Министерство науки и высшего образования Российской Федерации

федеральное государственное автономное образовательное учреждение высшего образования

«Национальный исследовательский университет ИТМО»

*Факультет программной инженерии и компьютерной техники*

**Лабораторная работа**

«Настройка подключения к сети и основные сетевые службы»

Группа: P33211

Выполнили: Аплавина А.А.,

Назирджонов Н.Ф.

Проверил:

к.т.н. преподаватель Белозубов А.В.

Санкт-Петербург

2024г.

# ОГЛАВЛЕНИЕ

[**ОГЛАВЛЕНИЕ**](#_itg5y9lmkl6t) **1**

[**ВВЕДЕНИЕ**](#_cb4bawhwgghd) **2**

[**СЕТЕВЫЕ КОМАНДЫ**](#_31w7w6eczsl2) **3**

[**НАСТРОЙКА СЕТЕВЫХ ИНТЕРФЕЙСОВ. КОНФИГУРАЦИЯ БРАНДМАУЭРА**](#_emsg5l6orceg) **13**

[**ЗАКЛЮЧЕНИЕ**](#_la25borwuc2) **31**

# ВВЕДЕНИЕ

В первой части данной лабораторной работы необходимо выполнить ряд сетевых команд, посмотреть на их результат. Во второй части необходимо настроить сетевые интерфейсы сервера и рабочей станции, проверить их работу. Далее следует настроить брандмауэр и DHCP-сервер.

# СЕТЕВЫЕ КОМАНДЫ

Команда ARP позволяет отображать и менять таблицы преобразования IP-адресов в физические, используемые протоколом разрешения адресов (рис. 1.1).

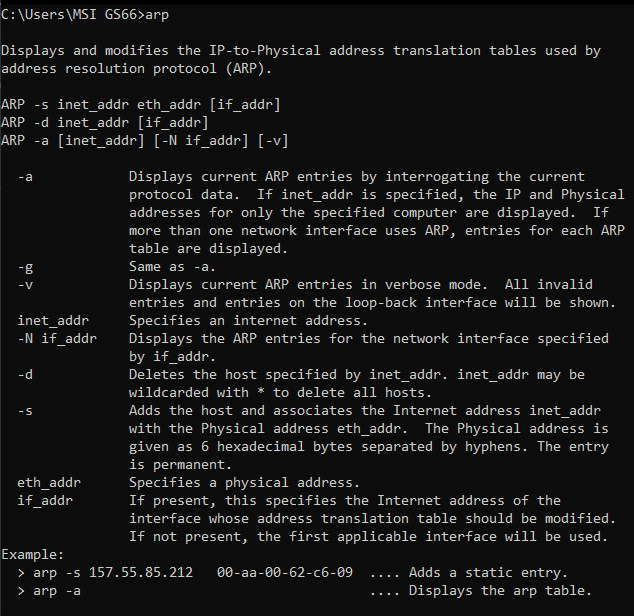


Рисунок 1.1 - Информация о команде ARP

Запустим команду и посмотрим на вывод (рис. 1.2).

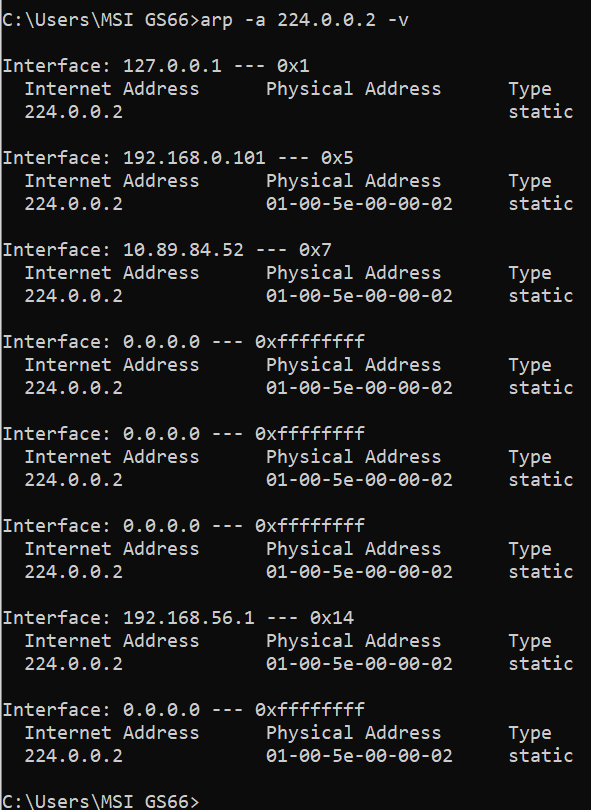


Рисунок 1.2 - Вывод команды ARP

Команда route позволяет обрабатывать таблицы сетевых маршрутов, управлять таблицами маршрутизации в сети (рис. 1.3).



Рисунок 1.3 - Описание команды route

Запустим эту команду для обоих типов ip (рис. 1.4).

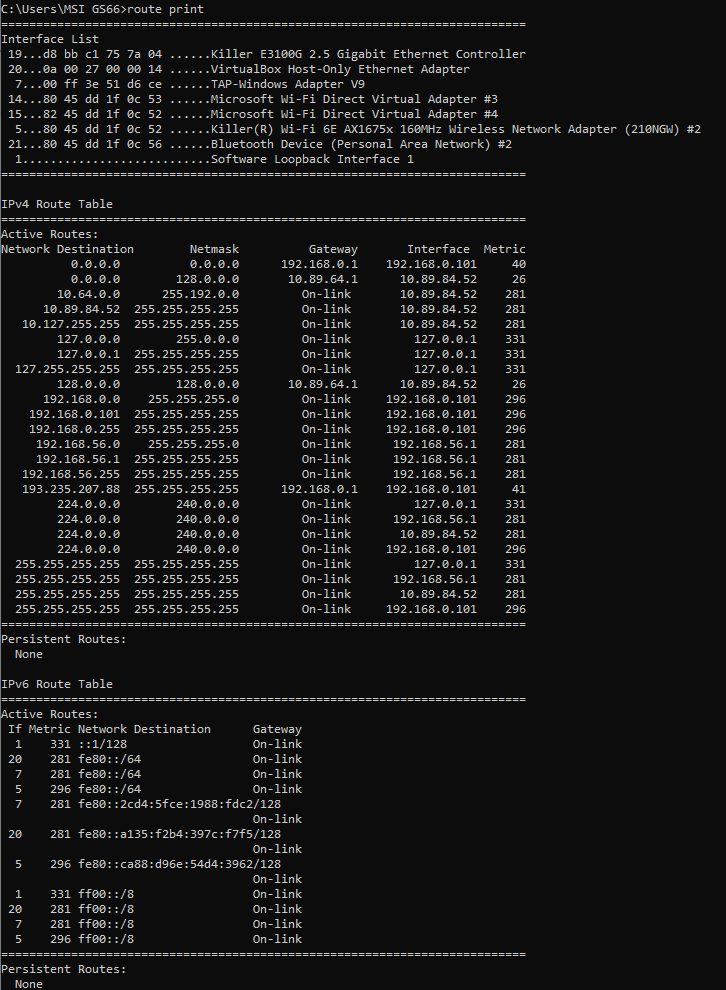


Рисунок 1.4 - Вывод команды route print

Команда netstat показывает статистику протокола и текущие соединения TCP/IP (рис. 1.5).

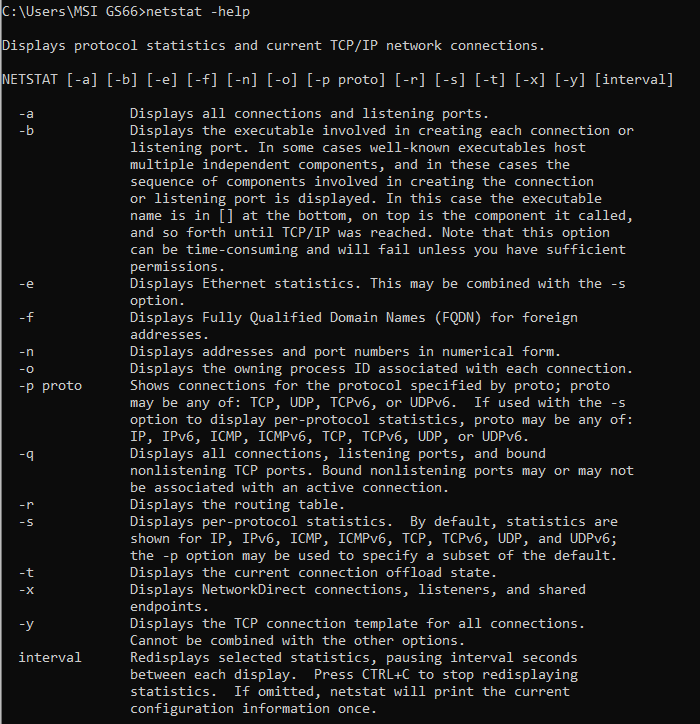


Рисунок 1.5 - Описание команды netstat

Посмотрим на порты и соединения, которые устанавливаются разными программами (рис. 1.6).

