Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Программирование сетевых приложений

Студент: Лопатнюк П.В.

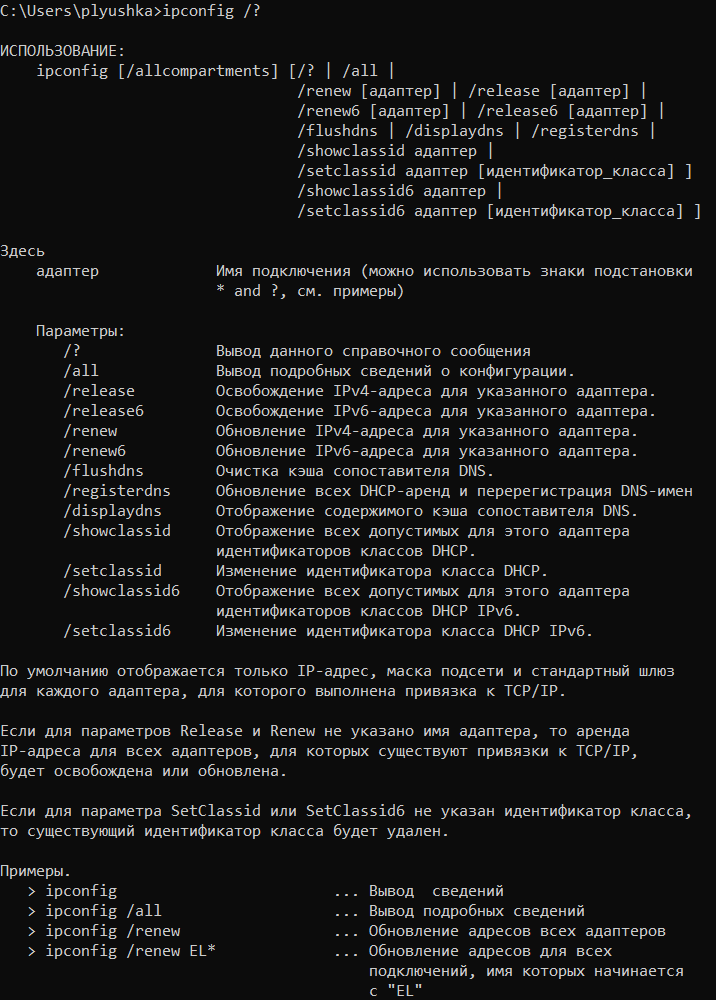
ФИТ 3 курс 1 группа

Преподаватель: Некрасова А.П.

