**Задание 1**.Получите справку о параметрах утилиты **ipconfig.**



Рис 1.1- справка о параметрах утилиты ipconfig

**Задание 2**.Получите короткий отчет утилиты исследуйте его**.**

Короткий отчет утилиты ipconfig получается вводом в командную строку строки ‘ipconfig’. Он включает в себя IPv4- и IPv6-адреса, маску подсети и адрес основного шлюза по умолчанию для всех сетевых адаптеров.

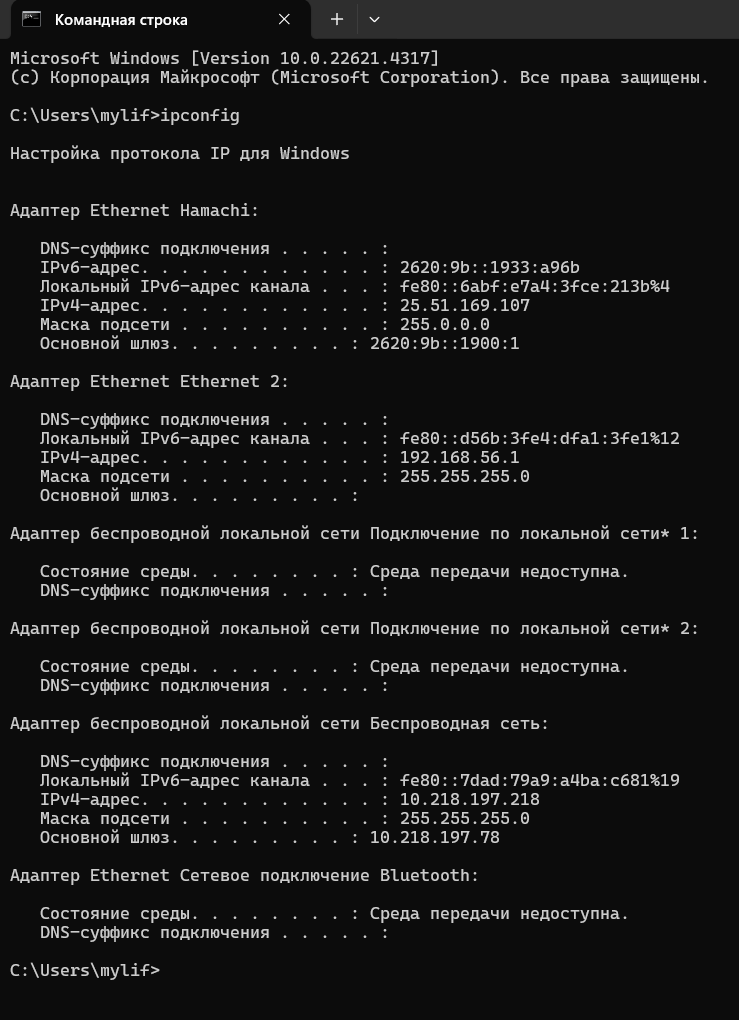


Рис 1.2- короткий отчет утилиты

**Задание 3.** Получите полный отчет утилиты**.** Выпишите символическое имя хоста, IP-адрес, маску подсети, MAC-адрес адаптера.

Полный отчет утилиты ipconfig получается вводом в командную строку строки ‘ipconfig /all’. В дополнение к основному отчету он показывает физический адрес(Mac адрес) сетевого адаптера, статус DHCP(включен/выключен), локальный IPv6-адрес канала, время аренды IPv6-адреса, описание сетевого адаптера, статус NetBios через TCP/IP и основное имя хоста и DNS-суффикс подключения.



Рис 1.3- полный отчет утилиты

Символическое имя хоста: Dasha-DTNTM6HQ

IPv4-адрес: 10.218.197.218(Основной)

Маска подсети: 255.255.255.0

Mac-адрес адаптера(физический адрес): C4-D0-E3-5C-57-B0

**Задание 4.** Определите, к какому классу адресов относится выписанный IP-адрес; вычислите максимальное количество хостов, которое может быть в подсети и укажите диапазон их адресов; определите код производителя сетевого адаптера.

IP-адрес 10.218.197.218 относится к классу А, так как начинается с 10.

Максимальное количество хостов в подсети:

Маска подсети 255.255.255.0 имеет 24 бита

n-количество битов в маске

2^(32-n) -2= 2^(32-24)-2= 254 хоста (без сетевого и broadcast).

Диапазон адресов:

And операция IP-адреса и маски: 10.218.197.0

Диапазон адресов хостов - от 10.218.197.1 до 10.218.197.254

Код производителя сетевого адаптера:

Физический адрес: C4-D0-E3-5C-57-B0

Код производителя- это первые три байта(C4-D0-E3) соответствуют производителю Intel Corporate)

**Задание 5.** Определите имя NetBIOS-имя компьютера с помощью утилиты **hostname**. Сравните его с именем полученным с помощью утилиты **ipconfig**.

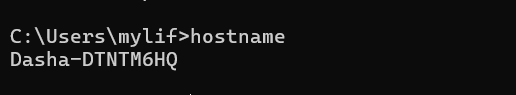


Рис 1.4- NetBios-имя компьютера

Имена, полученные с помощью двух разных утилит совпадают, что означает, что система использует одно и то же имя для NetBIOS и для сетевых конфигураций

**Задание 6.** Получите справку о параметрах утилиты **ping.**

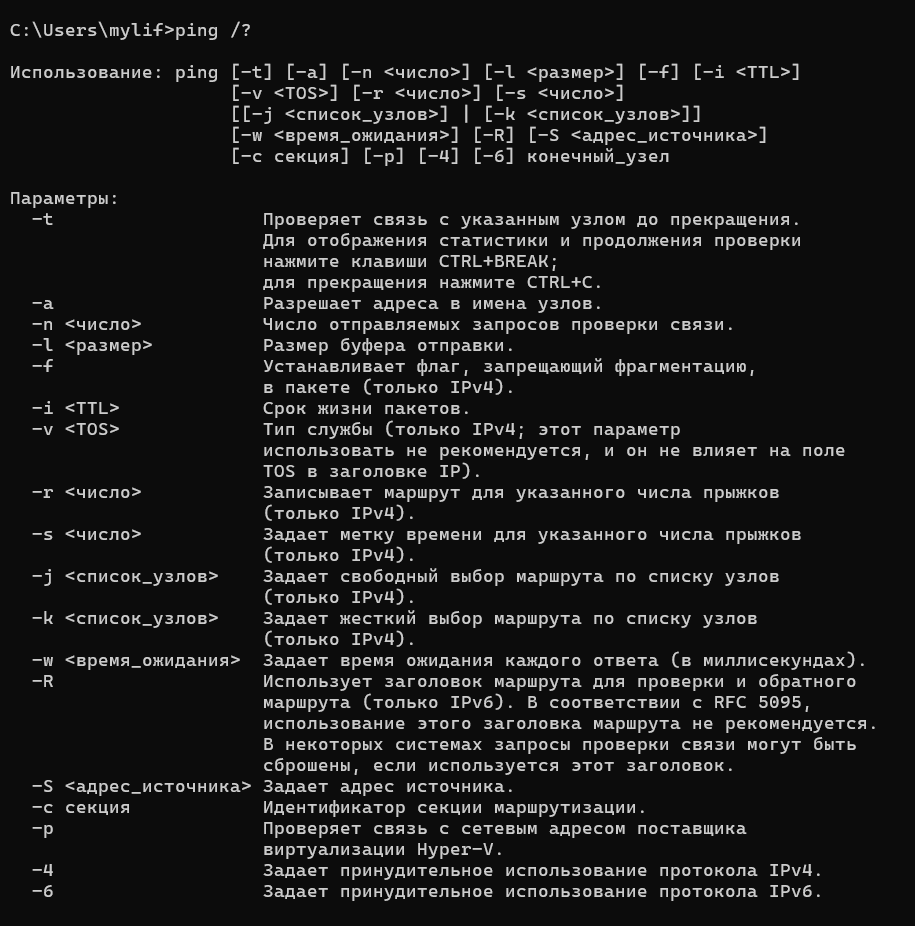


Рис 1.5- Параметры утилиты ping

Утилита ping- это удобный инструмент для проверки связи с другими устройствами в сети. Они могут помочь в определении задержек и стабильности сетевого соединения.