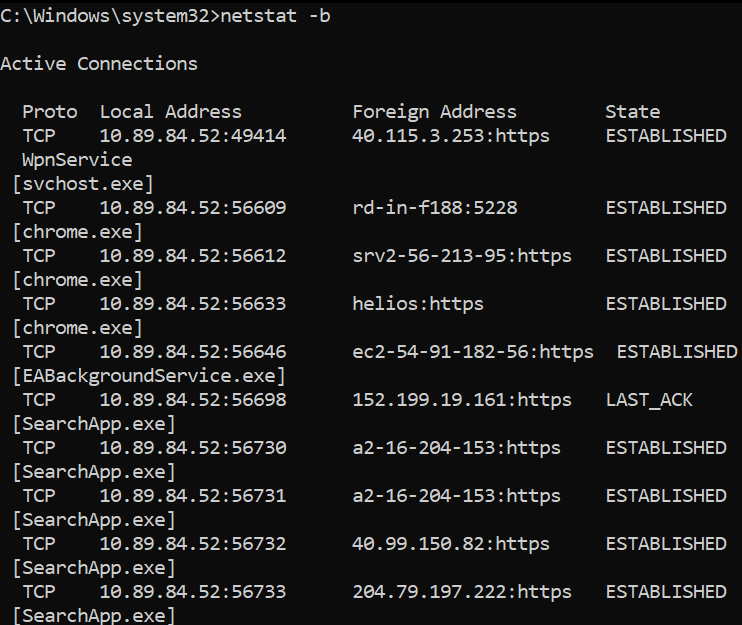


Рисунок 1.6 - Вывод команды netstat -b

Посмотрим статистику с помощью netstat -e (рис. 1.7).

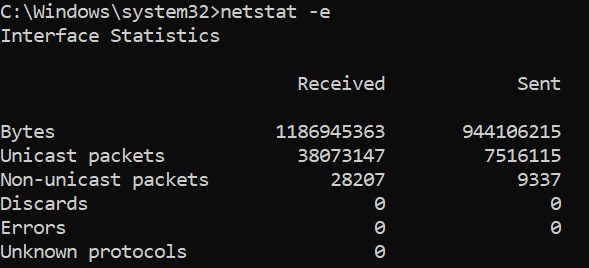


Рисунок 1.7 - Статистика с помощью netstat -e

Команда nbtstat отображает статистику протокола и текущих подключений TCP/IP с помощью NBT (NetBIOS через TCP/IP) (рис. 1.8).

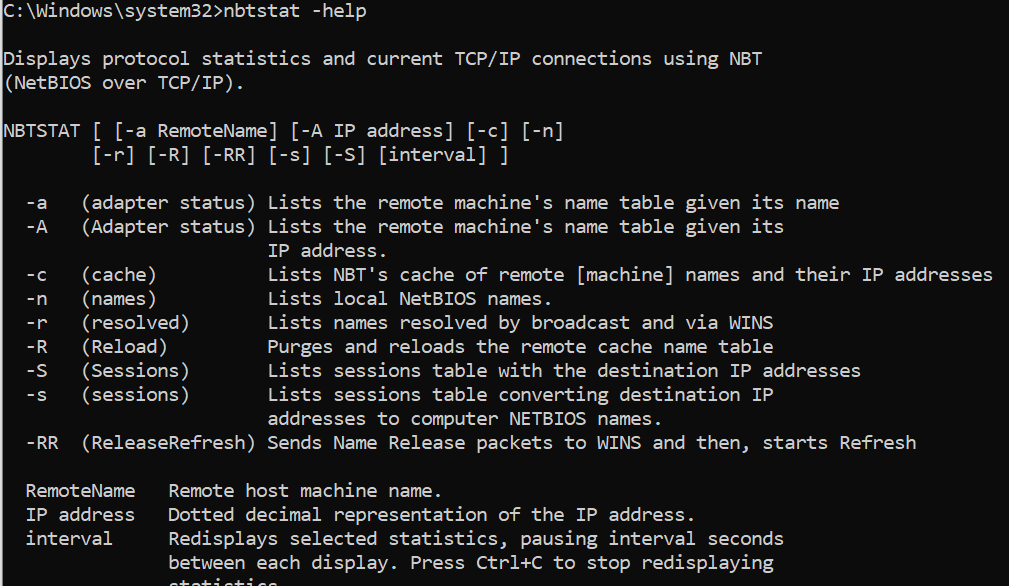


Рисунок 1.8 - Описание команды nbtstat

Эта команда также позволяет обновить кэш имен NetBIOS и имена, зарегистрированные в службе имен Windows (WINS).

Чтобы отобразить таблицу имен NetBIOS локального компьютера, используем nbtstat /n (рис. 1.9). Чтобы отобразить содержимое кэша имен NetBIOS локального компьютера, используем nbtstat /c (рис. 1.10).

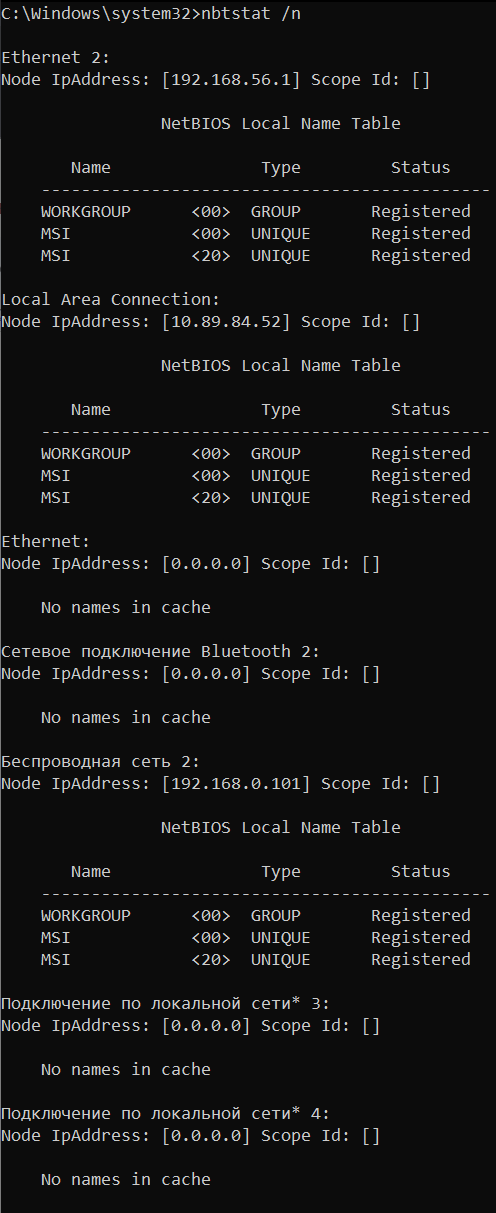


Рисунок 1.9 - Таблица имен NetBIOS локального компьютера

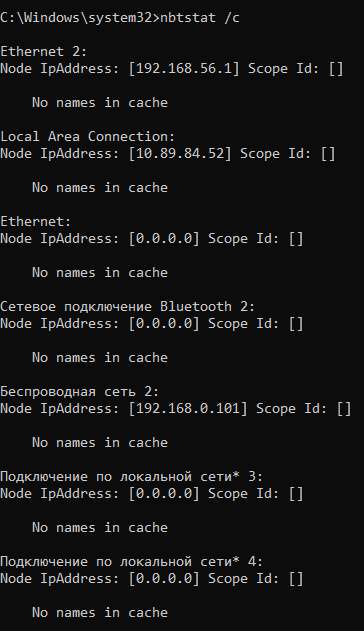


Рисунок 1.10 - Содержимое кэша имен NetBIOS локального компьютера

Команда ipconfig осуществляет вывод деталей текущего соединения и управления клиентскими сервисами DHCP и DNS (рис. 1.11).

