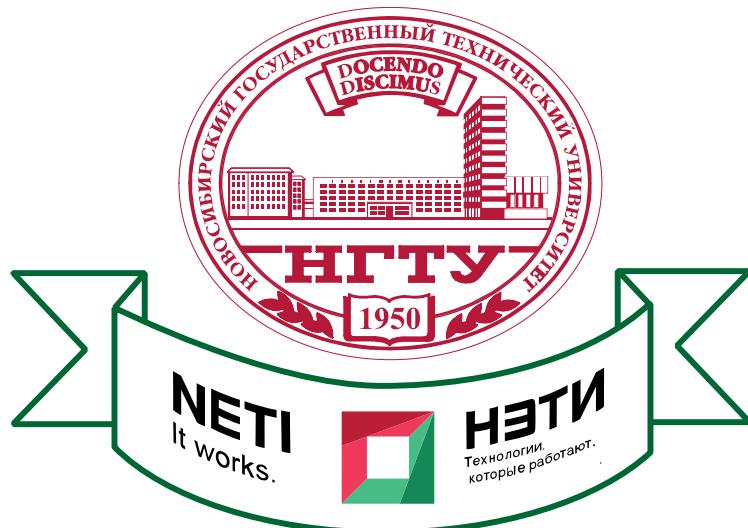


Министерство науки и высшего образования  
Российской Федерации

Федеральное государственное бюджетное  
образовательное учреждение высшего образования

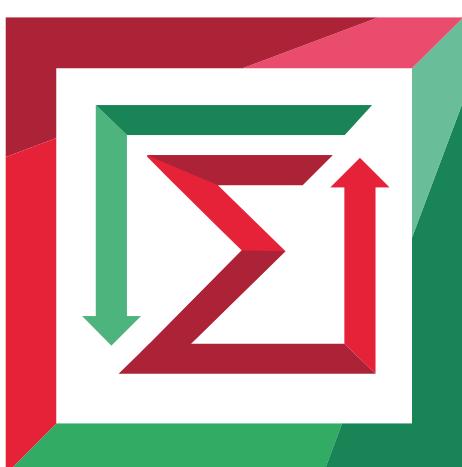
«НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»



Теоретической и прикладной математики

Лабораторная работа № 5  
по дисциплине «Операционные системы, среды и оболочки»

### Анализ функционирования и диагностика IP-сетей



Факультет: ПМИ  
Группа: ПМИ-02  
Вариант: 6  
Студент: Сидоров Даниил,  
Дюков Богдан  
Преподаватель: Кобылянский Валерий Григорьевич,  
Филиппова Елена Владимировна

Новосибирск

2026

## 1. Цель работы

Приобретение практических навыков работы с сетевыми командами операционных систем Windows и Linux, предназначенными для анализа и диагностики сетей TCP/IP, а также со средствами интерактивной диагностики сетей.

## 2. Ход работы для 1-го этапа

- Подключились с помощью клиента Putty к серверу **fpm2.ami.nstu.ru** и с помощью команды **uname** получили полную информацию об установленной операционной системе и аппаратной платформе.

```
[pmi-b0706@students ~]$ uname -a
Linux students.ami.nstu.ru 3.10.0-327.3.1.e17.x86_64 #1 SMP Wed Dec 9 14:09:15 UTC 2015 x86_64 x86_64
x86_64 GNU/Linux
[pmi-b0706@students ~]$ █
```

Linux – имя ядра

Students.ami.nstu.ru – имя машины в сети

3.10.0-327.3.1.e17.x86\_64 – номер выпуска ОС

#1 SMP Wed Dec 9 14.09.15 UTC 2015 – версия ядра

x86\_64 – тип оборудования машины

x86\_64 – тип процессора

x86\_64 – тип аппаратной платформы

GNU/Linux – имя ОС

- Получили статистику по сетевым интерфейсам РК и сервера **fpm2.ami.nstu.ru**.

```
[pmi-b0706@students ~]$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 217.71.130.131 netmask 255.255.255.128 broadcast 217.71.130.255
        inet6 fe80::215:5dff:fe82:8d01 prefixlen 64 scopeid 0x20<link>
          ether 00:15:5d:82:8d:01 txqueuelen 1000 (Ethernet)
            RX packets 49975733 bytes 9265496226 (8.6 GiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 18427929 bytes 7251932422 (6.7 GiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 0 (Local Loopback)
            RX packets 34330274 bytes 16011490897 (14.9 GiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 34330274 bytes 16011490897 (14.9 GiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
      inet 192.168.122.1 netmask 255.255.255.0 broadcast 192.168.122.255
        ether 52:54:00:d4:60:b6 txqueuelen 0 (Ethernet)
          RX packets 0 bytes 0 (0.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 0 bytes 0 (0.0 B)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[pmi-b0706@students ~]$ █
```

### 3 сетевых интерфейса:

- 1) Адрес виртуального интернет порта.
  - 2) Петлевой адрес.
  - 3) Виртуальным мост.

Для каждого интерфейса указываются физические и сетевые адреса (ether, inet, inet6), маска сети (netmask), максимальный размер кадра (MTU), число принятых и переданных пакетов (RX packets, TX packets).

