КОМИТЕТ ПО ОБРАЗОВАНИЮ ПРАВИТЕЛЬСТВА САНКТ-ПЕТЕРБУРГА

Санкт-Петербургское государственное

бюджетное профессиональное образовательное учреждение

«Колледж информационных технологий»

**ОТЧЁТ**

**по «УП 01.02 Организация, принципы построения и функционирования компьютерных сетей»**

**Специальность 09.02.06**

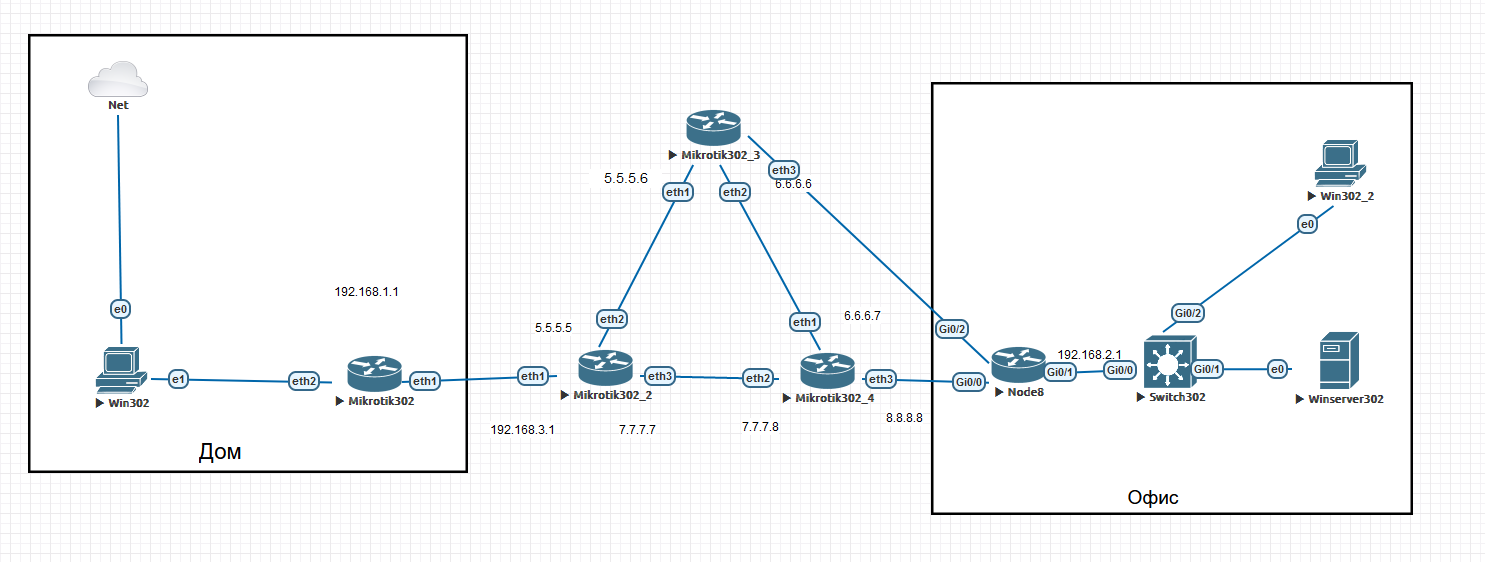
**«Сетевое и системное администрирование»**

Работу выполнил студент 302 гр. Голубев Е. Д.

Преподаватель: Антонов А. Ю.

