинга.
2. Какой тип сетевого кабеля следует использовать для подключения оконечного оборудования пользователя к маршрутизатору и почему? Для подключения оконечного оборудования пользователя к маршрутизатору следует использовать кабель категории 5е (Cat5e) или выше (например, Cat6). Эти кабели обеспечивают достаточную пропускную способность и скорость передачи данных для большинства домашних и офисных сетей, а также поддерживают гигабитные соединения.
3. Какой тип сетевого кабеля следует использовать для подключения оконечного оборудования пользователя к коммутатору и почему? Для подключения оконечного оборудования пользователя к коммутатору также рекомендуется использовать кабель категории 5е (Cat5e) или выше. Это обеспечит надежное соединение и высокую скорость передачи данных, что особенно важно в локальных сетях.
4. Какой тип сетевого кабеля следует использовать для подключения коммутатора к коммутатору и почему? Для подключения коммутатора к коммутатору лучше использовать кабель категории 6 (Cat6) или выше, особенно если предполагается высокая нагрузка на сеть или использование гигабитных соединений. Эти кабели обеспечивают большую пропускную способность и меньшие потери сигнала на больших расстояниях.

5. Какие существуют способы настройки доступа к сетевому оборудованию по паролю?
  - Настройка доступа через консольный порт с использованием пароля.
  - Настройка доступа по SSH с использованием пароля.
  - Настройка доступа по Telnet с использованием пароля (менее безопасный вариант).
  - Настройка доступа через веб-интерфейс с использованием пароля.
6. Какие существуют способы настройки удалённого доступа к сетевому оборудованию? Какой из способов предпочтительнее и почему? Способы настройки удалённого доступа:
  - SSH (Secure Shell) — безопасный способ удаленного доступа.
  - Telnet — менее безопасный, так как передает данные в открытом виде.
  - VPN (Virtual Private Network) — обеспечивает защищенное соединение через интернет.
  - Веб-интерфейс (HTTP/HTTPS) — доступ через браузер, может быть защищен паролем. Предпочтительнее использовать SSH, так как он обеспечивает шифрование данных и защиту от перехвата, что делает его более безопасным по сравнению с Telnet.

## Выводы

Получил основные навыки по начальному конфигурированию оборудования Cisco.

## 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—
2. — DOI: 10.1109/IEEESTD.2004.94569. — URL: <http://ieeexplore.ieee.org/servlet/opac?punumber=9155>.
3. 802.1Q - Virtual LANs. — URL: <http://www.ieee802.org/1/pages/802.1Q.html>.
4. A J. Packet Tracer Network Simulator. — Packt Publishing, 2014. — ISBN 9781782170426. — URL: [https://books.google.com/books?id=eVOcAgAAQBAJ&dq=cisco+packet+tracer&hl=es&source=gbs\\_navlinks\\_](https://books.google.com/books?id=eVOcAgAAQBAJ&dq=cisco+packet+tracer&hl=es&source=gbs_navlinks_)
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>.
6. McPherson D., Dykes B. VLAN Aggregation for Efficient IP Address Allocation, RFC 3069. — 2001. — URL: <http://www.ietf.org/rfc/rfc3069.txt>.
7. Moy J. OSPF Version 2 : RFC / RFC Editor. — 1998. — С. 244. — DOI: 10.17487/rfc2328. — URL: <https://www.rfc-editor.org/info/rfc2328>.
8. NAT Order of Operation. — URL: <https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/6209-5.html>.

9. NAT: вопросы и ответы / Сайт поддержки продуктов и технологий компании Cisco. — URL: [https://www.cisco.com/cisco/web/support/ RU/9/92/92029\\_nat-faq.html](https://www.cisco.com/cisco/web/support/ RU/9/92/92029_nat-faq.html).
10. Neumann J. C. Cisco Routers for the Small Business A Practical Guide for IT Professionals. — Apress, 2009.
11. Odom S., Nottingham H. Cisco Switching: Black Book. — The Coriolis Group,
12. — ISBN 9781576107065. — URL: <http://books.google.sk/books?id=GYsLAAAACAAJ>.
13. Tetz E. Cisco Networking All-in-One For Dummies. — Indianapolis, Indiana : John Wiley & Sons, Inc., 2011. — (For Dummies). — URL: <http://www.dummies.com/store/product/Cisco-Networking-All-in-One-For-Dummies.productCd-0470945583.html>.
14. ГОСТ Р ИСО/МЭК 7498-1-99. — «ВОС. Базовая эталонная модель. Часть
15. Базовая модель». — ОКС: 35.100.70. — Действует с 01.01.2000. — URL: <http://protect.gost.ru/v.aspx?control=7&id=132355>.
16. Кларк К., Гамильтон К. Принципы коммутации в локальных сетях Cisco. — М. : Вильямс, 2003. — (Cisco Press Core Series). — ISBN 5-8459- 0464-1.
17. Королькова А. В., Кулябов Д. С. Архитектура и принципы построения современных сетей и систем телекоммуникаций. — М. : Издательство РУДН, 2009.
18. Королькова А. В., Кулябов Д. С. Прикладные протоколы Интернет и www. Курс лекций. — М. : РУДН, 2012. — ISBN 9785209049500.
19. Королькова А. В., Кулябов Д. С. Прикладные протоколы Интернет и www. Лабораторные работы. — М. : РУДН, 2012. — ISBN 9785209049357.
20. Королькова А. В., Кулябов Д. С. Сетевые технологии. Лабораторные работы. — М. : РУДН, 2014. — ISBN 785209056065.
21. Куроуз Д. Ф., Росс К. В. Компьютерные сети. Нисходящий подход. — 6-е изд. — М. : Издательство «Э», 2016. — (Мировой компьютерный бестселлер).
22. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101. — М. : Вильямс, 2017. — (Cisco Press Core Series). — ISBN 978-5-8459-1906-9.
23. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101. Маршрутизация и коммутация. — М. : Вильямс, 2016. — (Cisco Press Core Series).
24. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. — 5-е изд. — Питер : Питер, 2017. — (Учебник для вузов). — ISBN 978-5-496-01967-5.
25. Сети и системы передачи информации: телекоммуникационные сети / К. Е. Самуйлов [и др.]. — М. : Изд-во Юрайт, 2016. — ISBN 978-5-9916- 7198-9.
26. Таненбаум Э., Уэзеролл Д. Компьютерные сети. — 5 изд. — Питер : Питер,
27. — (Классика Computer Science). — ISBN 978-5-496-00831-0.
28. Хилл Б. Полный справочник по Cisco. — М. : Вильямс, 2009. — ISBN 978-5-8459-1309-8.
29. Цикл статей «Сети для самых маленьких». — URL: <http://linkmeup.ru/blog/11.html>.



30. Часто задаваемые вопросы технологии NAT / Сайт поддержки продуктов и технологий компании Cisco. — URL: [https://www.cisco.com/c/ru\\_ru/support/docs/ip/network-address-translation-nat/26704-nat-faq00.html](https://www.cisco.com/c/ru_ru/support/docs/ip/network-address-translation-nat/26704-nat-faq00.html).