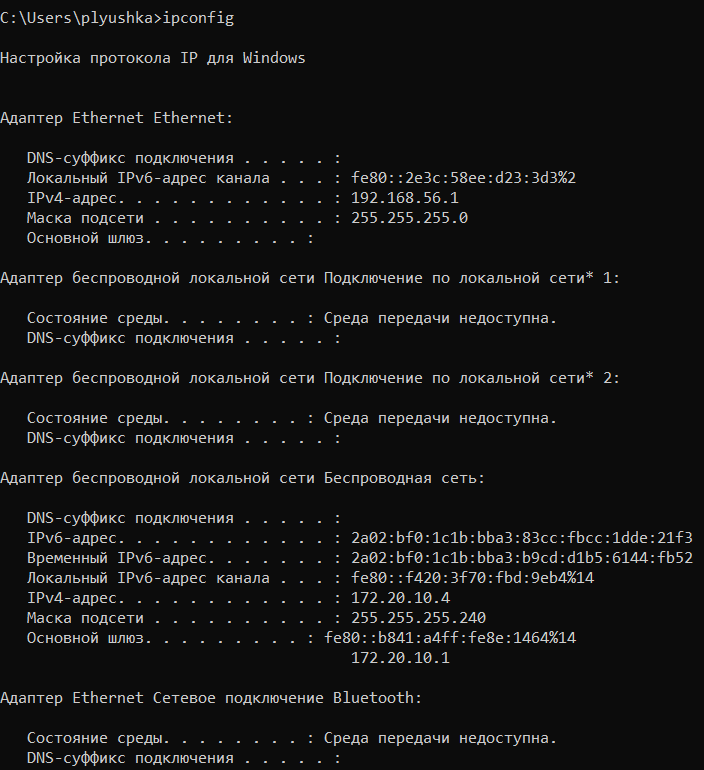
Минск 2024

**Лабораторная работа №1. Сетевые утилиты**

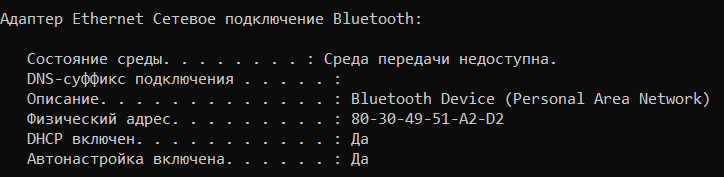
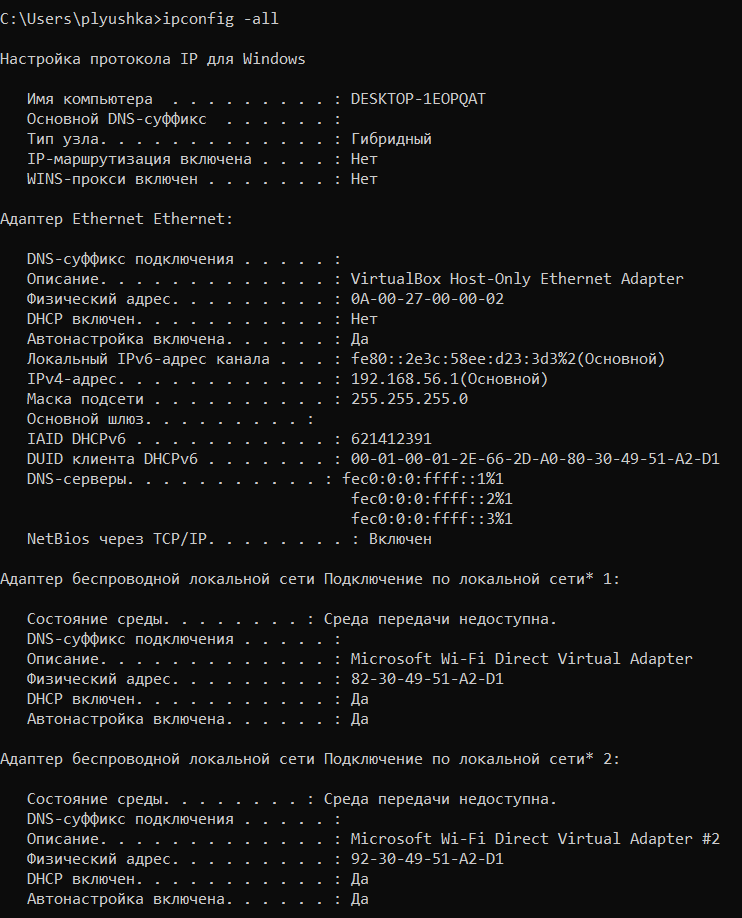
**Задание 1.** Получите справку о параметрах утилиты ipconfig.

****

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



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



Символическое имя хоста: DESKTOP-1EOPQAT

IP-адрес: 192.168.56.1(Основной)

Маска подсети: 255.255.255.0

MAC-адрес адаптерa: 80-30-49-51-A2-D2

**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.

**Класс С.** Число хостов: **254** (маска 255.255.255.0 = 8 бит , 2^8 – 2 = 254)

**Диапазон адресов**: 192.168.56.1 - 192.168.56.254 (192.168.56.0 – сетевой, 192.168.56.255 - широковещательный)

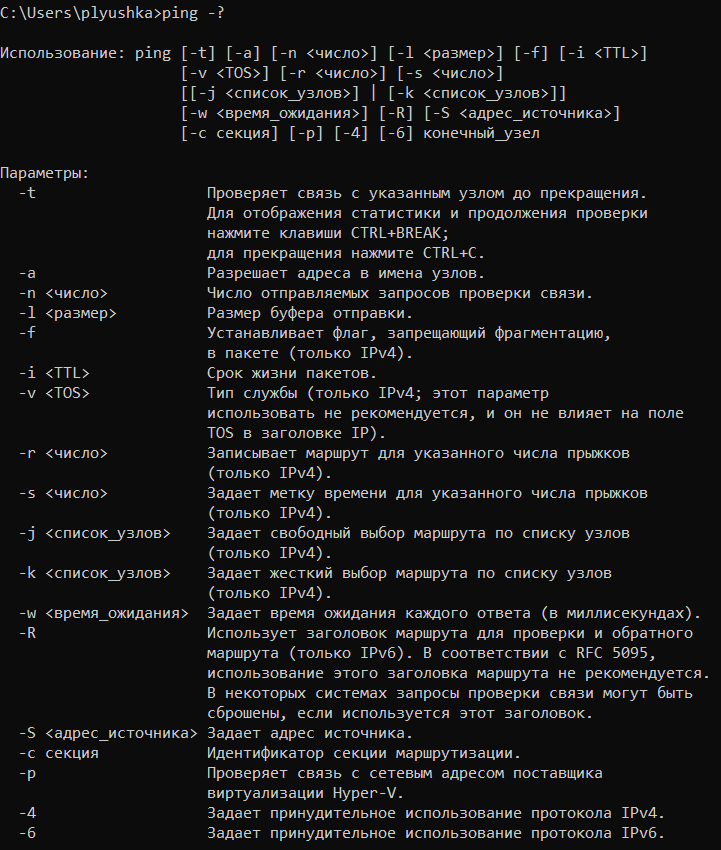
**Код производителя** – OUI – 80-30-49

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



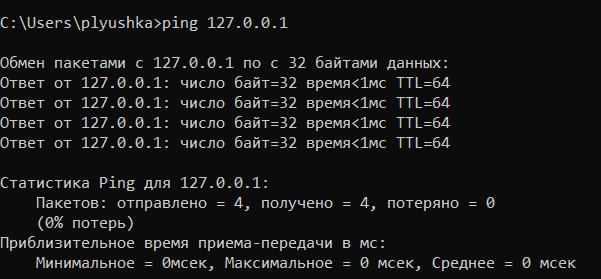
Имя совпадает с именем, которое получили при использовании утилиты ipconfig.