Санкт-Петербург 2023

# Топология

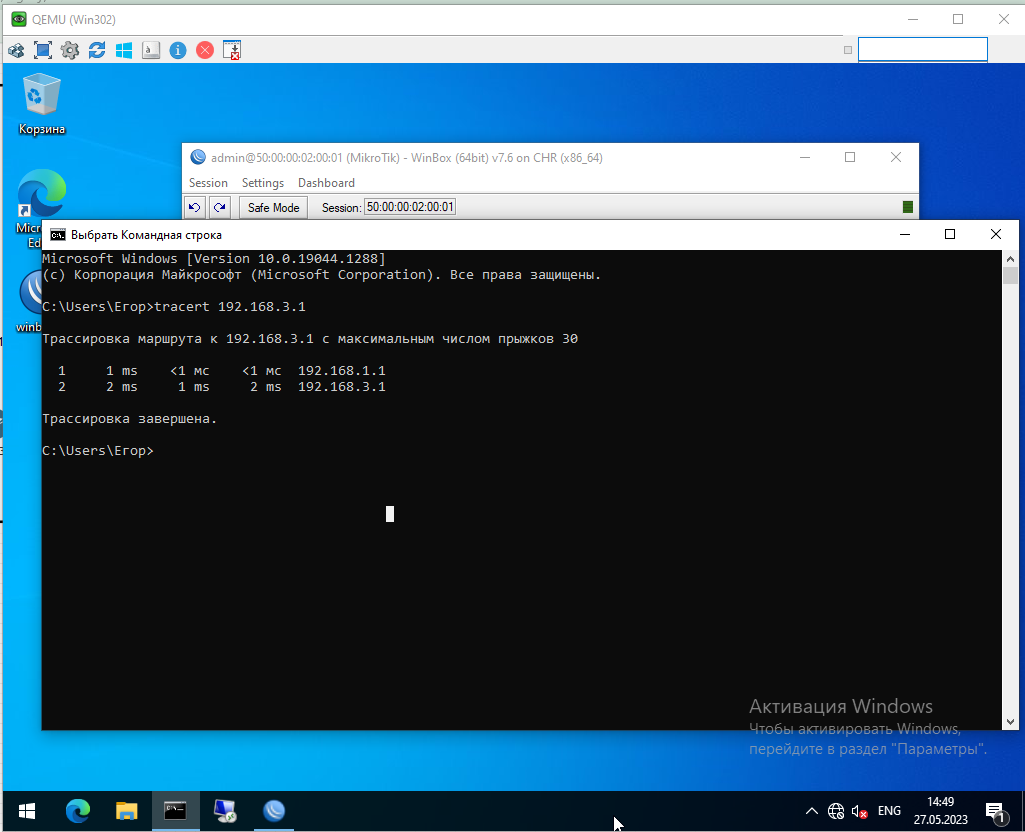


# Таблица адресации

|  |  |  |
| --- | --- | --- |
| Домашний ПК | DHCP | Без пароля |
| Домашний маршрутизатор | 192.168.1.1/DHCP | 1 |
| Левый “Провайдер” | 192.168.3.1/5.5.5.5/7.7.7.7 | 1 |
| Верхний “Провайдер” | 5.5.5.6/6.6.6.6 | 1 |
| Правый “Провайдер” | 7.7.7.8/6.6.6.7/8.8.8.8 | 1 |
| Офисный маршрутизатор | DHCP/192.168.5.1 | Без пароля |
| Офисный сервер | DHCP | P@ssw0rd |
| Офисный ПК | DHCP | Без пароля |

