

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: *И. П. Попов*

Группа: *8О-406Б*

Преподаватели: Филимонов Н. С.

Москва, 2023

## Цели ЛР:

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

## Задачи ЛР:

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).

### **Допустимые средства конфигурации:**

На хосте Win имеется установленный WinBox для конфигурации Mikrotik, его разрешается использовать. Также разрешается использовать консоль маршрутизатора и коммутатора без ограничений. Запрещается использовать web-интерфейс для настройки коммутатора.

### **Данные аутентификации для хостов:**

Windows – логин admin, пароль admin. Linux – логин user, пароль Test123.

### **Данные аутентификации для узлов:**

Логины и пароли для Mikrotik CHR и Cisco vIOS соответствуют данным по умолчанию для данных устройств в заводской конфигурации.

### **Особенности конфигурации для вариантов задания:**

Во всех значениях, приведенных ниже, макрос *N* означает номер варианта без лидирующего нуля (1, 2, ..., 12, 23, ...).

Пароль администратора для маршрутизатора и коммутатора *adminN*.

Префикс внутренней сети для маршрутизатора: *192.168.N.0/24*.

Внутренний адрес маршрутизатора R1: *192.168.N.1*.

Адрес коммутатора SW1 в management VLAN: *192.168.N.254*.

Пул IP-адресов для внутреннего DHCP: *192.168.N.50-192.168.N.150*.

# SW1

Building configuration...

Current configuration : 3149 bytes

!

! Last configuration change at 15:07:41 UTC Wed Apr 17 2024

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

service compress-config

!

hostname SW1

!

boot-start-marker

boot-end-marker

!

!

enable secret 5 \$1\$/dtu\$BaZPYQCgY4JzipmYNCY6E.

!

username admin privilege 15 password 7 050A020228421F5E

aaa new-model

!

!

aaa authentication login default local

!

!

!

!

!

!

aaa session-id common

!

!

!

!

!

!

!

!

ip domain-name labaz.org

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 192.168.17.254 255.255.255.0
!
ip forward-protocol nd
!
ip http server
ip http secure-server
!
```

```
ip route 0.0.0.0 0.0.0.0 192.168.17.1
ip ssh version 2
ip ssh server algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
!
!
!
!
!
!
!
!
control-plane
!
banner exec ^C
IOSv - Cisco Systems Confidential -
```

#### Supplemental End User License Restrictions

This IOSv software is provided AS-IS without warranty of any kind. Under no circumstances may this software be used separate from the Cisco Modeling Labs Software that this software was provided with, or deployed or used as part of a production environment.

By using the software, you agree to abide by the terms and conditions of the Cisco End User License Agreement at <http://www.cisco.com/g> o/eula. Unauthorized use or distribution of this software is expressly prohibited.  
^C

```
banner incoming ^C
IOSv - Cisco Systems Confidential -
```

#### Supplemental End User License Restrictions

This IOSv software is provided AS-IS without warranty of any kind. Under no circumstances may this software be used separate from the C

isco Modeling Labs Software that this software was provided with, or deployed or used as part of a production environment.

By using the software, you agree to abide by the terms and conditions of the Cisco End User License Agreement at <http://www.cisco.com/g> o/eula. Unauthorized use or distribution of this software is expressly prohibited.

```
^C
banner login ^C
IOSv - Cisco Systems Confidential -
```

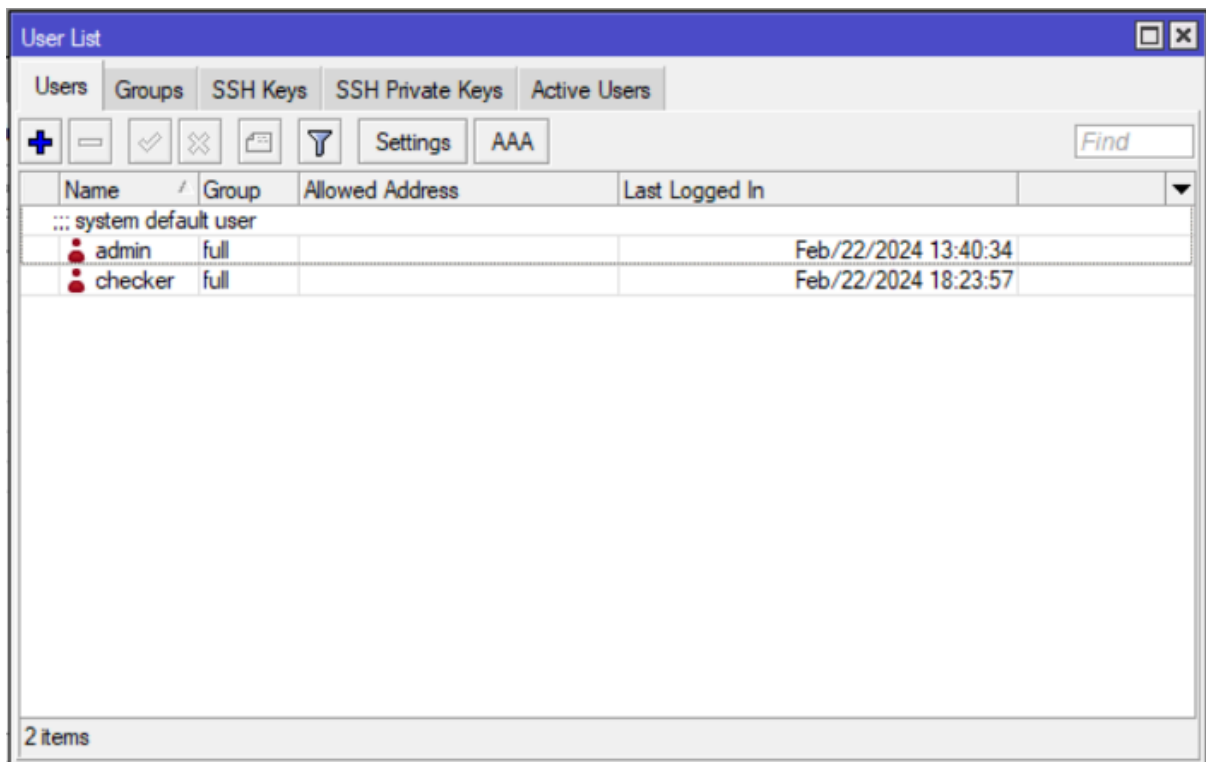
```
Supplemental End User License Restrictions
Supplemental End User License Restrictions
```