**Задание 7.** С помощью **ping** проверьте работоспособность интерфейса внутренней петли компьютера.

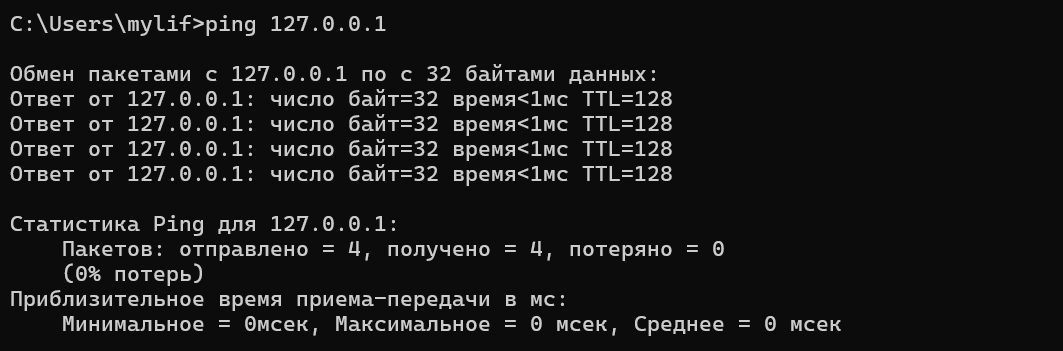


Рис 1.6- Pаботоспособность интерфейса внутренней петли компьютера.

Loopback-адрес- это специальный IP-адрес, который всегда указывает на собственный компьютер. Он используется для тестирования сетевого программного обеспечения без реальной отправки пакетов в сеть. Все пакеты, отправленные на этот адрес, возвращаются обратно на тот же компьютер.

Обмен пакетами прошел успешно, что означает, что сетевой стек TCP/IP работает корректно

**Задание 8.** С помощью утилиты **ping** проверьте доступность интерфейса какого-нибудь компьютера в локальной сети, указав в качестве параметров его IP-адрес.

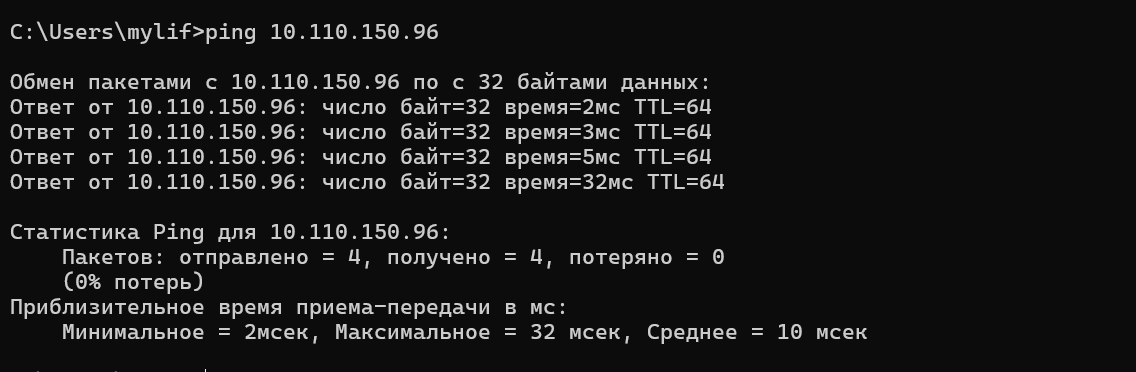


Рис 1.7- Доступность устройства в локальной сети

После ввода команды устройства успешно обменялись пакетами. Это означает, что второе устройство, чей IP-адрес указан, доступно в локальной сети.

**Задание 9.** С помощью утилиты **ping**  проверьте доступность интерфейса какого-нибудь компьютера в локальной сети, указав в качестве параметров символическое имя хоста.

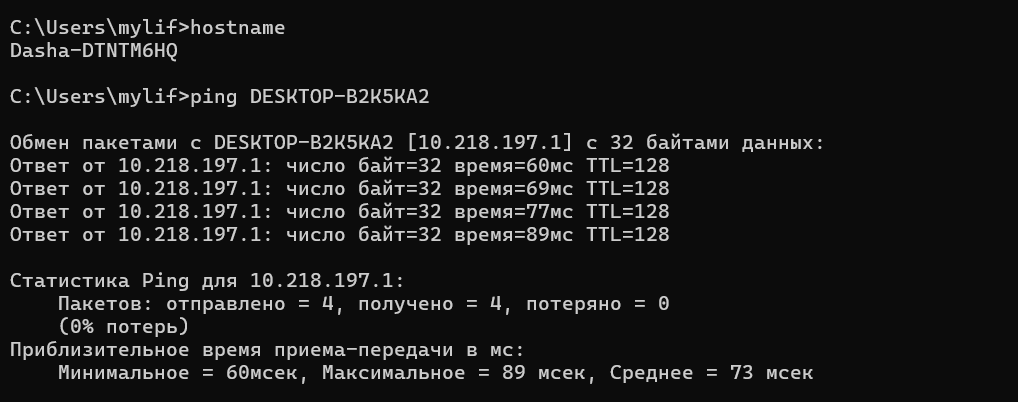


Рис 1.8- Доступность интерфейса компьютера в локальной сети

**Задание 10.** С помощью утилиты **ping** проверьте доступность интерфейса какого-нибудь компьютера в локальной сети, указав в качестве параметров символическое имя хоста и увеличив размер буфера отправки до 1000 байт

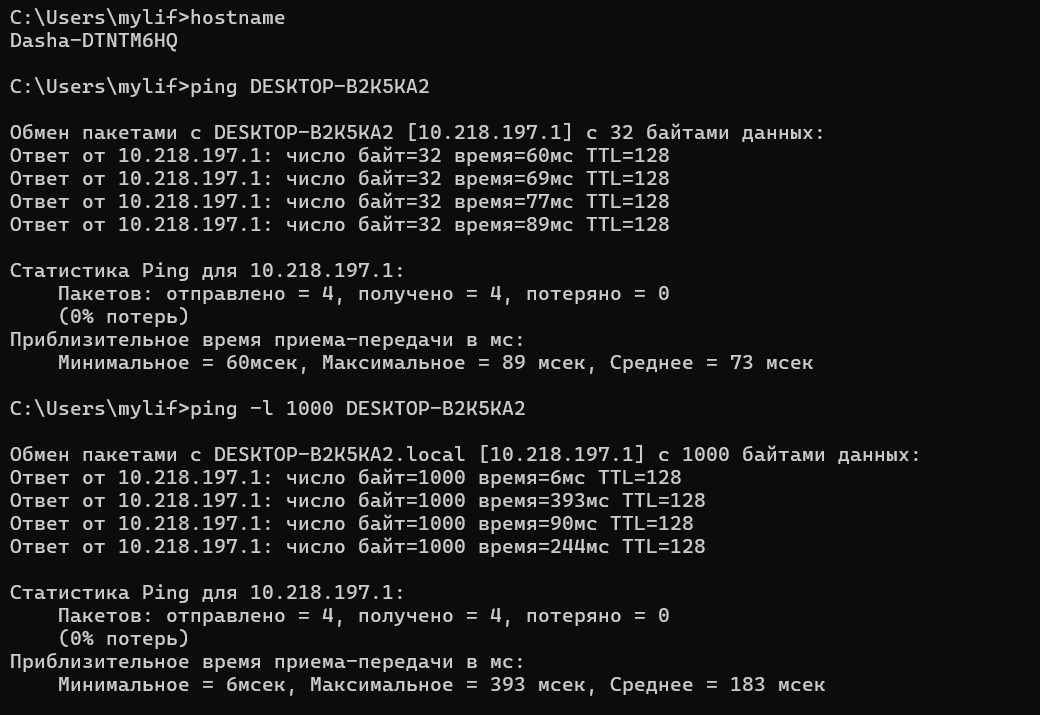


Рис 1.9- Доступность интерфейса компьютера в локальной сети

**Задание 11.** С помощью утилиты **ping** проверьте доступность интерфейса какого-нибудь компьютера в локальной сети, указав в качестве параметров его IP-адрес и установив количество отправляемых запросов равное 17.