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

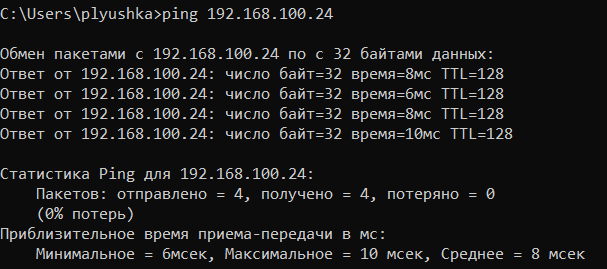


**Задание 7.** С помощью ping проверьте работоспособность интерфейса внутренней петли компьютера.

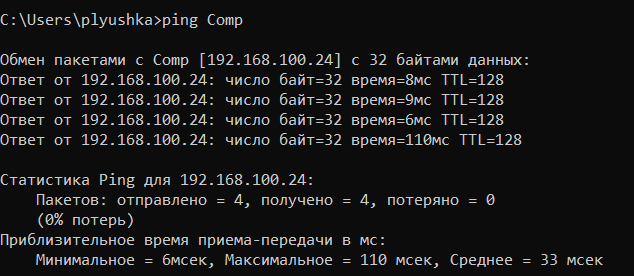
IP-адрес внутренней петли - 127.0.0.1



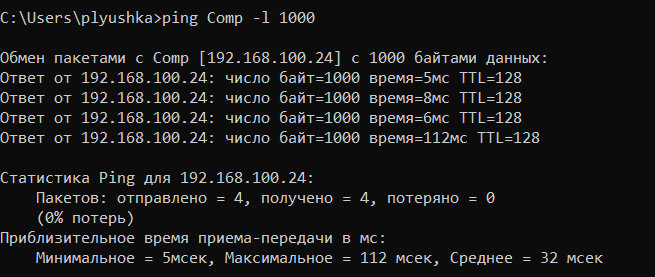
**Задание 8.** С помощью утилиты ping проверьте доступность интерфейса какого-нибудь компьютера в локальной сети, указав в качестве параметров его IP-адрес.



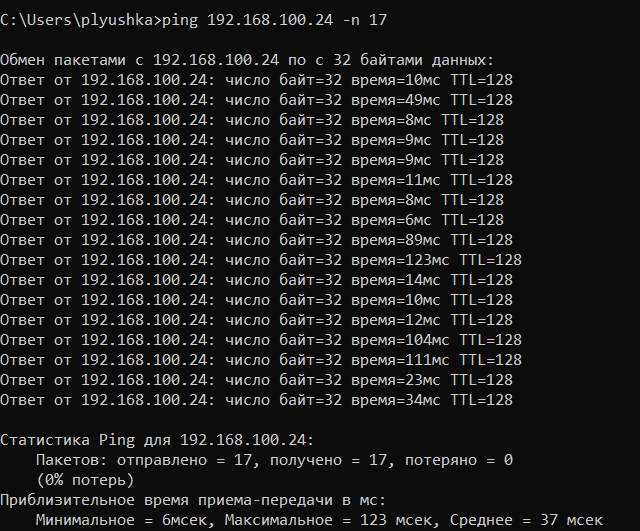
**Задание 9.** С помощью утилиты ping проверьте доступность интерфейса какого-нибудь компьютера в локальной сети, указав в качестве параметров символическое имя хоста.



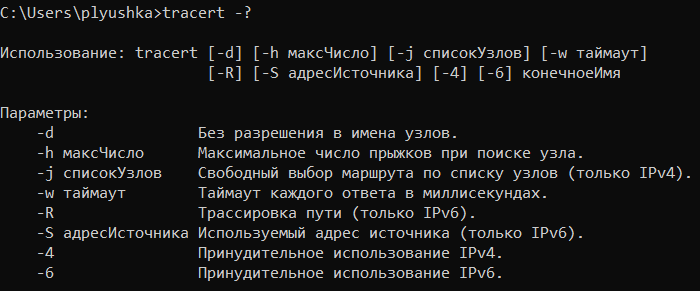
**Задание 10.** С помощью утилиты ping проверьте доступность интерфейса какого-нибудь компьютера в локальной сети, указав в качестве параметров символическое имя хоста и увеличив размер буфера отправки до 1000 байт



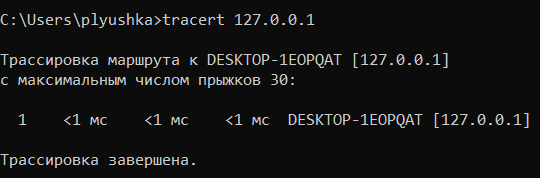
**Задание 11.** С помощью утилиты ping проверьте доступность интерфейса какого-нибудь компьютера в локальной сети, указав в качестве параметров его IP-адрес и установив количество отправляемых запросов равное 17.



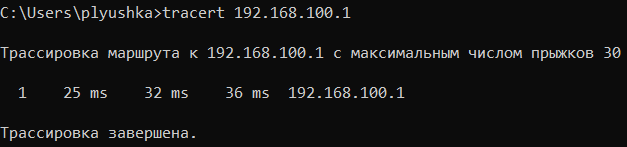
**Задание 12.** Получите справку о параметрах утилиты tracert.



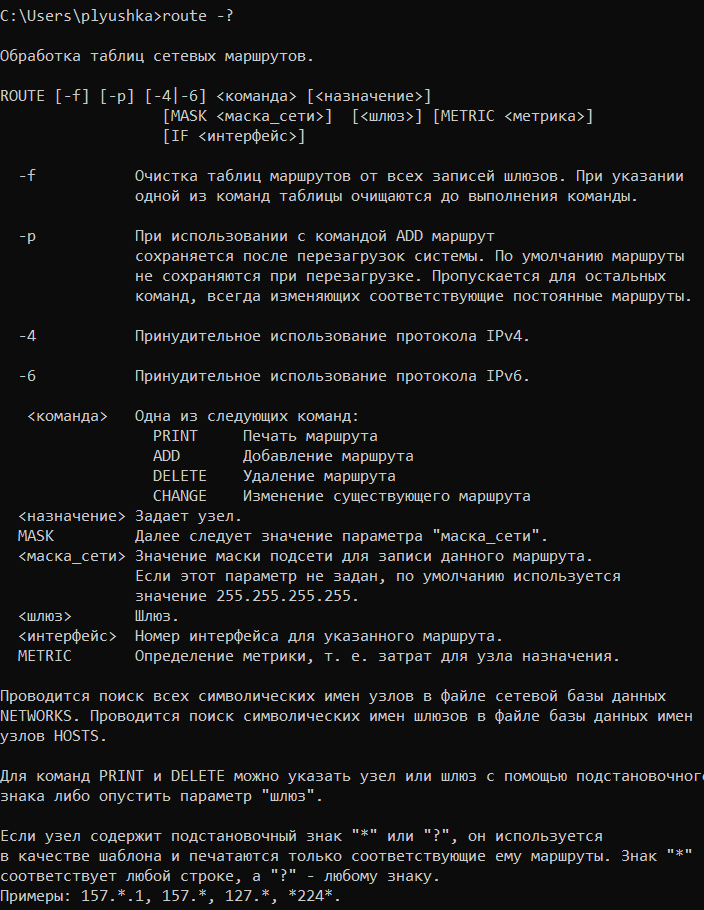
**Задание 13**. С помощью утилиты tracert определите маршрут хоста самого к себе (интерфейс внутренней петли).