```
This IOSv software is provided AS-IS without warranty of any kind.
Under no circumstances may this software be used separate from the
C
isco Modeling Labs Software that this software was provided with,
or deployed or used as part of a production environment.
```

```
By using the software, you agree to abide by the terms and
conditions of the Cisco End User License Agreement at
http://www.cisco.com/go/eula. Unauthorized use or distribution of this software is
expressly prohibited.
```

```
^C
!
line con 0
line aux 0
line vty 0 4
  transport input ssh
!
!
end
```

## Mikrotik R1



Name	Group	Allowed Address	Last Logged In
... system default user			
 admin	full		Feb/22/2024 13:40:34
 checker	full		Feb/22/2024 18:23:57

2 items

Рис. 1. Список пользователей











Address List					
<div>       <div>Find</div> </div>					
	Address	Network	Interface		
	 192.168.4.1/24	192.168.4.0	ether2		
D	 192.168.66.17...	192.168.66.0	ether1		
<div>2 items</div>					

Рис. 2. Список IP-адресов

DNS Settings

Servers: 9.9.9.9

Dynamic Servers: 8.8.8.8

Use DoH Server:

☐ Verify DoH Certificate

☒ Allow Remote Requests

Max UDP Packet Size: 4096

Query Server Timeout: 2.000 s

Query Total Timeout: 10.000 s

Max. Concurrent Queries: 100

Max. Concurrent TCP Sessions: 20

Cache Size: 2048 KiB

Cache Max TTL: 7d 00:00:00

Cache Used: 36 KiB

