МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ

(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)

Институт №8 «Компьютерные науки и прикладная математика»

Кафедра №806 «Вычислительная математика и программирование»

**Лабораторная работа №1**

**по курсу «Вычислительные сети и телекоммуникации»**

**Базовая настройка устройств**

Выполнил: Почечура А.А.

Группа: 8О-406Б

Преподаватель: Филимонов Н.С.

Москва, 2024

**Условие**

**Цель работы.** Научиться использовать интерфейсы управления и конфигурирования оборудования Cisco Systems и Mikrotik, настраивать ip-адреса устройств, пароли и логины, настраивать конечный пользовательский NAT на Mikrotik.

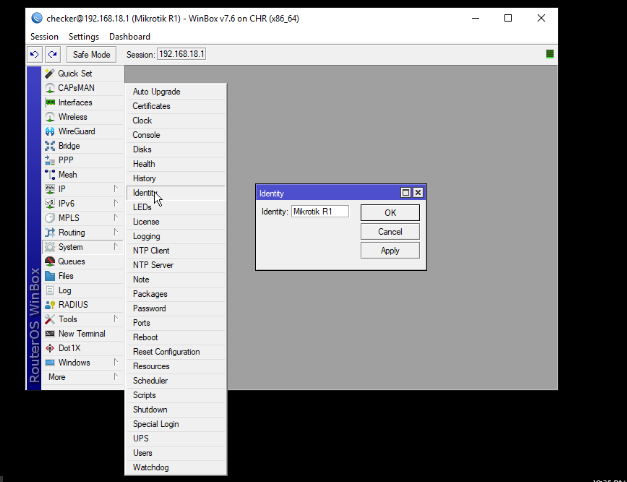
**Вариант 18.**

**Задачи**

1. Настроить имена узлов для коммутатора и маршрутизатора в соответствии с именами, указанными в топологии (SW1 и R1).
2. Сменить пароль администратора (пароль доступа к привилегированному режиму enable для Cisco) на приведенный в Вашем варианте ЛР для соответствующего устройства.
3. Создать пользователя checker с максимальным административным уровнем доступа и паролем “PfxtvXtrth!” без кавычек на коммутаторе и маршрутизаторе
4. Настроить на маршрутизаторе R1 IP-адреса интерфейсов в соответствии с вариантом задания.
5. Настроить на коммутаторе SW1 IP-адрес в соответствии с вариантом задания, адрес DNS-сервера (адрес маршрутизатора R1) и маршрут по умолчанию в управляющем VLAN.
6. Настроить на маршрутизаторе R1 встроенный DNS-сервер с передачей запросов на сервер QuadNine (9.9.9.9), включить удаленные запросы.
7. Настроить на маршрутизаторе R1 раздачу адресов с помощью DHCP из внутреннего пула, указанного в варианте задания с указанием в качестве маршрута по умолчанию и DNS-сервера внутреннего IP-адреса маршрутизатора R1 (eth2).
8. Настроить на маршрутизаторе R1 трансляцию сетевых адресов (NAT) из адресов внутренней сети в адрес на внешнем интерфейсе маршрутизатора (eth1).
9. Включить на коммутаторе и маршрутизаторе доступ по протоколу ssh, выключить web-интерфейсы коммутатора (причины см. например в CVE-2023-20198), убедиться, что доступ по ssh работает с хостов в сети для администратора и пользователя checker.
10. Убедиться в работоспособности сети путем проверки разрешения имен в сети Интернет, работоспособности ping/traceroute и открытия веб-сайтов с хостов Win и Linux в топологии в режиме автоматической настройки интерфейсов с помощью DHCP.
11. \* Настроить firewall на маршрутизаторе R1 (по желанию).