C:\Users\ПК>ipconfig /all

## Настройка протокола IP для Windows

Имя компьютера . . . . . : DESKTOP-MDKFVDK  
Основной DNS-суффикс . . . . .  
Тип узла . . . . . : Гибридный  
IP-маршрутизация включена . . . . . : Нет  
WINS-прокси включен . . . . . : Нет

Неизвестный адаптер Подключение по локальной сети:

Состояние среды . . . . . : Среда передачи недоступна.  
DNS-суффикс подключения . . . . . :  
Описание . . . . . : Kaspersky VPN  
Физический адрес . . . . . :  
DHCP включен . . . . . : Нет  
Автонастройка включена . . . . . : Да

### Адаптер Ethernet Ethernet:

```
DNS-суффикс подключения . . . . . : 
Описание. . . . . : Realtek Gaming 2.5GbE Family Controller
Физический адрес. . . . . : 18-C0-4D-DE-3B-71
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . . : fe80::610a:1856:29f6:49f8%6(Основной)
IPv4-адрес. . . . . : 192.168.0.157(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 10 ноября 2022 г. 18:18:04
Срок аренды истекает. . . . . : 10 ноября 2022 г. 20:18:04
Основной шлюз. . . . . : 192.168.0.1
DHCP-сервер. . . . . : 192.168.0.1
IAID DHCPv6 . . . . . : 85508173
DUID клиента DHCPv6 . . . . . : 00-01-00-01-29-5B-67-8B-18-C0-4D-DE-3B-71
DNS-серверы. . . . . : 192.168.0.1
NetBIOS через TCP/IP. . . . . : Включен
```

Локальный IPv4-адрес маршрутизатора 192.168.0.157

MAC-адрес маршрутизатора 18-C0-4D-DE-3B-71

Маска подсети: 255.255.255.0

Основной шлюз: 192.168.0.1 и прочее.

3. Просмотрели содержимое DNS-кэша, очистили кэш.

```
C:\Users\dansy>ipconfig /displaydns
```

Настройка протокола IP для Windows

```
s332myt.storage.yandex.net
-----
Имя записи. . . . . : s332myt.storage.yandex.net
Тип записи. . . . . : 1
Срок жизни. . . . . : 268
Длина данных. . . . . : 4
Раздел. . . . . . . : Ответ
А-запись (узла) . . . : 213.180.200.61
```

```
avatars.yandex.net
-----
Имя записи. . . . . : avatars.yandex.net
Тип записи. . . . . : 1
Срок жизни. . . . . : 359
Длина данных. . . . . : 4
Раздел. . . . . . . : Ответ
А-запись (узла) . . . : 87.250.247.183
```

```
Имя записи. . . . . : avatars.yandex.net
Тип записи. . . . . : 1
Срок жизни. . . . . : 359
Длина данных. . . . . : 4
Раздел. . . . . . . : Ответ
А-запись (узла) . . . : 87.250.247.184
```

```
Имя записи. . . . . : avatars.yandex.net
Тип записи. . . . . : 1
Срок жизни. . . . . : 359
Длина данных. . . . . : 4
Раздел. . . . . . . : Ответ
А-запись (узла) . . . : 87.250.247.181
```

```
Имя записи. . . . . : avatars.yandex.net
Тип записи. . . . . : 1
Срок жизни. . . . . : 359
Длина данных. . . . . : 4
Раздел. . . . . . . : Ответ
А-запись (узла) . . . : 87.250.247.182
```

```
services.gfe.nvidia.com
-----
Имя записи. . . . . : services.gfe.nvidia.com
Тип записи. . . . . : 5
Срок жизни. . . . . : 213
Длина данных. . . . . : 8
Раздел. . . . . . . . : Ответ
CNAME-запись. . . . . : cs1137.wpc.ea55a.phicdn.net
```

```
Имя записи. . . . . : cs1137.wpc.ea55a.phicdn.net
Тип записи. . . . . : 5
Срок жизни. . . . . : 213
Длина данных. . . . . : 8
Раздел. . . . . . . . : Ответ
CNAME-запись. . . . . : cs1137261584.wpc.phicdn.net
```

```
Имя записи. . . . . : cs1137261584.wpc.phicdn.net
Тип записи. . . . . : 1
Срок жизни. . . . . : 213
Длина данных. . . . . : 4
Раздел. . . . . . . . : Ответ
A-запись (узла) . . . . : 152.199.20.80
```

В состав DNS-записи входят следующие поля:

**Имя записи-** Определяет домен, к которому относится (привязана) данная ресурсная запись.

**Тип записи-** Указывает на тип (назначение) данной ресурсной записи.

**Срок жизни-** время жизни (хранения) DNS-записи в кэше DNS-сервера.

**Длина данных-** длина поля данных

**Class (Класс)**. Здесь указывается тип рабочей сети. Теоретически, система может работать во всех ее типах. Но, TCP/IP сети — самые распространенные. Поэтому, поле редко используется.

### **Наиболее важные типы записей:**

**A-запись-** Address record указывает на конкретный IP-адрес домена. Без нее сайт работать не будет. По этой записи система определяет к какому серверу обращаться за получением информации, когда пользователь вводит название сайта в адресную строку веб-браузера.

Например, запрос A-записи на имя refferrals.icann.org вернет его IPv4 адрес 192.0.34.164

**AAAA запись DNS** — аналог предыдущей A-записи. В значении указывается внешний IP-адрес в формате IPv6.

**MX-запись** задает почтовый сервер, который будет принимать и отправлять почту для данного домена. Запись может указывать на внутренний или внешний почтовый сервер.

**CNAME-запись**- CNAME («каноническое имя») указывает на расположение хостов на одном сервере. С ее помощью, можно прописать несколько доменов и поддоменов в рамках одного сервера. Используется для перенаправления на другое имя.

### Очистили кэш DNS:

```
C:\Users\danys>ipconfig /flushdns  
Настройка протокола IP для Windows  
Кэш сопоставителя DNS успешно очищен.  
...
```

4. Просмотрели содержимое ARP-таблицы, пояснили характеристики записей, выполнили добавление и удаление статических записей.

```
C:\Users\danys>arp -a  
  
Интерфейс: 26.70.89.129 --- 0xe  
адрес в Интернете   Физический адрес      Тип  
26.0.0.1           02-00-00-00-51-00    динамический  
26.255.255.255    ff-ff-ff-ff-ff-ff    статический  
224.0.0.22         01-00-5e-00-00-16    статический  
224.0.0.251        01-00-5e-00-00-fb    статический  
224.0.0.252        01-00-5e-00-00-fc    статический  
239.255.255.250   01-00-5e-7f-ff-fa    статический  
  
Интерфейс: 192.168.0.5 --- 0x13  
адрес в Интернете   Физический адрес      Тип  
192.168.0.1         e8-28-c1-ee-da-48    динамический  
192.168.0.255       ff-ff-ff-ff-ff-ff    статический  
224.0.0.22         01-00-5e-00-00-16    статический  
224.0.0.251        01-00-5e-00-00-fb    статический  
224.0.0.252        01-00-5e-00-00-fc    статический  
224.0.0.253        01-00-5e-00-00-fd    статический  
239.255.255.250   01-00-5e-7f-ff-fa    статический  
255.255.255.255   ff-ff-ff-ff-ff-ff    статический
```

В таблице 3 столбца:

- 1) Адрес в Интернете некоторого хоста
- 2) Физический адрес Хоста
- 3) Тип записи

Маршрутизатор в локальной сети имеет IP-адрес 192.168.0.1 и MAC-адрес e8-28-c1-ee-da-48.