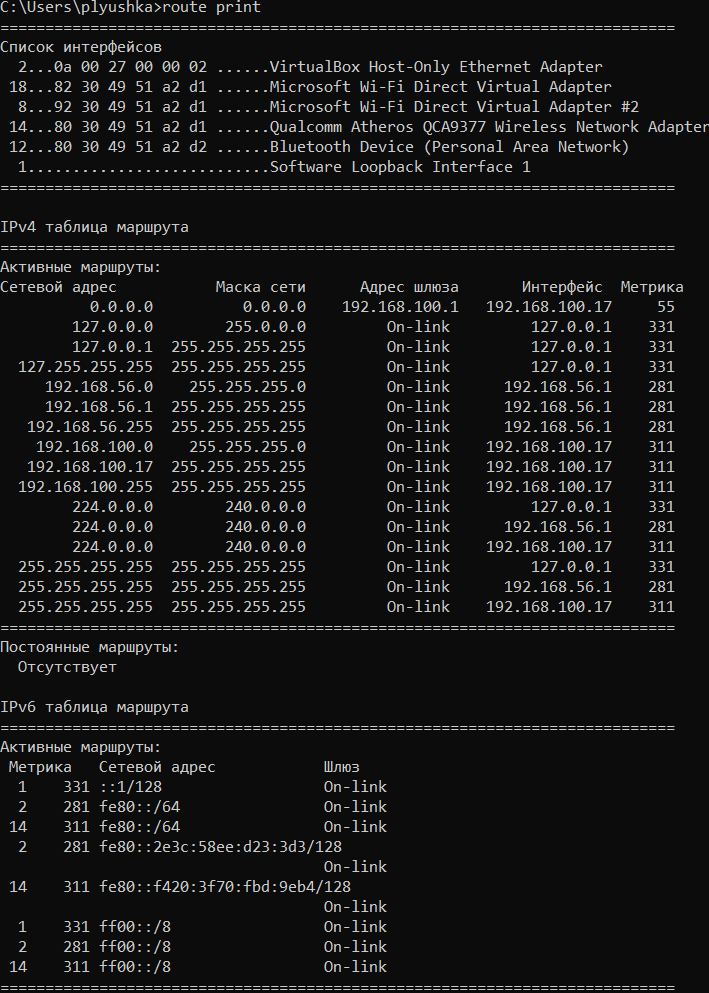
**Задание 14.** С помощью утилиты tracert определите маршрут к хосту в локальной сети. Определите количество прыжков в полученном маршруте.



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



**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.



Строки, соответствующие интерфейсу **внутренней петли** (loopback) 2, 3, 4:

127.0.0.0 (сетевая маска 255.0.0.0, интерфейс 127.0.0.1)

127.0.0.1 (сетевая маска 255.255.255.255, интерфейс 127.0.0.1)

127.255.255.255 (сетевая маска 255.255.255.255, интерфейс 127.0.0.1)

Строки, соответствующие **широковещательным** (broadcast) адресам:

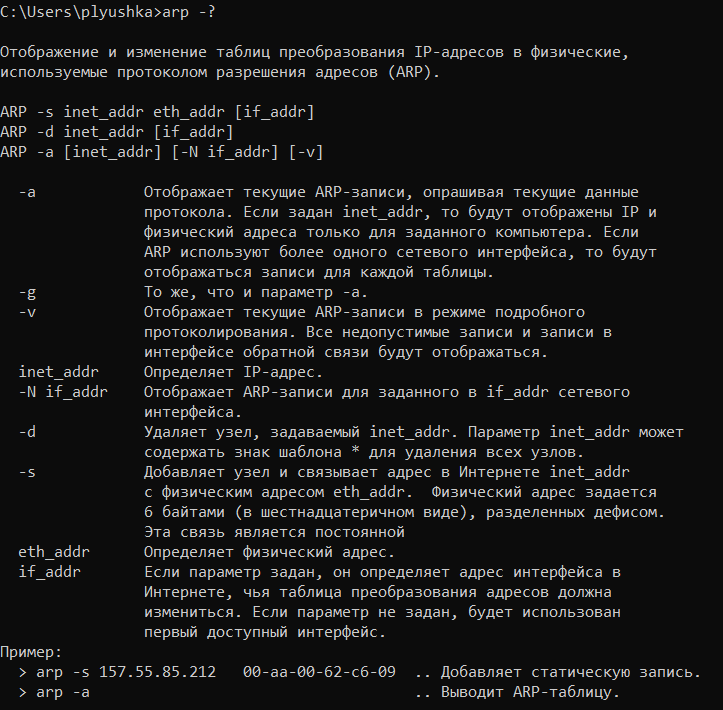
192.168.56.255 (сетевая маска 255.255.255.255, интерфейс 192.168.56.1)

192.168.100.255 (сетевая маска 255.255.255.255, интерфейс 192.168.100.17)

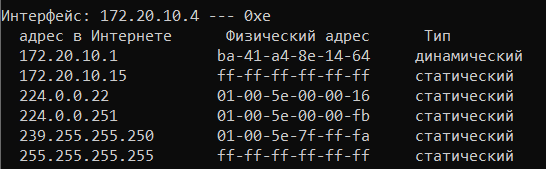
255.255.255.255 (сетевая маска 255.255.255.255, интерфейсы 192.168.56.1 и 192.168.100.17)

