

Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики

Факультет инфокоммуникационных технологий

Направление подготовки 11.03.02

Лабораторная работа №1

«Сетевые протоколы»

Выполнили:

Швалов Даниил Андреевич К34211

Кротова Милена Игоревна К34201

Проверила:

Казанова Полина Петровна

Санкт-Петербург

2024

1. Введение

Цель работы: протестировать устройств в сети, получить навыки работы с программой LanCalculator для расчета ip-адресов, маски подсети, определения количества хостов и имени узла, получить навыки работы с утилитой nslookup.

2. Ход работы

2.1. Тестирование IP-адреса

Были изучены параметры команды `ipconfig /?`, что представлено на рисунке 1.

```
C:\Users\Milena>ipconfig /?
ИСПОЛЬЗОВАНИЕ:
ipconfig [/allcompartments] [/? | /all |
        /renew [адаптер] | /release [адаптер] |
        /renew6 [адаптер] | /release6 [адаптер] |
        /flushdns | /displaydns | /registerdns |
        /showclassid адаптер |
        /setclassid адаптер [идентификатор_класса] |
        /showclassid6 адаптер |
        /setclassid6 адаптер [идентификатор_класса] ]

Здесь
адаптер          Имя подключения (можно использовать знаки подстановки
                  * and ?, см. примеры)

Параметры:
/?              Вывод данного справочного сообщения
/all           Вывод подробных сведений о конфигурации.
/release       Освобождение IPv4-адреса для указанного адаптера.
/release6      Освобождение IPv6-адреса для указанного адаптера.
/renew         Обновление IPv4-адреса для указанного адаптера.
/renew6        Обновление IPv6-адреса для указанного адаптера.
/flushdns      Очистка кэша сопоставителя DNS.
/registerdns   Обновление всех DHCP-аренд и перерегистрация DNS-имен
/displaydns    Отображение содержимого кэша сопоставителя DNS.
/showclassid   Отображение всех допустимых для этого адаптера
               идентификаторов классов DHCP.
/setclassid    Изменение идентификатора класса DHCP.
/showclassid6  Отображение всех допустимых для этого адаптера
               идентификаторов классов DHCP IPv6.
/setclassid6   Изменение идентификатора класса DHCP IPv6.
```

Рисунок 1 – Результат выполнения команды `ipconfig /?`

С помощью команды `ipconfig /all` были определены ip-адрес и маска данного компьютера – 192.168.0.105 и 255.255.255.0. Результат выполнения команды представлен на рисунке 2. Также из результата выполнения предыдущей команды можно выяснить, что шлюз и по совместительству роутер для данного компьютера имеет адрес 192.168.0.1, и главный адрес DNS-сервера так же 192.168.0.1.

```
C:\Users\Milena>ipconfig /all

Настройка протокола IP для Windows

Имя компьютера . . . . . : WIN-6K06P2A3258
Основной DNS-суффикс . . . . . :
Тип узла. . . . . : Гибридный
IP-маршрутизация включена . . . . : Нет
WINS-прокси включен . . . . . : Нет

Адаптер Ethernet Ethernet:

DNS-суффикс подключения . . . . . :
Описание. . . . . : Red Hat VirtIO Ethernet Adapter
Физический адрес. . . . . : 4A-12-9C-6A-B9-DF
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::e086:d907:8f41:a443%6(Основной)
IPv4-адрес. . . . . : 192.168.0.105(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 20 сентября 2024 г. 17:12:27
Срок аренды истекает. . . . . : 21 сентября 2024 г. 17:12:27
Основной шлюз. . . . . : 192.168.0.1
DHCP-сервер. . . . . : 192.168.0.1
IAID DHCPv6 . . . . . : 105517724
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2E-7C-F6-86-4A-12-9C-6A-B9-DF
DNS-серверы. . . . . : 192.168.0.1
                        0.0.0.0
```

Рисунок 2 – Результат выполнения команды `ipconfig /all`

Далее были изучены параметры команды `ping` с помощью команды `ping /?`, результат выполнения данной команды изображен на рисунке 3.