Статические записи создаются вручную и существуют до следующей перезагрузки устройства, динамические записи периодически обновляются.

Адрес 255.255.255.255 является широковещательным и интерпретируется как MAC-адрес FF-FF-FF-FF-FF-FF, который примут все машины согласно протоколу Ethernet.

Добавили запись:

```
C:\WINDOWS\system32>arp -s 129.35.251.23 00-AA-00-62-C6-09
C:\WINDOWS\system32>arp -a

Интерфейс: 26.70.89.129 --- 0xe
    адрес в Интернете      Физический адрес      Тип
 26.0.0.1                02-00-00-00-51-00    динамический
 26.255.255.255          ff-ff-ff-ff-ff-ff    статический
 129.35.251.23           00-aa-00-62-c6-09    статический
 224.0.0.22               01-00-5e-00-00-16    статический
 224.0.0.251              01-00-5e-00-00-fb   статический
 224.0.0.252              01-00-5e-00-00-fc   статический
 239.255.255.250          01-00-5e-7f-ff-fa  статический

Интерфейс: 192.168.0.5 --- 0x13
    адрес в Интернете      Физический адрес      Тип
 192.168.0.1              e8-28-c1-ee-da-48  динамический
 192.168.0.255             ff-ff-ff-ff-ff-ff  статический
 224.0.0.22               01-00-5e-00-00-16    статический
 224.0.0.251              01-00-5e-00-00-fb   статический
 224.0.0.252              01-00-5e-00-00-fc   статический
 224.0.0.253              01-00-5e-00-00-fd   статический
 239.255.255.250          01-00-5e-7f-ff-fa  статический
 255.255.255.255          ff-ff-ff-ff-ff-ff  статический

C:\WINDOWS\system32>
```

Удалили запись:

```
C:\WINDOWS\system32>arp -d 129.35.251.23
C:\WINDOWS\system32>arp -a

Интерфейс: 26.70.89.129 --- 0xe
    адрес в Интернете      Физический адрес      Тип
 26.0.0.1                02-00-00-00-51-00    динамический
 26.255.255.255          ff-ff-ff-ff-ff-ff    статический
 224.0.0.22               01-00-5e-00-00-16    статический
 224.0.0.251              01-00-5e-00-00-fb   статический
 224.0.0.252              01-00-5e-00-00-fc   статический
 239.255.255.250          01-00-5e-7f-ff-fa  статический

Интерфейс: 192.168.0.5 --- 0x13
    адрес в Интернете      Физический адрес      Тип
 192.168.0.1              e8-28-c1-ee-da-48  динамический
 192.168.0.255             ff-ff-ff-ff-ff-ff  статический
 224.0.0.22               01-00-5e-00-00-16    статический
 224.0.0.251              01-00-5e-00-00-fb   статический
 224.0.0.252              01-00-5e-00-00-fc   статический
 224.0.0.253              01-00-5e-00-00-fd   статический
 239.255.255.250          01-00-5e-7f-ff-fa  статический
 255.255.255.255          ff-ff-ff-ff-ff-ff  статический
```

## 5. Просмотрели содержимое таблицы маршрутизации, пояснили характеристики записей

```
C:\WINDOWS\system32>route print
=====
Список интерфейсов
 14...02 50 ee 4b 97 f4 .....Famatech RadminVPN Ethernet Adapter
 19...04 d4 c4 73 c3 82 .....Realtek PCIe GbE Family Controller
 6...de f5 05 d2 f8 5f .....Microsoft Wi-Fi Direct Virtual Adapter #3
 5...fe f5 05 d2 f8 5f .....Microsoft Wi-Fi Direct Virtual Adapter #4
 18...dc f5 05 d2 f8 5e .....Bluetooth Device (Personal Area Network)
 1.....Software Loopback Interface 1
 16...dc f5 05 d2 f8 5f .....Realtek 8821CE Wireless LAN 802.11ac PCI-E NIC
 13...00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
=====
```

### IPv4 таблица маршрута

```
=====
Активные маршруты:
Сетевой адрес      Маска сети      Адрес шлюза      Интерфейс      Метрика
  0.0.0.0          0.0.0.0          192.168.0.1    192.168.0.5      25
  0.0.0.0          0.0.0.0          26.0.0.1       26.70.89.129    9257
  26.0.0.0         255.0.0.0        On-link          26.70.89.129    257
 26.70.89.129   255.255.255.255  On-link          26.70.89.129    257
 26.255.255.255 255.255.255.255  On-link          26.70.89.129    257
 127.0.0.0         255.0.0.0        On-link          127.0.0.1       331
 127.0.0.1         255.255.255.255  On-link          127.0.0.1       331
127.255.255.255 255.255.255.255  On-link          127.0.0.1       331
 192.168.0.0      255.255.255.0   On-link          192.168.0.5      281
 192.168.0.5      255.255.255.255  On-link          192.168.0.5      281
 192.168.0.255   255.255.255.255  On-link          192.168.0.5      281
 224.0.0.0         240.0.0.0        On-link          127.0.0.1       331
 224.0.0.0         240.0.0.0        On-link          192.168.0.5      281
 224.0.0.0         240.0.0.0        On-link          26.70.89.129    257
 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          192.168.0.5      281
 255.255.255.255 255.255.255.255  On-link          26.70.89.129    257
=====
```