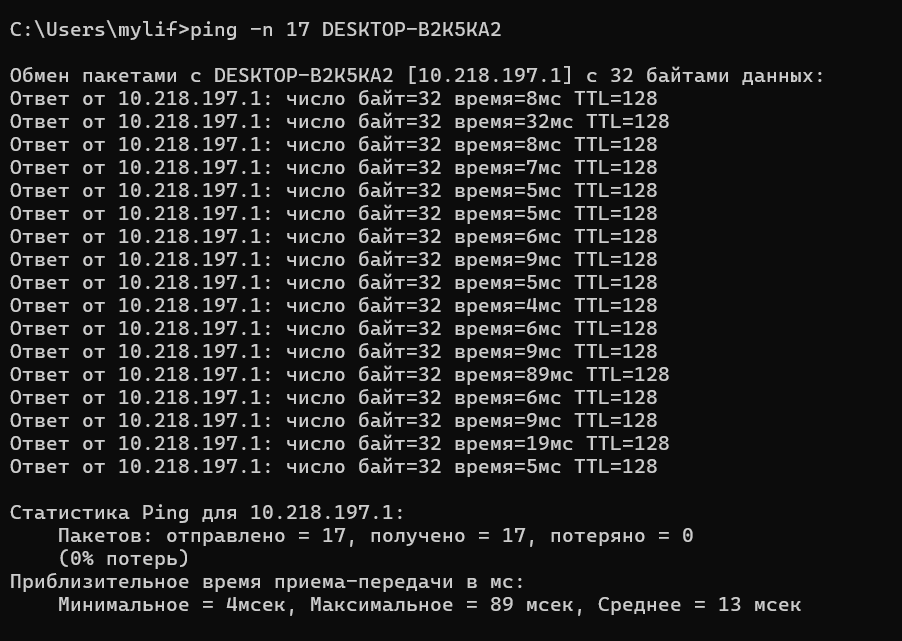


Рис 1.9- Доступность интерфейса компьютера в локальной сети

**Задание 12.** Получите справку о параметрах утилиты **tracert**.

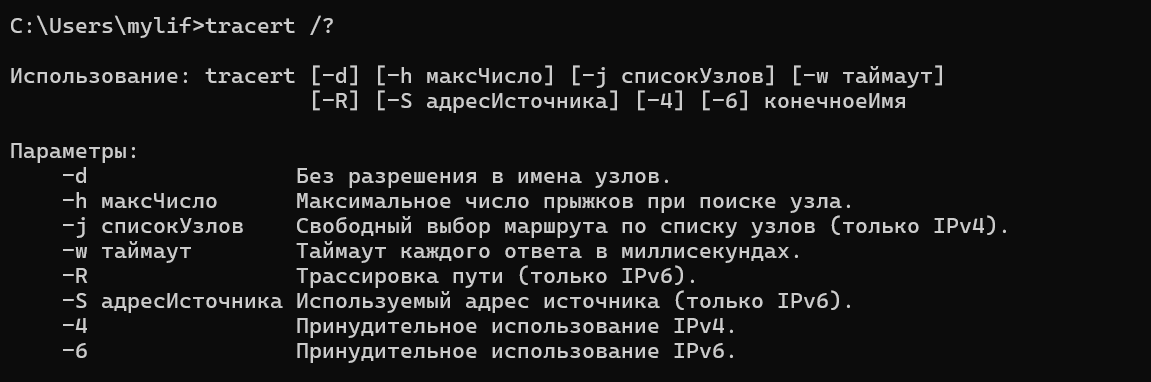


Рис 1.10- Параметры утилиты tracert

Утилита tracert помогает просмотреть весь путь от компьютера то сервера

**Задание 13.** С помощью утилиты **tracert** определите маршрут хоста самого к себе (интерфейс внутренней петли).

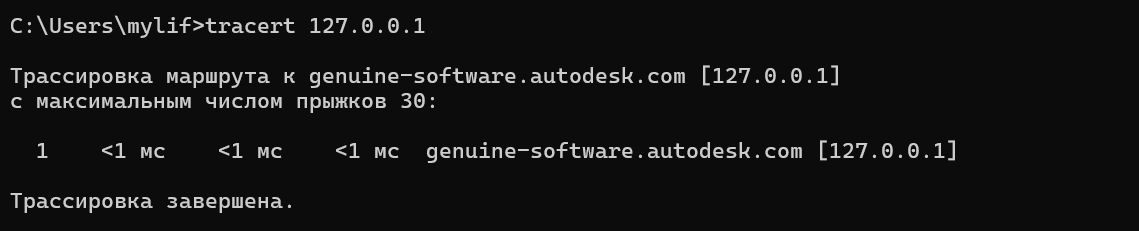


Рис 1.11- Mаршрут хоста самого к себе

Все пакеты доставлены успешно, время отклика менее 1 мс, только один прыжок-пакеты не выходят за пределы компьютера

**Задание 14.** С помощью утилиты **tracert** определите маршрут к хосту в локальной сети. Определите количество прыжков в полученном маршруте.

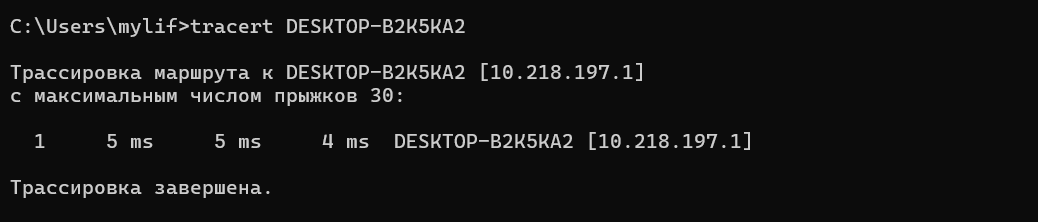


Рис 1.12- Маршрут к хосту в локальной сети

Количество прыжков- 1.

**Задание 15.** Получите справку о параметрах утилиты **route**.

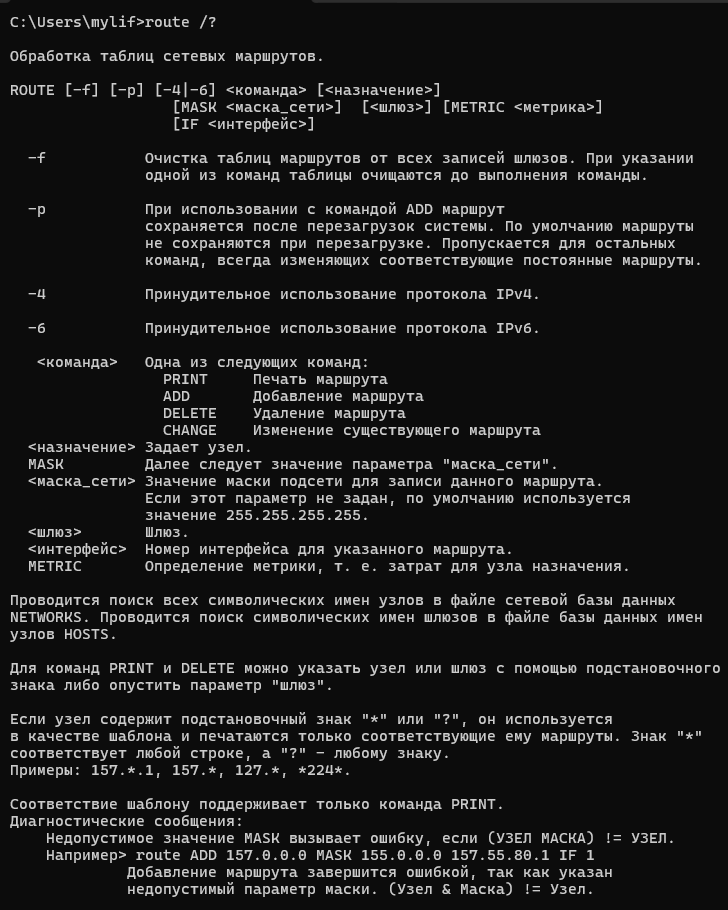
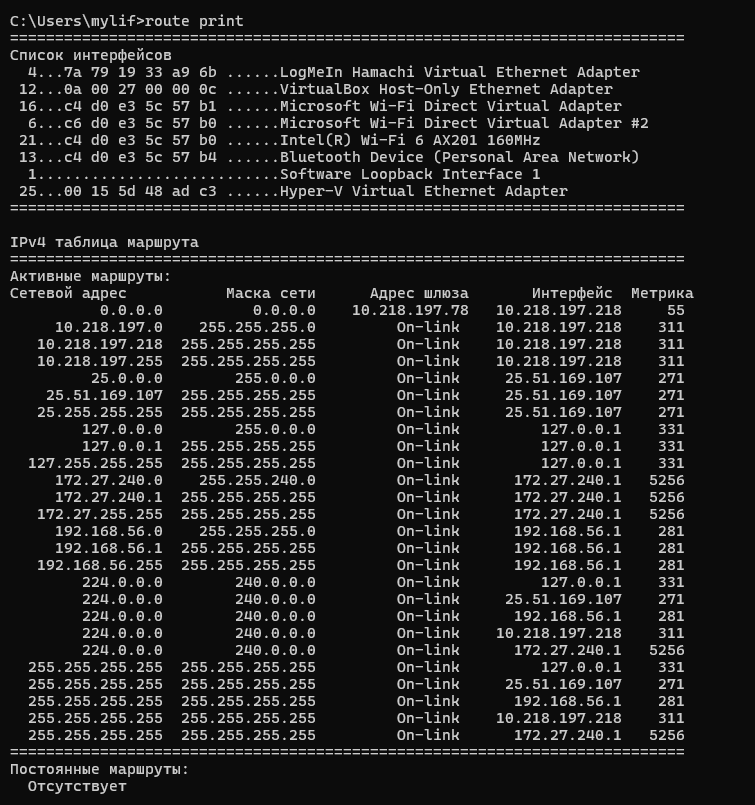