Параметры:	
-t	Проверяет связь с указанным узлом до прекращения. Для отображения статистики и продолжения проверки нажмите клавиши CTRL+BREAK; для прекращения нажмите CTRL+C.
-a	Разрешает адреса в имена узлов.
-n <число>	Число отправляемых запросов проверки связи.
-l <размер>	Размер буфера отправки.
-f	Устанавливает флаг, запрещающий фрагментацию, в пакете (только IPv4).
-i <TTL>	Срок жизни пакетов.
-v <TOS>	Тип службы (только IPv4; этот параметр использовать не рекомендуется, и он не влияет на поле TOS в заголовке IP).
-r <число>	Записывает маршрут для указанного числа прыжков (только IPv4).
-s <число>	Задаёт метку времени для указанного числа прыжков (только IPv4).
-j <список_узлов>	Задаёт свободный выбор маршрута по списку узлов (только IPv4).
-k <список_узлов>	Задаёт жесткий выбор маршрута по списку узлов (только IPv4).
-w <время_ожидания>	Задаёт время ожидания каждого ответа (в миллисекундах).
-R	Использует заголовок маршрута для проверки и обратного маршрута (только IPv6). В соответствии с RFC 5095, использование этого заголовка маршрута не рекомендуется. В некоторых системах запросы проверки связи могут быть сброшены, если используется этот заголовок.
-S <адрес_источника>	Задаёт адрес источника.
-c секция	Идентификатор секции маршрутизации.
-p	Проверяет связь с сетевым адресом поставщика виртуализации Hyper-V.
-4	Задаёт принудительное использование протокола IPv4.
-6	Задаёт принудительное использование протокола IPv6.

Рисунок 3 – Параметры команды ping

Согласно заданию, необходимо было запустить ping на собственный адрес компьютера, результат выполнения данной команды изображен на рисунке 4.

```
C:\Users\Milena>ping 192.168.0.105

Pinging 192.168.0.105 with 32 bytes of data:
Reply from 192.168.0.105: bytes=32 time<1ms TTL=128
Reply from 192.168.0.105: bytes=32 time<1ms TTL=128
Reply from 192.168.0.105: bytes=32 time<1ms TTL=128
Reply from 192.168.0.105: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.105:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 4 – Ping собственного адреса 192.168.0.105

После необходимо было пропинговать адрес партнера в классе. В данный момент им был использован ip-адрес 192.168.0.104, на который был запущен ping, что представлено на рисунке 5.

```
C:\Users\Milena>ping 192.168.0.104

Обмен пакетами с 192.168.0.104 по с 32 байтами данных:
Ответ от 192.168.0.104: число байт=32 время=122мс TTL=64
Ответ от 192.168.0.104: число байт=32 время=28мс TTL=64
Ответ от 192.168.0.104: число байт=32 время=17мс TTL=64
Ответ от 192.168.0.104: число байт=32 время=7мс TTL=64

Статистика Ping для 192.168.0.104:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 7мсек, Максимальное = 122 мсек, Среднее = 43 мсек
```

Рисунок 5 – Ping адреса соседа в той же подсети

Был запущен ping на внешний адрес DNS-сервера Google 8.8.8.8, что показано на рисунке 6.

```
C:\Users\Milena>ping 8.8.8.8

Обмен пакетами с 8.8.8.8 по с 32 байтами данных:
Ответ от 8.8.8.8: число байт=32 время=14мс TTL=108
Ответ от 8.8.8.8: число байт=32 время=10мс TTL=108
Ответ от 8.8.8.8: число байт=32 время=14мс TTL=108

Статистика Ping для 8.8.8.8:
    Пакетов: отправлено = 3, получено = 3, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 10мсек, Максимальное = 14 мсек, Среднее = 12 мсек
```

Рисунок 6 – Результат команды ping на адрес 8.8.8.8

Стандартный размер пакета здесь 32 байта, и для примера с измененным размером пакета была запущена команда ping с параметром -l 64 для отправки пакета с размером 64 байта, что представлено на рисунке 7.

```

C:\Users\Milena>ping -l 64 ya.ru

Обмен пакетами с ya.ru [5.255.255.242] с 64 байтами данных:
Ответ от 5.255.255.242: число байт=64 время=16мс TTL=247
Ответ от 5.255.255.242: число байт=64 время=17мс TTL=247
Ответ от 5.255.255.242: число байт=64 время=19мс TTL=247
Ответ от 5.255.255.242: число байт=64 время=18мс TTL=247

```

Рисунок 7 – Ping с измененным размером пакета

Были изучены основные параметры команды `tracert` с помощью команды `tracert /?`, результат выполнения команды представлен на рисунке 8.

```

C:\Users\Milena>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 – Параметры команды `tracert`

Согласно заданию, был запущен запрос на адрес шлюза 192.168.0.1, результат чего показан на рисунке 9.

```

C:\Users\Milena>tracert 192.168.0.1

Трассировка маршрута к ARCHER_C5 [192.168.0.1]
с максимальным числом прыжков 30:

  1      6 ms      6 ms      4 ms  ARCHER_C5 [192.168.0.1]

Трассировка завершена.

