Санкт-Петербургский Национальный
Исследовательский Университет Информационных
технологий, механики и оптики

Лабораторная работа #1

Сетевые протоколы

Выполнили: Шкода
Глеб Ярославович
Фисенко Максим Вячеславович
Группа № K34211
Проверила: Казанова
Полина Петровна

Санкт-Петербург
2024

Цель работы:

1. Тестирование связи устройства в сети
2. Работа с программой LanCalculator
3. Определение имени хоста

Задачи:

1.1. Изучение команды ipconfig
1.2. Изучение команды ping
1.3. Изучение команды tracert
1.4. Изучение команды arp
2.1. Работа с программой LanCalculator
3.1. Определение имени компьютера
3.2. Работа с командой nslookup

Ход работы:

Упражнение 1

Ipconfig – стандартная утилита в Windows, которая позволяет получить информацию о текущих подключениях компьютера через различные интерфейсы. Также данная команда позволяет работать с локальным кешом DNS: просматривать сохранённые сопоставления и, при необходимости, редактировать их.

Начать работу с командой можно с применения параметра /?, что приведёт к появлению на экране справки об использовании утилиты (рисунок 1).

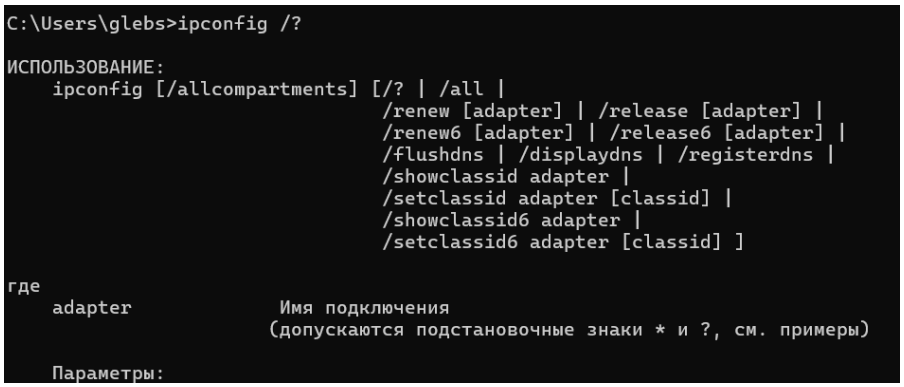


Рисунок 1 – Команда ipconfig /?

А чтобы получить необходимую информацию о текущем подключении, нужно выбрать один из параметров, который фильтрует выводимую на экран

информацию. Чтобы точно получить все необходимые сведенья, я вызвал команду с параметром /all (рисунок 2).

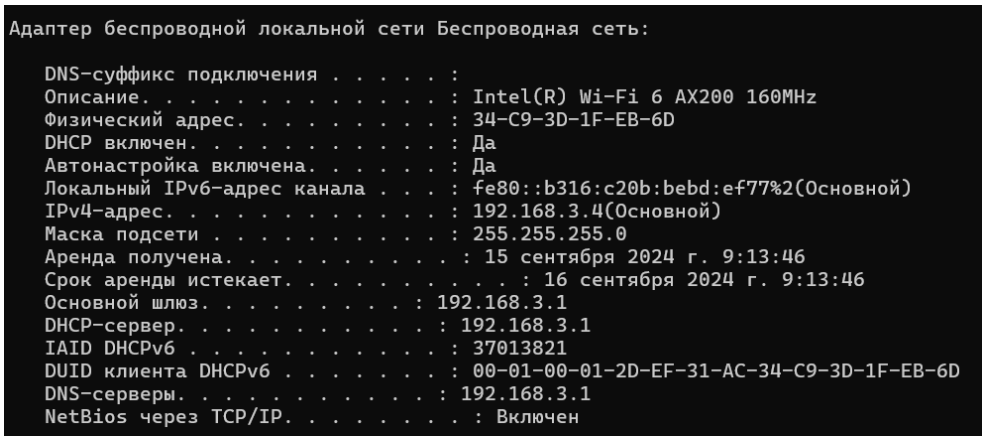


Рисунок 2 – Команда ipconfig /all

Итак, из результата работы команды, видна следующая информация: IPv4 адрес 192.168.3.4, маска подсети 255.255.255.0, шлюз и DNS сервер 192.168.3.1. Можно заметить, что адреса шлюза и DNS сервера совпадают – это адрес домашнего роутера, который одновременно служит и шлюзом в Интернет и локальным DNS сервером.