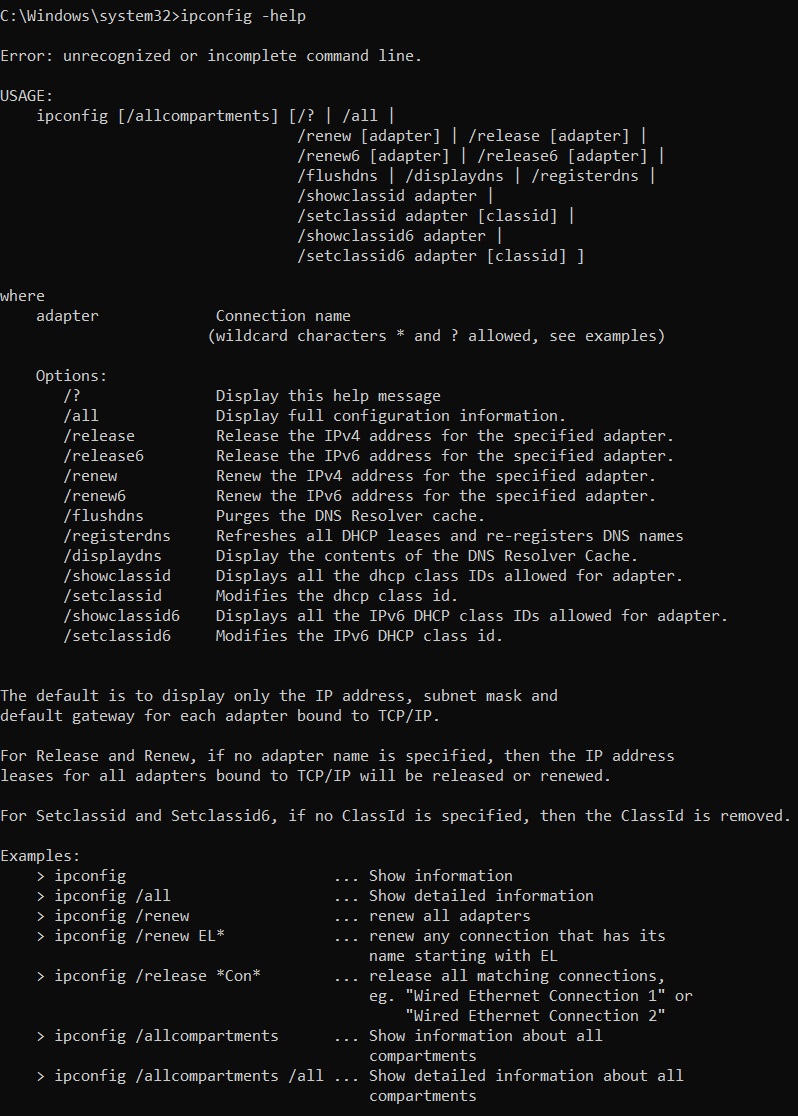


Рисунок 1.11 - Описание команды ipconfig

Выполним команду ipconfig и посмотрим на вывод (рис. 1.12).

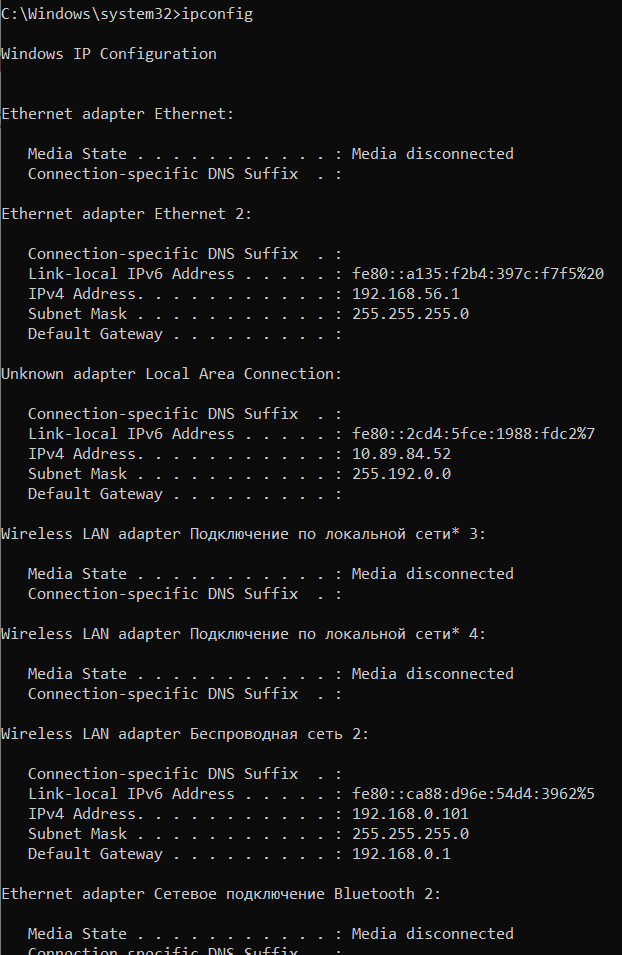


Рисунок 1.12 - Вывод команды ipconfig

Команда net позволяет управлять сетевой конфигурацией (рис. 1.13).

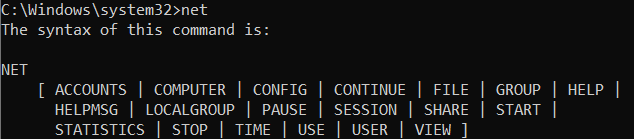


Рисунок 1.13 - Описание синтаксиса команды net

Команда NET CONFIG отображает информацию о настройке служб рабочей станции или службы сервера (рис. 1.14).

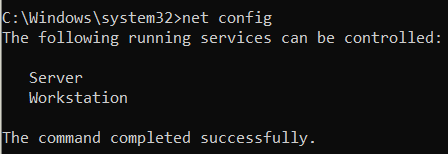


Рисунок 1.14 - Результат команды net config

# НАСТРОЙКА СЕТЕВЫХ ИНТЕРФЕЙСОВ. КОНФИГУРАЦИЯ БРАНДМАУЭРА

Проверим настройки сети виртуальных машин, установим у адаптера 1 тип подключения - внутренняя сеть (рис. 2.1).

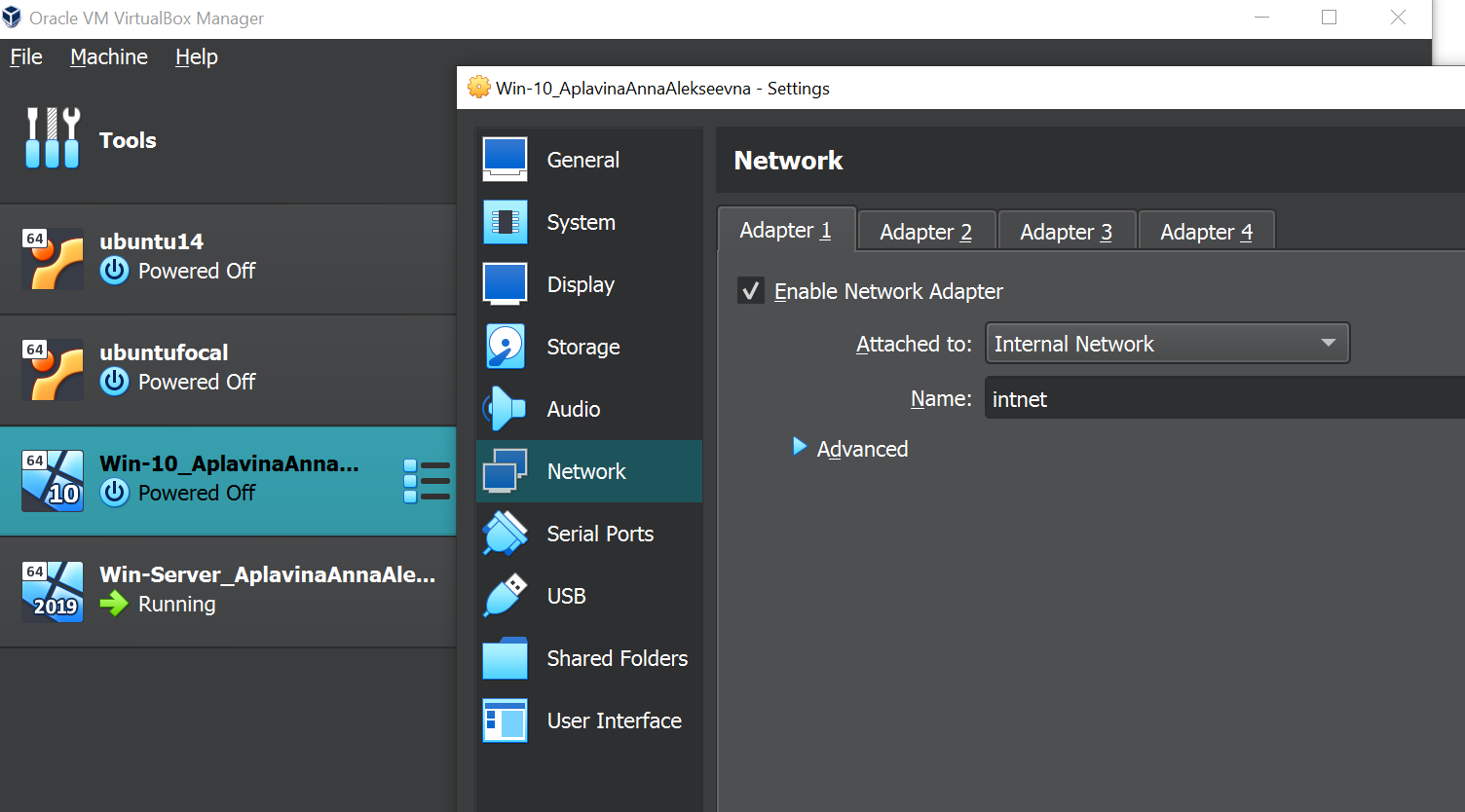


Рисунок 2.1 - Выбор типа подключения внутренняя сеть

Настроим сетевой интерфейс рабочей станции. Ознакомимся со сведениями о сетевом подключении (рис. 2.2).