### Постоянные маршруты:

Сетевой адрес	Маска	Адрес шлюза	Метрика
0.0.0.0	0.0.0.0	26.0.0.1	9256

```
=====
```

### IPv6 таблица маршрута

```
=====
Активные маршруты:
Метрика Сетевой адрес      Шлюз
 1     331 ::1/128        On-link
 13    331 2001::/32       On-link
 13    331 2001:0:284a:364:1c3b:3b0e:fa76:a883/128
                           On-link
 14    291 fdःd::/64       On-link
 14    291 fdःd::1a46:5981/128  On-link
 19    281 fe80::/64       On-link
 13    331 fe80::/64       On-link
 14    291 fe80::/64       On-link
 13    331 fe80::1c3b:3b0e:fa76:a883/128
                           On-link
 19    281 fe80::5d42:27b4:2080:74d7/128
                           On-link
 14    291 fe80::e39c:97a1:cf67:4357/128
                           On-link
 1     331 ff00::/8        On-link
 19    281 ff00::/8        On-link
 13    331 ff00::/8        On-link
 14    291 ff00::/8        On-link
=====
```

### Постоянные маршруты:

Отсутствует

Выведен список IPv4 и IPv6 интерфейсов.

Поле «Адрес шлюза» задает адрес ближайшего маршрутизатора для продвижения IP-пакета к заданной сети, поле «Интерфейс» указывает IP-адрес выходного сетевого интерфейса текущего маршрутизатора, а поле «Метрика» хранит целое число, используемое в качестве критерия выбора маршрута передачи пакета, например, количество промежуточных маршрутизаторов, которые должен пройти пакет, чтобы достигнуть адресата.

Рассмотрим IPv4 маршруты:

По ним видно, что пакеты отправляются на адрес маршрутизатора, как на адрес шлюза. А маршрутизатор в свою очередь, исходя из своих таблиц маршрутизации, определит куда переслать пакет.

6. В командном режиме на РК и на сервере определили IP-адреса поисковых систем в соответствии с вариантом из таблицы.

Вариант	Название
6	rambler.com

```
C:\WINDOWS\system32>nslookup rambler.com
Тип: Eltex.Home
Address: 192.168.0.1

Не заслуживающий доверия ответ:
С: rambler.com
Address: 68.178.199.243
```

```
[pmi-b0706@students ~]$ nslookup rambler.com
Server: 217.71.130.130
Address: 217.71.130.130#53

Non-authoritative answer:
Name: rambler.com
Address: 68.178.199.243

[pmi-b0706@students ~]$
```

В начале нам выводится адрес маршрутизатора локальной сети. Для РК это 192.168.0.1, для сервера 217.71.130.130. После выводится IP адрес поисковой системы.

7. В командном режиме на РК и на сервере определили IP-адрес узлов сети в соответствии с номером варианта, указанного в таблице, выполнили его пингование и трассировку.

Пингование и трассировка происходит при помощи протокола ICMP, который формирует ICMP - сообщения.



Таблица типов ICMP-сообщений

Значение в поле «Тип»	Тип сообщения
0	Эхо-ответ
3	Узел назначения недостижим
4	Подавление источника
5	Перенаправление маршрута
8	Эхо-запрос
11	Истечение времени диаграммы
12	Проблема с параметрами пакета
13	Запрос отметки времени
14	Ответ отметки времени
17	Запрос маски
18	Ответ маски

Таблица кодов причин ошибок 3

Код	Причина
0	Сеть недостижима
1	Узел недостижим
2	Протокол недостижим
3	Порт недостижим
4	Ошибка фрагментации
5	Ошибка в маршруте источника
6	Сеть назначения не известна
7	Узел назначения не известен
8	Узел-источник изолирован
9	Административный запрет
	• • • • •

? сообщение-запрос

i сообщение-ответ

↓ сообщение-ошибка

Вариант	Доменное имя
6	ucl.ac.uk, antiplagiat.ru

Определили IP-адрес:

```
C:\WINDOWS\system32>nslookup ucl.ac.uk
ТхӮтхӮ: Eltex.Home
Address: 192.168.0.1

Не заслуживающий доверия ответ:
Лъ : ucl.ac.uk
Address: 144.82.250.24
```

```
C:\Users\danys>nslookup antiplagiat.ru
ТхӮтхӮ: Eltex.Home
Address: 192.168.0.1

Не заслуживающий доверия ответ:
Лъ : antiplagiat.ru
Address: 89.208.199.193
```

Выполнили пингование на РК и сервере:

```
C:\WINDOWS\system32>ping ucl.ac.uk

Обмен пакетами с ucl.ac.uk [144.82.250.24] с 32 байтами данных:
Превышен интервал ожидания для запроса.

Статистика Ping для 144.82.250.24:
Пакетов: отправлено = 4, получено = 0, потеряно = 4
(100% потеря)
```

```
[pmi-b0706@students ~]$ ping -c 5 ucl.ac.uk
PING ucl.ac.uk (144.82.250.24) 56(84) bytes of data.
From gw-130.ami.nstu.ru (217.71.130.254): icmp_seq=1 Redirect Network(New nexthop: gate.ami.nstu.ru (217.71.130.129))
From gw-130.ami.nstu.ru (217.71.130.254): icmp_seq=1 Redirect NetworkFrom gw-130.ami.nstu.ru (217.71.130.254): icmp_seq=3 Redirect Network(New nexthop: gate.ami.nstu.ru (217.71.130.129))
From gw-130.ami.nstu.ru (217.71.130.254): icmp_seq=3 Redirect Network
--- ucl.ac.uk ping statistics ---
5 packets transmitted, 0 received, +2 errors, 100% packet loss, time 4002ms
```

```
C:\WINDOWS\system32>ping antiplagiat.ru

Обмен пакетами с antiplagiat.ru [89.208.199.193] с 32 байтами данных:
Ответ от 89.208.199.193: число байт=32 время=46мс TTL=53
Ответ от 89.208.199.193: число байт=32 время=48мс TTL=53
Ответ от 89.208.199.193: число байт=32 время=45мс TTL=53
Ответ от 89.208.199.193: число байт=32 время=46мс TTL=53

Статистика Ping для 89.208.199.193:
Пакетов: отправлено = 4, получено = 4, потеряно = 0
(0% потеря)
Приблизительное время приема-передачи в мс:
Минимальное = 45мсек, Максимальное = 48 мсек, Среднее = 46 мсек
```

```
[pmi-b0706@students ~]$ ping -c 5 antiplagiat.ru
PING antiplagiat.ru (89.208.199.193) 56(84) bytes of data.
64 bytes from 193.mcs.mail.ru (89.208.199.193): icmp_seq=1 ttl=50 time=51.4 ms
64 bytes from 193.mcs.mail.ru (89.208.199.193): icmp_seq=2 ttl=50 time=51.6 ms
64 bytes from 193.mcs.mail.ru (89.208.199.193): icmp_seq=3 ttl=50 time=51.6 ms
64 bytes from 193.mcs.mail.ru (89.208.199.193): icmp_seq=4 ttl=50 time=51.6 ms
64 bytes from 193.mcs.mail.ru (89.208.199.193): icmp_seq=5 ttl=50 time=51.6 ms

--- antiplagiat.ru ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 51.411/51.597/51.682/0.267 ms
```