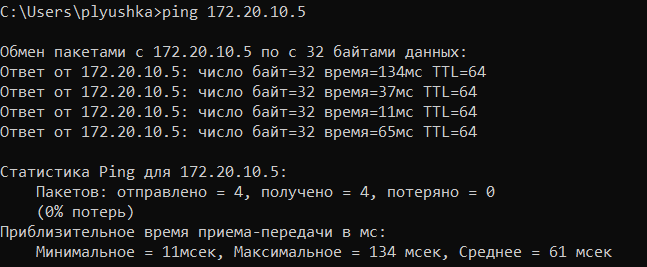
**IP-адрес шлюза**: 192.168.100.1

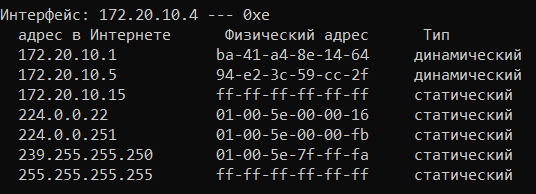
**Задание 17.** Получите справку о параметрах утилиты arp.



**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.





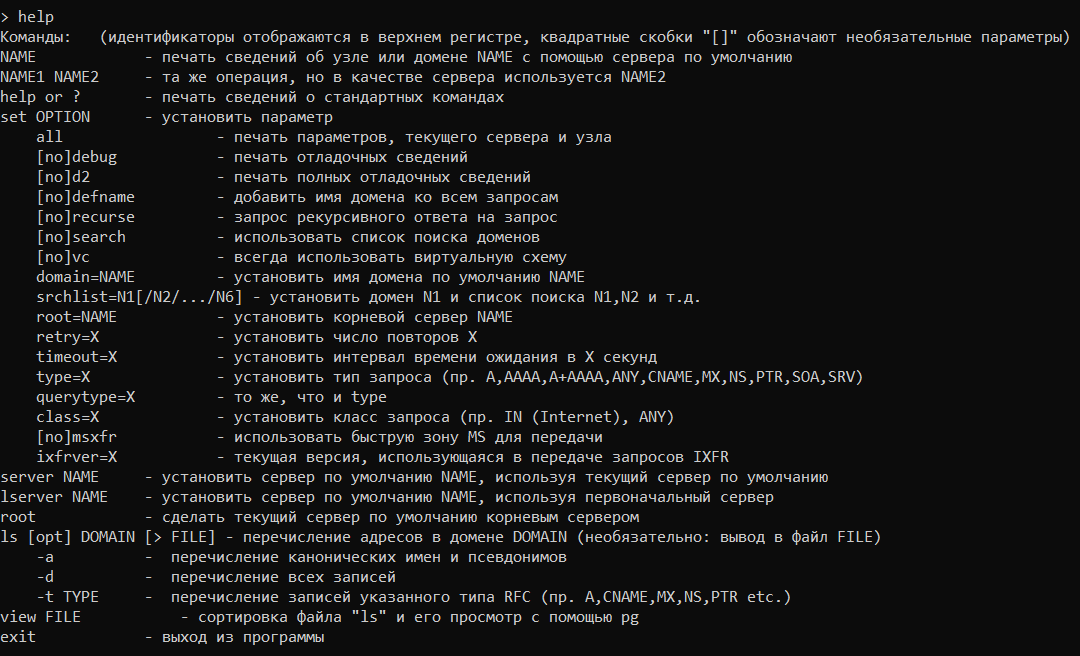


IP-адрес появляется в таблице. Хост с этим IP-адресом ответил на ping.

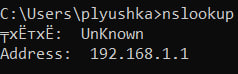
172.20.10.5 — MAC-адрес 94-e2-3c-59-cc-2f

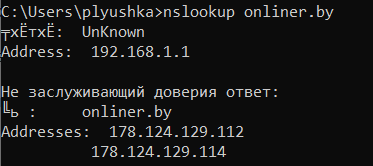
172.20.10.1 — MAC-адрес ba-41-a4-8e-14-64