Ping – утилита для проверки соединения к сети. Она посылает несколько ICMP пакетов, ждёт ответов и рассчитывает время между отправкой запроса и получением ответа. Справку об использовании утилиты можно получить, применив параметр /? (рисунок 3).

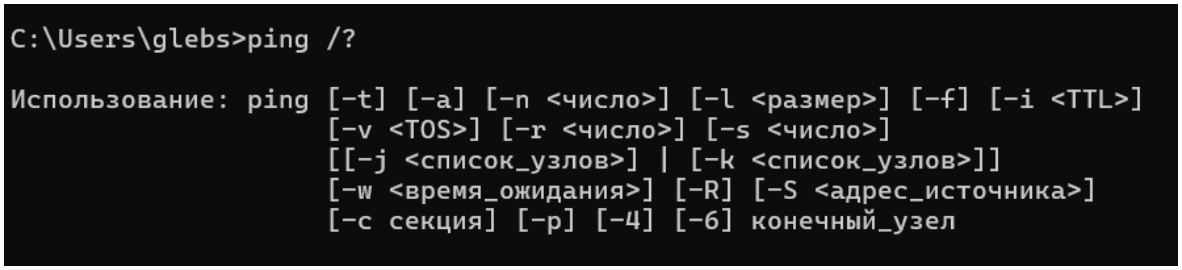


Рисунок 3 – Команда ping /?

Хорошим способом проверить, что все сетевые устройства и соответствующее ПО на компьютере работают корректно, является пинг своего собственного адреса. Так можно независимо от окружающей локальной сети убедиться, что устройство способно принимать и отправлять пакеты (рисунок 4).

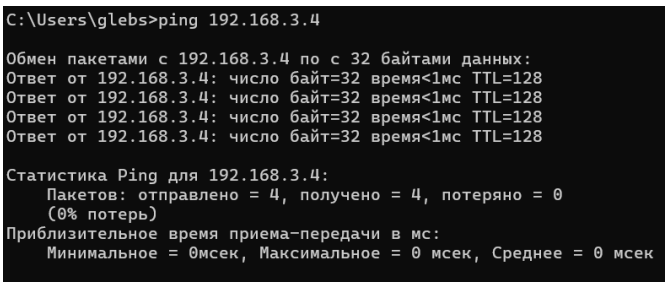


Рисунок 4 – результат работы ping 192.168.3.4

Далее, чтобы проверить соединение с другими устройствами локальной сети, я отправил пакеты на свой телефон с адресом 192.168.3.13 (рисунок 5).

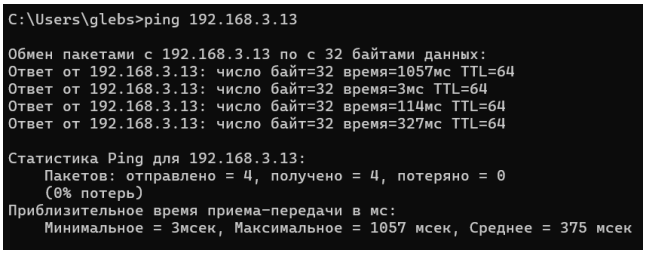


Рисунок 5 – результат работы ping 192.168.3.13

Можно заметить, что если запросы к самому себе, проходили почти мгновенно, то запросы на другое уже занимают некоторое время (375 мсек в среднем).