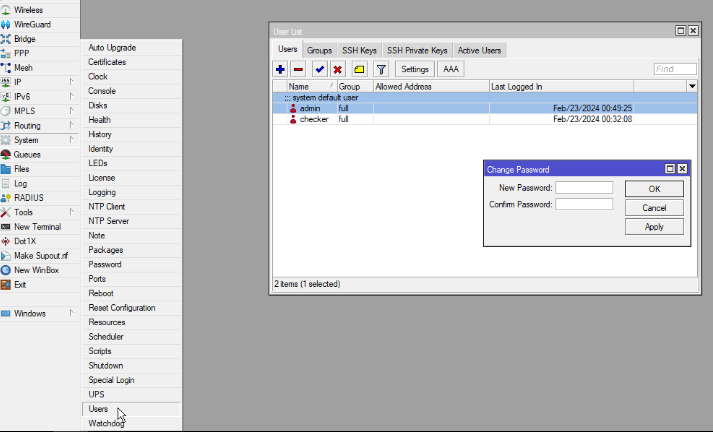
**Порядок выполнения работы**

1. Настройка имени узла для маршрутизатора производится в программе WinBox следующим образом:



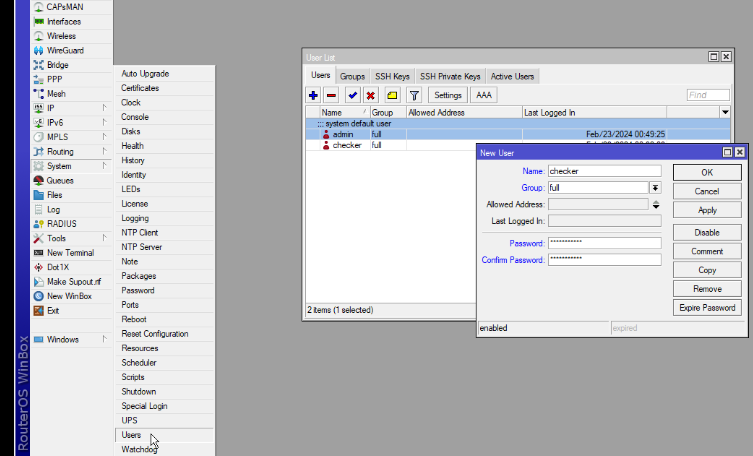
Настройка имени узла для коммутатора производится в консоли Cisco путём написания команды *hostname SW1* в режиме конфигурирования, находясь при этом в привилегированном режиме.

1. Смена пароля администратора на *admin18* для маршрутизатора производится следующим образом:



Для смены пароля привилегированного режима на *admin18* для коммутатора нужно воспользоваться командой *enable secret admin18.*

1. Создание пользователя *checker* с максимальным административным уровнем доступа и паролем *PfxtvXtrth!* на маршрутизаторе производится следующим образом:



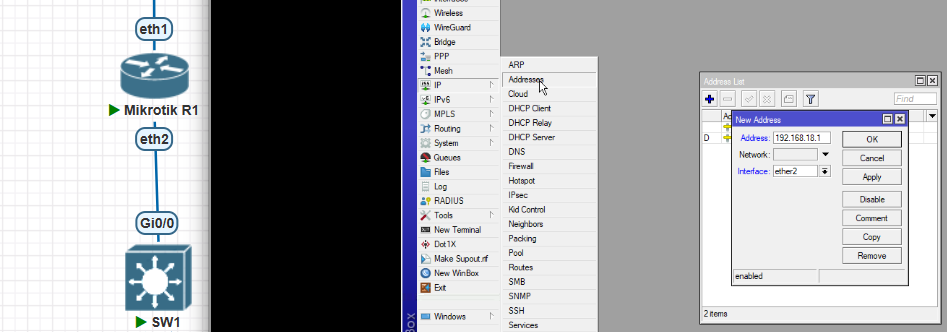
Создание пользователя *checker* с максимальным административным уровнем доступа и паролем *PfxtvXtrth!* на коммутаторе производится с помощью следующих команд:

*aaa new-model*

*service password-encryption*

*username checker privilege 15 password 0 PfxtvXtrth!*

1. Настройка на маршрутизаторе R1 IP-адреса интерфейсов производится следующим образом:



1. Настройка на коммутаторе SW1 IP-адреса осуществляется с помощью следующей команды:

*interface vlan 1*

*ip address 192.168.18.254 255.255.255.0*

*no shutdown*

Настройка адреса DNS-сервера (адреса маршрутизатора R1) осуществляется с помощью следующей команды:

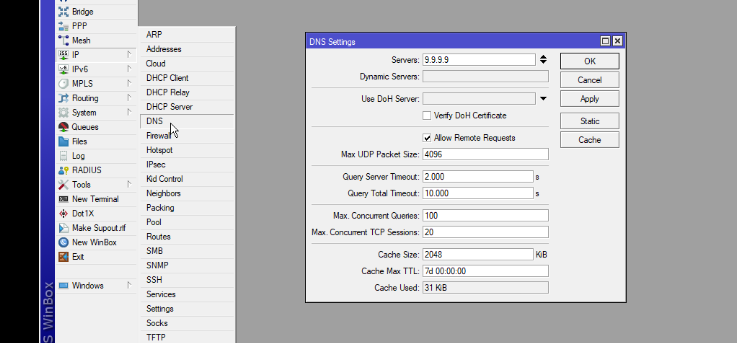
*ip domain-lookup*

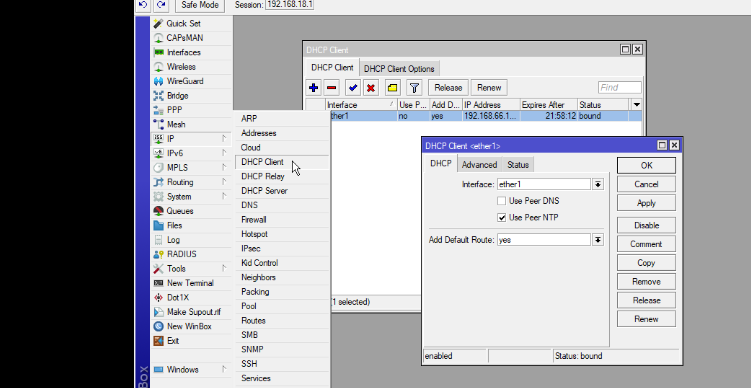
*ip name-server 192.168.18.1*

Настройка маршрута по умолчанию VLAN осуществляется следующим образом:

*ip route 0.0.0.0 0.0.0.0 192.168.18.1*

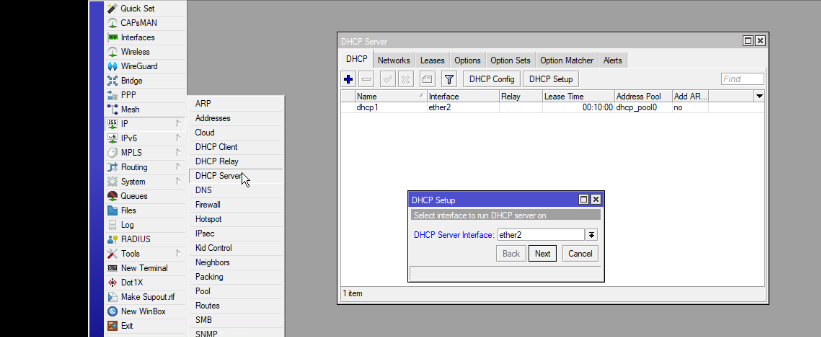
1. Настройка на маршрутизаторе R1 встроенного DNS-сервера с передачей запросов на сервер QuadNine (9.9.9.9) и включение удалённых запросов осуществляется следующим образом:



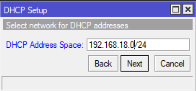
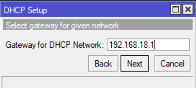


(тут требуется убрать галочку *Use Peer DNS*)

1. Настройка на маршрутизаторе R1 раздачи адресов с помощью DHCP из внутреннего пула с указанием в качестве маршрута по умолчанию и DNS-сервера внутреннего IP-адреса маршрутизатора R1 (eth2) осуществляется следующим образом:



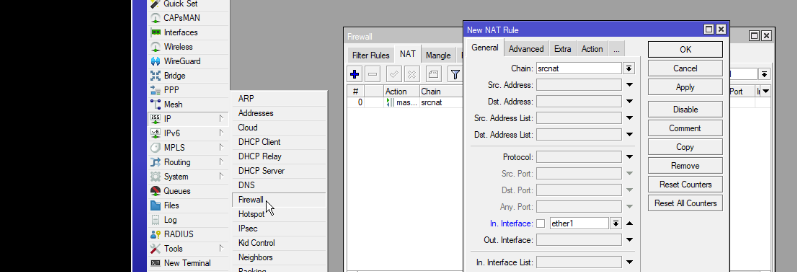
(*DHSP Setup*)

