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

# 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.

# Ход работы

# Тестирование IP-адреса

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

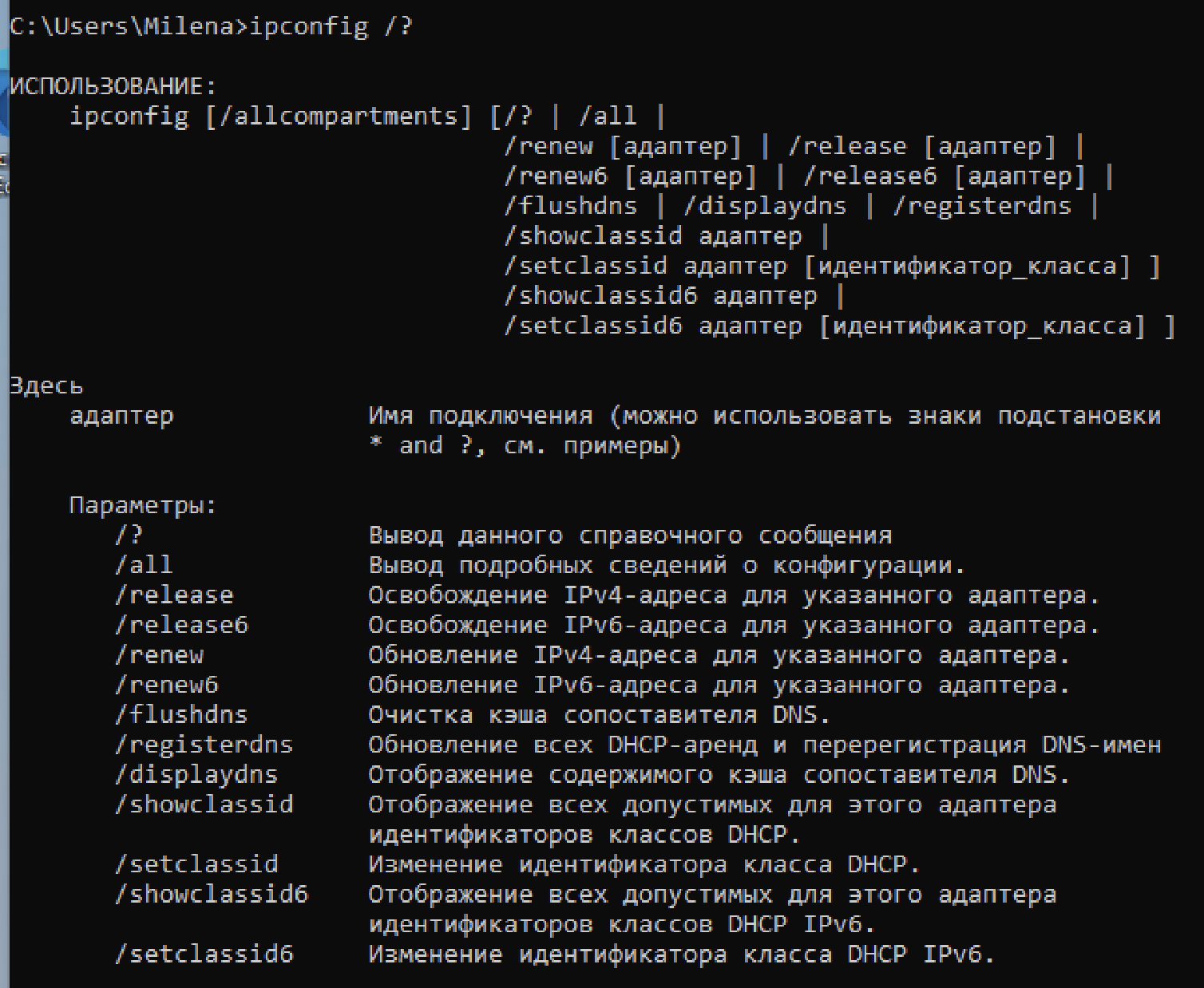


Рисунок 1 – Результат выполнения команды ipconfig /?

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.