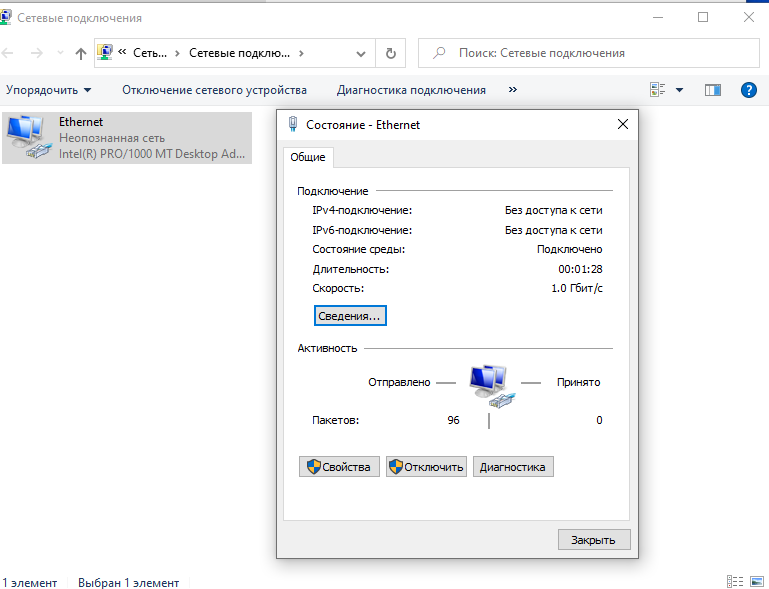


Рисунок 2.2 - Сведения и сетевом подключении

Данную информацию также можно получить из командной строки с помощью команды ipconfig.

Перейдем в раздел свойства и отключим IP версии 6 (рис. 2.3).

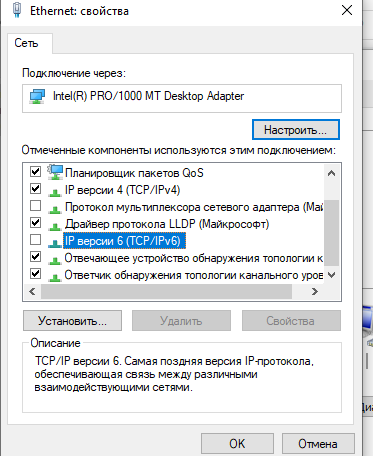


Рисунок 2.3 - Отключение TCP/IPv6

Перейдем в свойства IP версии 4 и установим значения (рис. 2.4).

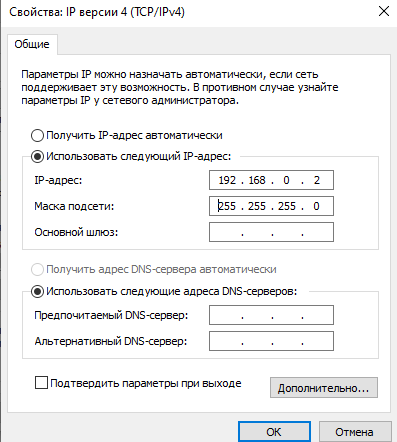


Рисунок 2.4 - Свойства IP версии 4

Аналогичным образом настраиваем сервер (ip - 192.168.0.1, маска - 255.255.255.0).

Запустим командную строку на рабочей станции и на сервере. С помощью программы Ping проверим сетевые подключения на рабочей станции (рис. 2.6) и на сервере (рис. 2.7). Но для начала разрешим получение ICMP пакетов в настройках брандмауэра для сервера и рабочей станции (рис. 2.5).

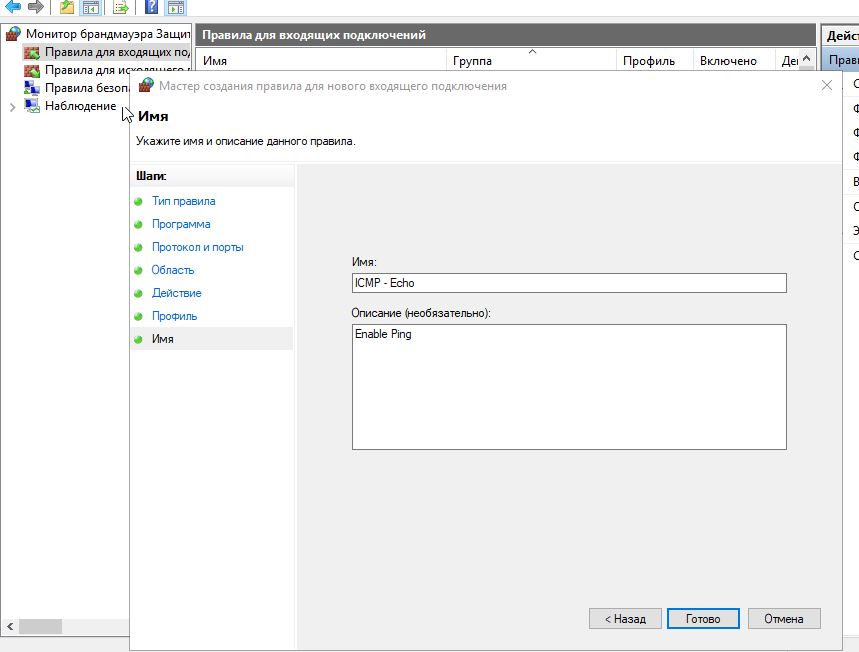


Рисунок 2.5 - Добавление правила для разрешения ICMP

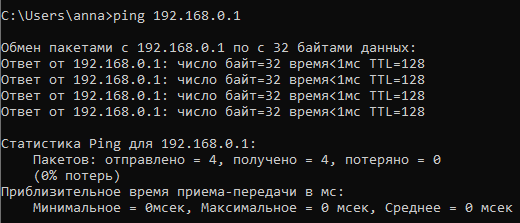
****

Рисунок 2.6 - Ping с рабочей станции на сервер

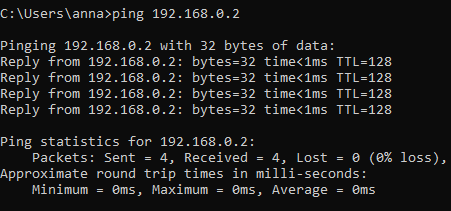


Рисунок 2.7 - Ping с сервера на рабочую станцию

На рабочей станции запустим Безопасность Windows и перейдем в раздел Брандмауэр и безопасность сети (рис. 2.8).

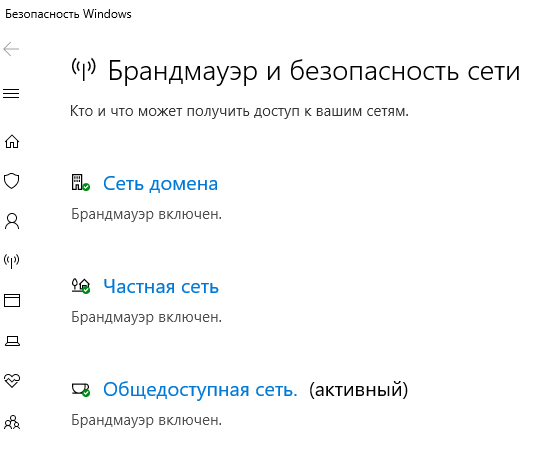


Рисунок 2.8 - Брандмауэр и безопасность сети

Сеть домена - это тип сети, в которой компьютеры объединены в домен, управляемый централизованно, обычно с помощью службы доменных контроллеров (например, Active Directory). Компьютеры в сети домена имеют доступ к общим ресурсам и могут управляться администраторами домена.

Частная сеть - это тип сети, в которой компьютеры подключены к локальной сети с ограниченным доступом. Компьютеры в частной сети могут обмениваться данными и ресурсами внутри сети, но доступ извне может быть ограничен, обычно с помощью маршрутизации или настроек брандмауэра.

В общедоступных сетях компьютеры могут быть доступны извне и подвержены различным угрозам безопасности, поэтому необходимы дополнительные меры защиты, такие как брандмауэры.

Если на рабочей станции отключить правило, разрешающее получать ICMP пакеты, и при этом оставить общедоступную сеть включенной в настройках брандмауэра, то с сервера на рабочую станцию нельзя достучаться с помощью ping (рис. 2.9).

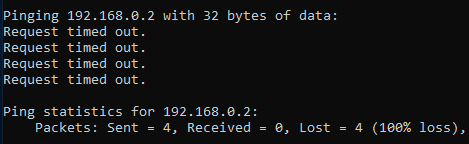


Рисунок 2.9 - Попытка сделать ping на рабочую станцию с сервера

Если отключить общедоступную сеть (рис. 2.10), то соединение снова заработает (рис. 2.11).

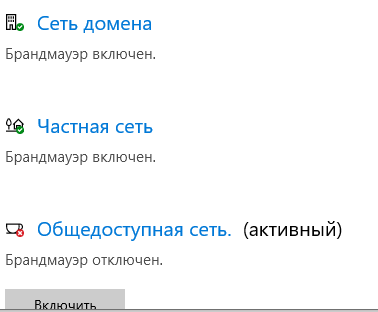


Рисунок 2.10 - Отключение общедоступной сети в брандмауэре

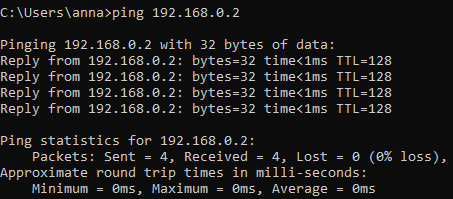


Рисунок 2.11 - Соединение с рабочей станцией через ping восстановлено

Перейдем в дополнительные параметры, группу правила для входящих сообщений и включим правило Общий доступ к файлам и принтерам (эхо-запрос- входящий трафик ICMPv4) (рис. 2.12).