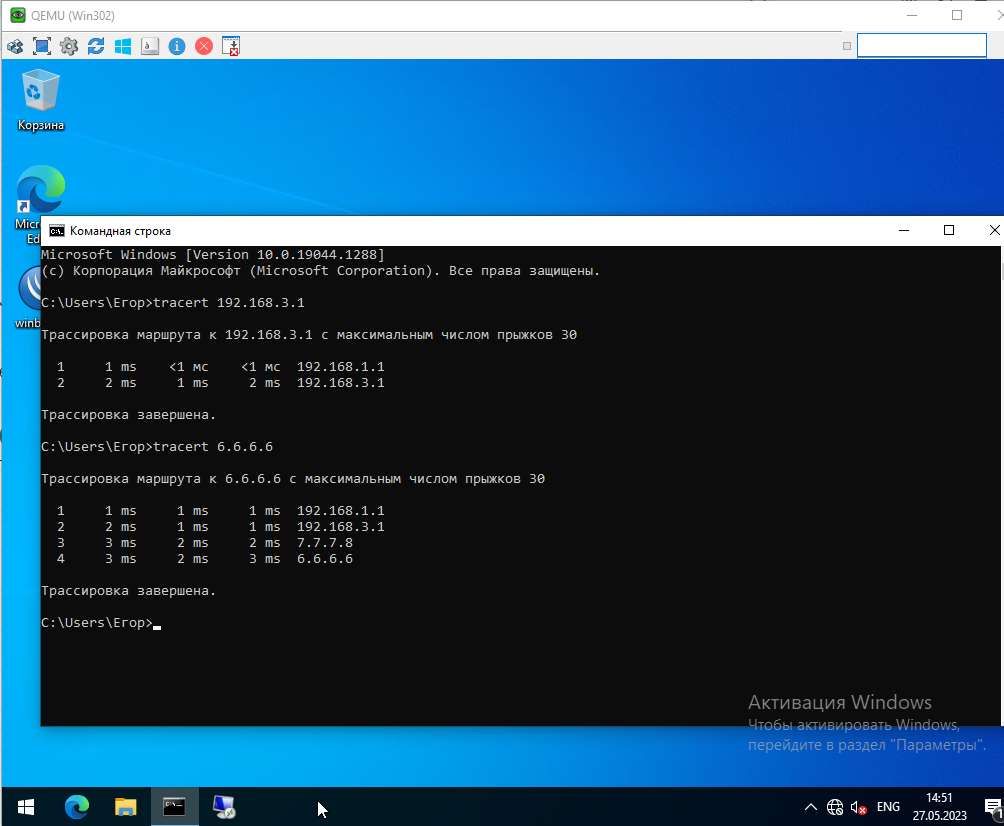
# Организация домашнего подключения к Интернет

Tracert c домашнего ПК до сети провайдера.