Выполнили трассировку на РК и сервере:

```
C:\WINDOWS\system32>tracert antiplagiat.ru
```

Трассировка маршрута к antiplagiat.ru [89.208.199.193]

с максимальным числом прыжков 30:

hop	time	time	time	time	host
1	1 ms	1 ms	<1 ms	Eltex.Home [192.168.0.1]	
2	2 ms	2 ms	4 ms	100.82.0.1	
3	5 ms	2 ms	3 ms	213.228.109.138	
4	44 ms	46 ms	45 ms	87.226.183.89	
5	*	*	*	Превышен интервал ожидания для запроса.	
6	*	*	*	Превышен интервал ожидания для запроса.	
7	*	*	*	Превышен интервал ожидания для запроса.	
8	*	*	*	Превышен интервал ожидания для запроса.	
9	*	*	*	Превышен интервал ожидания для запроса.	
10	*	*	*	Превышен интервал ожидания для запроса.	
11	*	*	*	Превышен интервал ожидания для запроса.	
12	*	*	*	Превышен интервал ожидания для запроса.	
13	45 ms	45 ms	45 ms	193.mcs.mail.ru [89.208.199.193]	

Трассировка завершена.

```
[pmi-b0706@students ~]$ traceroute antiplagiat.ru
traceroute to antiplagiat.ru (89.208.199.193), 30 hops max, 60 byte packets
 1 gw-130-208v.ami.nstu.ru (217.71.130.251)  6.689 ms  6.508 ms  6.441 ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *

[pmi-b0706@students ~]$
```

```
C:\WINDOWS\system32>tracert ucl.ac.uk
```

Трассировка маршрута к ucl.ac.uk [144.82.250.24]

с максимальным числом прыжков 30:

Прыжок	Время	Время	Время	Хост
1	1 ms	1 ms	<1 ms	Eltex.Home [192.168.0.1]
2	6 ms	3 ms	3 ms	100.82.0.1
3	2 ms	3 ms	3 ms	213.228.109.138
4	60 ms	62 ms	62 ms	ae45.stkm-cr4.intl.ip.rostelecom.ru [87.226.133.133]
5	*	*	*	Превышен интервал ожидания для запроса.
6	*	*	*	Превышен интервал ожидания для запроса.
7	99 ms	100 ms	99 ms	JANET.ear3.London2.Level3.net [212.187.216.238]
8	94 ms	91 ms	94 ms	ae24.londtt-sbr1.ja.net [146.97.35.193]
9	96 ms	97 ms	97 ms	ae28.londtw-sbr2.ja.net [146.97.33.62]
10	89 ms	89 ms	89 ms	ae26.londtw-ban1.ja.net [146.97.35.218]
11	91 ms	93 ms	93 ms	146.97.139.238
12	92 ms	92 ms	91 ms	193.60.255.210
13	*	*	*	Превышен интервал ожидания для запроса.
14	*	*	*	Превышен интервал ожидания для запроса.
15	*	*	*	Превышен интервал ожидания для запроса.
16	*	*	*	Превышен интервал ожидания для запроса.
17	*	*	*	Превышен интервал ожидания для запроса.
18	*	*	*	Превышен интервал ожидания для запроса.
19	*	*	*	Превышен интервал ожидания для запроса.
20	*	*	*	Превышен интервал ожидания для запроса.
21	*	*	*	Превышен интервал ожидания для запроса.
22	*	*	*	Превышен интервал ожидания для запроса.
23	*	*	*	Превышен интервал ожидания для запроса.
24	*	*	*	Превышен интервал ожидания для запроса.
25	*	*	*	Превышен интервал ожидания для запроса.
26	*	*	*	Превышен интервал ожидания для запроса.
27	*	*	*	Превышен интервал ожидания для запроса.
28	*	*	*	Превышен интервал ожидания для запроса.
29	*	*	*	Превышен интервал ожидания для запроса.
30	*	*	*	Превышен интервал ожидания для запроса.

Трассировка завершена.

```
C:\WINDOWS\system32>
```

```
[pmi-b0706@students ~]$ traceroute ucl.ac.uk
traceroute to ucl.ac.uk (144.82.250.24), 30 hops max, 60 byte packets
 1 gw-130-208v.ami.nstu.ru (217.71.130.251)  13.615 ms  13.667 ms  13.957 ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *

[pmi-b0706@students ~]$
```

Исходя из результатов можно сделать вывод, что доступ к данным сайтам заблокирован на сервере, в то время как на РК доступ есть только для **antiplagiat.ru** и на трассировке видно каждый конечный пункт.