После проверки корректной работы локальной сети, остаётся проверить работоспособность подключения к Интернету, для этого нужно запустить команду ping в адрес внешнего IP (рисунок 6).

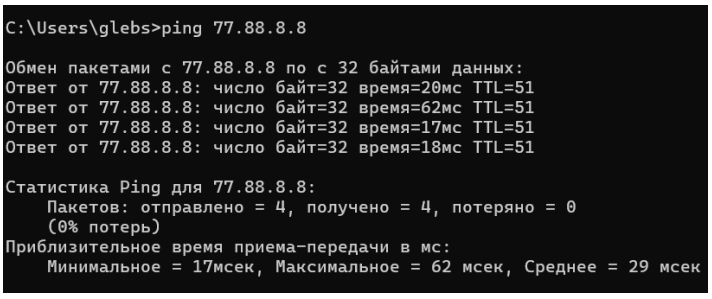


Рисунок 6 – результат работы ping 77.88.8.8

Стоит обратить внимание на параметр TTL, при маршрутизации в Интернете пакет проходит множество хостов, и каждый из них уменьшает этот параметр на единицу. С помощью TTL можно прикинуть, какое количество хостов посетил пакет, перед тем как попасть на адрес назначения.

Команда ping также позволяет менять размеры отправляемых пакетов, увеличение размеров пакетов может быть полезно при тестирование пропускной способности сети. Размер задаётся в байтах, с помощью специального флага -l (рисунок 7).

```
C:\Users\glebs>ping 77.88.8.8 -l 1024

Обмен пакетами с 77.88.8.8 по с 1024 байтами данных:
Ответ от 77.88.8.8: число байт=1024 время=58мс TTL=51
Ответ от 77.88.8.8: число байт=1024 время=19мс TTL=51
Ответ от 77.88.8.8: число байт=1024 время=17мс TTL=51
Ответ от 77.88.8.8: число байт=1024 время=18мс TTL=51

Статистика Ping для 77.88.8.8:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 17мсек, Максимальное = 58 мсек, Среднее = 28 мсек
```

Рисунок 7 – Результат работы ping 77.88.8.8 -l 1024

Таким образом, команда ping позволяет проверить работу сетевого оборудования на устройстве, подключение к локальной сети и к Интернету.

Tracert – утилита, которая позволяет отследить маршрут пакета, на пути к пункту назначения. Достигается это за счёт отправки ICMP пакетов с TTL начиная от 1 и увеличивающемся пока не будет достигнут целевой адрес. Как и с другими утилитами, справку по ней можно получить, применив параметр /? (рисунок 8).

```
C:\Users\glebs>tracert /?

Использование: tracert [-d] [-h максЧисло] [-j списокУзлов] [-w таймаут]
                       [-R] [-S адресИсточника] [-4] [-6] конечноеИмя

Параметры:
    -d                  Без разрешения в имена узлов.
    -h максЧисло        Максимальное число прыжков при поиске узла.
    -j списокУзлов      Свободный выбор маршрута по списку узлов (только IPv4).
    -w таймаут          Таймаут каждого ответа в миллисекундах.
    -R                  Трассировка пути (только IPv6).
    -S адресИсточника   Используемый адрес источника (только IPv6).
    -4                  Принудительное использование IPv4.
    -6                  Принудительное использование IPv6.
```

Рисунок 8 – Результат работы tracert /?

Убедиться, что исходящие пакеты в первую очередь идут на адрес шлюза, можно применив эту утилиту к его адресу (рисунок 9).

```
C:\Users\glebs>tracert 192.168.3.1

Трассировка маршрута к 192.168.3.1 с максимальным числом прыжков 30

  1     4 ms     1 ms     1 ms  192.168.3.1

Трассировка завершена.
```

Рисунок 9 – Результат работы tracert 192.168.3.1.

Как видно из результата работы утилиты, пакеты сразу же идут на шлюз, не посещая никаких промежуточных адресов.