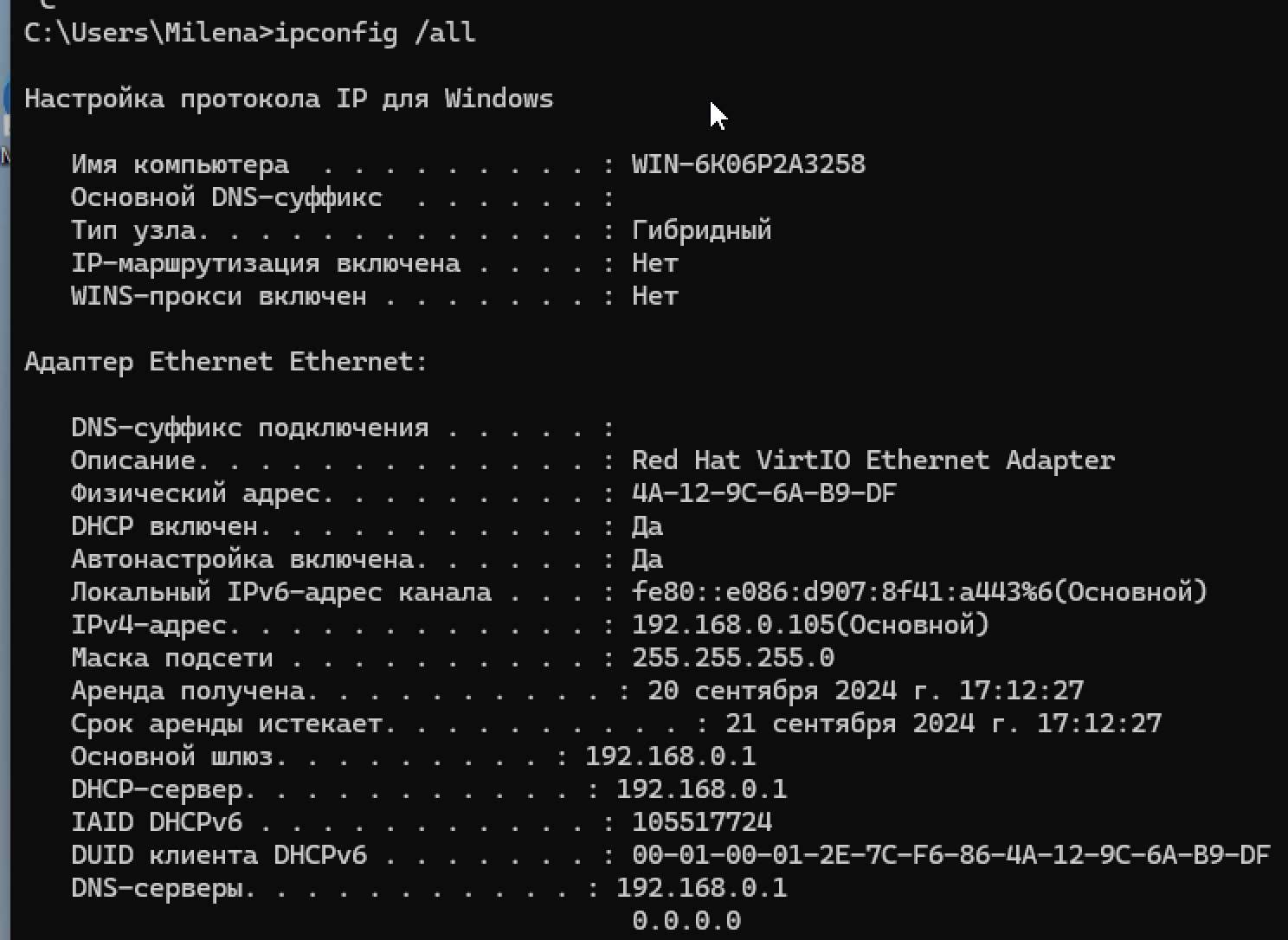


Рисунок 2 – Результат выполнения команды ipconfig /all

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