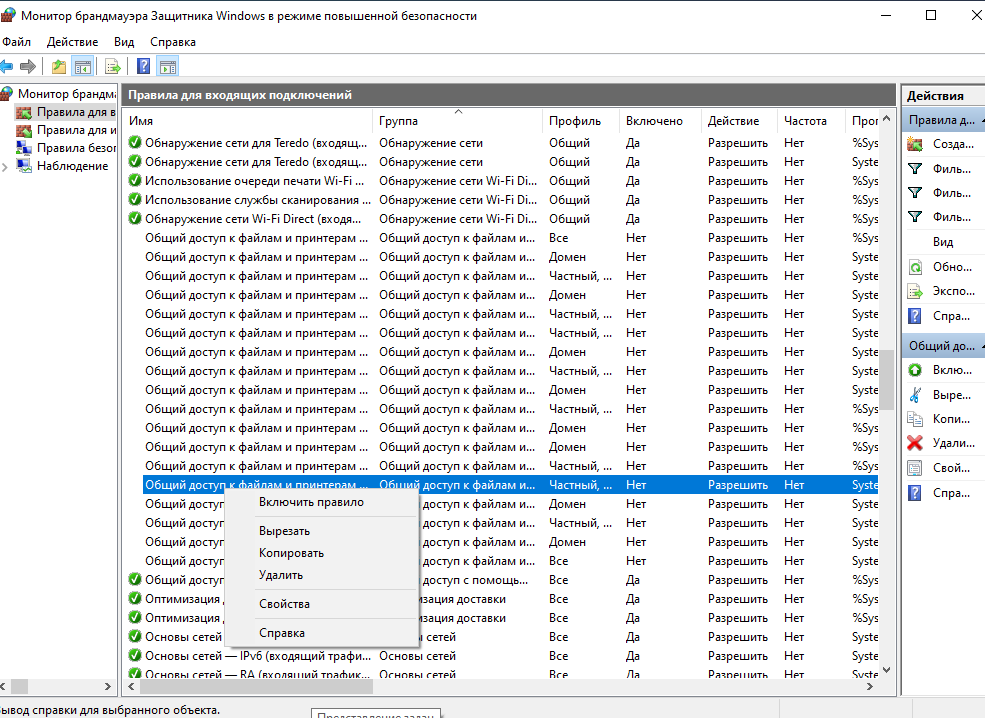


Рисунок 2.12 - Включение правила Общий доступ к файлам и принтерам (эхо-запрос- входящий трафик ICMPv4)

Проверим соединение - соединение снова работает (рис. 2.13).

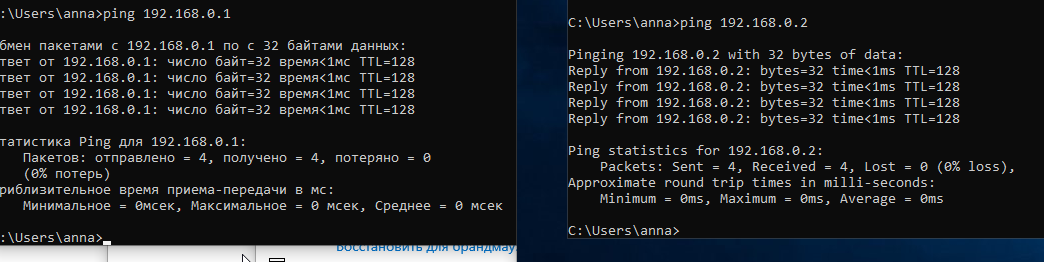


Рисунок 2.13 - Соединение снова работает

Создадим несколько IP адресов (алиасов) на одном сетевом интерфейсе. На рабочей станции откроем Свойства IP версии 4. Перейдем по кнопке Дополнительно в раздел Параметры IP (рис. 2.14).

Добавим IP-адреса:

* IP-адрес 192.168.0.12
* Маска 255.255.255.0

* IP-адрес 192.168.0.222
* Маска 255.255.255.0

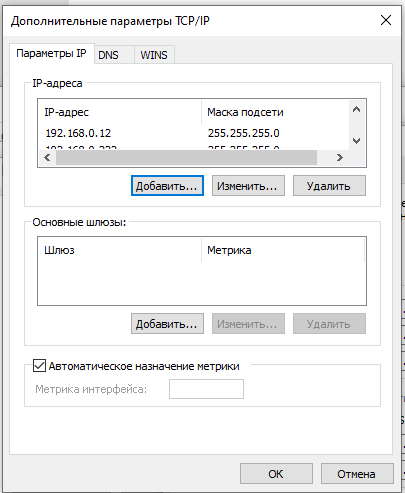


Рисунок 2.14 - Добавление IP адресов на рабочей станции

Проверим ping с сервера на эти IP (рис. 2.15).

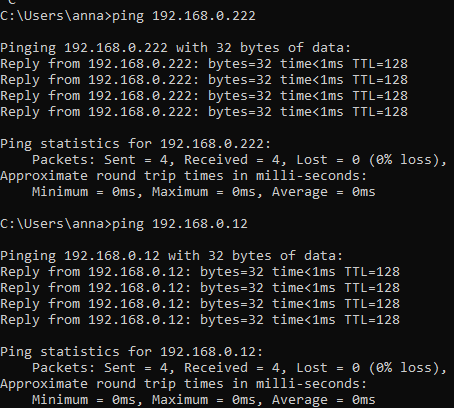


Рисунок 2.15 - Проверка новых IP

Настроим DHCP-сервер. На рабочей станции откроем Свойства IP версии 4. Установим следующие значения: Получить IP-адрес автоматически, Получить адрес DNS-сервера автоматически (рис. 2.16).

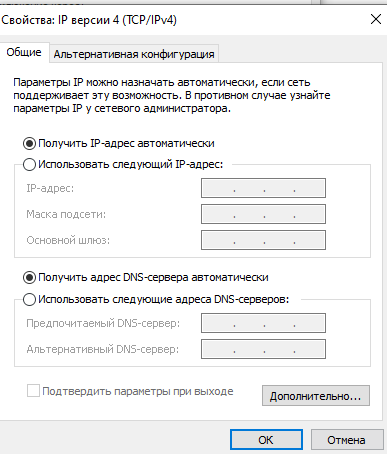


Рисунок 2.16 - Свойства IP версии 4, автоматическое получение IP и адреса DNS-сервера

На сервере запустим Диспетчер серверов, выберем Добавить роли или компоненты в мастере настроек сервера выберите Установка ролей и компонентов, выберем сервер из пула серверов. Выберем DHCP – сервер. При выборе требуется добавить компоненты сервера (рис. 2.17).

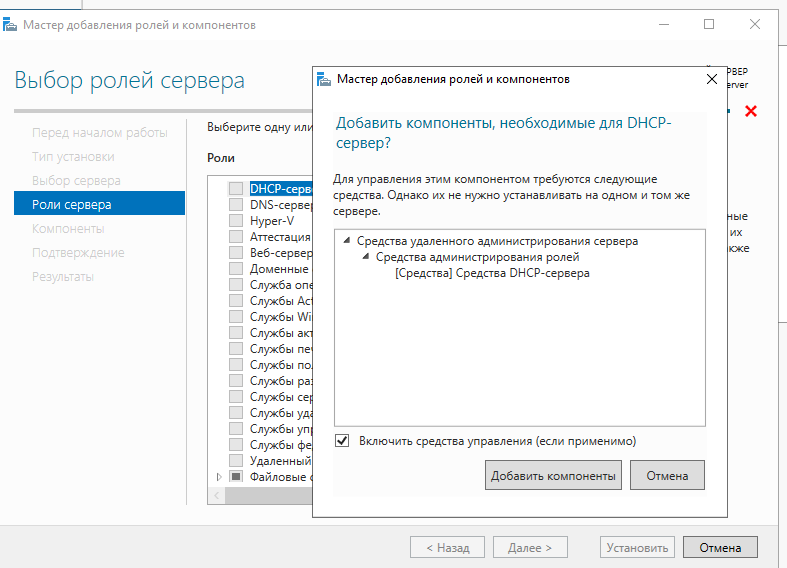


Рисунок 2.17 - Необходимо добавить компоненты сервера

Оставим компоненты по умолчанию и нажмем далее, установим сервер (рис. 2.18).

