ФГБОУ ВО “Чувашский государственный университет им. И. Н. Ульянова” Факультет: ИВТ

Кафедра: Вычислительной техники

Предмет: Сети и телекоммуникации

Лабораторная работа 7

**Научиться настраивать роутер**

Выполнил: студент группы ИВТ-41-20

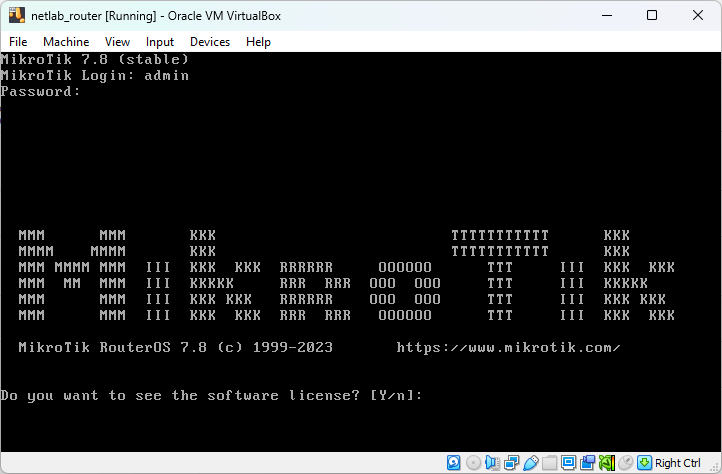
Галкин Дмитрий

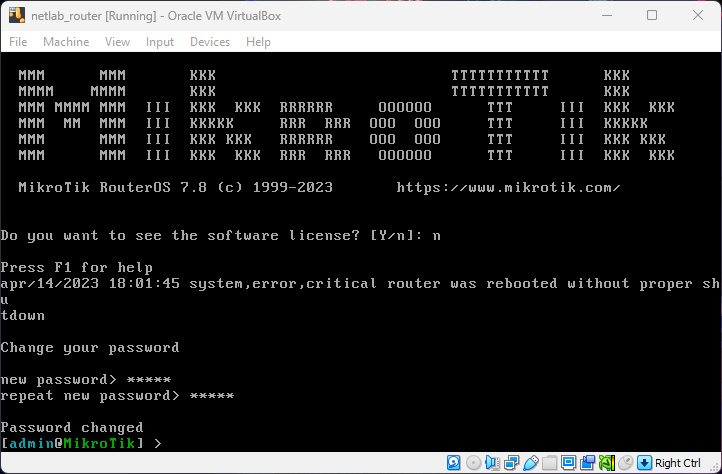
Проверила: Путевская И.В.

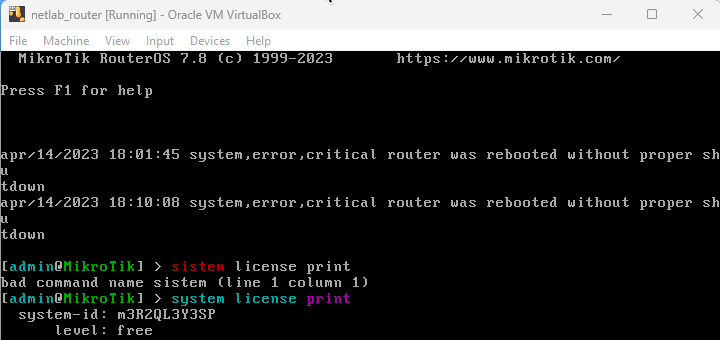
Чебоксары 2023 г.