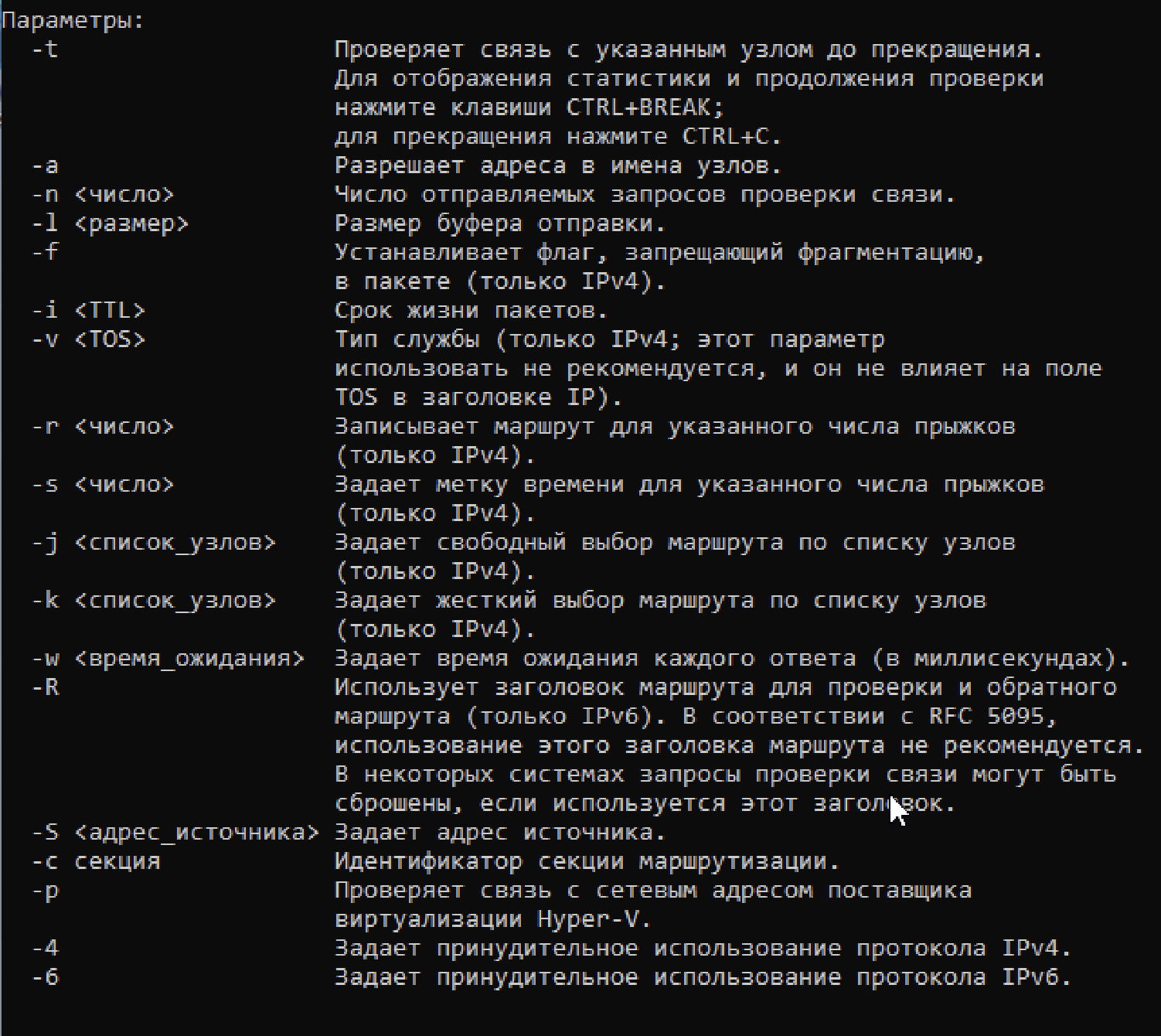


Рисунок 3 – Параметры команды ping

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