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

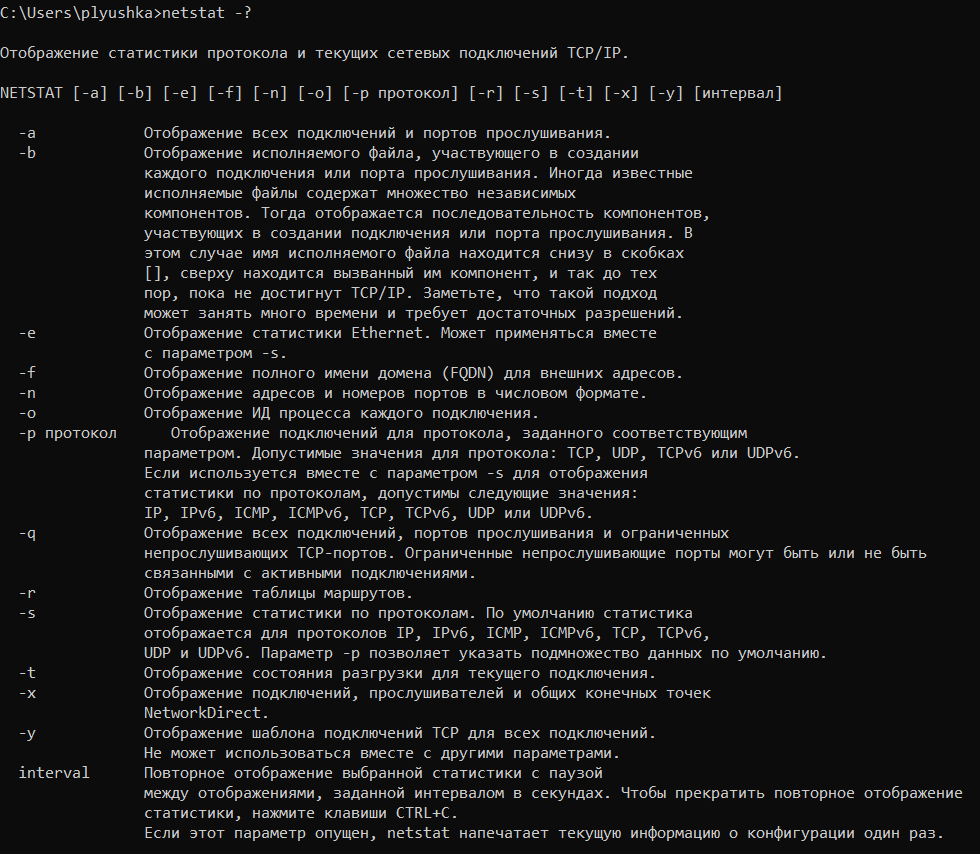


**Задание 20.**  Запустите утилиту nslookup в диалоговом режиме. Определите имя и IP-адрес хоста, на котором установлен DNS-сервер по умолчанию. Определите IP-адреса хостов по их именам (имена хостов выдаст преподаватель).

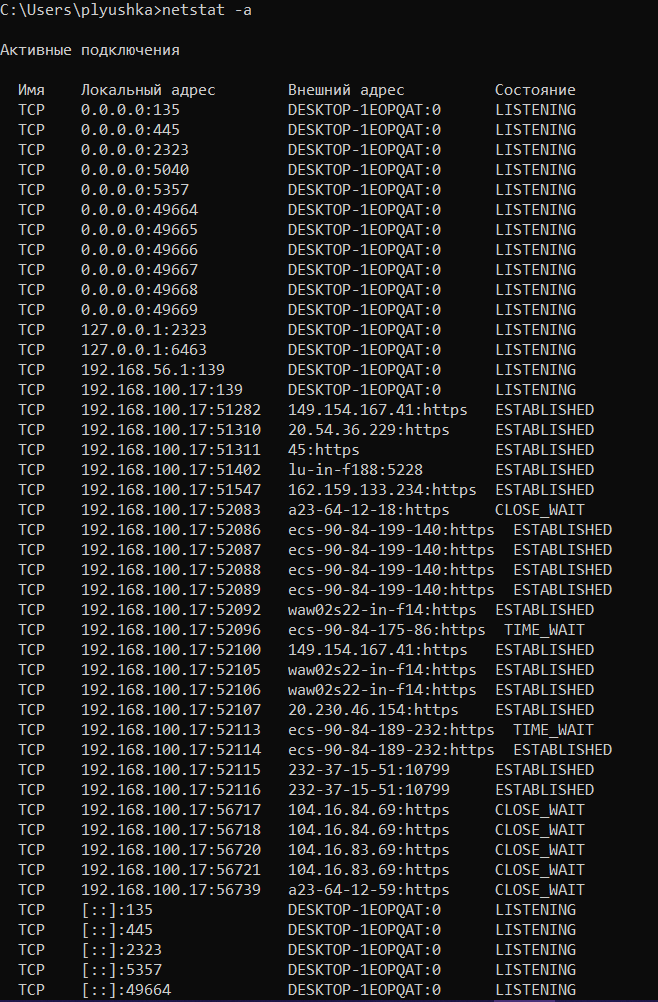




**Задание 21.** Получите справку о параметрах утилиты netstat.

****

**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 .



В столбце "Локальный адрес" указаны адреса и порты, которые система использует для прослушивания соединений. Основные порты и службы, которые их прослушивают:

135 (TCP) — используется службой DCE/RPC (Microsoft RPC).

445 (TCP) — используется для SMB (Microsoft-DS), обычно используется для совместного использования файлов в сети.

49664–49669 (TCP) — это динамически выделяемые порты для внутреннего использования, часто используются различными службами ОС Windows, в том числе службами RPC.

5357 (TCP) — используется для Web Services for Devices (WSD), это протокол обнаружения устройств в сети.

3702 (UDP) — также используется для WSD.

5353 (UDP) — используется mDNS (multicast DNS) для обнаружения устройств в локальной сети.

В столбце "Внешний адрес" указаны внешние узлы, с которыми установлены соединения. Например:

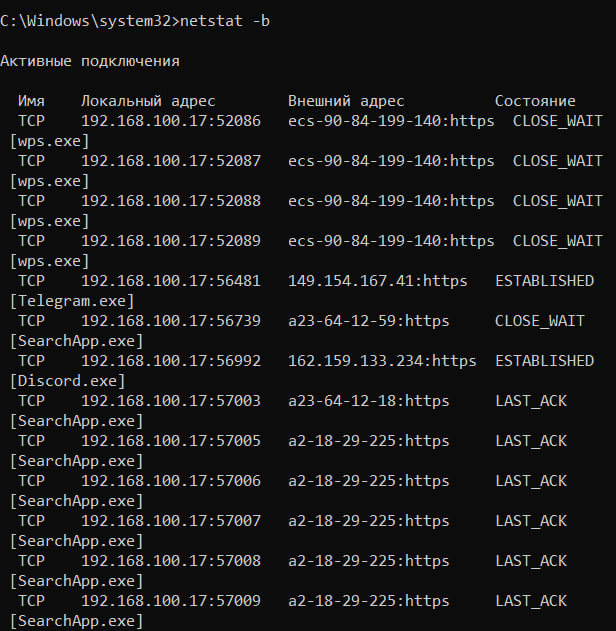
20.54.36.229:443 (https) — соединение установлено с сервером по HTTPS (порт 443).