Рис 1.13- Справка о параметрах утилиты route

Используется для получения данных о маршрутизации.

**Задание 16.** Распечатайте на экран монитора таблицу активных маршрутов компьютера. Исследуйте полученный отчет. Определите строки таблицы, соответствующие интерфейсу внутренней петли и широковещательным адресам. Определите IP- адреса шлюзов.



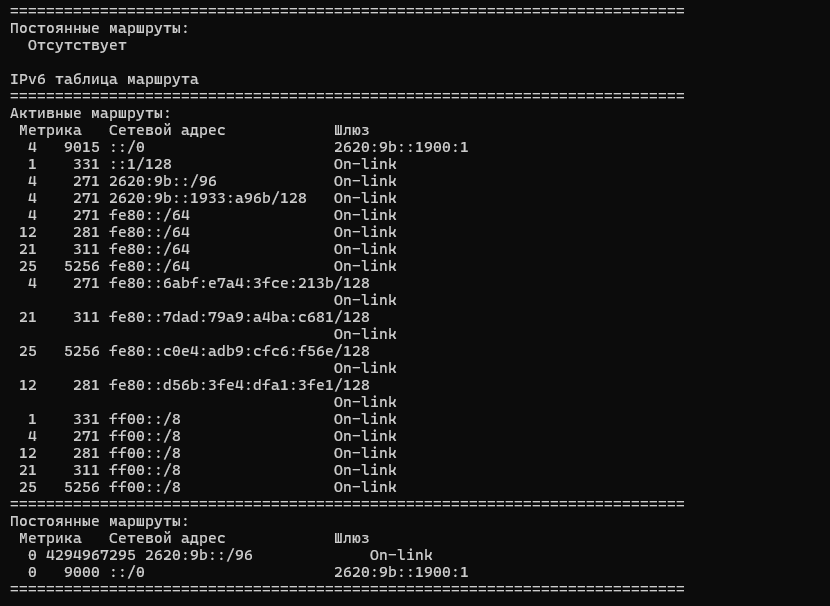


Рис 1.14- Таблица активных маршрутов

Cтроки таблицы, соответствующие интерфейсу внутренней петли:

Вся loopback-сеть:

127.0.0.0 255.0.0.0 On-link 127.0.0.1 331

127.27.240.0 255.255.240.0 On-link 127.27.240.1 5256

Конкретные loopback-адреса:

127.0.0.1 255.255.255.255 On-link 127.0.0.1 331

127.27.240.1 255.255.255.255 On-link 127.27.240.1 5256

Широковещательные адреса для loopback:

127.255.255.255 255.255.255.255 On-link 127.0.0.1 331

172.27.255.255 255.255.255.255 On-link 172.27.240.1 5256

Строки таблицы, соответствующие широковещательным адресам:

25.255.255.255 255.255.255.255 On-link 25.51.169.107 271

127.255.255.255 255.255.255.255 On-link 127.0.0.1 331

172.27.255.255 255.255.255.255 On-link 172.27.240.1 5256

255.255.255.255 255.255.255.255 On-link 127.0.0.1 331

255.255.255.255 255.255.255.255 On-link 25.51.169.107 271

255.255.255.255 255.255.255.255 On-link 192.168.56.1 281

255.255.255.255 255.255.255.255 On-link 10.218.197.218 311

255.255.255.255 255.255.255.255 On-link 172.27.240.1 5256

IP-адреса шлюзов: 10.218.197.78

**Задание 17.** Получите справку о параметрах утилиты **arp**.



Рис 1.15- Параметры утилиты arp

Используется для диагностики локальной сети

**Задание 18.** Распечатайте на экран монитора arp-таблицу. Исследуйте полученный отчет. Определите хосты, которым соответствуют строки arp-таблицы. Определите IP-адрес, которого нет в arp-таблице, но есть в локальной сети. Выполните утилиту **ping** в адрес этого хоста. Распечатайте снова arp-таблицу и объясните произошедшие изменения. Определите MAC-адреса двух хостов с ближайшими IP-адресами.

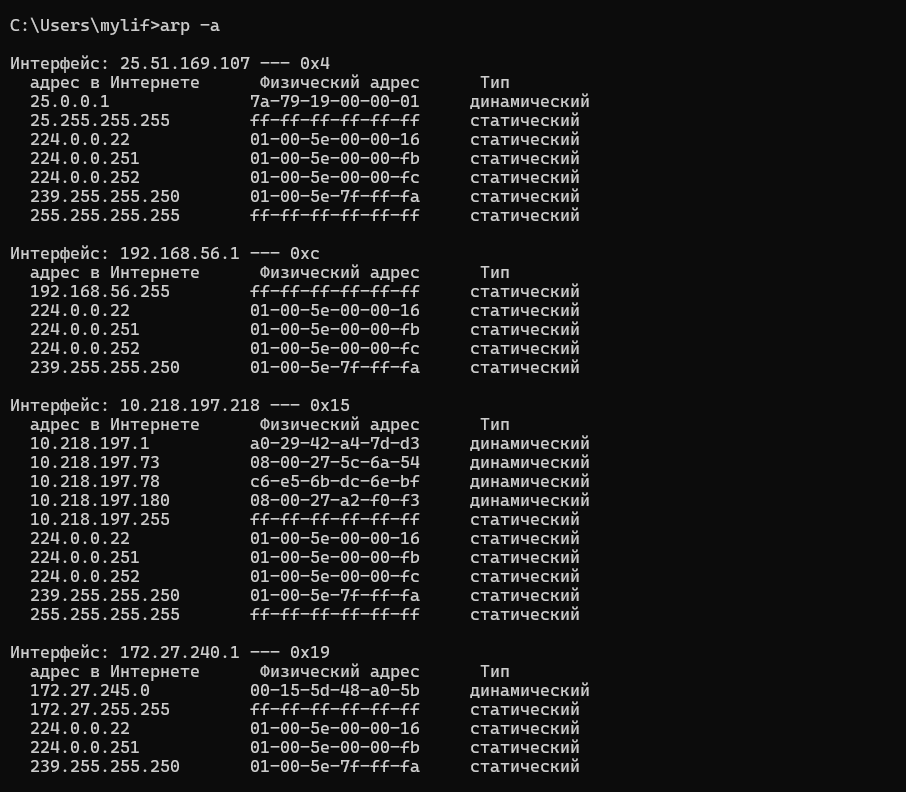


Рис 1.16- arp-таблица в начальном состоянии

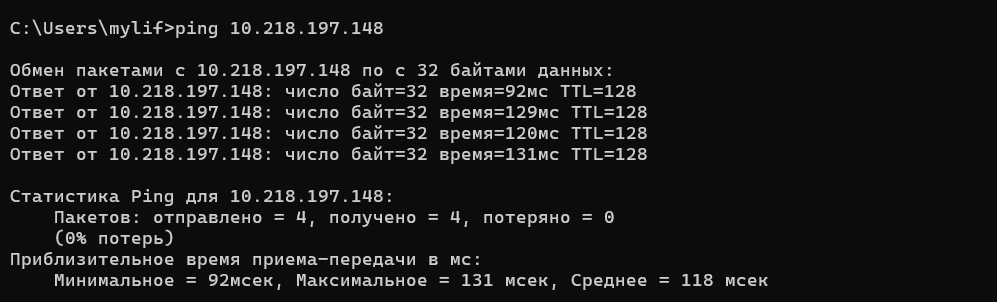


Рис 1.16.1- Обмен данными с компьютером, который есть в локальной сети, но отсутствует в arp-таблице