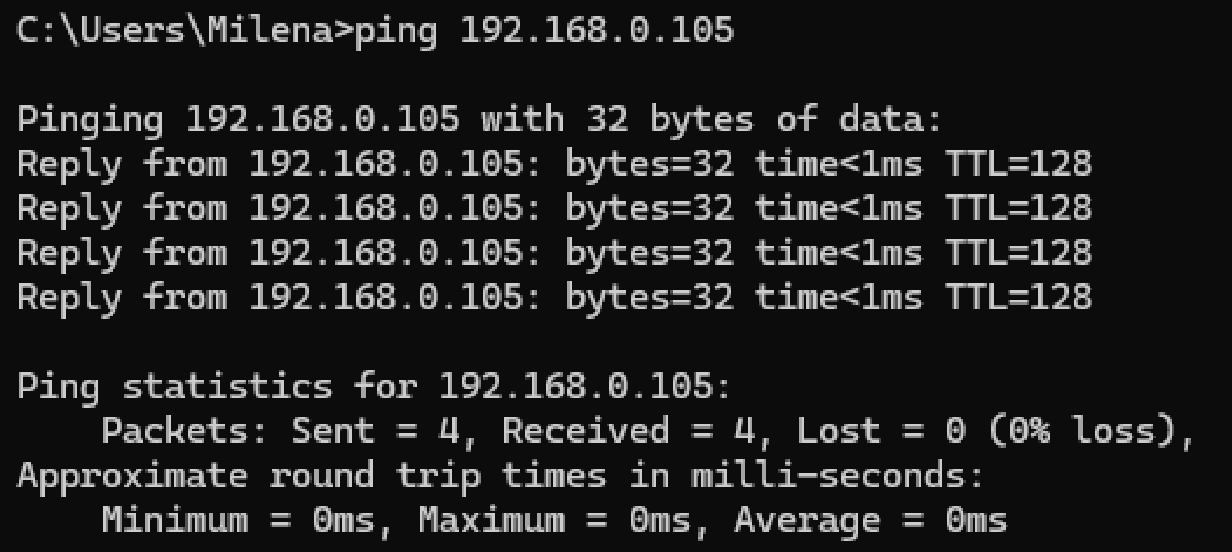


Рисунок 4 – Ping собственного адреса 192.168.0.105

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.