Изучить маршрутизацию пакетов в Интернете, можно применив tracert к внешнему IP адресу (рисунок 10).

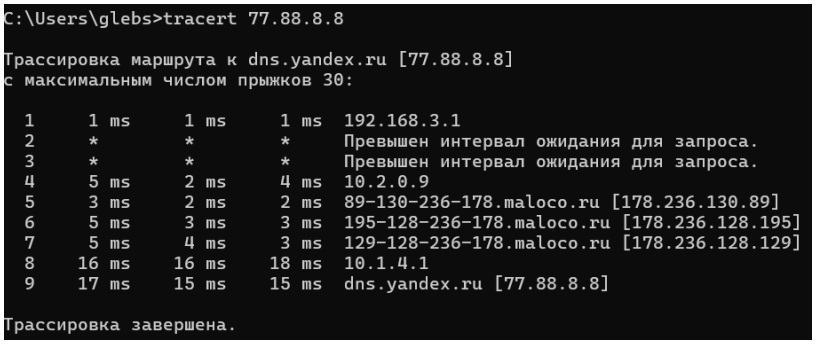


Рисунок 10 – Результат работы tracert 77.88.8.8

К сожалению, не все промежуточные точки раскрывают свои адреса, но общий маршрут отследить всё равно можно. Также легко заметить, что первый хост на пути к назначению – шлюз по умолчанию. Также можно заметить, что по умолчанию мы получаем не только адрес, но и доменное имя промежуточных точек, если же при работе tracert DNS не нужен, его можно отключить специальным флагом -d (рисунок 11).

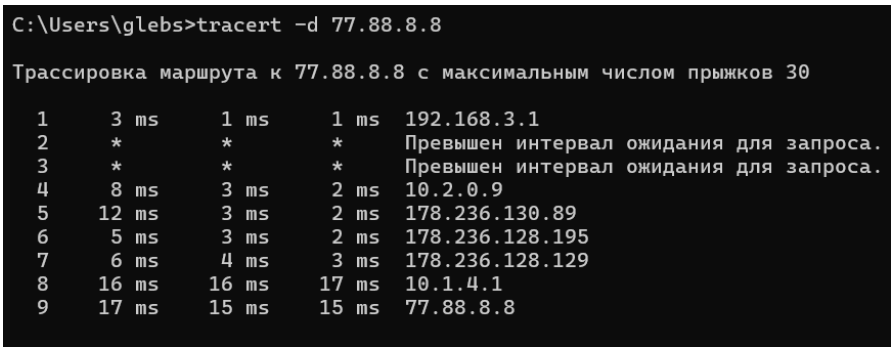


Рисунок 11 – Результат работы tracert -d 77.88.8.8

Протокол ARP существуют для установления соответствия между IP и MAC адресом устройства. На компьютере храниться специальная таблица таких соответствий, доступ к которой можно получить с помощью утилиты arp (рисунок 12).

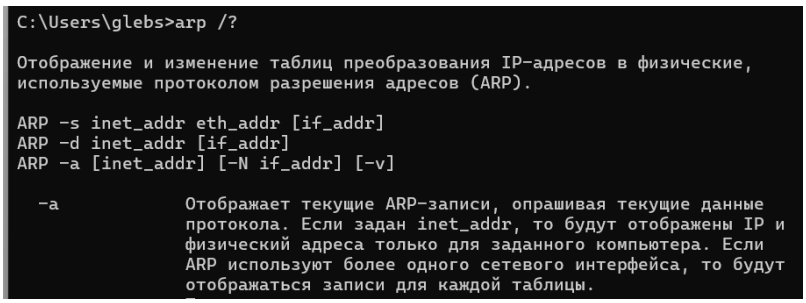


Рисунок 12 – результат работы arp /?

Просмотреть эту таблицу на компьютере, можно с помощью флага -a (рисунок 13).