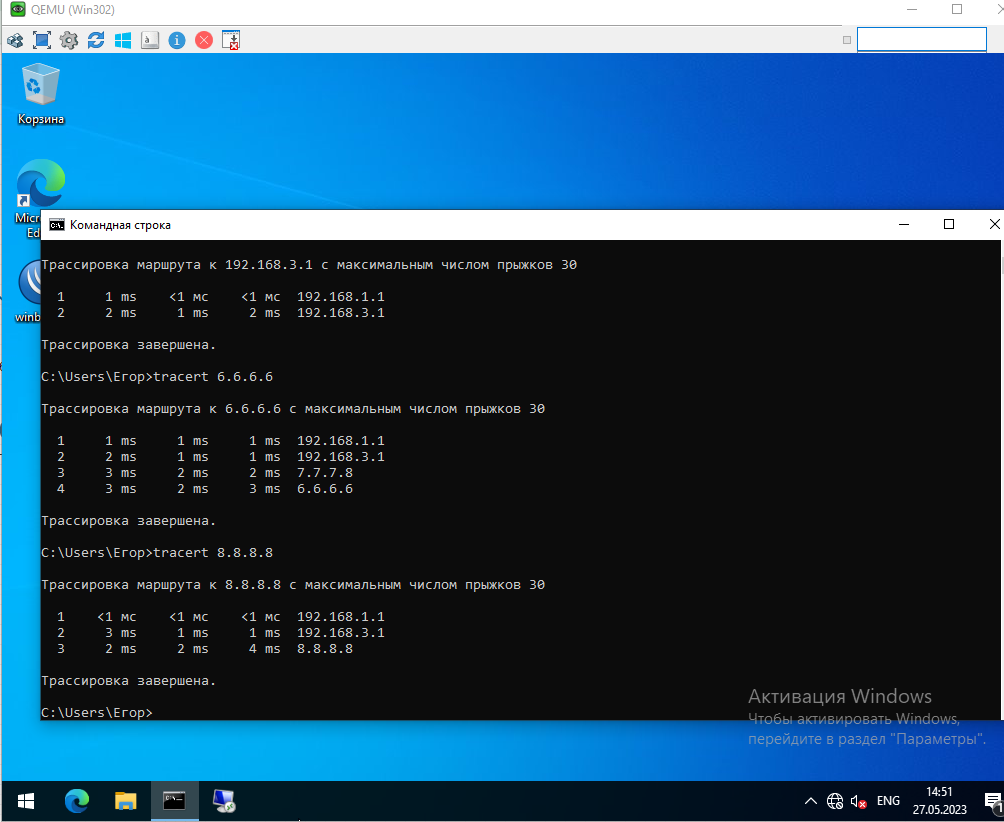


# Организация связей между тремя «провайдерами»

Теперь нам необходимо оптимизировать сеть провайдеров с помощью протокола OSPF  
  
В сети провайдера присутствуют 3 устройства, а также 1 домашний и 1 офисный маршрутизаторы.

Фигура 1: Tracert к одному из провайдеров доказывающих работу протокола OSPF

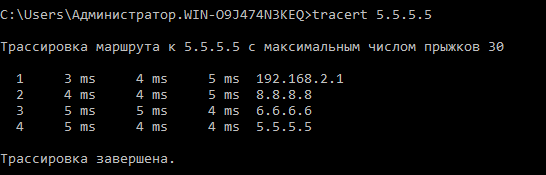
Трасерт до одного из дальних провайдеров.

Фигура 2: Tracert к одному из провайдеров доказывающих работу протокола OSPF

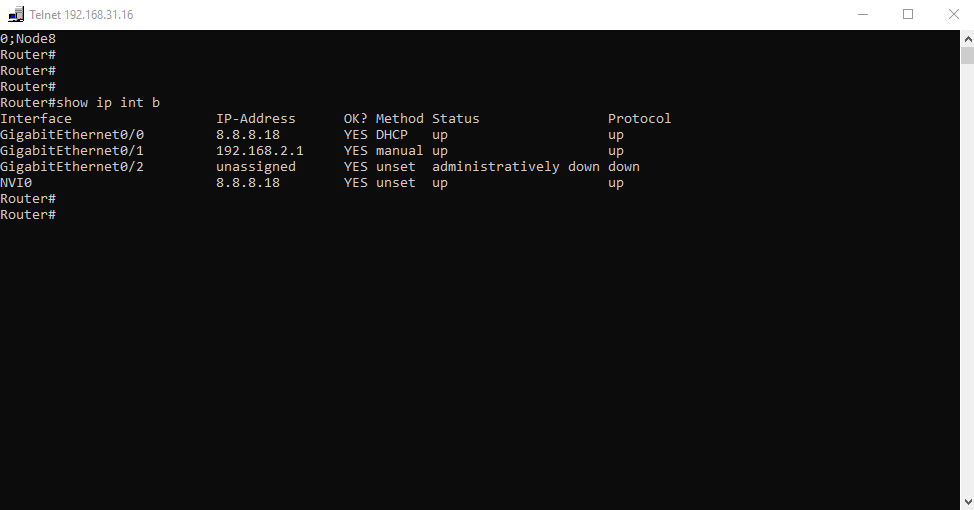
# Организация подключения головного офиса к Интернет с получением публичного IP

Как уже было показано выше мы имеем не только сеть с протоколом OSPF но также и протокол NAT для возможности пинговать «Провайдеров», а также проброс портов для подключения до нашего сервера в офисе.

Проверяем наличие Ping’а до дальних провайдеров.