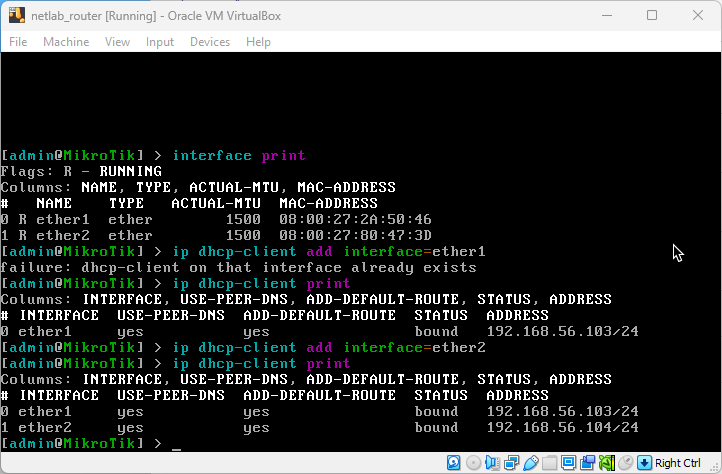
**Цель:** научиться настраивать роутер

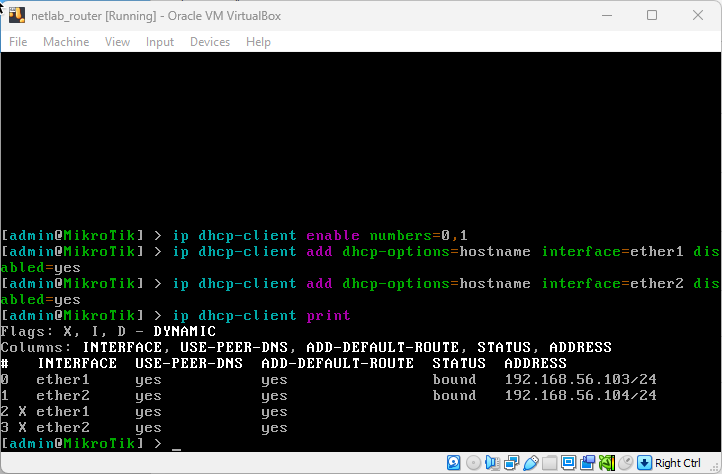
**Задача 1:** настроить локальную сеть между роутером и станциями