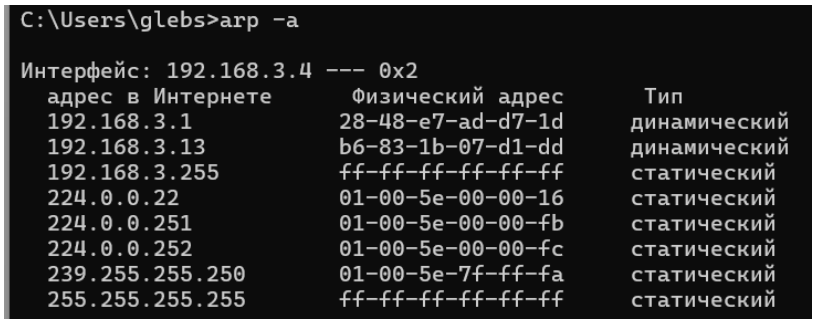


Рисунок 13 – результат работы arp -a

Итак, можно заметить, что на компьютере хранятся MAC адреса только устройств из локальной сети, а также различные зарезервированные под различные протоколы адреса.

Упражнение 2

Для выполнения этого упражнения потребуется программа LanCalculator, поэтому первом делом её необходимо установить (рисунок 14).

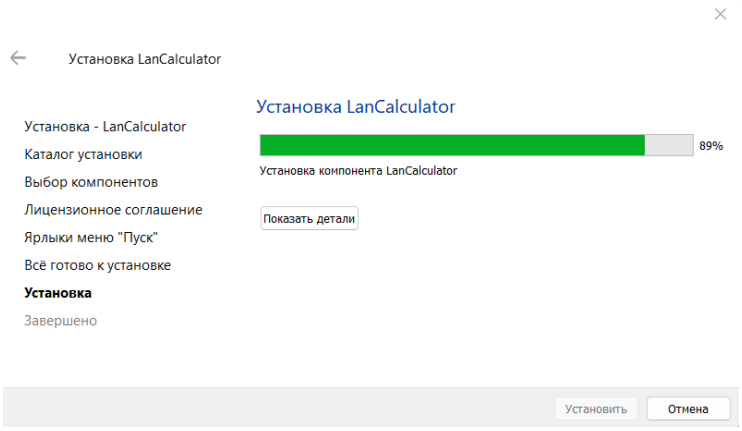
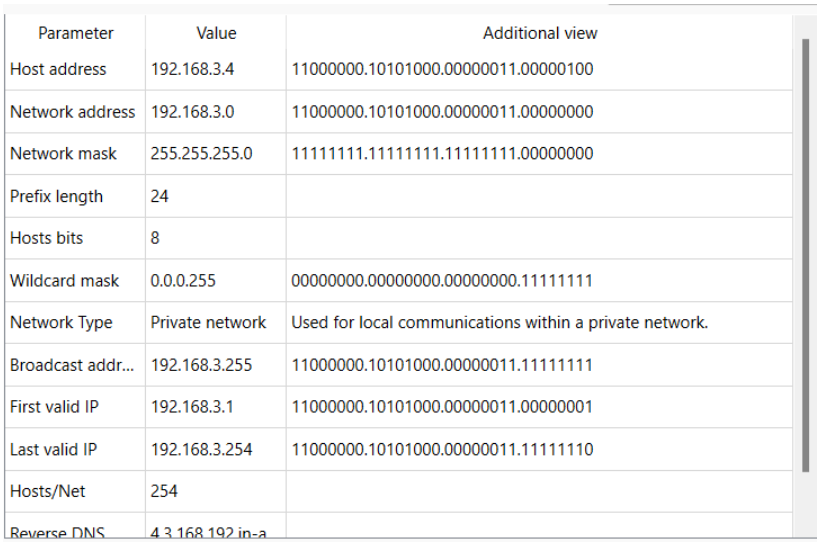


Рисунок 14 – Установка LanCalculator

При запуске, программа отображает информацию о подсети, в которой находится компьютер (рисунок 15).