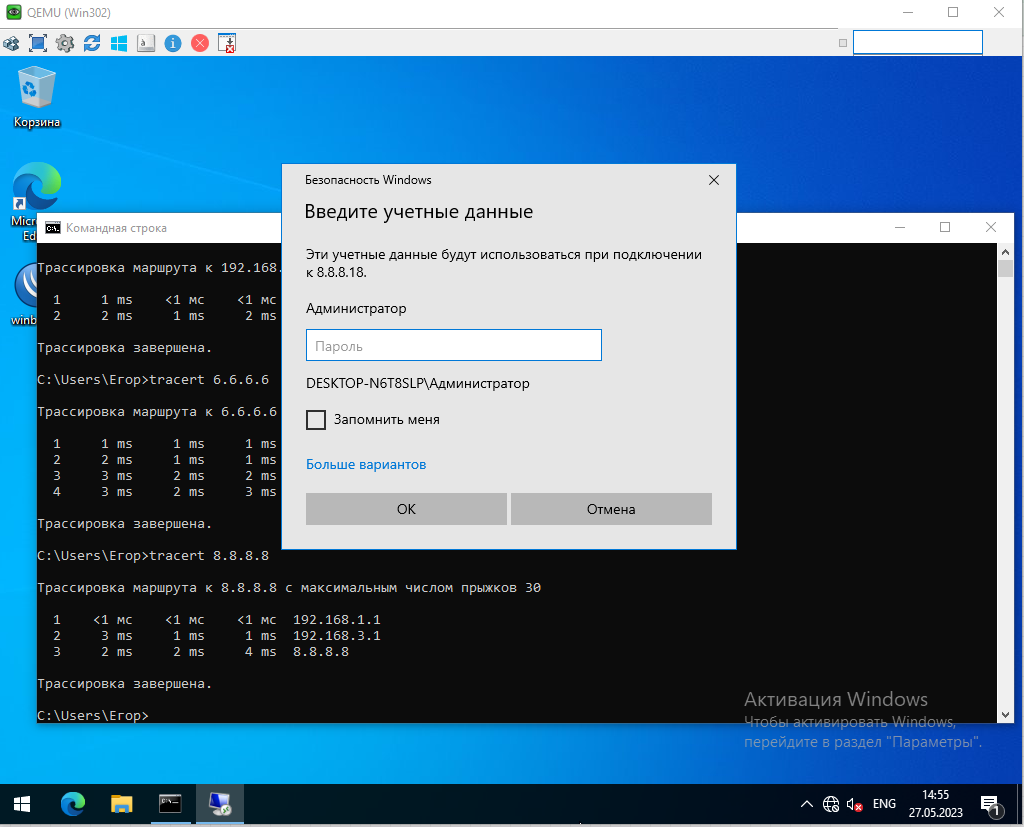
Фигура 3: Проверка ping-запроса до дальнего "Провайдера"

Стоит упомянуть, что офис подключен к провайдеру по DHCP, который раздаёт ему белый IP адресс.

Фигура 4: Настройка интерфейсов на cisco, в первой строчке виден DHCP.

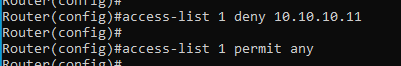
# Организация удаленного доступа к серверу с домашнего ПК

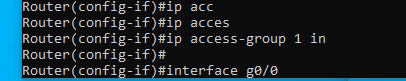
Для подключения по RDP нам необходим проброс портов, подключаясь по IP маршрутизатора в офисе, мы подключаемся к серверу внутри офиса.