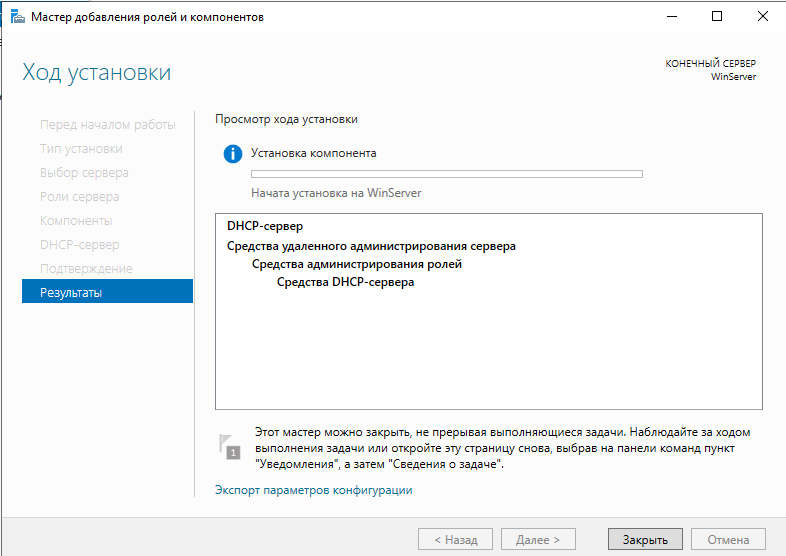


Рисунок 2.18 - Установка DHCP сервера

После окончания установки добавилась новая роль – DHCP нажмем на нее и перейдем в Диспетчер серверов – DHCP (рис. 2.19).

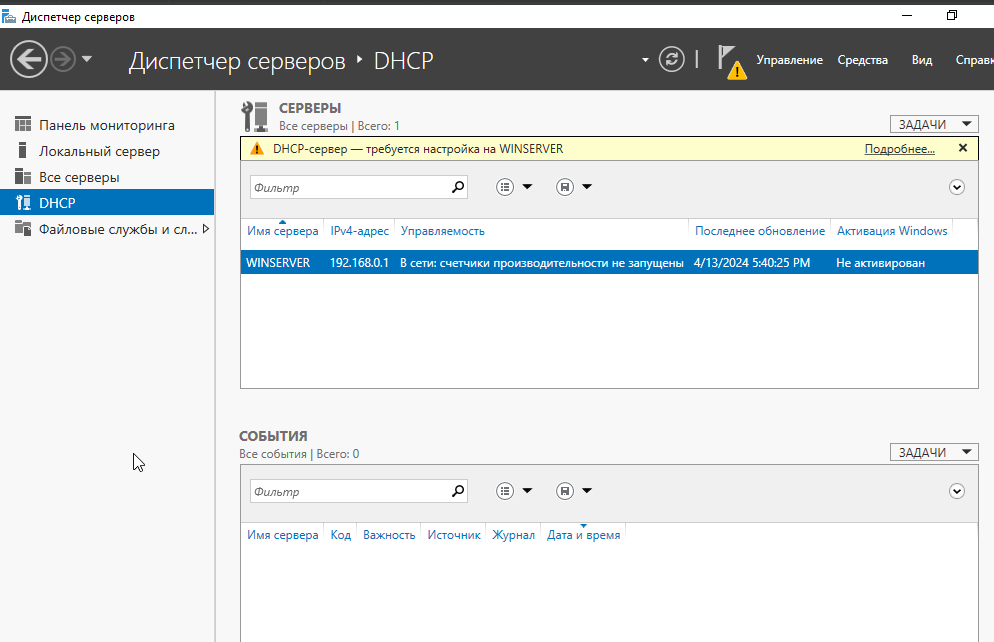


Рисунок 2.19 - Диспетчер серверов, DHCP

Откроем диспетчер DHCP (рис. 2.20). Правой кнопкой мыши на название сервера и выбрать Диспетчер DHCP.

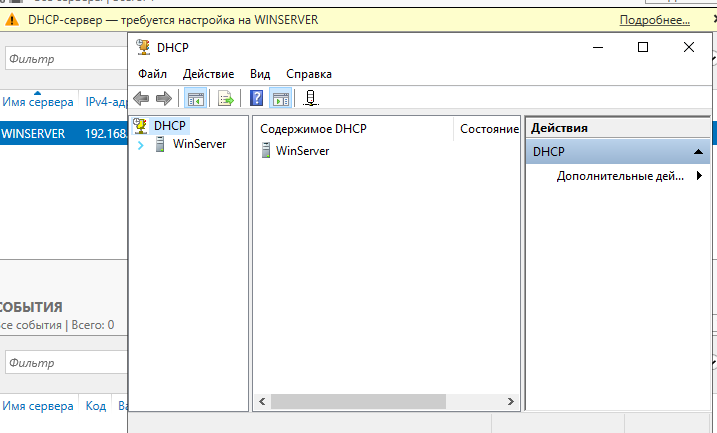


Рисунок 2.20 - Диспетчер DHCP

Создадим область адресов. Нажмем правой кнопкой мыши на IPv4, Создать область… (рис. 2.21).

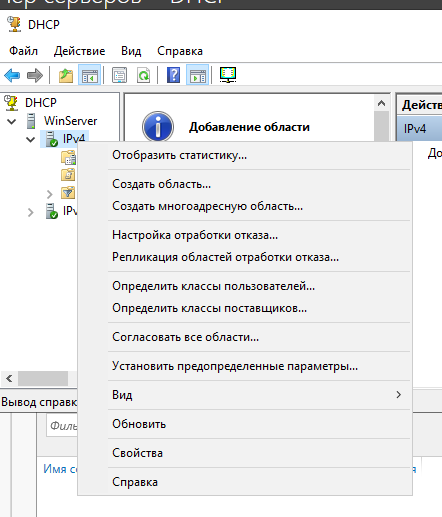


Рисунок 2.21 - Переход к созданию области

Открылся мастер создания области. Зададим имя области Рабочие станции и диапазон адресов (рис. 2.22).

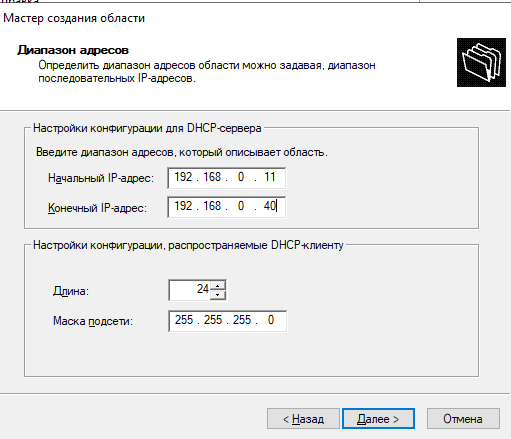


Рисунок 2.22 - Задание диапазона адресов

Исключения IP адресов из диапазона добавлять не будем. Зададим срок действия аренды адреса (рис. 2.23).

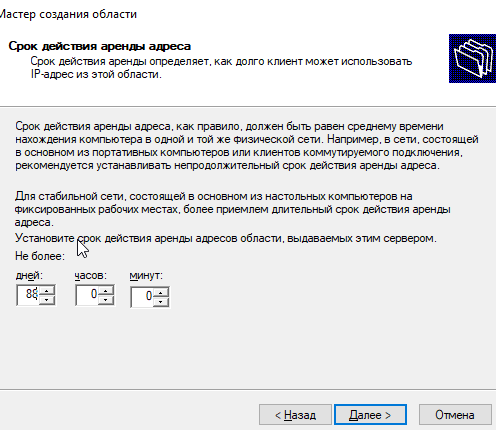


Рисунок 2.23 - Задание срока действия аренды адреса

Откажемся от предложения мастера настроить общие параметры сервера DHCP. Активируем созданную область (рис. 2.24).

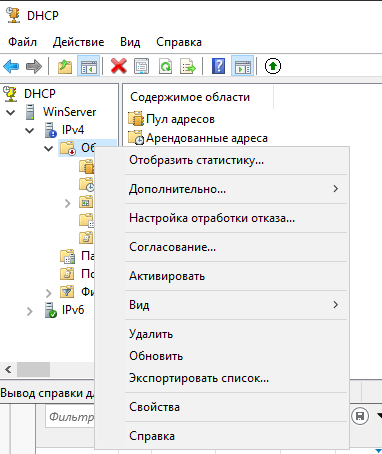


Рисунок 2.24 - Активация области

Проверим установлена ли привязка сервера DHCP только к внутреннему интерфейсу 192.168.0.1. Для этого вызовем через контекстное меню сервера IPv4 окно Свойства. На закладке Дополнительно нажмем на кнопку Привязки. Необходимо, чтобы флажок был установлен только напротив сетевого адреса внутреннего интерфейса (рис. 2.25).

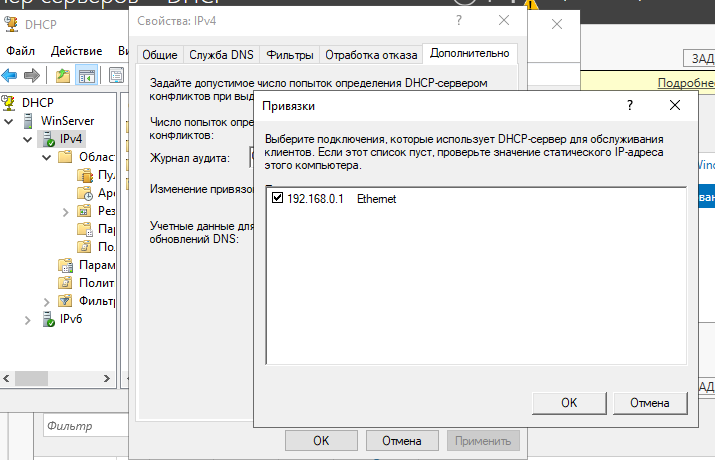


Рисунок 2.25 - Проверка привязки сервера DHCP

Проверим подключение к серверу с рабочей станции (рис. 2.26).