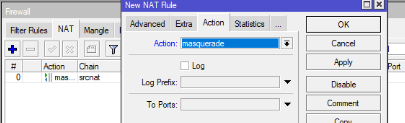
 

*Address to Give Out:* 192.168.18.50 – 192.168.18.150

*DNS Server:* 192.168.18.1

1. Настройка на маршрутизаторе R1 трансляции сетевых адресов (NAT) из адресов внутренней сети в адрес на внешнем интерфейсе маршрутизатора (eth1) осуществляется следующим образом:





1. Включение на коммутаторе доступа по протоколу ssh осуществляется с помощью следующих команд:

*ip domain-name labaz.org*

*crypto key generate rsa (1024)*

*aaa authentication login default local*

*line vty 0 4*

*transport input ssh*

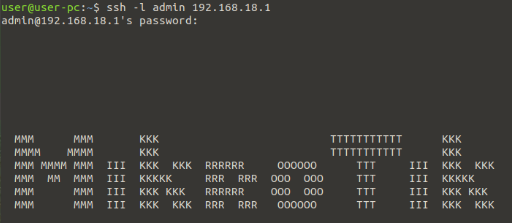
*login authentication default*

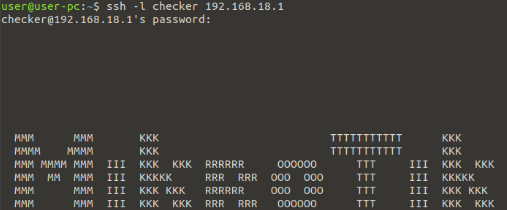
Выключение web-интерфейсов коммутатора осуществляется с помощью следующих команд:

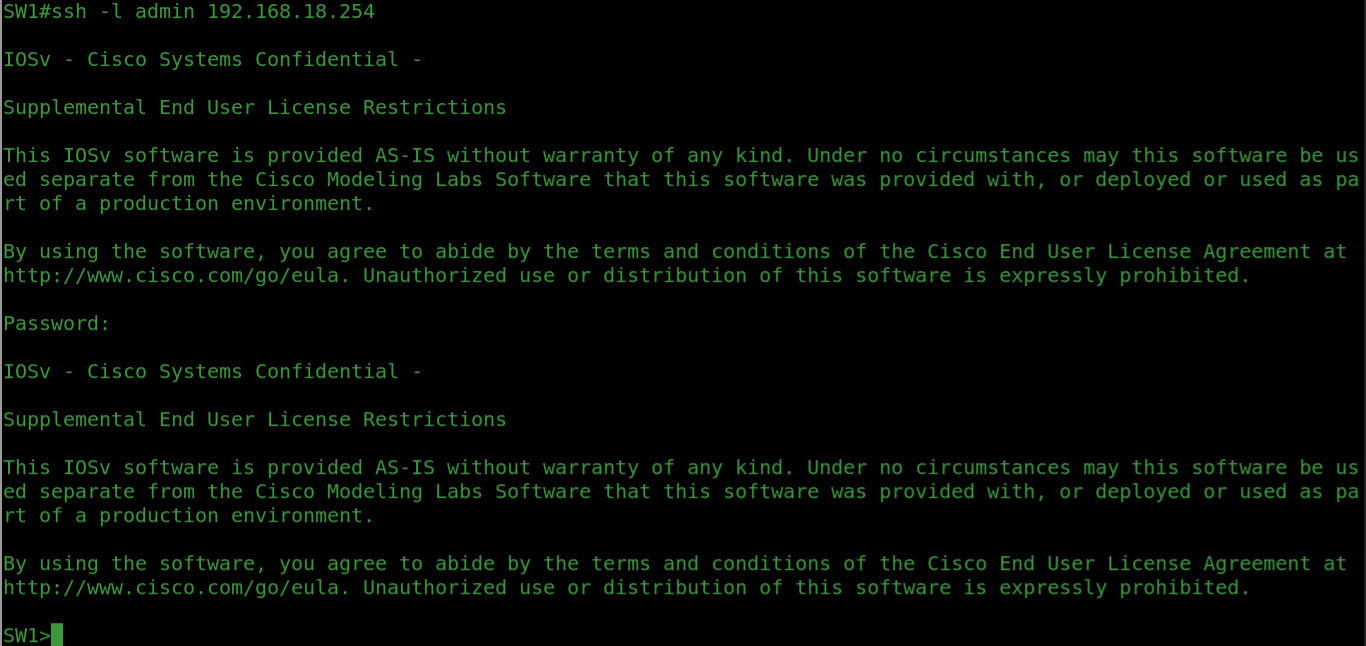
*no ip http server*

*no ip http secure-server*

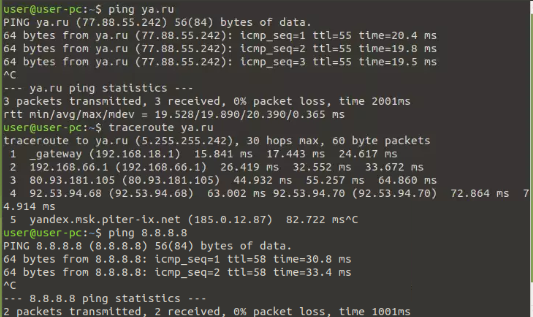
Далее нужно убедиться, что доступ по ssh работает с хостов в сети для администратора и пользователя checker:

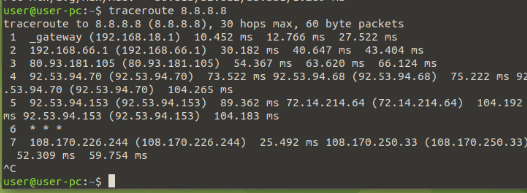


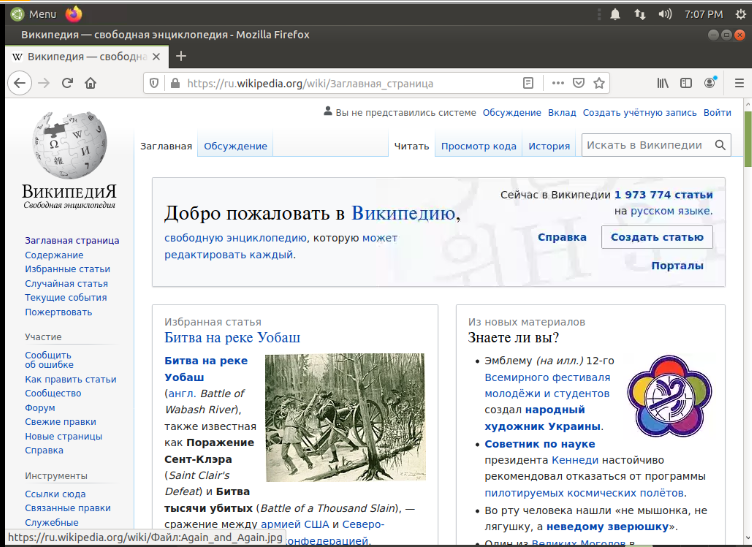


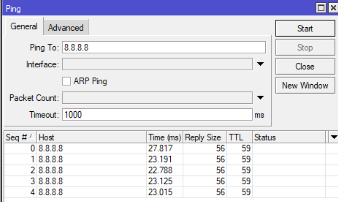
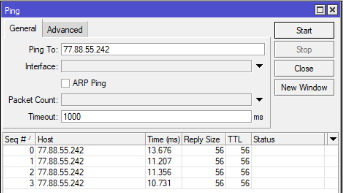


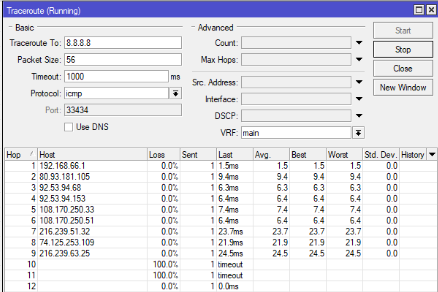
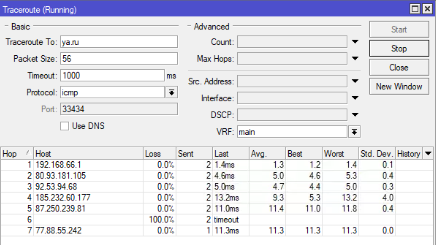
1. Убеждаемся в работоспособности сети:

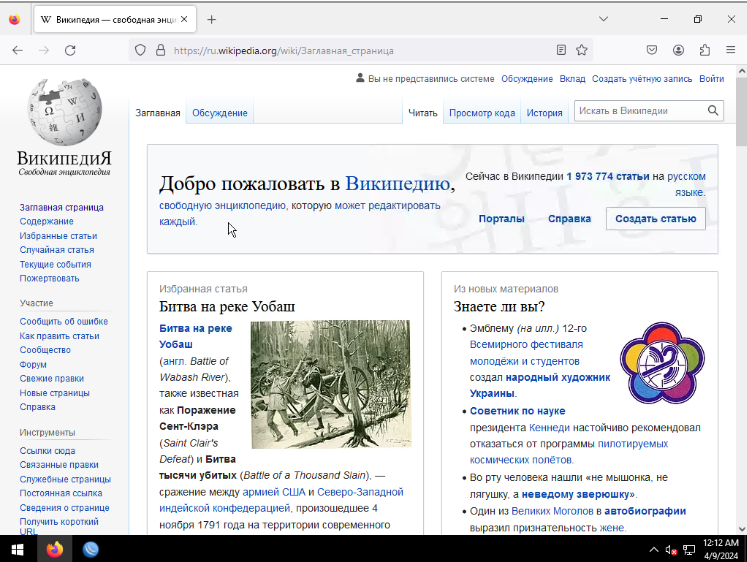




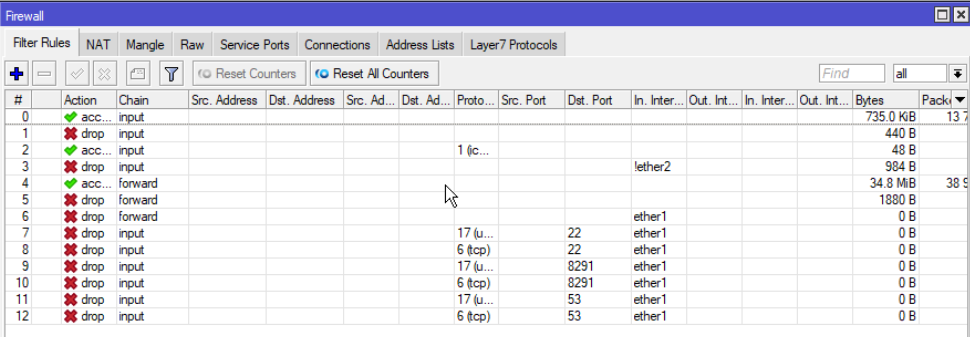




1. Настройка firewall на маршрутизаторе R1 выглядит следующим образом:



**Конфигурация на R1**

*enable secret 5 $1$W08I$Xupx9XZtSaHHdkCkdnC3a/*

*!*

*username checker privilege 15 password 7 107E0F0111012A1F1E10226A*

*username admin privilege 15 password 7 11081D081E1C5A54*

*aaa new-model*

*!*

*aaa authentication login default local*

*!*

*aaa session-id common*

*!*

*ip domain-name labaz.org*

*ip name-server 192.168.18.1*

*ip cef*

*no ipv6 cef*

*!*

*spanning-tree mode pvst*

*spanning-tree extend system-id*

*!*

*interface GigabitEthernet0/0*

*negotiation auto*

*!*

*interface GigabitEthernet0/1*

*negotiation auto*

*!*

*interface GigabitEthernet0/2*

*negotiation auto*

*!*

*interface GigabitEthernet0/3*

*negotiation auto*

*!*

*interface GigabitEthernet1/0*

*negotiation auto*

*!*

*interface GigabitEthernet1/1*

*negotiation auto*

*!*

*interface GigabitEthernet1/2*

*negotiation auto*

*!*

*interface GigabitEthernet1/3*

*negotiation auto*

*!*

*interface Vlan1*

*ip address 192.168.18.254 255.255.255.0*

*!*

*ip forward-protocol nd*

*!*

*no ip http server*

*no ip http secure-server*

*!*

*ip route 0.0.0.0 0.0.0.0 192.168.18.1*

*ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr*

*ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr*

*!*

*line con 0*

*line aux 0*

*line vty 0 4*

*transport input ssh*

*!*

*end*

**Выводы**

В процессе выполнения лабораторной работы я познакомился с процессом настройки устройств в простейшей сети. Данная задача была довольно интересной, так как практически всё в данной работе было для меня новым (работа в WinBox и на коммутаторе Cisco, конфигурирование и настройка dhsp, dns, firewall и т.д.). Теперь я смогу осуществить настройку подобной сети в бытовых условиях, если это потребуется.