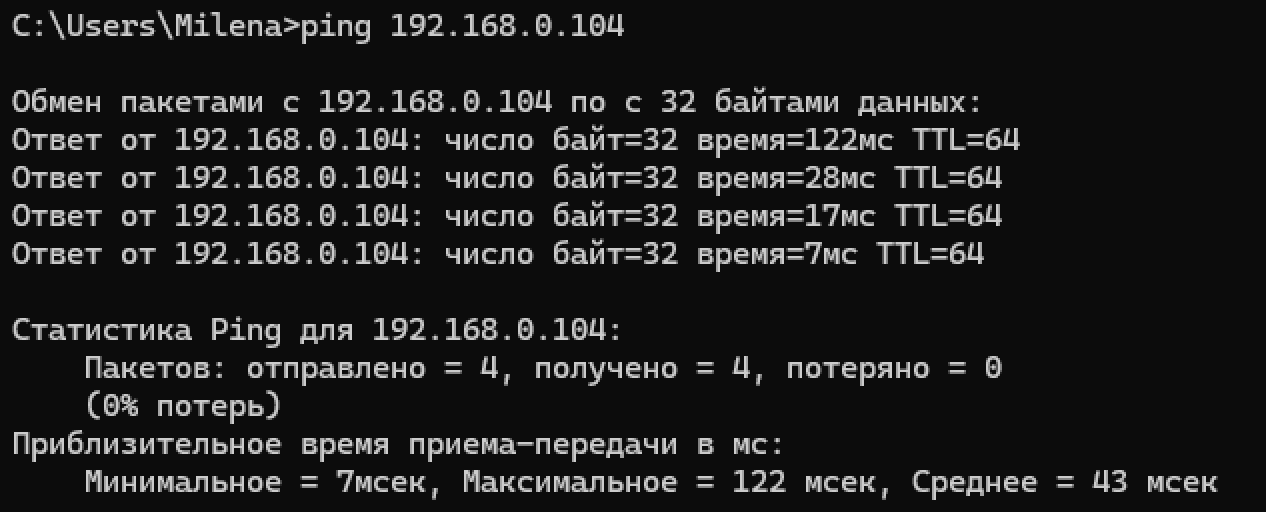


Рисунок 5 – Ping адреса соседа в той же подсети

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

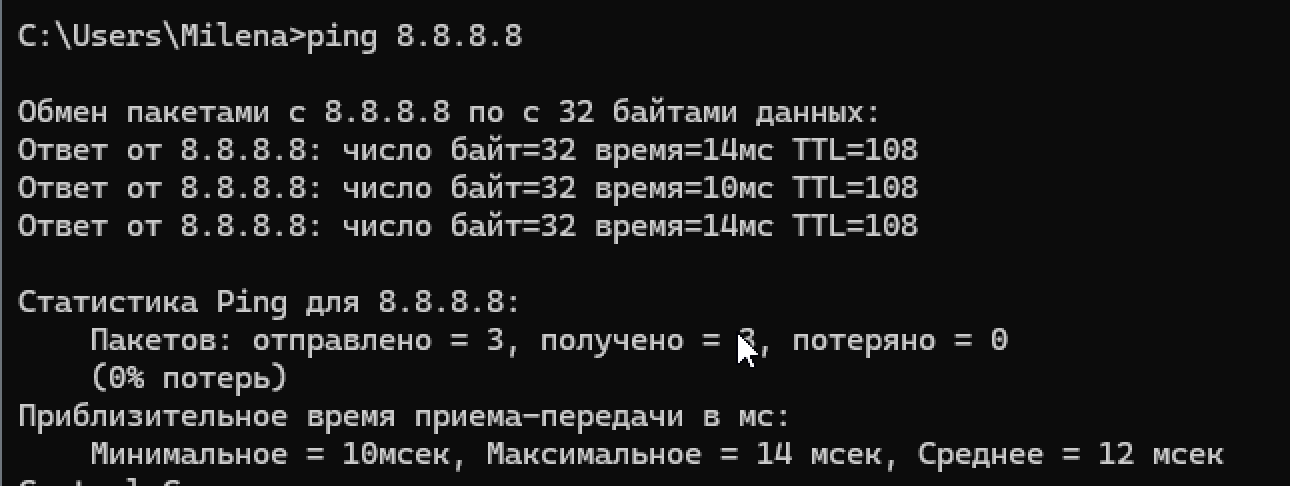


Рисунок 6 – Результат команды ping на адрес 8.8.8.8

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

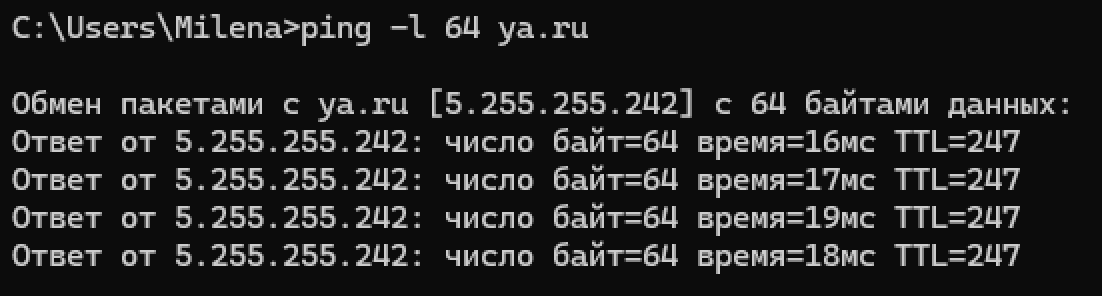


Рисунок 7 – Ping с измененным размером пакета

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