Parameter	Value	Additional view
Host address	192.168.3.4	11000000.10101000.00000011.00000100
Network address	192.168.3.0	11000000.10101000.00000011.00000000
Network mask	255.255.255.0	11111111.11111111.11111111.00000000
Prefix length	24	
Hosts bits	8	
Wildcard mask	0.0.0.255	00000000.00000000.00000000.11111111
Network Type	Private network	Used for local communications within a private network.
Broadcast addr...	192.168.3.255	11000000.10101000.00000011.11111111
First valid IP	192.168.3.1	11000000.10101000.00000011.00000001
Last valid IP	192.168.3.254	11000000.10101000.00000011.11111110
Hosts/Net	254	
Reverse DNS	4.3.168.192.in-a	

Рисунок 15 – Информация из LanCalculator

С помощью данной программы рассчитаем возможные подсети для заданного числа хостов

Таблица 1 – Распределение IP адресов

Начальный IP адрес	Конечный IP адрес	Маска подсети	Число хостов	CIDR
172.16.0.1	172.16.1.255	255.255.254.0	500	172.16.0.0/23
172.16.0.1	172.16.7.254	255.255.248.0	1023	172.16.0.0/21
192.168.0.1	192.168.0.6	255.255.255.248	5	192.168.0.0/29
192.168.0.1	192.168.0.30	255.255.255.224	29	192.168.0.0/27
172.16.0.1	172.16.15.254	255.255.240.0	3201	172.16.0.0/20
10.0.0.1	10.7.255.254	255.248.0.0	336754	10.0.0.0/13

Упражнение 3

Имя компьютера можно посмотреть в командной строке с помощью команды hostname (рисунок 16).

```
C:\Users\glebs> hostname
Gosya
```

Рисунок 16 – Результат работы hostname

Аналогичную информацию можно получить и в настройках компьютера (рисунок 17).