```

Рисунок 9 – Трассировка маршрута до шлюза

Был послан `tracert` запрос на адрес DNS-сервера Yandex 77.88.8.8, также на тот же адрес необходимо было послать запрос, но без обращения к DNS-

серверам, для чего был использован параметр -d. Как видно на рисунке 10, в случае без обращения к DNS- серверам имена адресов не указываются, а только ip-адреса.

```
C:\Users\Milena>tracert 77.88.8.8

Трассировка маршрута к dns.yandex.ru [77.88.8.8]
с максимальным числом прыжков 30:

 1    4 ms    4 ms    4 ms  ARCHER_C5 [192.168.0.1]
 2   104 ms   11 ms   19 ms  dynamicip-109-195-88-57.pppoe.spb.ertelecom.ru [109.195.88.57]
 3    7 ms    8 ms    5 ms  dynamicip-109-195-88-58.pppoe.spb.ertelecom.ru [109.195.88.58]
 4    6 ms    7 ms    6 ms  bbr01.spb.ertelecom.ru [188.234.129.214]
 5   15 ms   36 ms   13 ms  31x131x196x151.static.ertelecom.ru [31.131.196.151]
 6   28 ms   24 ms   23 ms  sas-32z8-lag-1.yndx.net [87.250.239.211]
 7   34 ms   28 ms   29 ms  10.2.8.1
 8   24 ms   25 ms   22 ms  dns.yandex.ru [77.88.8.8]

Трассировка завершена.

C:\Users\Milena>tracert -d 77.88.8.8

Трассировка маршрута к 77.88.8.8 с максимальным числом прыжков 30

 1    4 ms    4 ms   10 ms  192.168.0.1
 2   159 ms   75 ms   51 ms  109.195.88.61
 3    6 ms    5 ms    5 ms  109.195.88.58
 4    7 ms    7 ms    8 ms  188.234.129.214
 5    6 ms   12 ms   11 ms  31.131.196.151
 6   26 ms   22 ms   24 ms  87.250.239.211
 7   24 ms   23 ms   24 ms  10.2.8.1
 8   23 ms   22 ms   22 ms  77.88.8.8
```

Рисунок 10 – Запросы tracert с обращением к DNS-серверам и без

При работе с командой arp сначала были изучены параметры данной команды с помощью arp /?, результат чего показан на рисунке 11.

```
-a          Displays current ARP entries by interrogating the current
           protocol data. If inet_addr is specified, the IP and Physical
           addresses for only the specified computer are displayed. If
           more than one network interface uses ARP, entries for each ARP
           table are displayed.
-g          Same as -a.
-v          Displays current ARP entries in verbose mode. All invalid
           entries and entries on the loop-back interface will be shown.
inet_addr   Specifies an internet address.
-N if_addr  Displays the ARP entries for the network interface specified
           by if_addr.
-d          Deletes the host specified by inet_addr. inet_addr may be
           wildcarded with * to delete all hosts.
-s          Adds the host and associates the Internet address inet_addr
           with the Physical address eth_addr. The Physical address is
           given as 6 hexadecimal bytes separated by hyphens. The entry
           is permanent.
eth_addr    Specifies a physical address.
if_addr     If present, this specifies the Internet address of the
           interface whose address translation table should be modified.
           If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a          .... Displays the arp table.
```

Рисунок 11 – Результат выполнения команды arp /?

2.2. Преобразование двоичного числа в десятичное

Для начала работы была установлена и запущена программа LanCalculator. При запуске программы автоматически показывает настройки компьютера и предварительный расчет с учетом собственного ip-адреса и маски подсети, как представлено на рисунке 12.