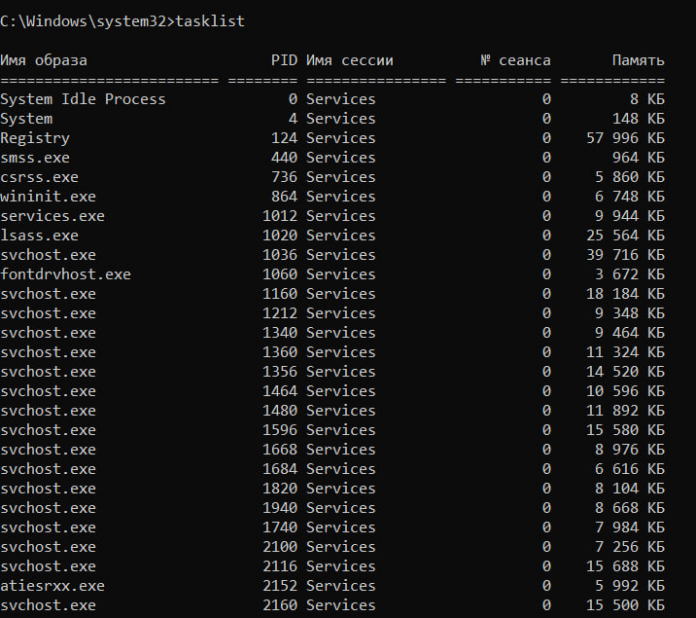
104.16.83.69:443 (https) — это также соединение по HTTPS с внешним сервером.

ecs-90-84-199-140

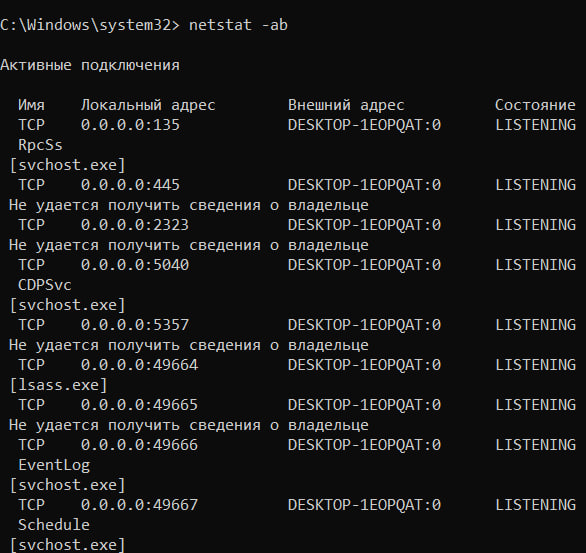
— это внешний сервер с доменным именем, установленное по HTTPS.

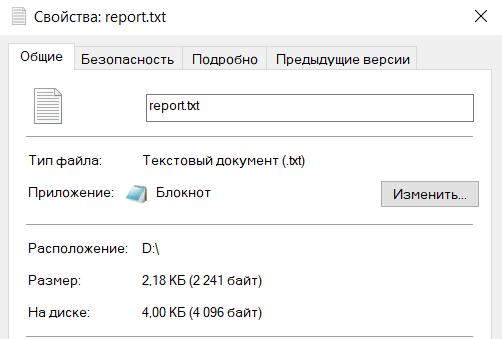
**Задание 23.** Запустите утилиту netstat -b для отображения исполняемых файлов участвующих в создании подключений. Определите исполняемые файлы служб, прослушивающих порты, идентификаторы процессов операционной системы.



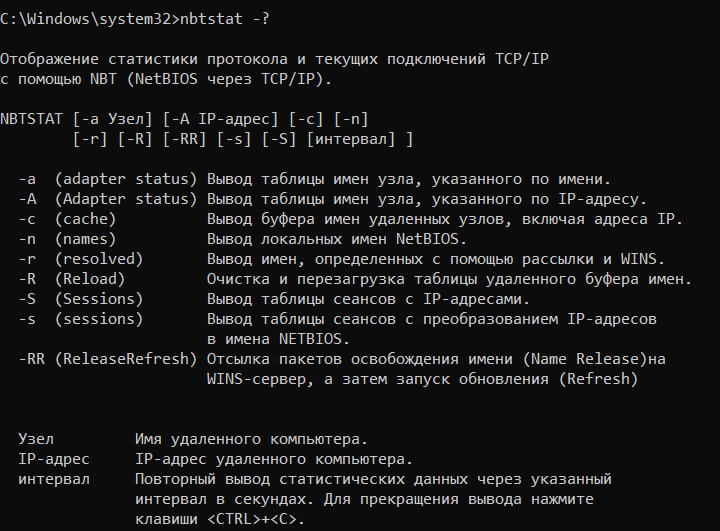


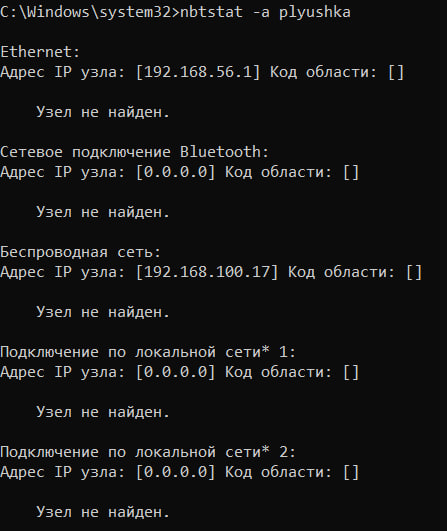
**Задание 24.** Запустите утилиту netstat -ab. Исследуйте полученный отчет. Для формирования файла отчета утилиты, перенаправьте вывод утилиты в файл с помощью команды: netstat -ab > c:\report.txt. Проконтролируйте наличие отчета в файле.