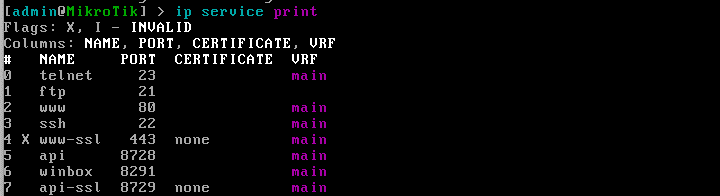
1. Запустить netlab\_router  
   

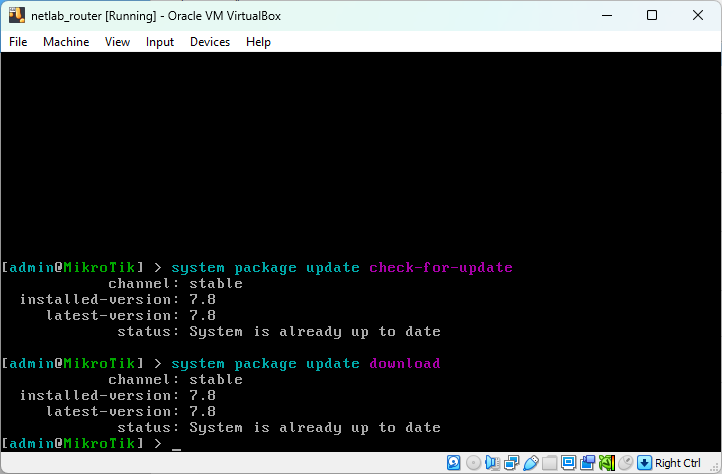


1. Настройка  
   

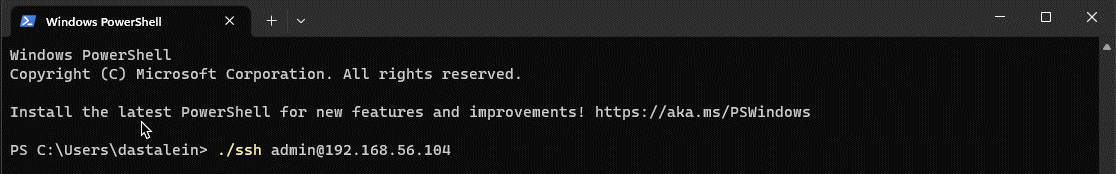




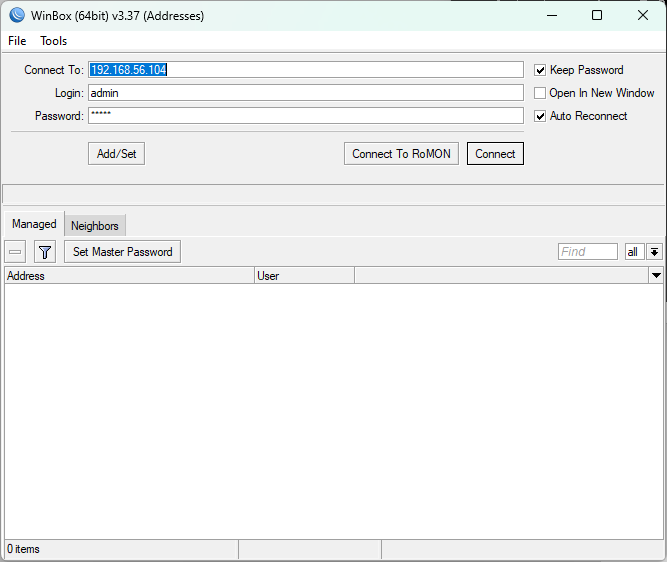


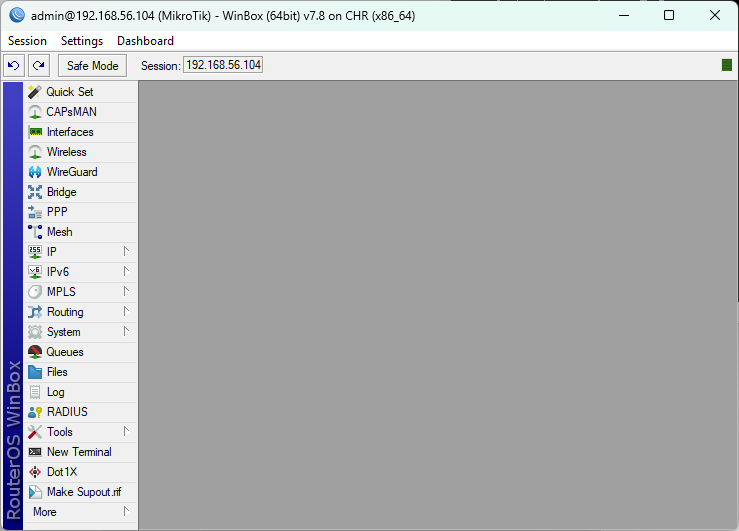


1. Подключение по ssh



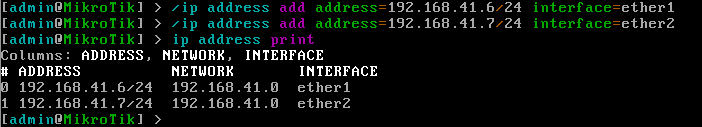
1. Подключение по winbox



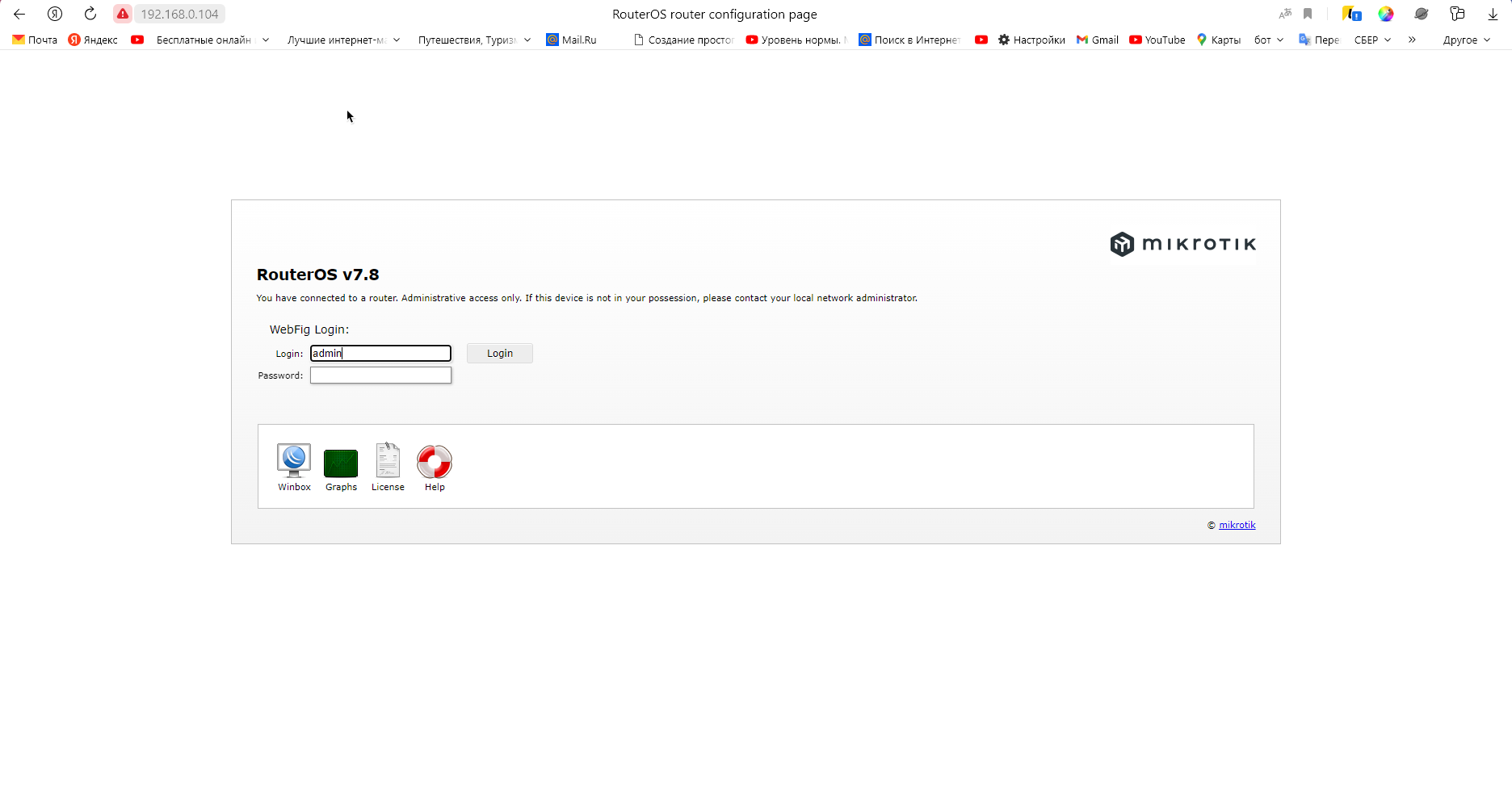


**Задача 2:** настроить интернет на роутере

1. Настройка статического ip
2. Настройка ip на хосте адаптера VirtualHostOnly



