Лабораторная работа №2

Предварительная настройка оборудования Cisco

Шияпова Дарина Илдаровна

Содержание

# 1 Цель работы

Получить основные навыки по начальному конфигурированию оборудования Cisco.

# 2 Задание

1. Сделать предварительную настройку маршрутизатора:

* задать имя в виде «город-территория-учётная\_записьтип\_оборудования-номер»;
* 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.

1. Сделать предварительную настройку коммутатора:

* задать имя в виде «город-территория-учётная\_записьтип\_оборудования-номер»
* 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.

# 3 Выполнение лабораторной работы

В логической рабочей области Packet Tracer разместим коммутатор, маршрутизатор и 2 оконечных устройства типа PC, соединим один PC с маршрутизатором консольным и кроссовым кабелем, другой PC — с коммутатором консольным и прямым кабелем (рис. 1).

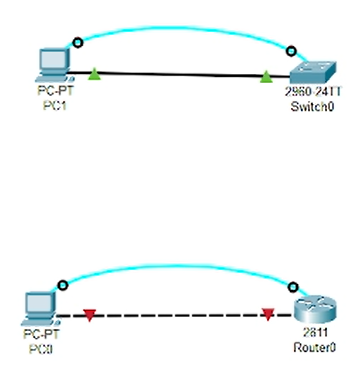


Рис. 1: Схема подключения оборудования для проведения его предварительной настройки

Для начала зададим статический ip-адрес PC0 192.168.1.10 с соответствующей маской подсети 255.255.255.0 (рис. 2).

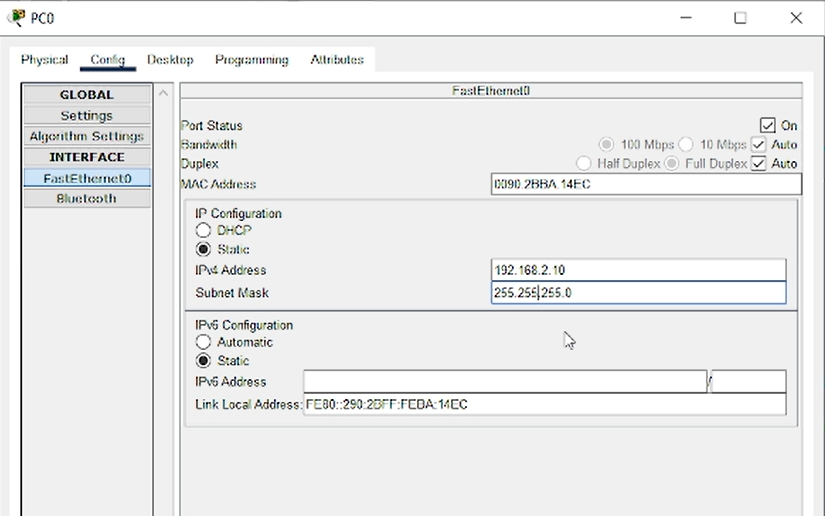


Рис. 2: Задание статического ip-адреса PC0

## 3.1 Настройка маршрутизатора

Теперь проведем настройку маршрутизатора в соответствии с заданием. Откроем Command Line Interface (CLI) у маршрутизатора, который идентичен терминалу ПК. Для перехода в привилегированный режим из пользовательского режима воспользуемся командой enable. А для перехода в режим глобальной конфигурации из привилегированного режима используем команду configure terminal или её сокращённый аналог conf t. И в этом режиме зададим имя хоста, введя команду hostname msk−donskaya −gw−1 (рис. 3).

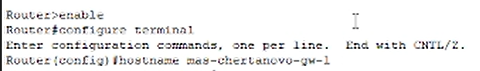


Рис. 3: Задание имени оборудованию

Зададим интерфейсу Fast Ethernet с номером 0 ip-адрес 192.168.1.254 и маску 255.255.255.0, затем поднимем интерфейс командой no shutdown (рис. 4).

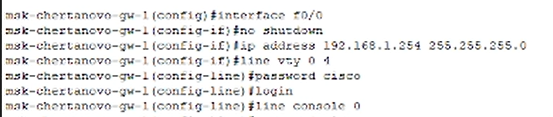


Рис. 4: Задание интерфейсу Fast Ethernet с номером 0 ip-адреса

Проверим работоспособность соединения с помощью команды ping. Увидим, что было полсано 4 пакета и принято тоже 4, потерь нет. Так что соединение успешно работает (рис. 5).