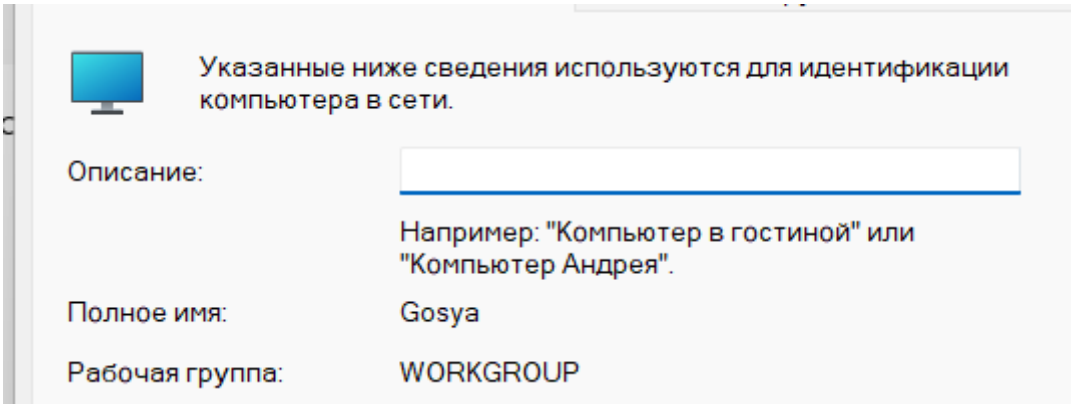


Рисунок 17 – Имя компьютера

Nslookup – утилита позволяющая работать с DNS сервером и получать IP адрес в ответ на имя хоста. Перед использованием утилиты можно получить справку (рисунок 18).

```
> ?
Команды:   (идентификаторы отображаются в верхнем регистре, квадратные скобки "[]" обозначают необязательные параметры)
NAME            - печать сведений об узле или домене NAME с помощью сервера по умолчанию
NAME1 NAME2     - та же операция, но в качестве сервера используется NAME2
help or ?       - печать сведений о стандартных командах
set OPTION      - установить параметр
    all             - печать параметров, текущего сервера и узла
    [no]debug       - печать отладочных сведений
    [no]d2          - печать полных отладочных сведений
    [no]defname     - добавить имя домена ко всем запросам
    [no]recurse     - запрос рекурсивного ответа на запрос
    [no]search      - использовать список поиска доменов
    [no]vc          - всегда использовать виртуальную схему
    domain=NAME     - установить имя домена по умолчанию NAME
    srchlist=N1[/N2/.../N6] - установить домен N1 и список поиска N1,N2 и т.д.
    root=NAME       - установить корневой сервер NAME
    retry=X         - установить число повторов X
    timeout=X       - установить интервал времени ожидания в X секунд
    type=X          - установить тип запроса (пр. A,AAAA,A+AAAA,ANY,CNAME,MX,NS,PTR,SOA,SRV)
    querytype=X     - то же, что и type
    class=X         - установить класс запроса (пр. IN (Internet), ANY)
    [no]msxfr       - использовать быструю зону MS для передачи
    ixfrver=X       - текущая версия, использующаяся в передаче запросов IXFR
server NAME     - установить сервер по умолчанию NAME, используя текущий сервер по умолчанию
lserver NAME    - установить сервер по умолчанию NAME, используя первоначальный сервер
root            - сделать текущий сервер по умолчанию корневым сервером
```

Рисунок 18 – Справка nslookup

Попробуем получить IP адреса имени microsoft.ru (рисунок 19).

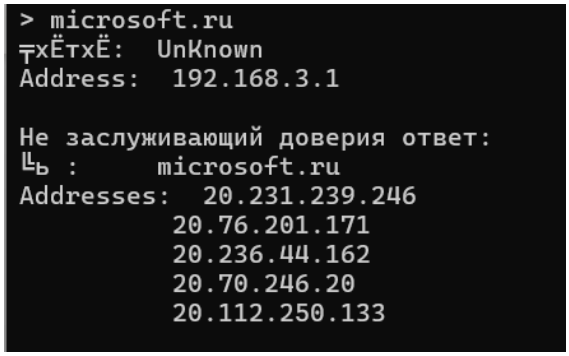


Рисунок 19 – Адреса microsoft.ru

Как видно из рисунка, в качестве DNS сервера используется домашний роутер. Но nslookup поддерживает возможность самостоятельно задать DNS сервер для запроса (рисунок 20).

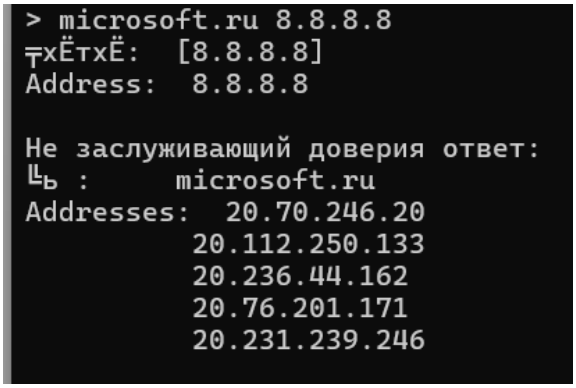


Рисунок 20 – Запрос к DNS серверу Google

Можно заметить, что 2 запроса отличаются лишь порядком адресов, но не содержанием. Наконец, можно дополнительно задать тип DNS запроса. Так, тип MX вернёт список почтовых серверов протокола SMTP, поэтому запрос вида nslookup -type=mx mail.ru >> C:\Users\glebs\q.txt сохранит список таких сервером mail.ru в текстовый файл (рисунок 21).