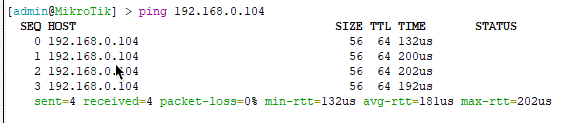
1. Вход в Web интерфейс



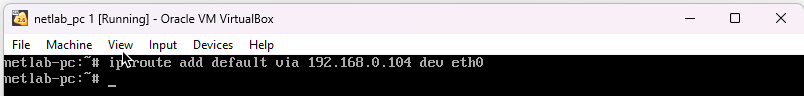


**Задача 3:** настроить роутер как шлюз в интернет

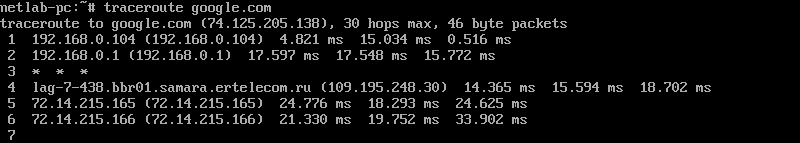
1. проверить связь между станциями и роутером (ping)



1. добавить маршрут по-умолчанию на станциях узла через роутер netlab\_pc: ip route add default via <router-ip> dev <if>



1. проверить связь со станций до внешнего узла (например google dns-server-8.8.8.8): traceroute/tracepath <ip>