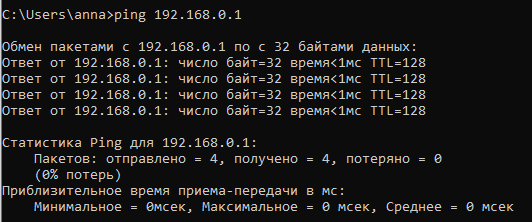


Рисунок 2.26 - Проверка соединения с сервером после настройки DHCP сервера

На сервере в Области – Рабочие станции перейдем в раздел Арендованные адреса, проверим список арендованных адресов (рис. 2.27).

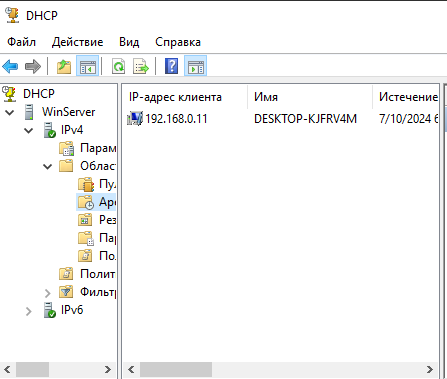


Рисунок 2.27 - Проверка списка арендованных адресов

Запретим выдавать клиентам IP-адреса 192.168.0.11, … , 192.168.0.30. Для этого на сервере выберем в контекстном меню папки Пул адресов пункт Диапазон исключения … и укажем соответствующий диапазон. Нажмем кнопку Добавить, а затем Закрыть (рис. 2.28).

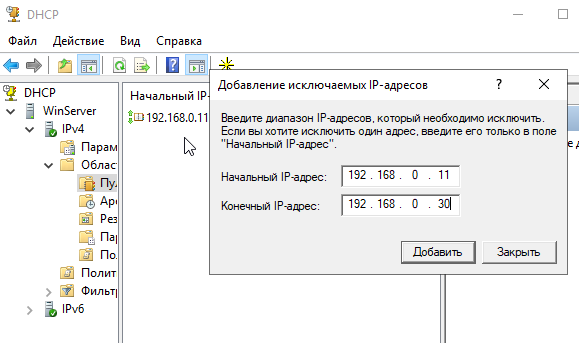


Рисунок 2.28 - Задание диапазона исключений

На рабочей станции переподключимся к локальной сети. Обновить сетевой адрес позволяет команда ipconfig /renew. Проверим получила рабочая станция (рис. 2.29).

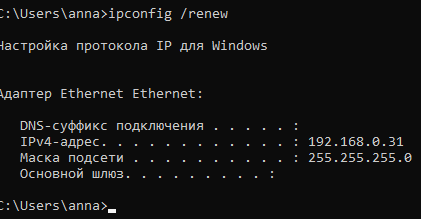


Рисунок 2.29 - Новый адрес с помощью ipconfig /renew

Удалим диапазон исключений, из папки Арендованных адресов удалим адрес рабочей станции. Узнаем MAC сетевой карты рабочей станции с помощью ipconfig /all (рис. 2.30).

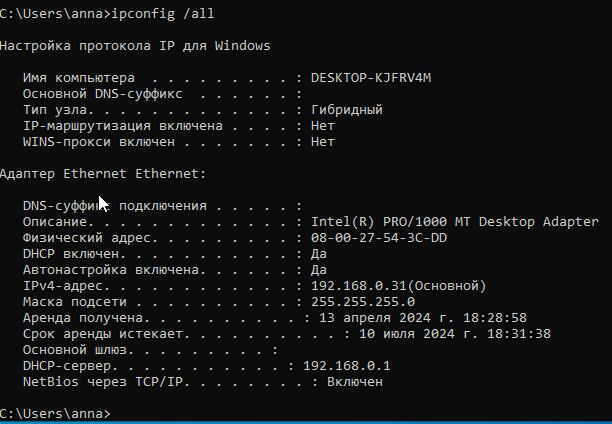


Рисунок 2.30 - Проверка MAC-адреса на рабочей станции

MAC-адрес - 08-00-27-54-3C-DD. Зарезервируем для рабочей станции IP-адрес 192.168.0.15 (рис. 2.31).

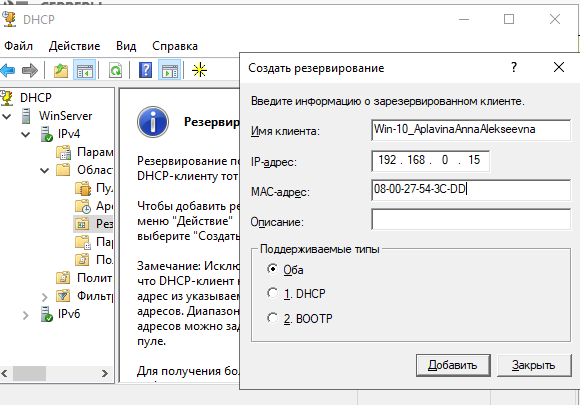


Рисунок 2.31 - Создание резервирования для рабочей станции

Теперь рабочая станция получила зарезервированный адрес (рис. 2.32).

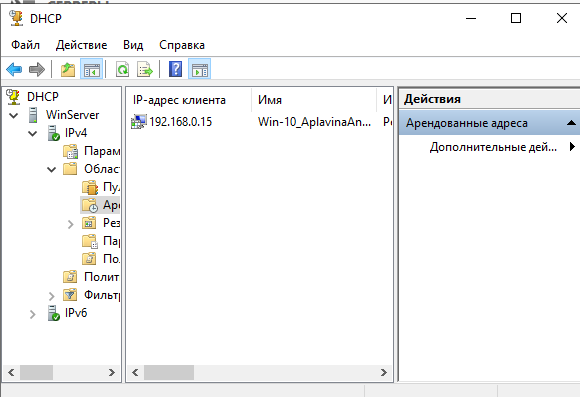


Рисунок 2.32 - Зарезервированный адрес у рабочей станции

Настроим маршрутизацию и обеспечим подключение к сети интернет.

На сервере в настройках виртуальной машины включим сетевой адаптер и установим тип подключения Сетевой мост (рис 2.33).

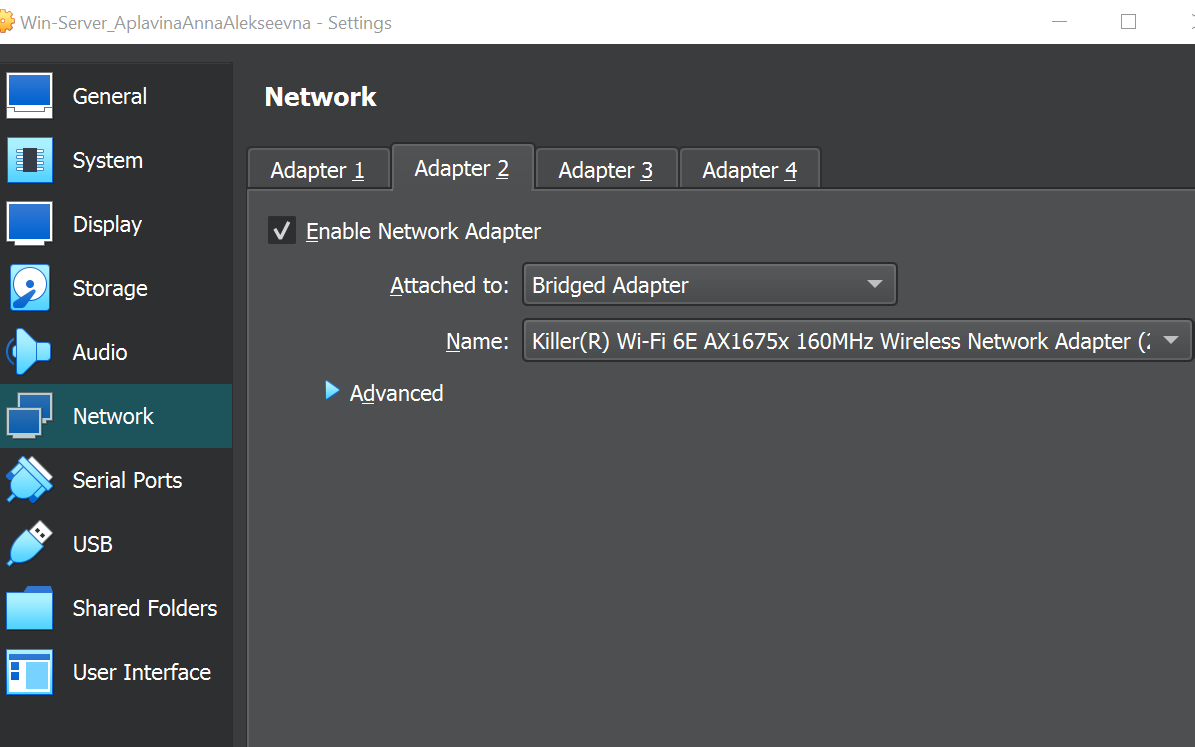


Рисунок 2.33 - Добавление серверу адаптера с типом подключения Сетевой мост

Снова запустим сервер и рабочую станцию. На сервере в настройках параметров адаптеров переименуем сетевые интерфейсы. Интерфейс с адресом 192.168.0.1 – Локальный, другой – Внешний (рис. 2.34).