IP Address: 192.168.0.105 Protocol: IPv4

Mask: 255.255.255.0 Prefix: /24

Network Subnets

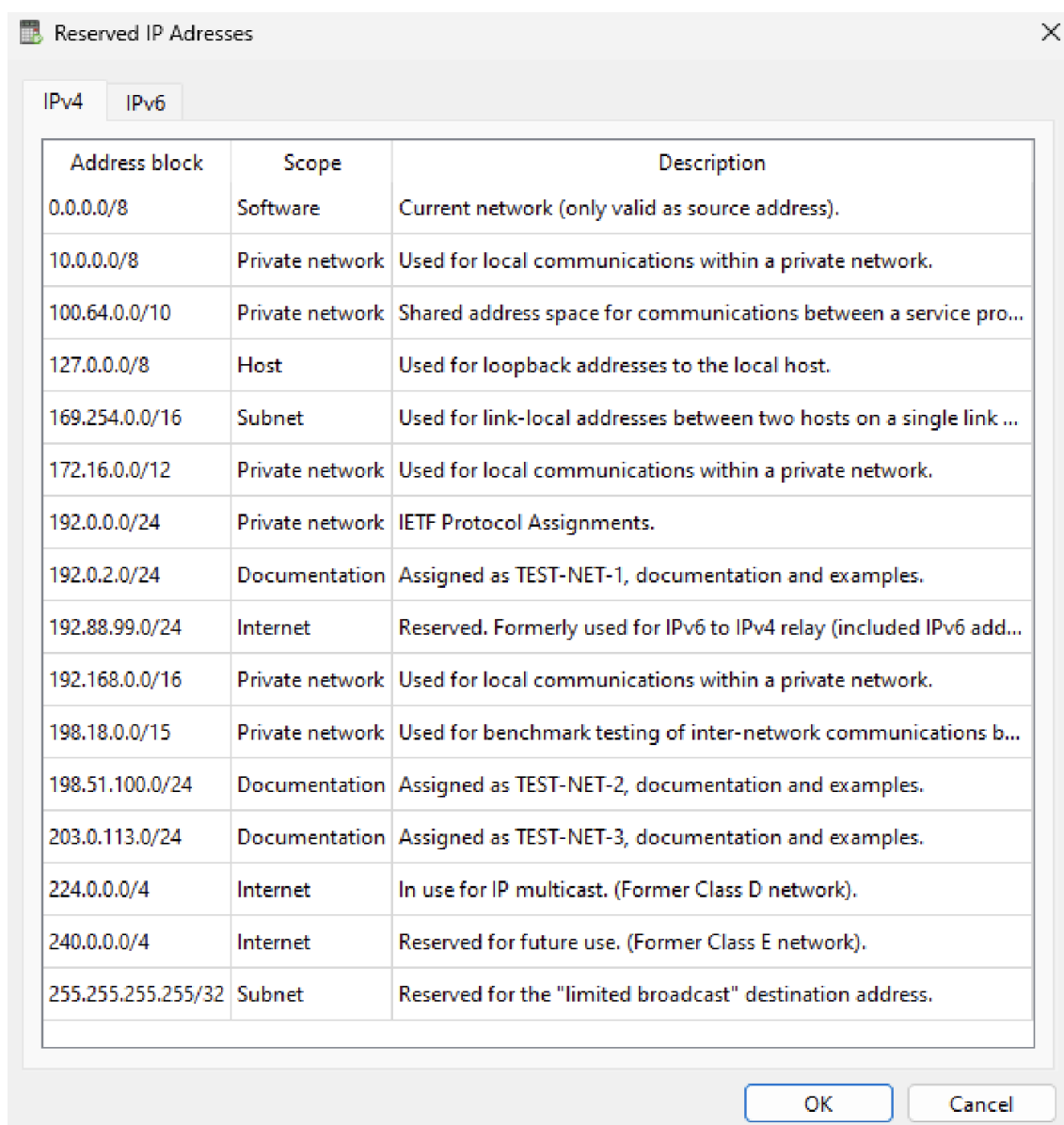
☒ Additional view Delimited Binary

Parameter	Value	Additional view
Host address	192.168.0.105	11000000.10101000.00000000.01101001
Network address	192.168.0.0	11000000.10101000.00000000.00000000
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...	192.168.0.255	11000000.10101000.00000000.11111111
First valid IP	192.168.0.1	11000000.10101000.00000000.00000001
Last valid IP	192.168.0.254	11000000.10101000.00000000.11111110
Hosts/Net	254	
Reverse DNS	105.0.168.192.in-addr.arpa.	

Copy Save Save hosts

Рисунок 12 – Первый запуск программы LanCalculator

Предварительно перед началом работы была просмотрена информация о масках в самой программе для понимания какие частные (private) адреса можно использовать для дальнейшего заполнения таблицы с адресами. Данная таблица с масками и адресами представлена ниже на рисунке 13.