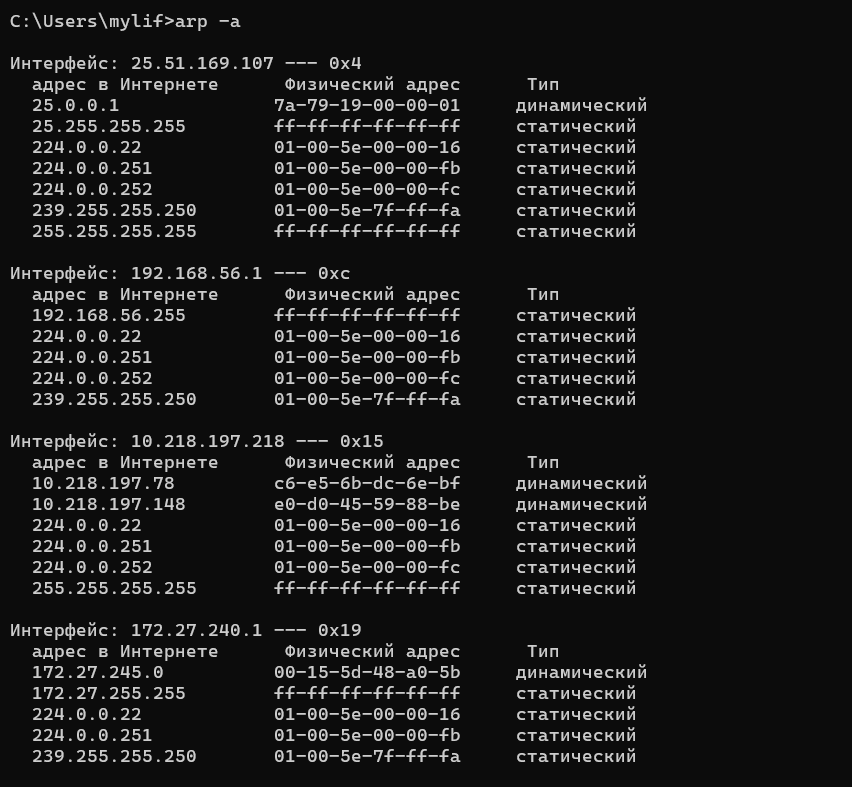


Рис 1.16.2- Обновленная arp-таблица

После обмена пакетами с другим устройством, в таблице появилась строка «10.218.197.148 e0-d0-45-59-88-be динамический», что значит, что после использования утилиты ping, компьютер обновляет таблицу.

Mac-адреса двух ближайших адресов:

IP-адрес: 224.0.0.251 MAC-адрес: 01-00-5e-00-00-fb

IP-адрес: 224.0.0.252 MAC-адрес: 01-00-5e-00-00-fc

**Задание 19. З**апустите утилиту **nslookup** в диалоговом режиме и наберите команду **help**. Ознакомьтесь с полученным отчетом, отражающим возможности утилиты **nslookup**.

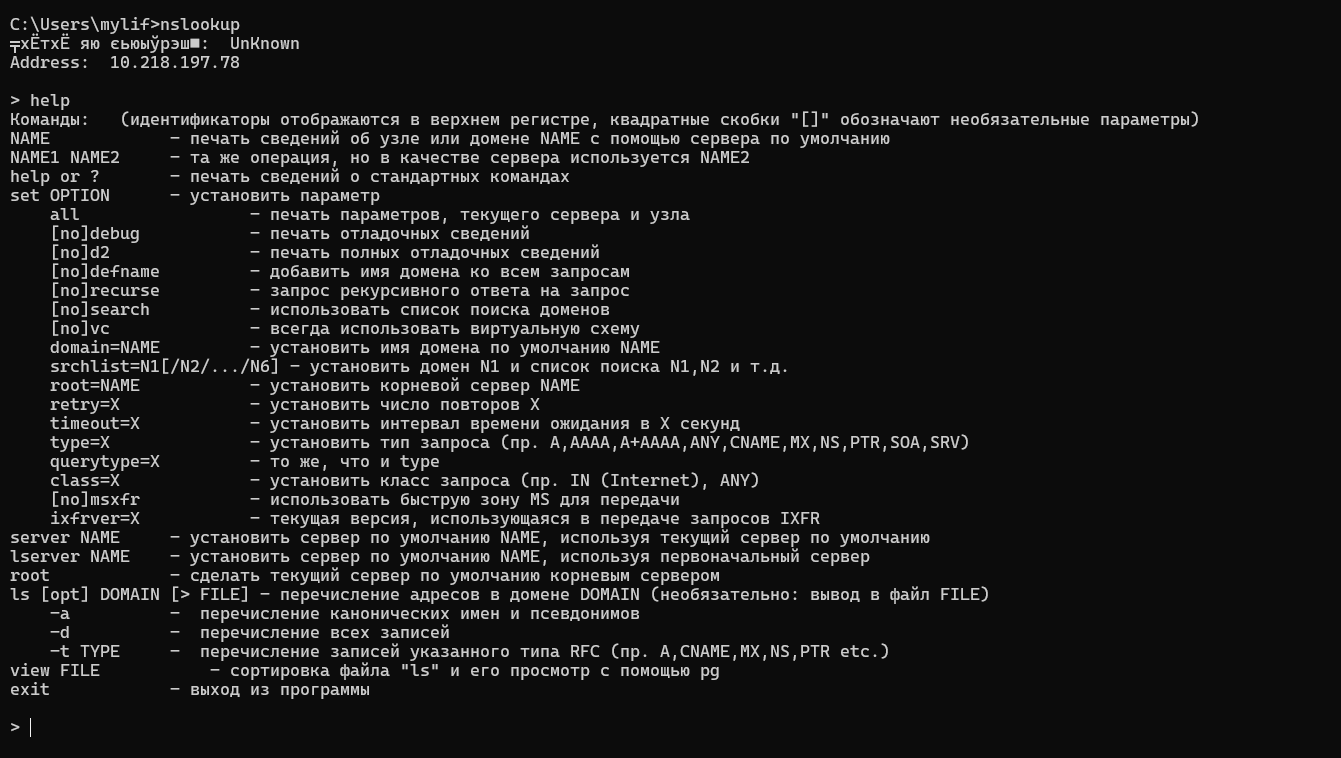


Рис 1.17- Возможности утилиты nslookup

Она используется для получения информации о доменных именах, IP-адресах, почтовых серверах и других ресурсах, связанных с сетевыми узлами.

**Задание 20. З**апустите утилиту **nslookup** в диалоговом режиме. Определите имя и IP-адрес хоста, на котором установлен DNS-сервер по умолчанию. Определите IP-адреса хостов по их именам (имена хостов выдаст преподаватель).

Сервер не имеет обратной DNS записи(PTR записи), поэтому его имя отображается как UnKnown (╤хЁтхЁ яю єьюыўрэш■: UnKnown).