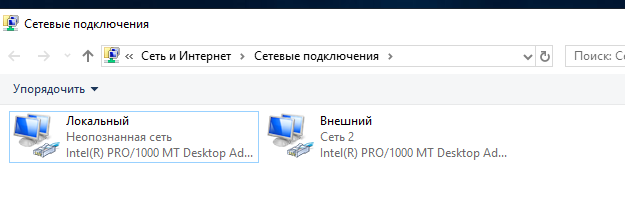


Рисунок 2.34 - Переименованные сетевые интерфейсы

В диспетчере DHCP проверим привязку только к локальному интерфейсу (рис. 2.35).

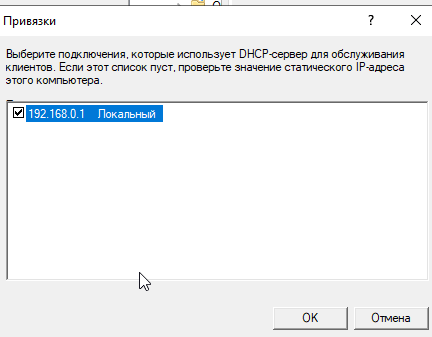


Рисунок 2.35 - Проверка привязки только к локальному интерфейсу

В мастере настроек сервера выберем Установка ролей и компонентов. Выберем сервер из пула серверов. Выберем Удаленный доступ. При выборе требуется добавить компоненты сервера. Компоненты оставляем по умолчанию. В Службе ролей выбираем Маршрутизацию. После установки завершить работу-разрешить добавить Локальные группы безопасности, процесс установки на рис. 2.36.

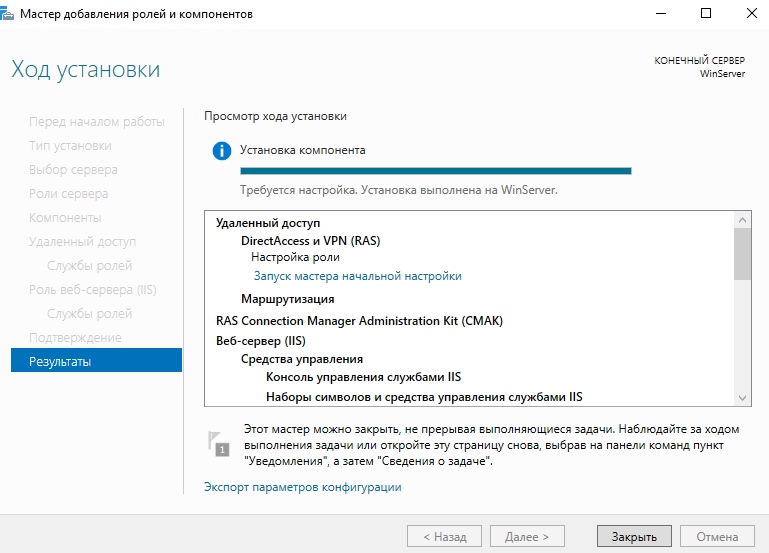


Рисунок 2.36 - Установка компонентов для удаленного доступа

Запустим Пуск - Средства администрирования - Маршрутизация и удаленный доступ (рис. 2.37).

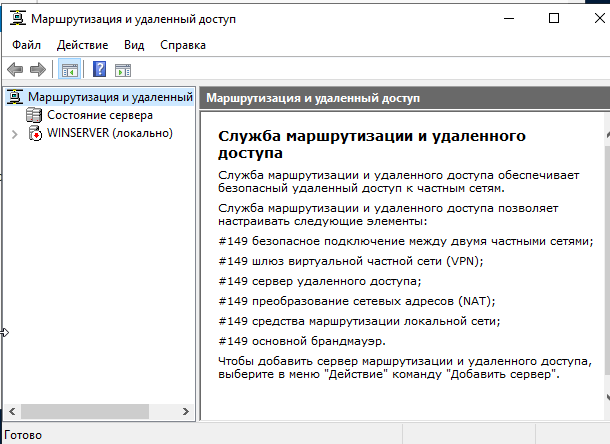


Рисунок 2.37 - Маршрутизация и удаленный доступ

Выберем пункт конфигурации Маршрутизации – Настроить и включить маршрутизацию и удаленный доступ Выберем пункт Преобразование сетевых адресов (NAT). В качестве Подключения к Интернет выберем Внешний интерфейс. Завершим работу мастера. Проверим соединение на рабочей станции с помощью программы ping IP-адрес на внешнем интерфейсе и nslookup 8.8.8.8 (рис. 2.38).

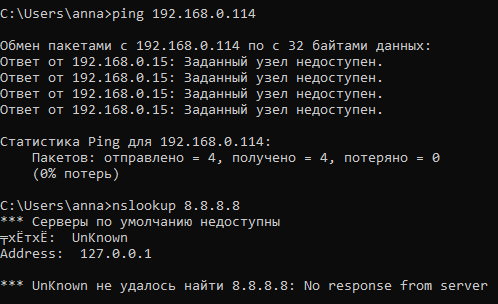


Рисунок 2.38 - Проверка доступа к интернету на рабочей станции

Ничего не работает. Необходимо настроить DNS для DHCP (рис. 2.39).

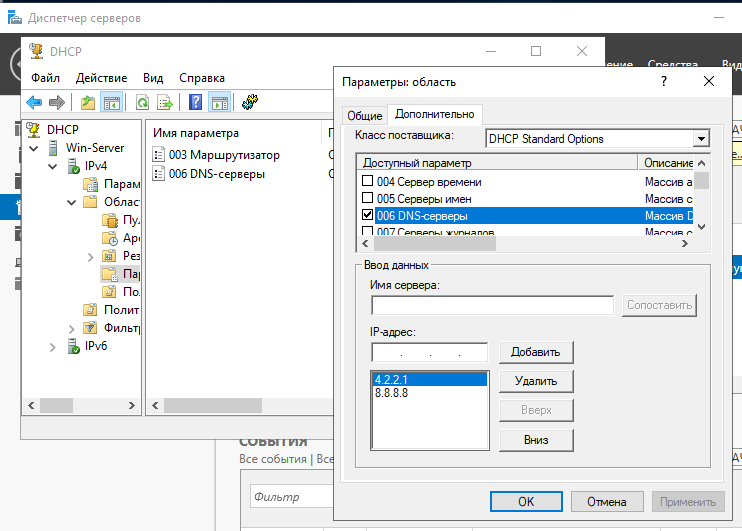


Рисунок 2.39 - Настройка DNS в диспетчере DHCP

Теперь проверим соединение к интернету на рабочей станции (рис. 2.40).

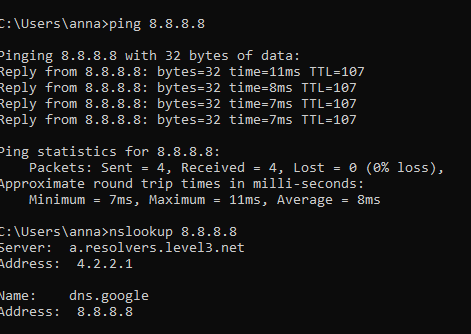


Рисунок 2.40 - Проверка подключение к интернету на рабочей станции после настройки DNS в диспетчере DHCP

Чтобы DNS работал на сервере, в настройках для интерфейса, который дает доступ в интернет также укажем DNS сервер (рис. 2.41).

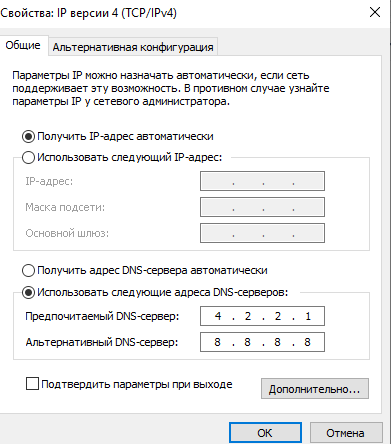


Рисунок 2.41 - Настройка DNS для интерфейса Внешний на сервере

# ЗАКЛЮЧЕНИЕ

1. Целью данной лабораторной работы было настроить рабочую станцию и сервер.
2. Был настроен DHCP и проверено автоматическое назначение IP, была настроена маршрутизация, рабочая станция была подключена к интернету.
3. Каждый этап был описан, скриншоты приведены в отчете.