Address block	Scope	Description
0.0.0.0/8	Software	Current network (only valid as source address).
10.0.0.0/8	Private network	Used for local communications within a private network.
100.64.0.0/10	Private network	Shared address space for communications between a service pro...
127.0.0.0/8	Host	Used for loopback addresses to the local host.
169.254.0.0/16	Subnet	Used for link-local addresses between two hosts on a single link ...
172.16.0.0/12	Private network	Used for local communications within a private network.
192.0.0.0/24	Private network	IETF Protocol Assignments.
192.0.2.0/24	Documentation	Assigned as TEST-NET-1, documentation and examples.
192.88.99.0/24	Internet	Reserved. Formerly used for IPv6 to IPv4 relay (included IPv6 add...
192.168.0.0/16	Private network	Used for local communications within a private network.
198.18.0.0/15	Private network	Used for benchmark testing of inter-network communications b...
198.51.100.0/24	Documentation	Assigned as TEST-NET-2, documentation and examples.
203.0.113.0/24	Documentation	Assigned as TEST-NET-3, documentation and examples.
224.0.0.0/4	Internet	In use for IP multicast. (Former Class D network).
240.0.0.0/4	Internet	Reserved for future use. (Former Class E network).
255.255.255.255/32	Subnet	Reserved for the "limited broadcast" destination address.

Рисунок 13 – Таблица с информацией о масках и адресах

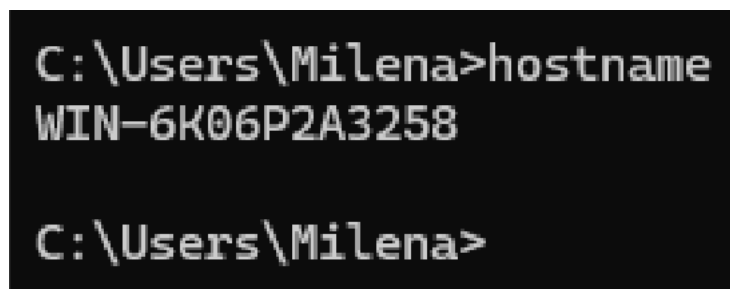
Таблица была заполнена с помощью программы LanCalculator с учетом возможности использования исключительно частных адресов и количества хостов, а также добавлены строки с номерами ИСУ Швалова Даниила и Кротовой Милены – 336729 и 413539, соответственно. Результат представлен в таблице 1.

Таблица 1 – Параметры сети с учетом количества хостов.

Начальный ip-адрес	Конечный ip- адрес	Маска подсети	Число хостов	Идентификатор сети в формате CIDR
192.168.0.1	192.168.1.254	255.255.254.0	500	192.168.0.1/23
192.168.0.1	192.168.7.254	255.255.248.0	1023	192.168.0.0/21
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
192.168.0.1	192.168.15.254	255.255.240.0	3201	192.168.0.0/20
172.16.0.1	172.23.255.254	255.248.0.0	336729	172.16.0.0/13
172.16.0.1	172.23.255.254	255.248.0.0	413539	172.16.0.0/13

2.3. Имя компьютера

С помощью команды `hostname`, запущенной в командной строке, было определено имя данного компьютера – WIN-6K06P2A3258, что показано на рисунке 14.



```

C:\Users\Milena>hostname
WIN-6K06P2A3258

C:\Users\Milena>
  
```

Рисунок 14 – Имя компьютера в командной строке

В Панели управления в Системе так же было определено полное имя компьютера, которое никак не отличается от имени в командной строке, результат представлен на рисунке 15.