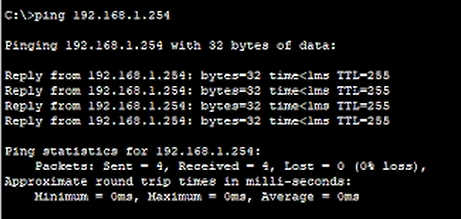


Рис. 5: Проверка соединения с помощью команды ping

Зададим пароль для доступа к привилегированному режиму (сначала в открытом виде, затем — в зашифрованном). Зададим пароль для доступа к терминалу, к консоли, и поставим пароль на enable (привилегированным режим) (рис. 6).

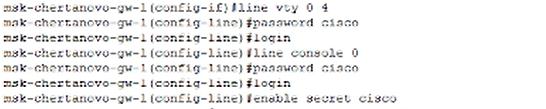


Рис. 6: Задание паролей

Если использовать команду secret, то пароль сразу будет зашифрованным. Но там, где мы использовали команду password пароль не скрыт, и любой может его посмотреть. Чтобы это исправить, надо зашифровать наши пароли с помощью команды service password −encryption (рис. 7).

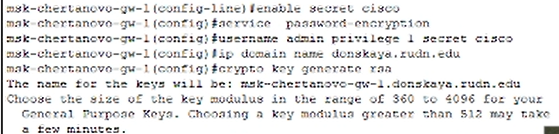


Рис. 7: Шифрование паролей

В качестве дополнительного уровня защиты для пользователя admin зададим доступ 1-го уровня по паролю (рис. 8).

Рис. 8: Задание доступа 1-го уровня по паролю пользователю admin

Рис. 8: Задание доступа 1-го уровня по паролю пользователю admin

Теперь настроим доступ к оборудованию сначала через telnet, затем — через ssh (используя в качестве имени домена donskaya.rudn.edu) (рис. 9).

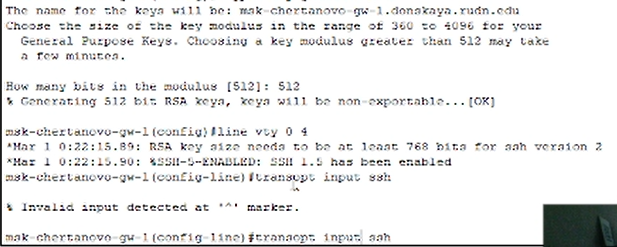


Рис. 9: Настройка доступа через telnet и ssh

Так как мы оставили возможным доступ только через ssh, то при попытке доступа через telnet нам будет отказано. А при доступе через ssh запрашивается пароль, как и должен, и доступ успешно предоставляется (рис. 10).



Рис. 10: Проверка работы доступа через telnet и ssh

Наконец сохраним нашу конфигурацию маршрутизатора.

## 3.2 Настройка коммутатора

Для начала зададим ста тический ip-адрес PC0 192.168.2.10 с соответствующей маской подсети 255.255.255.0 (рис. 11).