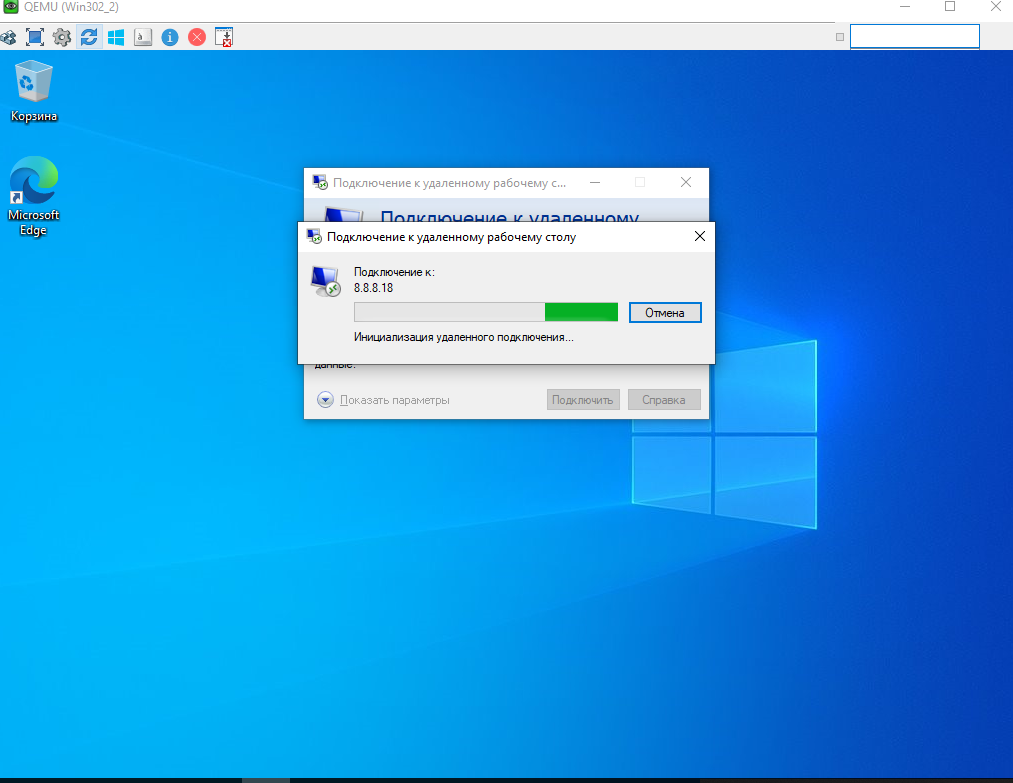
Рисунок 1: Нас попросили ввести данные от пользователя, а значит RDP работает

# Защита подключения к головному офису с помощью списков контроля доступа

Теперь для защиты, мы должны установить правила трафика в нашей сети, для примера мы запретим доступ с рабочей станции в интернете с ip-адрессом 10.10.10.11

Рисунок 2: Правила ACL

Рисунок 3: Добавление ACL-списка на внешний порт

Рисунок 4: Как видим, ACL-список не разрешает подключиться к серверу

# Организация VPN подключения к головному офису

Используя встроенные в Windows службы, можно использовать защищенное подключение к серверу.

Как и в rdp подключаемся мы по IP маршрутизатора.