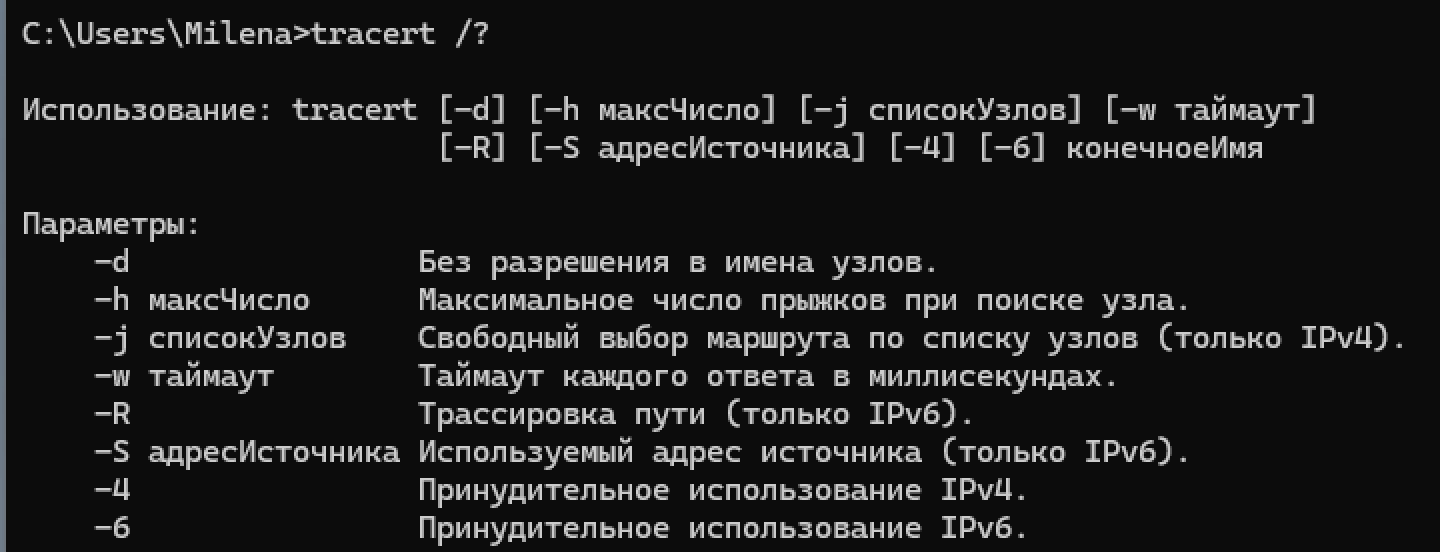


Рисунок 8 – Параметры команды tracert

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

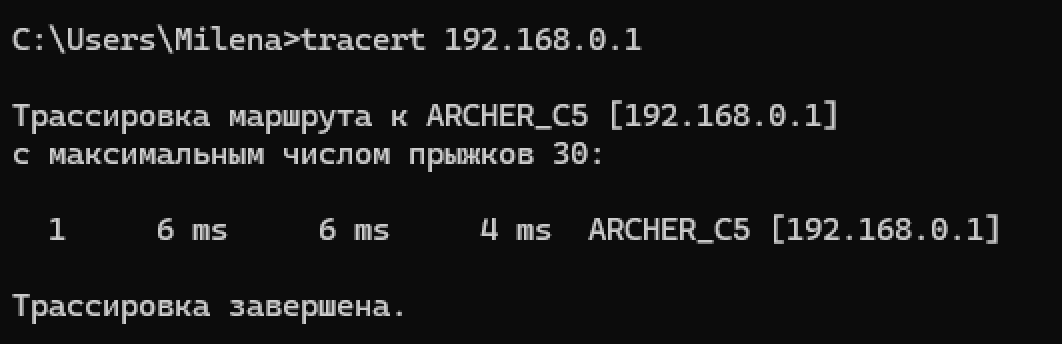


Рисунок 9 – Трассировка маршрута до шлюза

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 видено на рисунке 10, в случае без обращения к DNS- серверам имена адресов не указываются, а только ip-адреса.