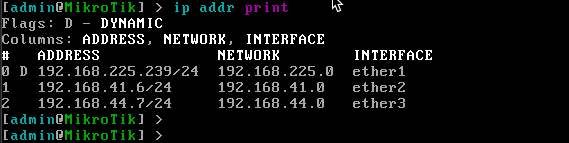


**Задача 4:** настроить роутер как шлюз в соседние сети

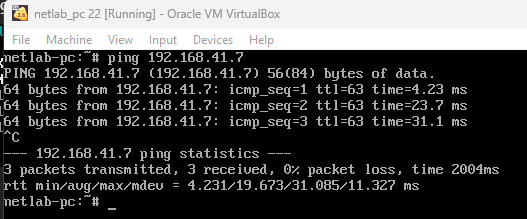
1. на роутере добавить маршруты в соседние сети (ip route add)

для netlab\_pc2: ip addr add 192.168.41.7/24 dev eth0

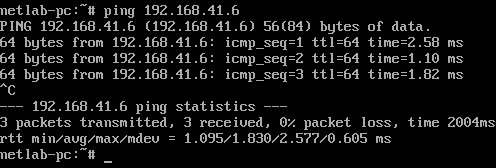
для netlab\_pc2: ip addr add 192.168.44.8/24 dev eth0



ping netlab\_pc2



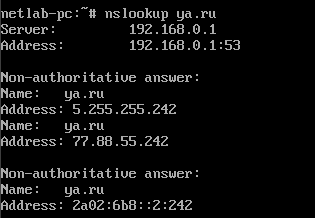
ping netlab\_pc1



1. добавить адрес dns-server на netlab\_pc: echo ‘nameserver <ip-dns>’ /etc/resolv.conf



1. проверить доступ к ресурсам интернета по имени: nslookup ya.ru



**Ответы на вопросы:**

1. Зачем нужно разрешать форвардинг?

Разрешение форвардинга необходимо для пересылки сообщений между разными узлами или устройствами в компьютерных сетях. Это позволяет устройствам в сети отправлять и получать данные, не ограничиваясь только своей локальной сетью. Форвардинг также позволяет оптимизировать передачу данных и обеспечивать более эффективную работу.

1. Что делает NAT?

NAT (Network Address Translation) переводит локальные IP-адреса устройств в сети в общедоступный публичный IP-адрес. Это позволяет устройствам в локальной сети обмениваться данными через интернет, не раскрывая свои локальные IP-адреса публично. NAT также может использоваться для связывания нескольких устройств в локальной сети с одним общедоступным IP-адресом. Кроме того, NAT может повысить безопасность локальной сети, так как он скрывает IP-адреса устройств в локальной сети от внешней сети.

1. Из чего состоит маршрут?

Последовательность IP-адресов

1. Как посмотреть имеющиеся маршруты?

Можно использовать команды: route print или ip route show

1. Что такое путь по умолчанию?

Это IP-адрес маршрутизатора, который используется для пересылки сетевых пакетов из локальной сети во внешнюю сеть (как правило, это интернет). Если устройство в локальной сети хочет отправить пакет данных за пределы сети, оно отправляет его на адрес по умолчанию, который пересылает пакет в другие сети и к конечному получателю. Адрес по умолчанию должен быть настроен на каждом устройстве в локальной сети, что обеспечить доступ к Интернету и другим сетям.

1. Как проверить путь отправки сообщений?

Нужно использовать traceroute <ip>

1. Как настроить преобразование имен?

Для настройки преобразования имен необходимо настроить файл hosts или использовать службу DNS (Domain Name System)

1. Какие обязательные настройки нужны для wifi-сети?

* Настройка точки доступа: необходимо выбрать устройство, которое будет служить точкой доступа (например, беспроводной маршрутизатор) и настроить его параметры, такие как SSID(имя сети), тип безопасности и пароль
* Настройка защиты: важно настроить механизм защиты, чтобы предотвратить несанкционированной доступ к сети
* Настройка IP-адресации: необходимо настроить статические или динамические IP-адреса для каждого устройства в сети
* Настройка DHCP-сервера: DHCP-сервер автоматически назначает IP-адреса устройством сети, что упрощает процесс подключения к сети
* Проверка качества сигнала: важно проверить качество сигнала Wi-Fi в различных местах внутри и вокруг помещений
* Настройка фильтрации MAC-адресов: фильтрация MAC-адресов позволяет ограничить доступ к сети только устройствам, которые имеют разрешение на подключение.
* Настройка портов: если требуется удаленный доступ к сети, необходимо настроить порты и настроить механизмы аутенфикации и шифрования, чтобы защитить сеть от несанкционированного доступа