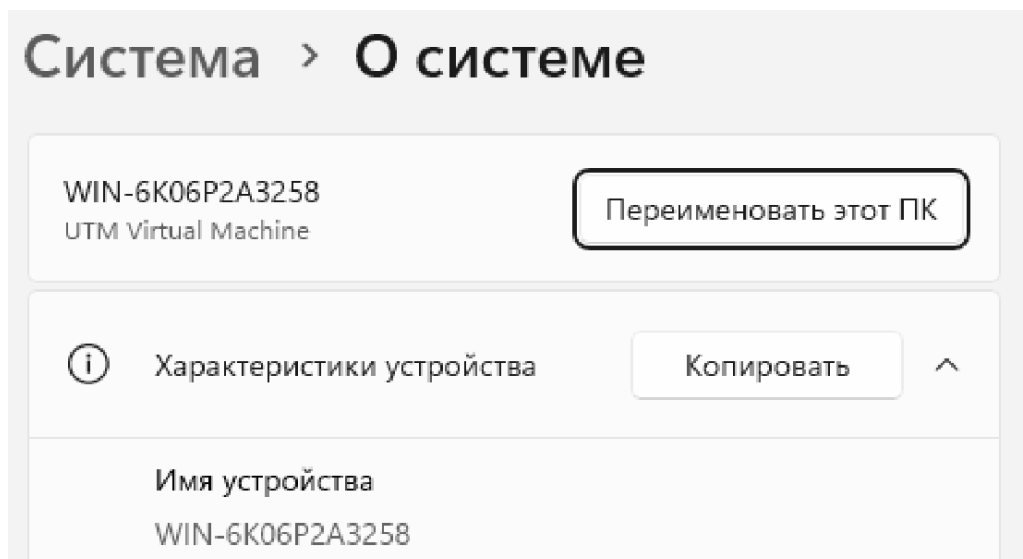


Рисунок 15 – Полное имя компьютера в Панели управления

В командной строке была запущена утилита nslookup в интерактивном режиме, просмотрены ее параметры, представленные на рисунке 16.

```
C:\Users\Milena>nslookup /?
Usage:
  nslookup [-opt ...]           # interactive mode using default server
  nslookup [-opt ...] - server  # interactive mode using 'server'
  nslookup [-opt ...] host      # just look up 'host' using default server
  nslookup [-opt ...] host server # just look up 'host' using 'server'
```

Рисунок 16 – Параметры утилиты nslookup

При первом запуске nslookup пишет DNS-сервер компьютера по умолчанию, что совпадает с тем, который был указан в ipconfig – 192.168.0.1, что так же показано на рисунке 17.

```
C:\Users\Milena>nslookup
Default Server:  UnKnown
Address:  192.168.0.1
```

Рисунок 17 – DNS-сервер по умолчанию

Согласно заданию, был запрошен список ip-адресов для имени microsoft.com. Результат запроса представлен на рисунке 18.

```

C:\Users\Milena>nslookup microsoft.com
Server:   UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:     microsoft.com
Addresses: 2603:1020:201:10::10f
           2603:1010:3:3::5b
           2603:1030:b:3::152
           2603:1030:20e:3::23c
           2603:1030:c02:8::14
           20.76.201.171
           20.70.246.20
           20.236.44.162
           20.112.250.133
           20.231.239.246

```

Рисунок 18 – Список ip-адресов для имени Microsoft.com

Далее необходимо было определить адреса для имени microsoft.com, но с помощью DNS-сервера Google 8.8.8.8 вместо сервера по умолчанию. Результат сохранен в файле res1.txt, что показано на рисунке 19.