8. С помощью интерактивных сетевых сервисов (**ping-admin.ru, whois.ru**) выполнили трассировку, определили местонахождение и владельца узла сети в соответствии с номером варианта, указанного в таблице. Результат трассировки в виде скриншота географической карты представили в отчете и выполнили его анализ. Начальный пункт трассировки – г. Новосибирск.

### Бесплатная проверка «Traceroute» из различных частей мира

[ucl.ac.uk](#)

Проверка выполнена 10 ноября 2022 года в 15:30:43 по московскому времени из точки мониторинга «Россия, Новосибирск, север». К сожалению, из выбранной точки мониторинга не удалось выполнить проверку.

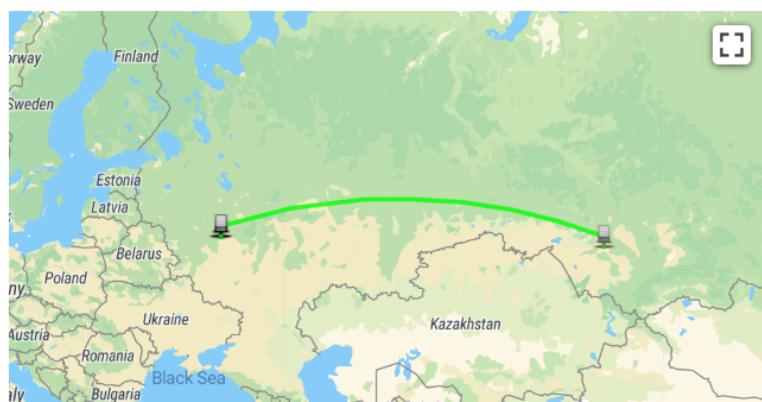
ucl.ac.uk

X

Проверить

ucl.ac.uk не удалось проверить

### Бесплатная проверка «Traceroute» из различных частей мира



[antiplagiat.ru](#)

Проверка выполнена 10 ноября 2022 года в 15:32:02 по московскому времени из точки мониторинга «Россия, Новосибирск, север».

№	Имя	IP	AS	Время, мс
1	192.168.10.1	192.168.10.1		0,254
2	217.65.85.193	217.65.85.193	AS12389	9,819
3	87.226.181.89	87.226.181.89	AS12389	41,891
4	*	*		

**Информация по данным whois.nic.ru**

domain: ANTIPLAGIAT.RU  
nserver: ns1.r01.ru  
nserver: ns2.r01.ru  
state: REGISTERED, DELEGATED  
admin-contact: <https://www.nic.ru/whois/send-message/?domain=antiplagiat.ru>  
org: JSC AntiPlagiat  
registrar: RU-CENTER-RU  
created: 2005.04.28  
paid-till: 2023.04.28  
source: RU-CENTER

>>> Last update of WHOIS database: 2022.11.10T15:40:54Z <<<

Исходя из результатов трассировки видно, что для доступа к сайту выбирается определённый доступный шлюз, ближайший к нужному нам ресурсу, доступным маршрутизатору. Например, для компьютера шлюз – локальный маршрутизатор, для маршрутизатора – маршрутизатор провайдера, для маршрутизатора провайдера – маршрутизатор ещё более высшего уровня и так далее. Наш пакет проходит пороутерам для того, чтобы получить доступ к нужному нам ресурсу.

### **3. Ход работы для 2-го этапа**

Вариант задания:

Вариант	Аналог	ОС	Функция
6	traceroute	Linux	трассировка маршрута передачи данных

Наша программа выполняет трассировку маршрута до указанного узла. Трассировка обеспечивается путем отправки ICMP эхо-запроса с постепенным увеличением TTL. По его истечении промежуточный узел будет нам сообщать об этом. Процесс повторяется до тех пор, пока пакет не достигнет целевого узла и при получении ответа от этого узла трассировка считается завершённой.

## Текст программы

### Файл traceroute.h

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>
#include <sys/time.h>
#include <sys/ioctl.h>
#include <arpa/inet.h>
#include <sys/socket.h>
#include <pthread.h>
#include <stdbool.h>
#include <sys/types.h>
#include <netinet/ip.h>
#include <netinet/ip_icmp.h>
#include <netdb.h>

/*Максимальный размер пакета*/
#define MAX_SPACK 4096

/* Структура, описывающая заголовок IP пакета */
struct header_ipv4
{
    u_char ver_len;          /* 4 бита - версия + 4 бита - длина заголовка в октетах */
    u_char dscp_ecn;         /* 6 бит - тип обслуживания + 2 бита - перегрузка */
    short length;
    short ident;             /* Идентификатор фрагмента */
    short flag_offset;        /* 3 бита флаги, остальное - смещение фрагмента */
    u_char ttl;
    u_char proto;            /* Тип инкапсулированного протокола */
    short chsum;
    int    sip;               /* IP адрес источника */
    int    dip;               /* IP адрес назначения */
};

/*

```

```

* Структура, описывающая формат ICMP пакета для отправки и приема echo reply и
* echo request
*/
struct icmp_echo
{
    u_char          type;    /* Тип сообщения */
    u_char          code;    /* Код сообщения */
    u_short         chsum;
    u_short         id;     /* Идентификатор */
    u_short         nseq;   /* Номер последовательности */
    struct timeval time;   /* Временная метка */
};

/*
* Структура, описывающая формат ICMP пакета, получаемого от узла при
* истечении TTL
*/
struct icmp_timeexp
{
    u_char          type;    /* Тип сообщения */
    u_char          code;    /* Код сообщения */
    u_short         chsum;
    u_short         zero;
    struct header_ip4  hip;   /* Заголовок пакета, TTL которого закончился */
};

/* Функция принятия ICMP пакета*/
int icmp_recv(int sock, char *ipto, char *ipfrom);

/* Функция подсчета контрольной суммы ICMP пакета */
u_short icmp_checksum(u_char *packet);

/*Функция формирования ICMP пакета для эхо запроса/ответа */
void icmp_build(struct icmp_echo *header, u_char type, u_char code);

```

## Файл icmp.c