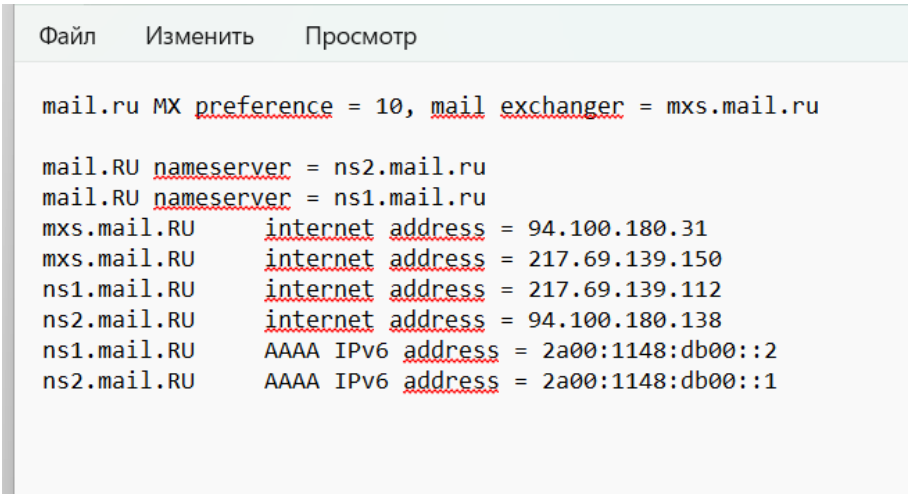


Рисунок 21 – Список SMTP серверов mail.ru

Вывод:

В результате данной работы были изучены базовые утилиты для диагностики сети, проверено собственное подключение к локальной сети и Интернету. А также изучена работа компьютера с DNS серверами и произведён расчёт локальных подсетей для различного числа хостов.

Ответы на контрольные вопросы:

1. Адрес моей локальной сети 192.168.3.0/24, данная сеть принадлежит классу C
2. Маска подсети 24, которая даёт возможность подключить 254 устройства
3. На моём роутере настроен DHCP сервер, поэтому все IP адреса выдаются роутером автоматически
4. Ping на свой адрес поможет выявить неисправность сетевого оборудования устройства или сбой в работе какого-либо протоколов, что не даёт устройству принимать или отправлять пакеты
5. Ping в локальную сеть позволяет удостовериться об успешной отправки пакетов в пределах локальной сети, однако этого не достаточно, чтобы гарантировать работу Интернета
6. Успешная отправка пакетов на внешний адрес говорит о том, что на устройстве есть подключение к Интернету, сетевое оборудование работает исправно, шлюз по умолчанию функционирует и посылает пакеты из локальной сети в Интернет
7. Утилиты ping и tracert используют протокол ICMP специально созданный для тестирования сетей

8. Tracert отлично подходит для того, чтобы определить на каком именно хосту происходит сбой, и таким образом локализировать проблему с сетью
9. Динамические адреса в таблице arp – это адреса локальной сети, заданные динамически с помощью DHCP, а статические – это зарезервированные адреса, которые не мгут измениться ни при каких обстоятельствах
10. Маска представляет из себя 32 битную двоичную последовательность, начинающуюся с единиц, а после первого нуля продолжающуюся исключительно нулями. В этом случае сегмент IP адреса соответствующий единицам будет отвечать за адрес сети, а оставшаяся часть – за адрес хоста.
11. Верно обратное – чем больше маска, тем меньше доступно хостов
12. В моём случае имя компьютера и полное имя совпали
13. FQDN – полное доменное имя, включающее в себя имена всех родительских доменов иерархии DNS
14. DNS в локальной сети, аналогично DNS в Интернете, позволяет обращаться к конкретным хостам по уникальному имени, вместо IP адреса
15. Файл hosts хранит локальную таблицу соответствий имён и IP адресов, именно к нему в первую очередь обращается компьютер перед запросом на DNS сервер.
16. Корневые DNS сервера – несколько ключевых сервером по всему миру, которые принимают запросы от других серверов более низкого уровня и позволяют получить список DNS серверов для любого домена верхнего уровня.
17. Это сообщение означает, что информации об адресах получена не от доменного DNS сервера, являющегося владельцем соответствующей зоны, а из другого источника.