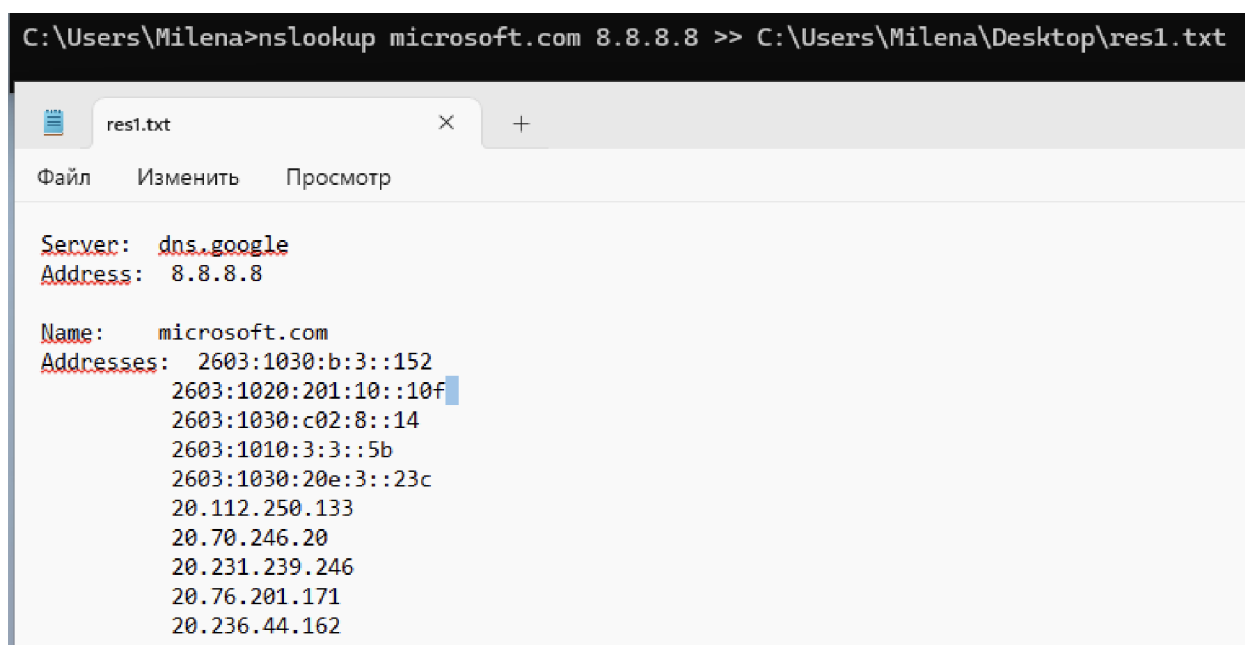
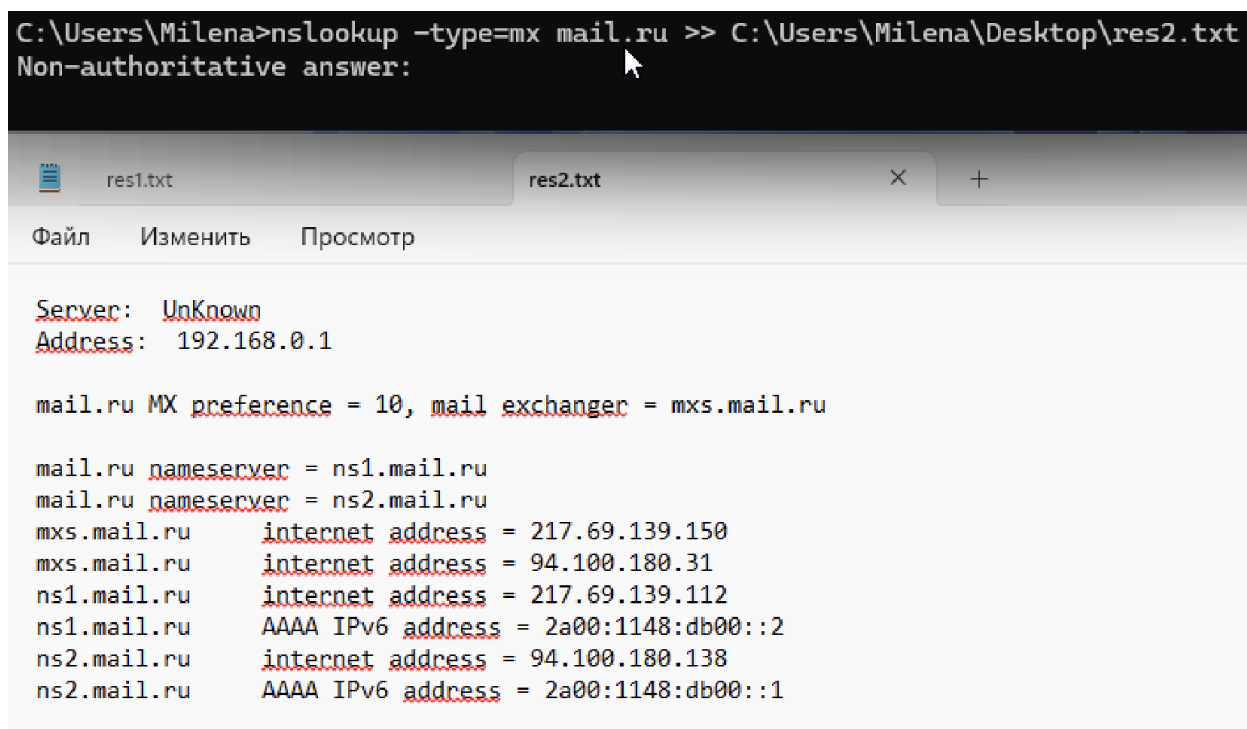


Рисунок 19 – Сохранение в файл адресов microsoft.com, собранных dns-сервером Google 8.8.8.8

После этого таким же образом нужно было запросить список почтовых серверов для домена mail.ru и перенаправить это в файл. Результат запроса представлен на рисунке 20.



```
C:\Users\Milena>nslookup -type=mx mail.ru >> C:\Users\Milena\Desktop\res2.txt
Non-authoritative answer:

Server: UnKnown
Address: 192.168.0.1

mail.ru MX preference = 10, mail exchanger = mxs.mail.ru

mail.ru nameserver = ns1.mail.ru
mail.ru nameserver = ns2.mail.ru
mxs.mail.ru internet address = 217.69.139.150
mxs.mail.ru internet address = 94.100.180.31
ns1.mail.ru internet address = 217.69.139.112
ns1.mail.ru AAAA IPv6 address = 2a00:1148:db00::2
ns2.mail.ru internet address = 94.100.180.138
ns2.mail.ru AAAA IPv6 address = 2a00:1148:db00::1
```

Рисунок 20 – Результат запроса nslookup -type=mx mail.ru >> c:\users\desktop\res2.txt

3. Ответы на вопросы

1) К какому классу сети относится ip-адрес вашего компьютера?