```
#include "traceroute.h"
```

```

/* Функция подсчета контрольной суммы ICMP пакета */
u_short icmp_checksum(u_char *packet)
{
    int      length; /* Длина ICMP пакета */
    u_short fbyte;   /* Первый байт 16 битного блока */
    u_short sbyte;   /* Второй байт 16 битного блока */
    int      chsum;

    length = sizeof(struct icmp_echo);
    chsum = 0;
    /*
     * Считаем контрольную сумму, разворачивая по 2 байта. Обязательно до
     * этого поле контрольной суммы в заголовке должно быть обнулено
     */
    for(int i = 0; i < length; i += 2)
    {
        fbyte = packet[i];
        sbyte = packet[i + 1];
        chsum += (fbyte<<8)|sbyte;
    }

    chsum = chsum + (chsum>>16);

    return (u_short)~chsum;
}

/*
 * Формирует ICMP пакет для эхо запроса/ответа
 *
 * первый параметр - Указатель на пакет, который будет сформирован
 * второй параметр - Тип пакета
 * третий параметр - Код сообщения
 */
void icmp_build(struct icmp_echo *packet, u_char type, u_char code)

```

```

{

    packet->type = type;
    packet->code = code;
    packet->id   = htons(rand()%256);
    packet->nseq = htons(rand()%256);

    /*
     * Наличие временной метки является обязательным для корректной
     * обработки узлом назначения.
     */
    gettimeofday(&(packet->time), NULL);

    packet->chsum = 0;
    packet->chsum = htons(icmp_checksum((u_char *)packet));
}

/*
 * Принимает ICMP пакет
 *
 * Первый параметр - сокет, на котором принимаем
 *
 * Возврат -1 Истекло время ожидания ответа
 * Возврат 0 Ответ пришел от конечного узла
 * Возврат 1 Ответ пришел от промежуточного маршрутизатора
*/
int icmp_recv(int sock, char *ipto, char *ipfrom)
{
    u_char          packet[MAX_SPACK]; /* Перехваченный пакет */
    int             length;           /* Длина перехваченной части */
    struct header_ipv4 *hdr_ip;      /* Заголовок IP */
    struct icmp_echo *hdr_icmpe;    /* ICMP ответ от конечного узла */
    struct icmp_timeexp *hdr_icmpt; /* ICMP, ответ от промежуточного узла */
    struct in_addr   tmp;            /* Нужен для конвертации IP в строку */

    /* Принимаем пакеты, пока не попадется нужный или не истечет время ожидания ответа */
    while (1)

```

```

{

length = recvfrom(sock, &packet, MAX_SPACK, 0, NULL, NULL);

if (length == -1)
{
    return -1;
}

hdr_ip = (struct header_ipv4 *)&packet;

/* Проверяем является ли это ответом конечного узла */
if (hdr_ip->sip == inet_addr(ipto))
    return 0;

/* Проверяем является ли это сообщением о истечении TTL */
if (packet[sizeof(struct header_ipv4)] == 11)
{
    hdr_icmpt = (struct icmp_timeexp *)(packet + sizeof(struct header_ipv4));

    /* Убеждаемся, что это пакет для нас */
    if (hdr_icmpt->hip.dip == inet_addr(ipto))
    {
        tmp.s_addr = hdr_ip->sip;
        strcpy(ipfrom, inet_ntoa(tmp));
        return 1;
    }
}

return -1;
}

```

## Файл main.c

```
#include "traceroute.h"
```

```

#define MAX_HOPE    30

/*Подсчет времени с момента отправки пакета до его получения*/
static double GetTimeout(struct timeval start)
{
    struct timeval end;
    gettimeofday(&end, NULL);

    double seconds = end.tv_sec - start.tv_sec;
    double useconds = end.tv_usec - start.tv_usec;

    return (seconds * 1000.0 + useconds / 1000.0) + 0.5;
}

/*Получение Ip адреса из доменного имени*/
static bool GetIPFromHostname(const char* hostname, char* host_ip)
{
    struct hostent* he;
    struct in_addr** addr_list;

    if ((he = gethostbyname(hostname)) == NULL)
    {
        perror("gethostbyname");
        return false;
    }

    addr_list = (struct in_addr**)he->h_addr_list;

    for(int i = 0; addr_list[i] != NULL; ++i)
    {
        strcpy(host_ip , inet_ntoa(*addr_list[i]));
        return true;
    }

    return false;
}

```

```
int main(int argc, void *argv[])
{
    int                      sock;
    struct sockaddr_in      addr;
    struct icmp_echo        packet;
    u_short                  ttl;           /*Текущий TTL*/
    struct timeval           time;          /*Время ожидания ответа*/
    char                     ipfrom[16];     /*IP промежуточного узла*/
    int                      reply;         /*Тип ответа на посланный запрос*/

    /*Проверка параметров на валидность*/
    if (argc != 2)
    {
        printf("Неверно указаны параметры\n");
        exit(-1);
    }

    /*Получаем ip-адрес из доменного имени*/
    char host_ip[16];
    GetIPFromHostname(argv[1], host_ip);

    if(inet_addr(host_ip) == INADDR_NONE)
    {
        printf("Некорректно задан адрес\n");
        exit(-1);
    }

    sock = socket(AF_INET, SOCK_RAW, IPPROTO_ICMP);

    if (sock == -1) {
        perror("socket");
        exit(-1);
    }

    if (strcmp(host_ip, "EMPTY") != -1)
    {
```

```

printf("traceroute to %s (%s), 30 hops max:\n", argv[1], host_ip);

}

/*Задаем таймаут для получения*/
time.tv_sec          = 2;
time.tv_usec         = 0;

/*Заполняем ip-назначения*/
addr.sin_family      = AF_INET;
addr.sin_addr.s_addr = inet_addr(host_ip);

if (setsockopt(sock, SOL_SOCKET, SO_RCVTIMEO,&time,sizeof(time)) == -1)
{
    perror("Не удалось настроить таймер. Возможна блокировка");
}