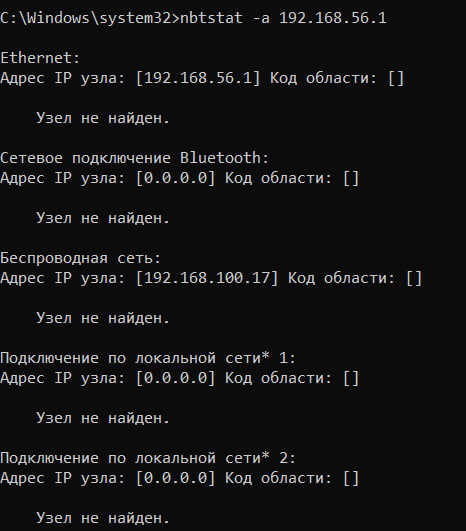


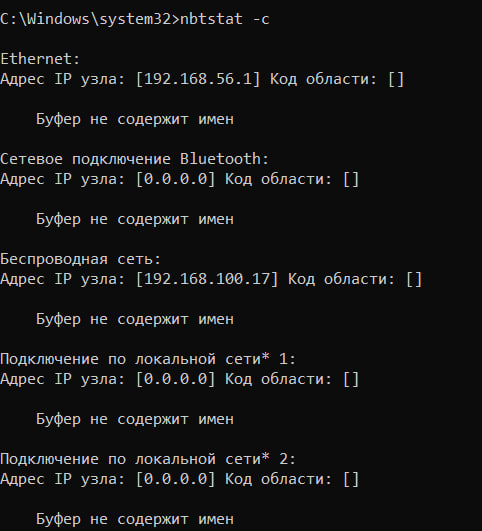


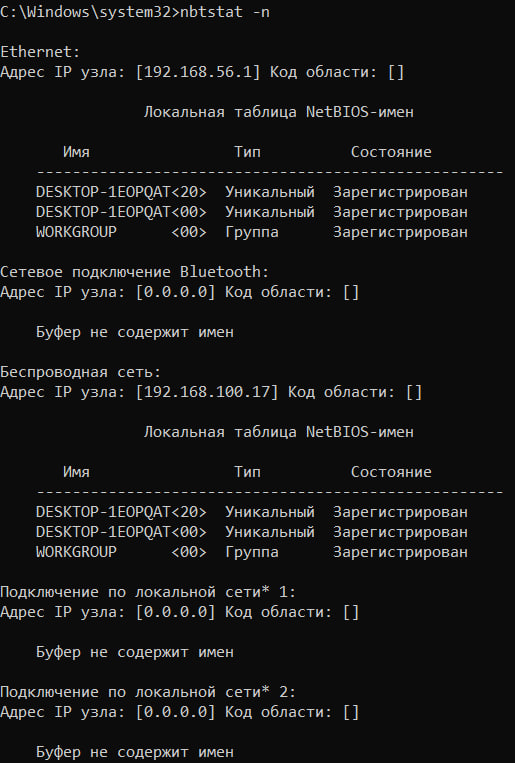
**Задание 25.** Получите справку о параметрах утилиты nbtstat. Выполните все команды отраженные в справке. Исследуйте полученные отчеты.

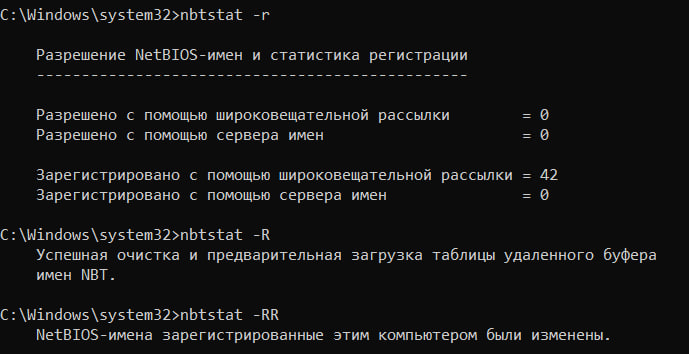


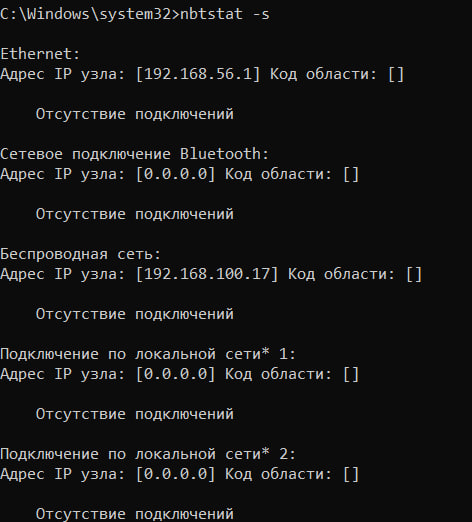


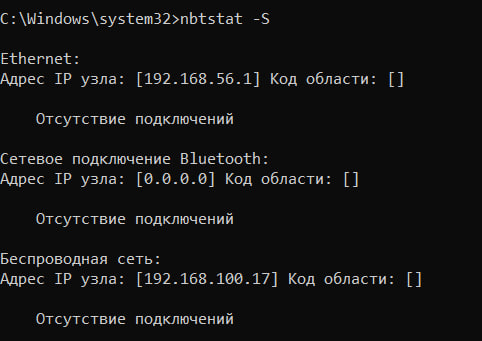












**Задание 26.** Получите справку о параметрах утилиты net. Получите справку по отдельным командам утилиты с помощью команды help. Получите статистику рабочей станции и сервера компьютера с помощью команды statistics. Перешлите сообщение на соседний компьютер с помощью команды send. Получите список пользователей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