IP-адрес сервера: 10.218.197.78

IP-адреса хостов популярных сайтов:

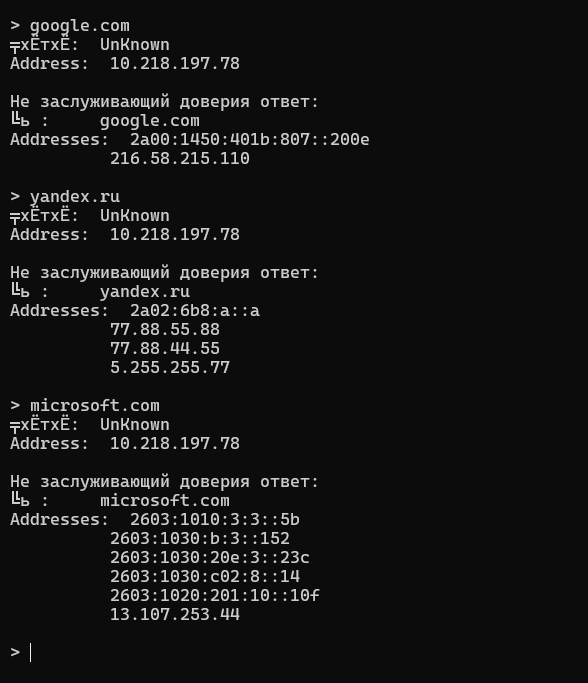


Рис 1.18- утилита nslookup в диалоговом режиме

**Задание 21.** Получите справку о параметрах утилиты **netstat**.

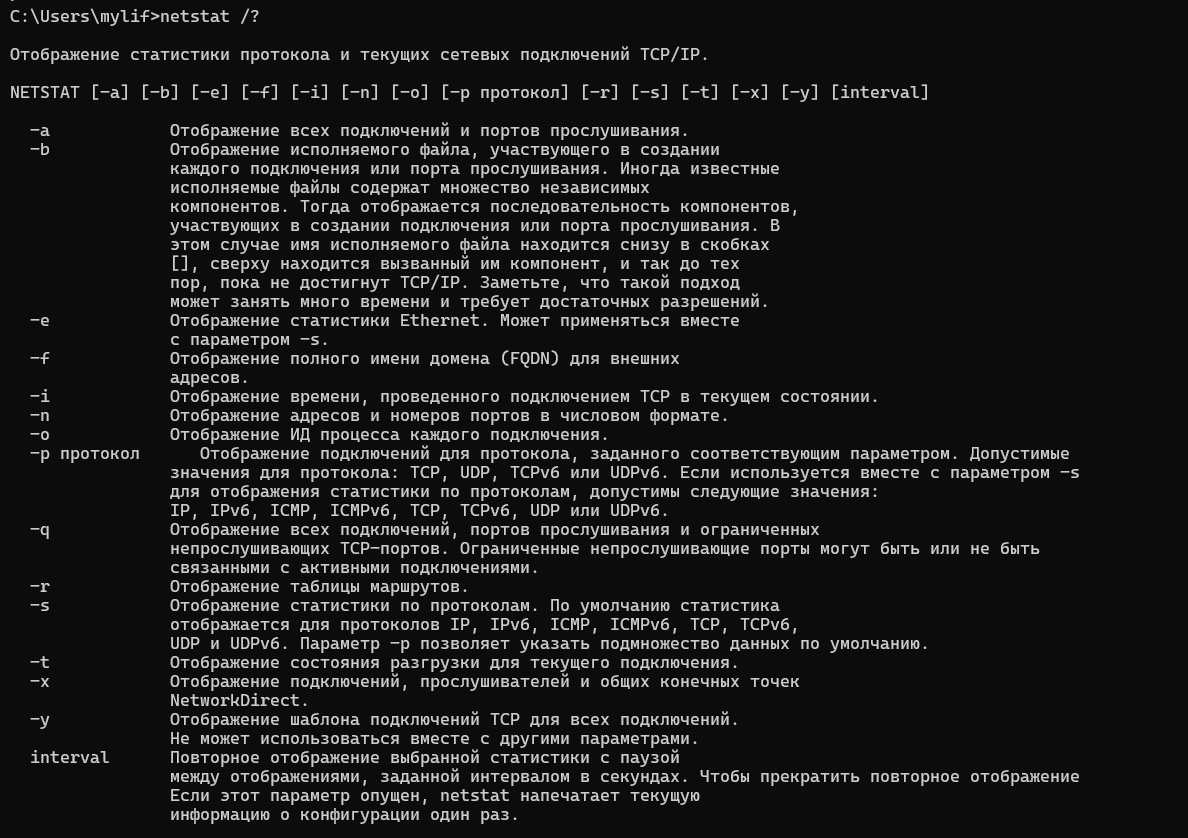


Рис 1.19- Параметры утилиты netstat

Утилита netstat в операционных системах используется для отображения сетевой статистики, подключений, маршрутов и открытых портов.

**Задание 22.** Запустите утилиту **netstat -a** для отображения всех подключений и ожидающих портов. Исследуйте отчет. Выясните, какие из известных служб прослушивают порты. С какими из этих портов поддерживается внешнее соединение и по какому протоколу? Определите имена хостов и номера портов внешних соединений.

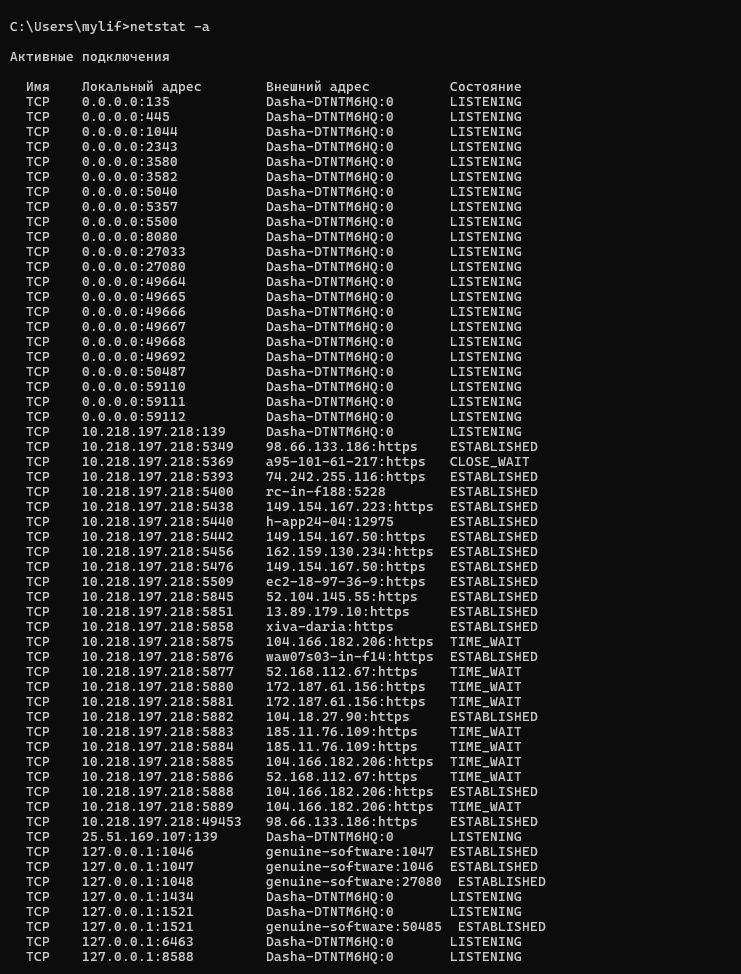


Рис 1.20- Отчет утилиты netstat-a

Известные службы, прослушивающие порты (Listening):

135-RFC, 445-SMB, 139-NetBios, 5357-Net Services, 8080-HTTP alt

Все внешние соединения (Established) поддерживают порт 443(HTTPS) по протоколу TCP.

Имена хостов и номера портов внешних соединений:

98.66.133.186:443 (HTTPS)

74.242.255.116:443 (HTTPS)

**Задание 23.** Запустите утилиту **netstat -b** для отображения исполняемых файлов участвующих в создании подключений. Определите исполняемые файлы служб, прослушивающих порты, идентификаторы процессов операционной системы.