OK

Cancel

Apply

Static

Cache

Рис. 3. Настройки DNS-сервера

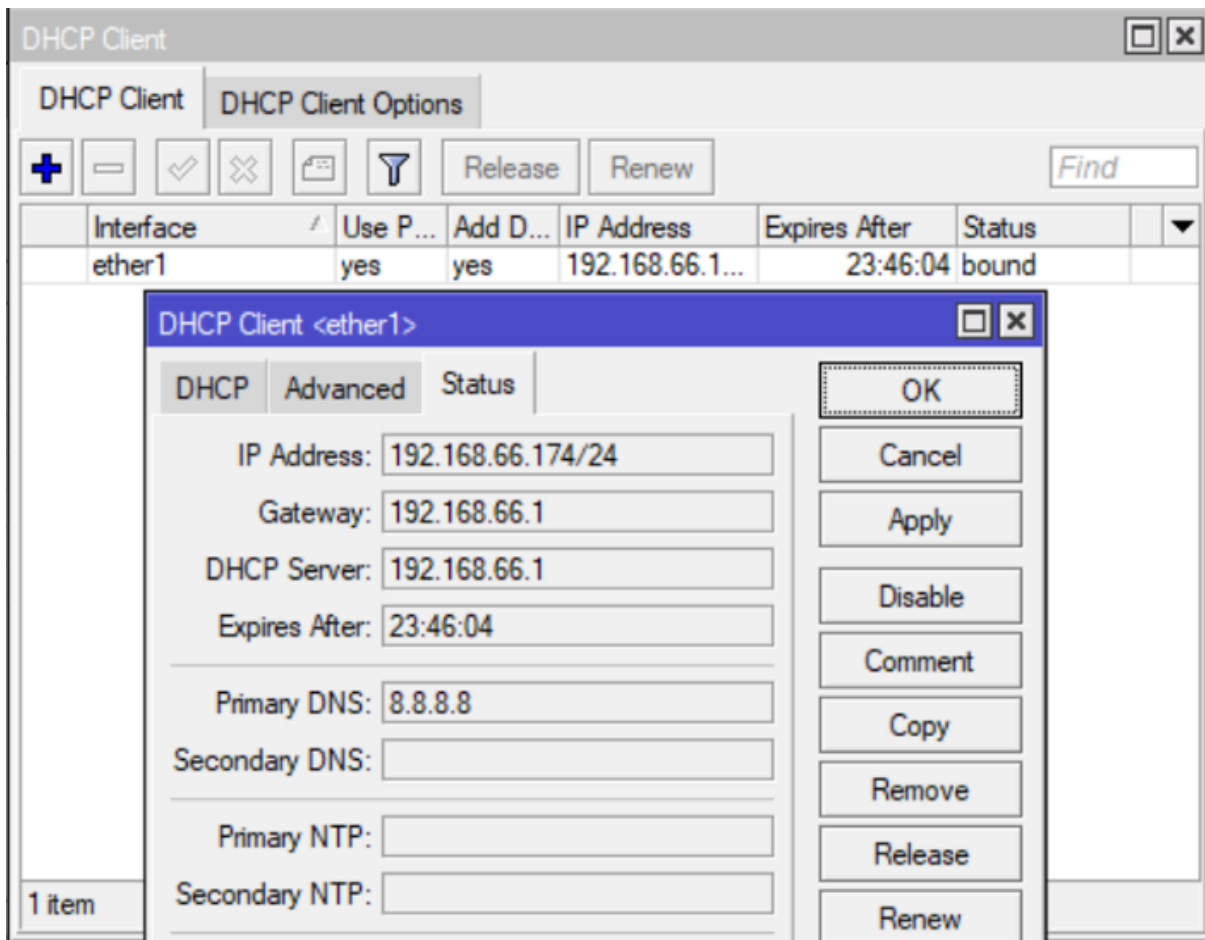


Рис. 4. Настройка DHCP сервера

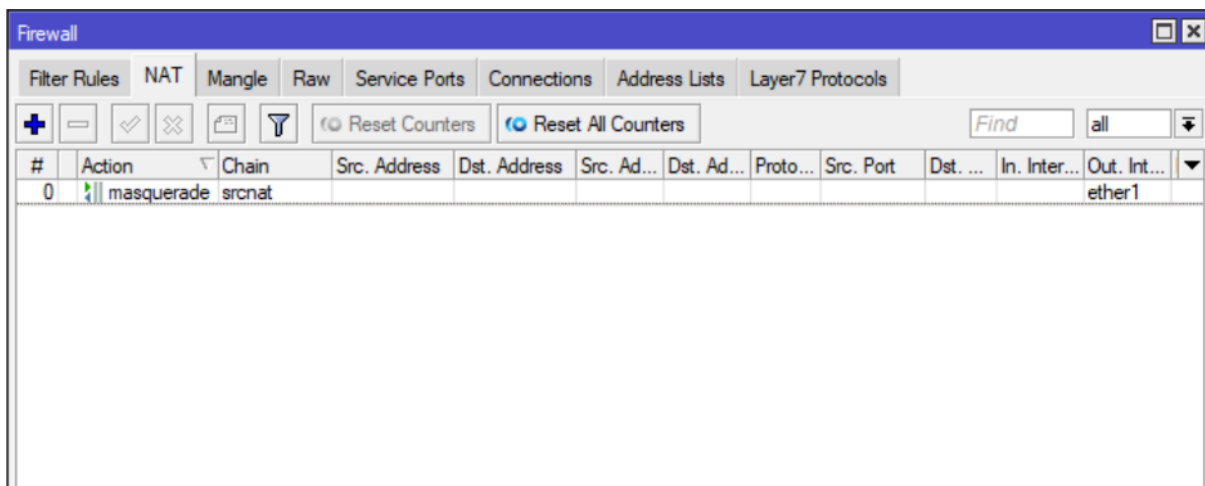


Рис. 5. Настройки NAT

#	Action	Chain	Src. Address	Dst. Address	Src. Ad...	Dst. Ad...	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...
0	drop	input					17 (u...		53	ether1	
1	drop	input					6 (tcp)		53	ether1	
2	drop	input					17 (u...		22	ether1	
3	drop	input					6 (tcp)		22	ether1	
4	drop	input					17 (u...		443	ether1	
5	drop	input					6 (tcp)		443	ether1	
6	drop	input					6 (tcp)		80	ether1	
7	drop	input					17 (u...		80	ether1	

Рис. 6. Настройки firewall-a

## Выводы

В ходе выполнения данной лабораторной работы я освоил навыки работы с интерфейсами управления и настройки оборудования Cisco Systems и Mikrotik. Это включало настройку IP-адресов, установку паролей и логинов, а также настройку NAT для конечных пользователей на устройствах Mikrotik. Было непросто обнаружить, что для доступа в Интернет через коммутатор SW1 требуется активация IP-маршрутизации. Также, я не оптимально настроил фаервол на Mikrotik, ограничив лишь определенные соединения, вместо того чтобы запретить все соединения по умолчанию и разрешить необходимые, используя механизмы established и related для эффективной проверки уже существующих и связанных соединений.