/*Начинаем отправлять icmp-пакеты, постепенно увеличивая TTL*/
for(int ttl = 1; ttl < MAX_HOP; ttl++)
{
    /*Запускаем таймер*/
    struct timeval start;
    gettimeofday(&start, NULL);

    /*установка параметров сокета*/
    setsockopt(sock, SOL_IP, IP_TTL, &ttl, sizeof(ttl));

    /*Формирование icmp-пакета
     * 1й параметр - указатель на пакет
     * 2й параметр - тип пакета
     * 3й параметр - код сообщения
     */
    icmp_build(&packet, 8, 0);

    /*Отправляем пакет*/
    sendto(sock, (void *)&packet, sizeof(packet), 0,
           (struct sockaddr *)&addr, sizeof(addr));
}

```

```

/*Получаем ответ*/
reply = icmp_recv(sock, (char *)host_ip, ipfrom);

switch(reply)
{
    /*В случае, если истекло время ожидания ответа*/
    case -1:
        printf("%2d %s\n", ttl, "* * *");
        break;

    /*В случае, если ответ от конечного узла*/
    case 0:
        /*Фиксируем время получения первого пакета*/
        printf("%2d\t%s\t%06.3lf ms", ttl, (char *)host_ip,
GetTimeout(start));

        /*Делаем то же самое еще с двумя пакетами*/
        for (uint8_t packet_num = 0; packet_num != 2; ++packet_num)
        {
            gettimeofday(&start, NULL);

            sendto(sock, (void *)&packet, sizeof(packet), 0,
(struct sockaddr *)&addr, sizeof(addr));

            reply = icmp_recv(sock, (char *)host_ip, ipfrom);

            printf("\t%06.3lf ms", GetTimeout(start));
        }

        /* Завершаем выполнение программы*/
        ttl = MAX_HOPE;
        printf("\n");
        break;

    /*Если ответ пришел от промежуточного маршрутизатора*/
    case 1:
        /*Фиксируем время получения первого пакета*/

```

```

printf("%2d\t%s\t\t%06.3lf ms", ttl, ipfrom, GetTimeout(start));

/*Делаем то же самое еще с двумя пакетами*/
for (uint8_t packet_num = 0; packet_num != 2; ++packet_num)
{
    gettimeofday(&start, NULL);

    sendto(sock, (void *)&packet, sizeof(packet), 0,
           (struct sockaddr *)&addr, sizeof(addr));

    reply = icmp_recv(sock, (char *)host_ip, ipfrom);

    printf("\t%06.3lf ms", GetTimeout(start));
}

printf("\n");
break;
}

}

close(sock);
}

```

Компиляция программы и генерация объектного файла осуществлялась с помощью команды:

**gcc traceroute.h main.c icmp.c -o Traceroute**

А запуск программы:

**sudo ./Traceroute ya.ru**

## 4. Набор тестов

Выполним трассировку до узлов, которые были использованы на 1-м этапе и для сайта ngs.ru

```
bogdan@DESKTOP-L5KKVKR:~/TracerouteNewProgram$ sudo ./Traceroute ucl.ac.uk
traceroute to ucl.ac.uk (144.82.250.24), 30 hops max:
 1         192.168.0.1          03.055 ms      02.047 ms      05.209 ms
 2         5.128.217.253        03.242 ms      04.620 ms      06.647 ms
 3         10.245.138.241       05.221 ms      03.336 ms      02.841 ms
 4         10.245.138.242       03.589 ms      02.867 ms      06.625 ms
 5         178.49.128.50        03.432 ms      02.526 ms      02.671 ms
 6         87.245.228.193       42.259 ms      42.022 ms      42.466 ms
 7         87.245.228.192       53.476 ms      52.030 ms      52.318 ms
 8         87.245.233.99        89.174 ms      89.810 ms      88.728 ms
 9         195.66.224.15        85.621 ms      86.653 ms      84.989 ms
10        146.97.35.169         85.439 ms      86.965 ms      86.450 ms
11        146.97.33.62         100.859 ms     90.044 ms      91.485 ms
12        146.97.35.218         85.900 ms      84.999 ms      85.004 ms
13        146.97.139.238        117.720 ms     95.637 ms      107.675 ms
14        193.60.255.210        94.682 ms      92.092 ms      92.248 ms
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
```

```
bogdan@DESKTOP-L5KKVKR:~/TracerouteNewProgram$ sudo ./Traceroute antiplagiat.ru
traceroute to antiplagiat.ru (89.208.199.193), 30 hops max:
 1         192.168.0.1          01.688 ms      01.569 ms      01.600 ms
 2         5.128.217.253        04.254 ms      09.132 ms      09.252 ms
 3         10.245.138.241       03.195 ms      03.498 ms      04.218 ms
 4         10.245.138.242       03.639 ms      03.313 ms      04.405 ms
 5         188.43.236.138       04.565 ms      05.070 ms      05.414 ms
 6         217.150.55.234       45.860 ms      45.246 ms      45.367 ms
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15         89.208.199.193       47.599 ms      47.489 ms      47.100 ms
```

```
bogdan@DESKTOP-L5KKVKR:~/TracerouteNewProgram$ sudo ./Traceroute ngs.ru
traceroute to ngs.ru (195.19.220.25), 30 hops max:
 1         192.168.0.1         03.173 ms         01.676 ms         01.572 ms
 2         5.128.217.253       02.845 ms         05.406 ms         04.357 ms
 3         10.245.138.241      02.371 ms         02.692 ms         02.382 ms
 4         10.245.138.242      03.095 ms         03.233 ms         05.953 ms
 5         193.106.112.5       62.066 ms         65.222 ms         61.572 ms
 6 * * *
 7         10.0.9.185          51.834 ms         50.776 ms         50.895 ms
 8         109.202.27.98        51.381 ms         49.146 ms         49.456 ms
 9         195.19.220.25        50.291 ms         51.442 ms         50.821 ms
```

## 5. Вывод

Контрольные вопросы проработаны.