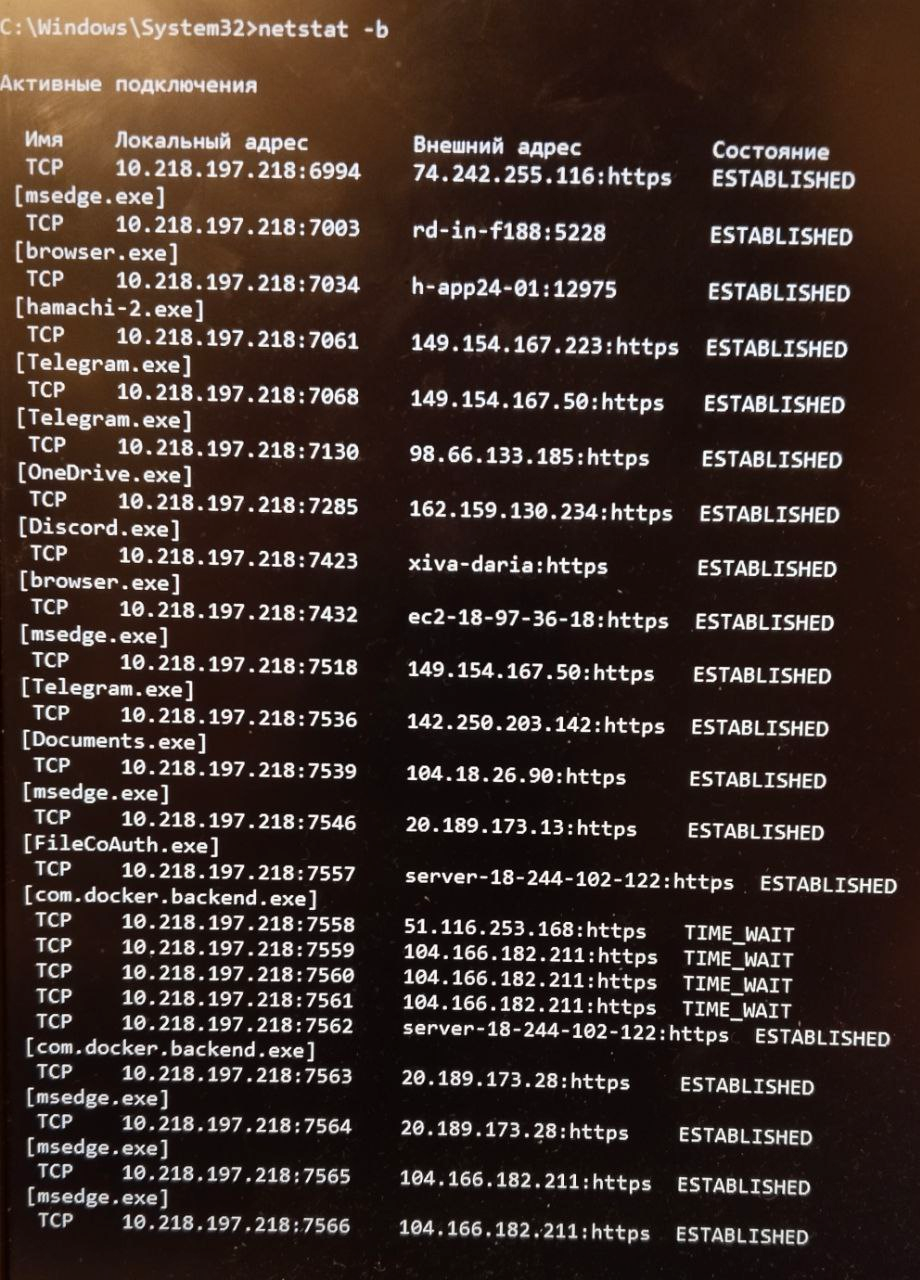


Рис 1.21- Отчет утилиты netstat-b

Исполняемые файлы служб, прослушивающие порты:

msedge.exe, browser.exe, hamachi-2.exe, Telegram.exe, OneDrive.exe, Discord.exe, Documents.exe, FileCoAuth.exe, FileCoAuth.exe, com.docker.backend.exe, BasicService.exe, lkcitdl.exe, lkads.exe, NIWebServiceContainer.exe, NIWebServiceContainer.exe и т.д.

Идентификаторы процессов операционной системы:

Порт:135 (TCP) - PID:136

Порт:445 (TCP) - PID:4

Порт:2343 (TCP) - PID:5560

Порт:3580 (TCP) - PID:5784

Порт:3582 (TCP) - PID:8864

Порт:5040 (TCP) - PID:10932

Порт:5500 (TCP) - PID:6040

Порт:5357 (TCP) - PID:4

**Задание 24.** Запустите утилиту **netstat -ab**. Исследуйте полученный отчет. Для формирования файла отчета утилиты, перенаправьте вывод утилиты в файл с помощью команды: **netstat -ab > c:\report.txt.** Проконтролируйте наличие отчета в файле.

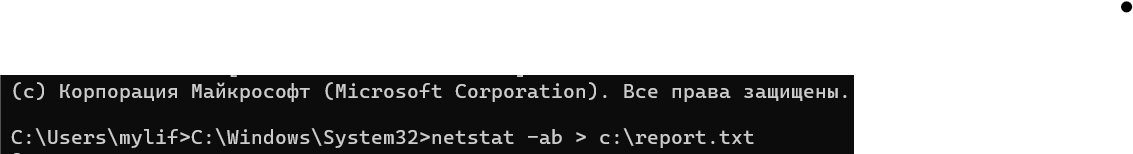
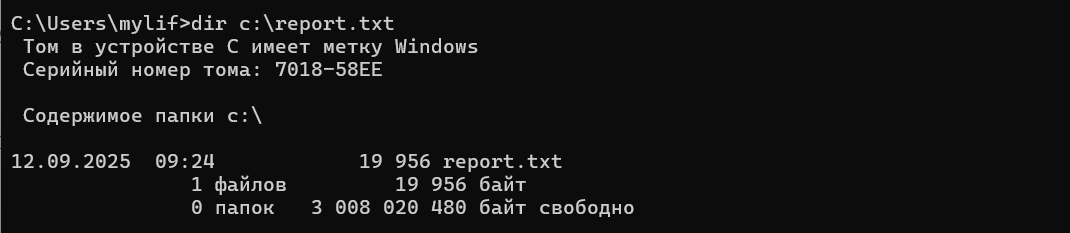


Рис 1.22- Запуск утилиты netstat-ab



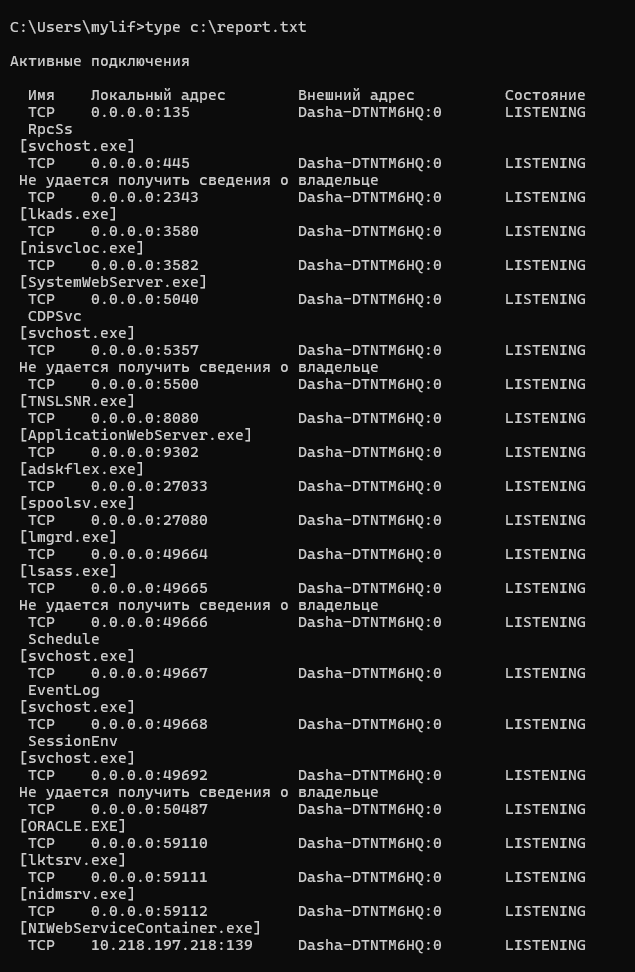


Рис 1.23- отчет в файле

Отчет успешно создан, имеет размер 19 956 байт, содержит информацию о всех сетевых подключениях, включает исполняемые файлы.

**Задание 25.** Получите справку о параметрах утилиты **nbtstat**. Выполните все команды отраженные в справке. Исследуйте полученные отчеты.