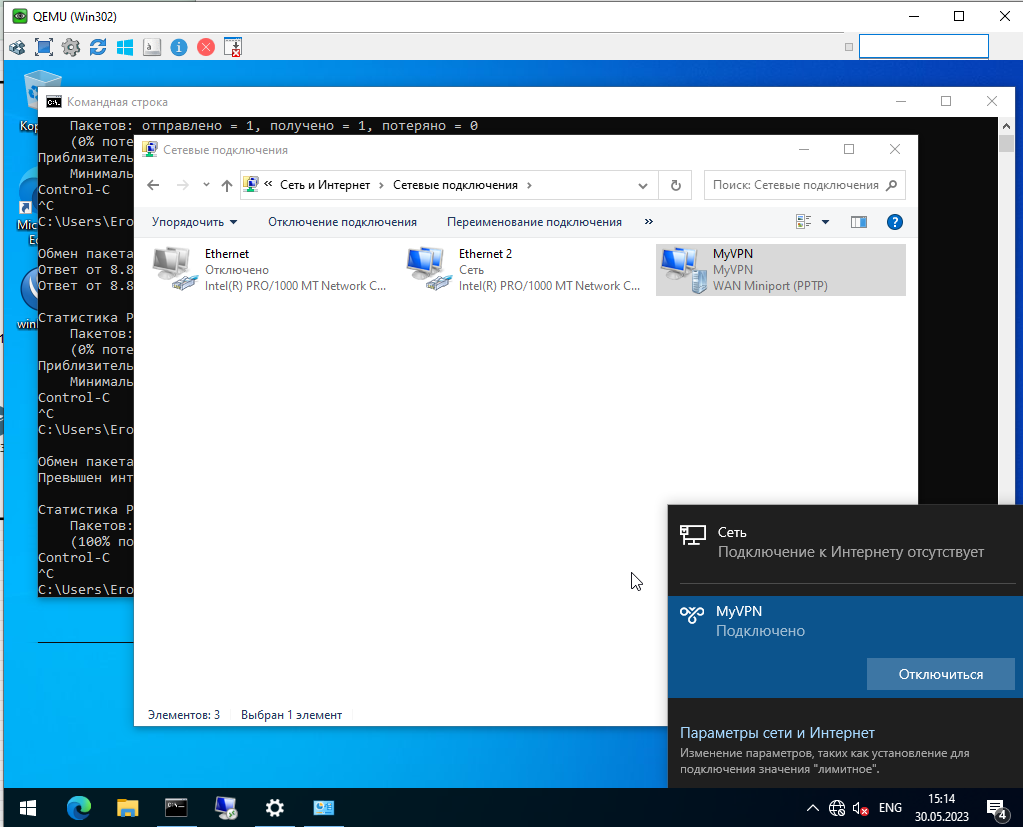


Рисунок Подключение удалось!

Рисунок Подключение удалось!

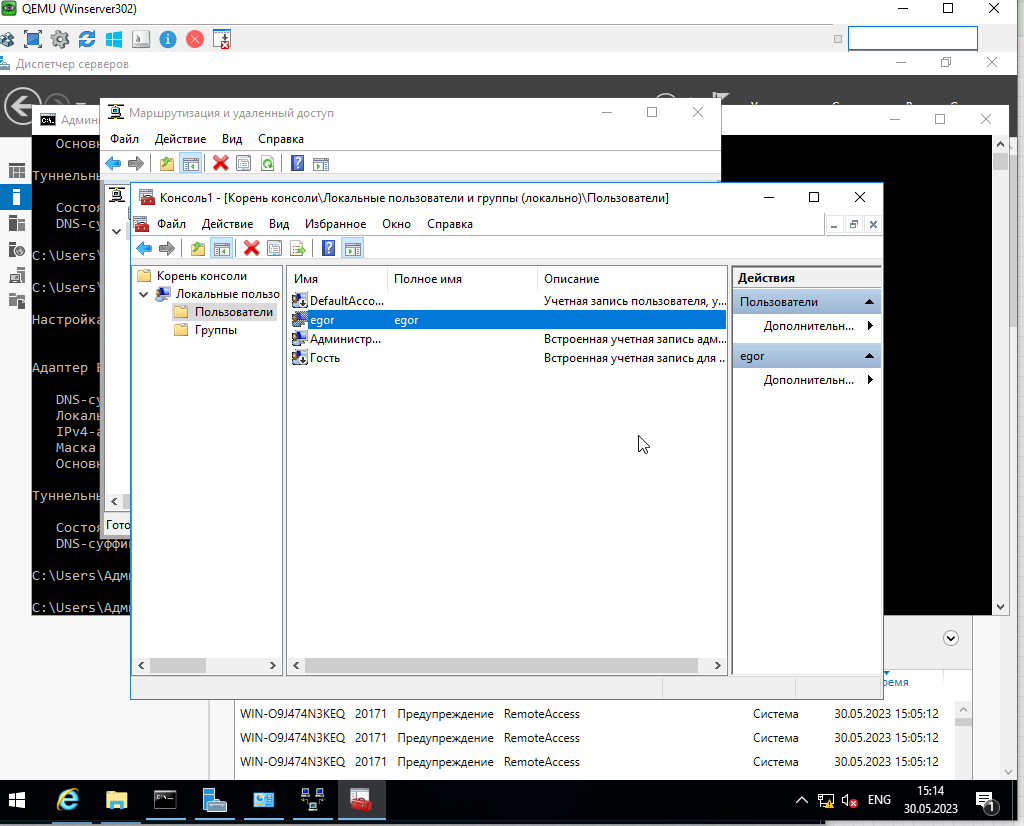


Рисунок Созданный пользователь для VPN