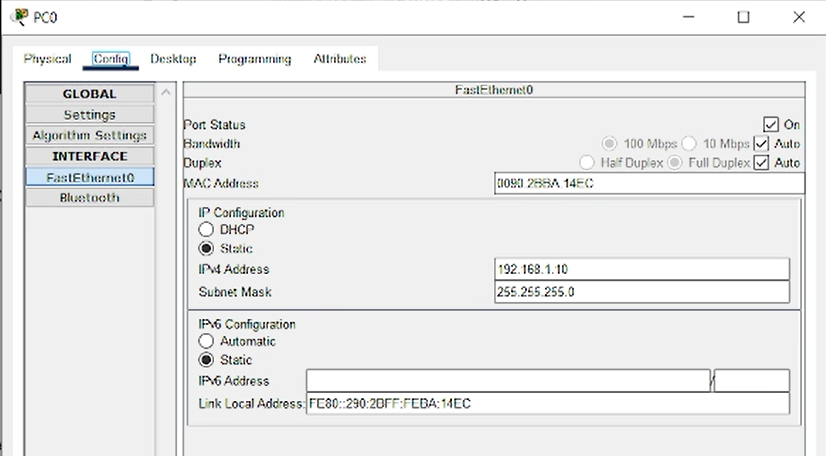


Рис. 11: Задание статического ip-адреса PC2

Теперь проведем настройку коммутатора в соответствии с заданием. Откроем Command Line Interface (CLI) у маршрутизатора, который идентичен терминалу ПК. Для перехода в привилегированный режим из пользовательского режима воспользуемся командой enable. А для перехода в режим глобальной конфигурации из привилегированного режима используем команду configure terminal или её сокращённый аналог conf t. И в этом режиме зададим имя хоста, введя команду hostname msk−donskaya −gw−1. Также зададим интерфейсу Fast Ethernet с номером 0 ip-адрес 192.168.1.254 и маску 255.255.255.0, затем поднимем интерфейс командой no shutdown (рис. 12).

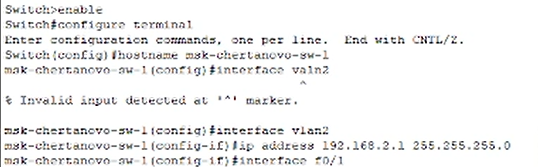


Рис. 12: Задание имени оборудованию

Привяжем интерфейс Fast Ethernet с номером 1 к vlan 2 (рис. 13).

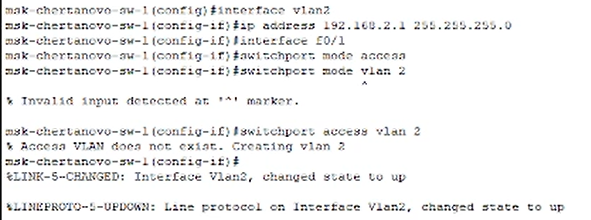


Рис. 13: Привязка интерфейса Fast Ethernet с номером 1 к vlan 2

И зададим в качестве адреса шлюза по умолчанию адрес 192.168.2.254 (рис. 14).

Рис. 14: Задание в качестве адреса шлюза адрес 192.168.2.254

Рис. 14: Задание в качестве адреса шлюза адрес 192.168.2.254

Проверим работоспособность соединения с помощью команды ping. Увидим, что было полсано 4 пакета и принято тоже 4, потерь нет. Так что соединение успешно работает (рис. 15).

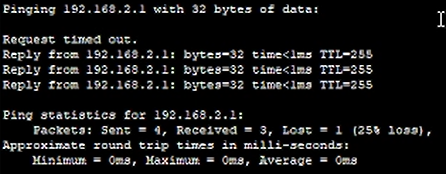


Рис. 15: Проверка соединения с помощью команды ping

Зададим пароль для доступа к привилегированному режиму (сначала в открытом виде, затем — в зашифрованном). Зададим пароль для доступа к терминалу, к консоли, и поставим пароль на enable (привилегированным режим). Зашифруем наши пароли с помощью команды service password −encryption.

В качестве дополнительного уровня защиты для пользователя admin зададим доступ 1-го уровня по паролю.

Теперь настроим доступ к оборудованию сначала через telnet, затем — через ssh (используя в качестве имени домена donskaya.rudn.edu).

Так как мы оставили возможным доступ только через ssh, то при попытке доступа через telnet нам будет отказано. А при доступе через ssh запрашивается пароль, как и должен, и доступ успешно предоставляется.

Сохраним нашу конфигурацию маршрутизатора.

# 4 Выводы

В процессе выполнения данной лабораторной работы я получила основные навыки по начальному конфигурированию оборудования Cisco.

# 5 Контрольные вопросы

1. Укажите возможные способы подключения к сетевому оборудованию.

Можно подключиться с помощью консольного кабеля или удаленно по ssh или telnet.

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

Кроссовым кабелем

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

Прямым кабелем (витой парой).

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

Кроссовым кабелем (для соединения одинокого оборудования используют кроссовый кабель)

1. Укажите возможные способы настройки доступа к сетевому оборудованию по паролю.

С помощью команды password или с помощью команды secret

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

Через telnet или ssh. SSH обеспечивает шифрование и аутентификацию по умолчанию, в отличие от Telnet, который не предоставляет эти функции, поэтому он лучше.