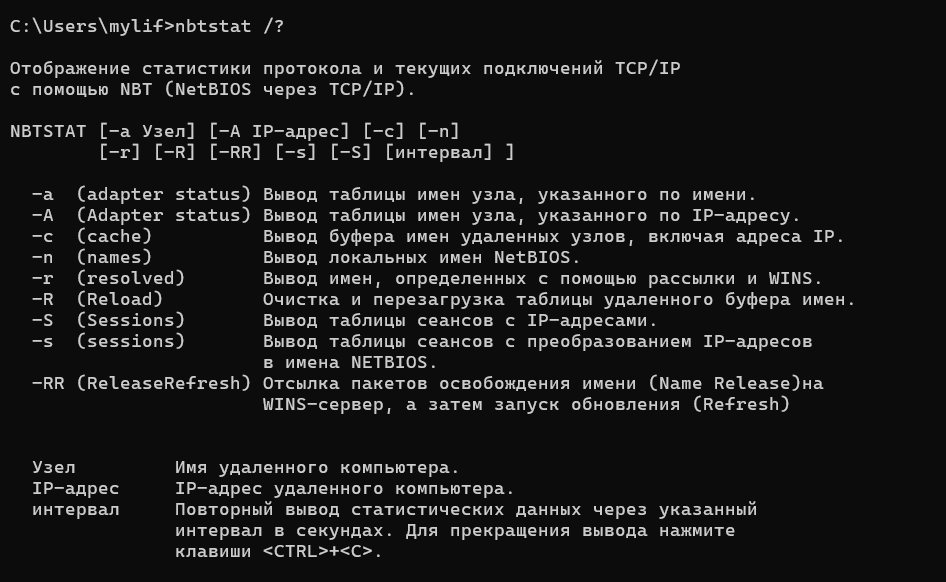


Рис 1.24- Параметры утилиты nbtstat.

Данная утилита используется для отображения статистики и диагностики протокола NetBIOS на компьютере.

**Задание 26.** Получите справку о параметрах утилиты **net**. Получите справку по отдельным командам утилиты с помощью команды **help.** Получите статистику рабочей станции и сервера компьютера с помощью команды **statistics**.Перешлите сообщение на соседний компьютер с помощью команды **send**. Получите список пользователей компьютера с помощью команды **user**.

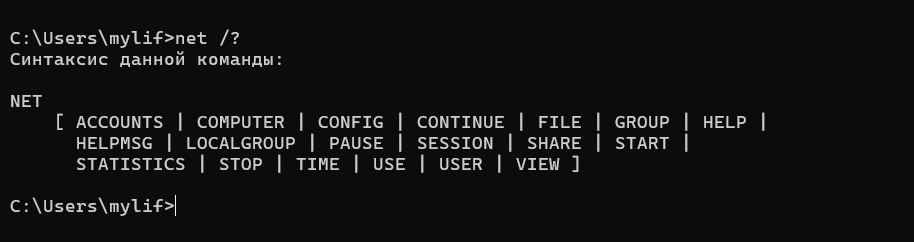


Рис 1.25- Параметры утилиты net.

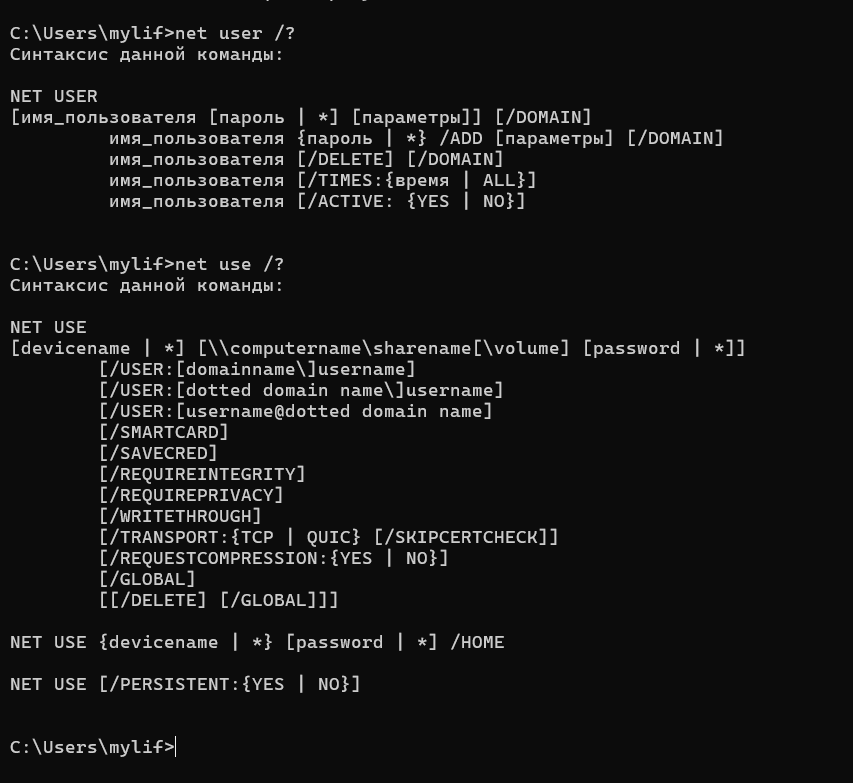


Рис 1.25- Справки о отдельных командах утилиты

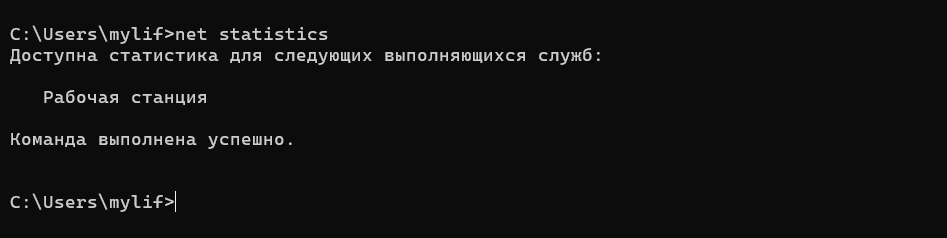


Рис 1.26- Справки о отдельных командах утилиты

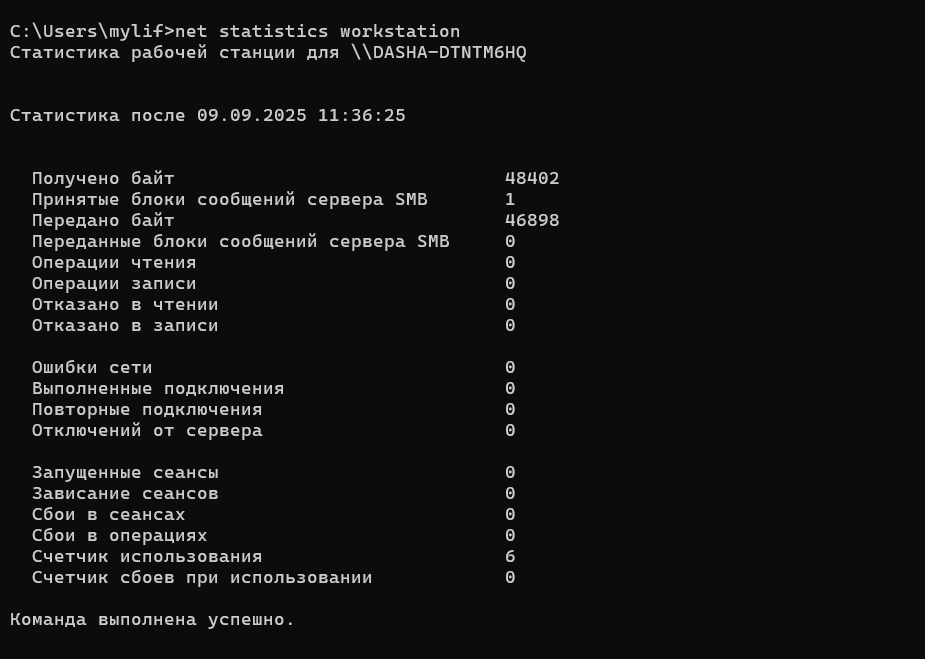


Рис 1.27- Статистика рабочей станции компьютера



Рис 1.28- Отправка сообщения и получения списка пользователей