IP-адрес 192.168.0.105 относится к классу C, так как маска сети 255.255.255.0.

2) Какое максимальное количество компьютеров в данном сегменте сети?

Максимальное количество компьютеров в данном сегменте будет составлять 254 с учетом, что первый и последний адреса — служебные.

3) Каким образом назначен ip-адрес вашего компьютера?

Его назначил DHCP-сервер, которым представлен роутер.

4) Какие ошибки в настройке может выявить ping на свой

собственный адрес?

Неправильная настройка брандмауэра или существование компьютера с таким же ip-адресом в сети (из-за чего возникает коллизия)

5) Что показывает успешная отправка пакетов с помощью команды ping на адрес партнера?

Что компьютер подключен к сети, партнер тоже, у него разрешено получение icmp пакетов в брандмауэре, роутер видит оба компьютера и успешно их направляет.

6) О чём говорит успешная/не успешная отправка пакетов с помощью команды ping на внешний адрес?

Что доступ в интернет есть или его нет по той или иной причине (в том числе проблемы с настройкой динамического адреса у сервера или клиента, неправильная настройка брандмауэра или что-то еще).

7) Какой протокол используется для отправки запросов с помощью команд ping и tracert?

ICMP протокол.

8) В каких случаях для выявления неполадок в локальной сети можно использовать команду tracert?

При проблемах работы маршрутизатора/коммутатора (или если мы пускаем пакеты через какую-то машину, то может быть не включен forwarding или неправильно настроена iptables) и пакеты не достигая точки назначения теряются и/или время ожидания истекает.

9) Почему при запуске команды arp -а отображаются динамические и статические записи?

ARP-таблица пополняется за счет поступающих на интерфейс ARP-ответов и в результате извлечения полезной информации из широковещательных ARP-запросов.

10) Как представлена маска в двоичном представлении ip-адреса?

Вместо десятичных чисел от 0 до 255 маска представлена нулями и единицами (32-битное число), где нули показывают, где находится номер хоста, а единицы — номер сети, причем единицы всегда слева, а нули справа.

11) Верно ли утверждение: чем больше маска, тем больше хостов?

Неверно, наоборот — чем больше маска, тем меньше хостов.

12) Чем отличаются имя компьютера и полное имя?

Полное имя компьютера — объединение имени узла и DNS-имени домена, необходимое для идентификации компьютера в сети. Если компьютер не имеет отношения к какому-либо домену, то его имя и полное имя будут одинаковы.

13) Что такое FQDN?

Полное доменное имя (полное имя компьютера или хостинга), которое включает в себя всех родительских доменов иерархии DNS. Представляет собой уникальную текстовую метку, которая позволяет однозначно идентифицировать ресурс в сети и выглядит примерно таким образом:

<Имя хоста>.<Поддомен>.<Домен второго уровня>.<Домен верхнего уровня>.<Корневой домен>

14) Для чего используется DNS-имя компьютера в локальной сети?

Для удобства работы человека, так как намного проще запоминать и работать с названиями, а не с ip-адресами.

15) Когда и для чего используется файл hosts?

Он работает как локальный DNS-сервер и нужен в случаях, когда пользователь хочет локально разработать сайт, чтобы удобно было обращаться, для блокировки сайтов (перенаправления) или решения DNS-проблем. Также для удобного направления запросов на компьютеры в локальной сети.

16) Что такое и когда используются корневые DNS-сервера?

Корневой сервер отвечает на самые первые вопросы в цепочке операций, конечной целью которой является преобразование доменных имен в адреса

интернет-протокола (IP) или другие данные, которые используются для работы Интернета. В основном используются, когда сайты только созданы, далее все запросы приходят к серверам «ниже».

17) При работе с утилитой nslookup на экране отображается «Не заслуживающий доверия ответ: (Non-authoritative answer:)— что он означает?

Сообщение "Не заслуживающий доверия ответ:" (Non-authoritative answer:) говорит о том, что выполняющий запрос DNS-сервер, не является владельцем зоны запрашиваемого ресурса, то есть записей о запрашиваемом отсутствуют в его базе и запрос был передан другому DNS-серверу.

4. Вывод

В ходе выполнения лабораторной работы отработаны команды по тестированию связи устройств в сети, получены навыки работы с программой LanCalculator для расчета ip-адреса, маски подсети, определения количества хостов, определено имя узла, получены навыки работы с утилитой nslookup.