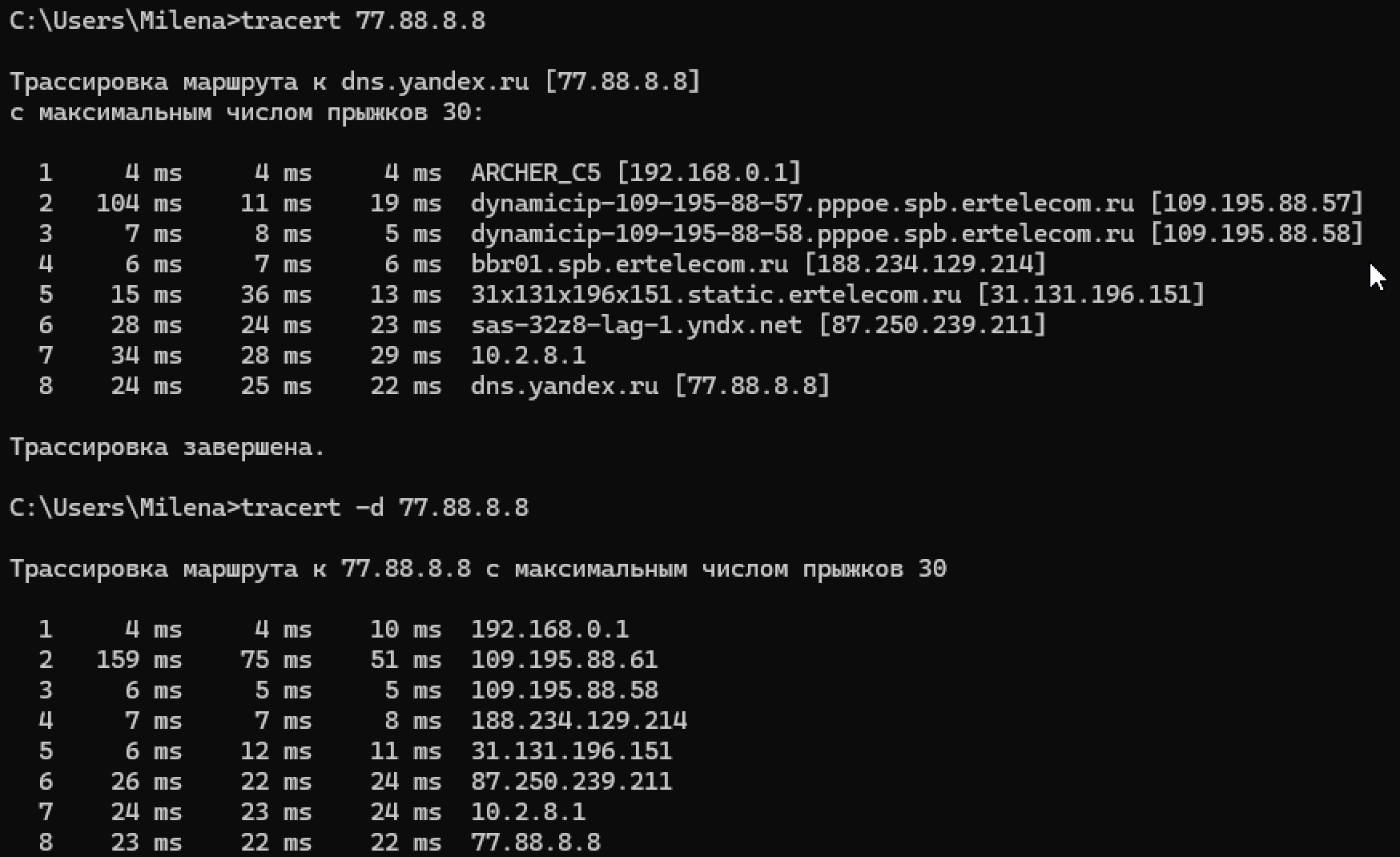


Рисунок 10 – Запросы tracert с обращением к DNS-серверам и без

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

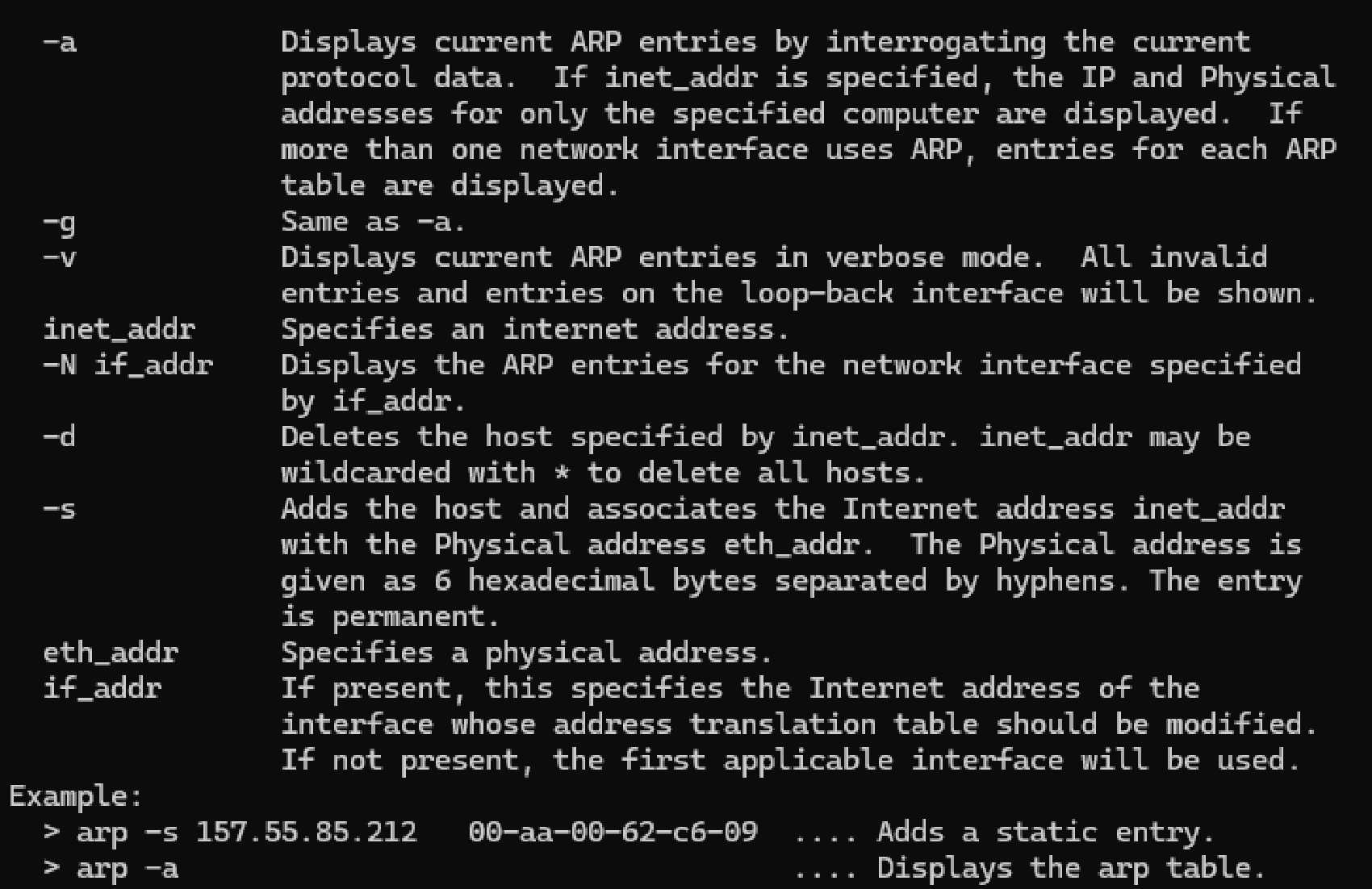


Рисунок 11 – Результат выполнения команды arp /?

# 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-адресы и маски подсети, как представлено на рисунке 12.

# 

# Рисунок 12 – Первый запуск порграммы 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 адресам. Данная таблица с масками и адресами представлена ниже на рисунке 13.

# 

# 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 |

# Имя компьютера

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

# 

# 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.

# 

# 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.

# 

# Рисунок 17 – DNS-сервер по умолчанию

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

# 

# 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.

# 

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

# Ответы на вопросы

# К какому классу сети относится ip-адрес вашего компьютера?

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

# 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.

# Каким образом назначен ip-адрес вашего компьютера?

# Его назначил DHCP-сервер, которым представлен роутер.

# 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)

# 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.

# 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).

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

# ICMP протокол.

# 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.

# Почему при запуске команды arp -a 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.

# 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.

# Верно ли утверждение: чем больше маска, тем больше хостов?

# Неверно, наоборот – чем больше маска, тем меньше хостов.

# 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.

# 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>

# 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.

# 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.

# 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».

# 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.

# 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.