Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина» (УрФУ)

Институт радиоэлектроники и информационных технологий – РтФ

Школа профессионального и академического образования

Отчет по дисциплине   
«Безопасность компьютерных сетей»

Лабораторная работа №1  
«Инструменты для базового исследования сети»

Студенты: Клоченко И.Е., Юсупов Д.А.

Преподаватель: Ваулин С.С.

Группа: РИ-300024

Екатеринбург

2023

**Оглавление**

[1. Определение сетевых настроек 3](#_Toc132549169)

[2. Измерение скорости 7](#_Toc132549170)

[3. Эхо-тестирование 10](#_Toc132549171)

[4. Трассировка маршрута 17](#_Toc132549172)

[5. Работа с DNS 22](#_Toc132549173)

**Цель работы:**

Ознакомление со встроенными в ОС Windows и облачными инструментами для базового исследования сети. Практика использования утилит *ping*, *tracert*, *route* и сервисов глобальной сети, позволяющих работать с ASN, данными Whois и др.

## Определение сетевых настроек

* 1. В разделе «Изменение параметров адаптера» системе «Центр управления сетями и общим доступом» находятся следующие сетевые адаптеры:
* Ethernet адаптер - Realtek PCIe GbE Family Controller
* Wi-Fi адаптер - Realtek 8822CE Wireless LAN 802.11ac PCI-E NIC
  1. Информация о подключении (Ethernet адаптер). Адаптер не подключен. Информацию о MAC-адресе можно получить, выполнив команду *ipconfig /all.* MAC-адрес адаптера - 3C-7C-3F-59-C3-83.

Информация о подключении (Wi-Fi):

* Описание: Realtek 8822CE Wireless LAN 802.11ac PCI-E NIC
* Физический адрес (MAC-адрес): ‎94-08-53-3A-1F-8D
* DHCP включен: Да
* Адрес IPv4: 192.168.0.104
* Маска подсети IPv4: 255.255.255.0
* Шлюз по умолчанию IPv4: 192.168.0.1
* Локальный IPv6-адрес канала: fe80::bf09:1a26:93d:ed60%10 (link-local)
* Текущая канальная скорость подключения: 585-650 Мбит/с

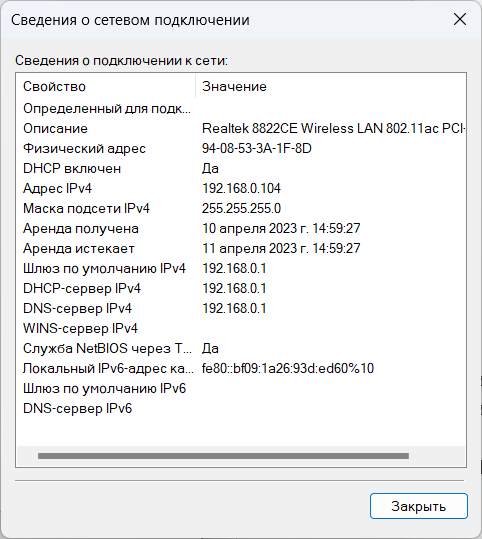


Рисунок 1. Настройки основного подключения (Wi-Fi)

* 1. Определяем по MAC-адресу производителей сетевых адаптеров.

Wi-Fi адаптер: Liteon Technology Corporation

Ethernet адаптер: ASUSTek COMPUTER INC.

* 1. В выводе команды ipconfig /all присутствуют дополнительные сведения об Автонастройке, IAID DHCPv6, DUID клиента DHCPv6. Этих сведений в не было получено в предыдущих пунктах.
  2. Информация о IPv6 интерфейсах на рабочем месте:



Рисунок 2. IPv6 интерфейсы на рабочем месте

* 1. При посещении ресурса по определению IP-адреса был получен следующий IP-адрес: 94.140.147.96. Он не совпадает ни с одним из ранее указанных IP-адресов по причине того, что предыдущие IP-адреса это локальные адреса, а полученный – глобальный IP-адрес маршрутизатора, к которому подключено устройство.
  2. Получаем вывод команды *route print.*

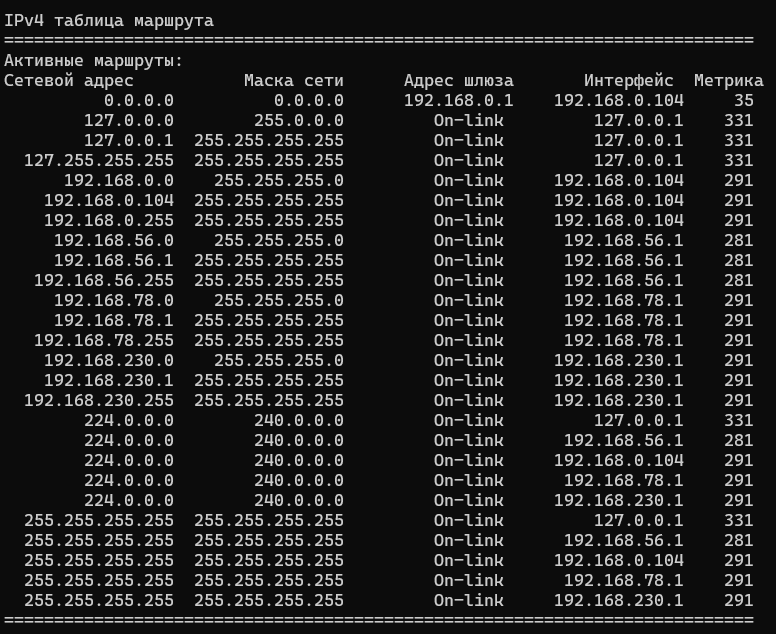


Рисунок 3. Вывод команды route print

Маршрутом по умолчанию является 0.0.0.0. Интерфейс: Wi-Fi адаптер (192.168.0.104).

Известные адреса сети:

* 127.0.0.0 255.0.0.0 – сеть частных IP-адресов
* 127.0.0.1 255.255.255.0 – localhost
* 192.168.0.0 255.255.255.0 – адрес локальной сети
  1. Запускаем с правами администратора утилиту *cmd* и выполняем команду *netstat -b- f*. Приложения, используемые в системе помимо браузера:
* Searchhost.exe
* EABackgroundService.exe
* OneDrive.exe
* Widgets.exe
* svchost.exe
* asus\_framework.exe
* AcPowerNotification.exe
* ROGLiveService.exe
* ArmouryCrate.Service.exe
* nvcontainer.exe
* AcPowerNotification.exe
* ArmourySocketServer.exe
* ArmouryCrate.UserSessionHelper.exe
* NVIDIA Share.exe
* nvcontainer.exe
* Widgets.exe
  1. Выполняем команду *netstat -b- f -a.*

Новые активные соединения со статусом *LISTENING*, также появились соединения *UDP*.

## Измерение скорости

* 1. Тестируем скорость соединения на *https://speedtest.net/*

Результат:

* Оператор связи: МТС
* Город расположения для сервера: Екатеринбург (Ростелеком)
* Входящее соединение: 260.33 Мбит/с
* Исходящее соединение: 277.18 Мбит/с
* IP-адрес совпадает с глобальным адресом маршрутизатора
* Время отклика: 5 мс
  1. Тестируем скорость соединения на [*https://internet.yandex.ru*](https://internet.yandex.ru)*.*

Результат:

* Входящее соединение: 175.54 Мбит/с
* Исходящее соединение: 32.19 Мбит/с
* IP-адрес совпадает с глобальным адресом маршрутизатора
* Город расположения для сервера: Екатеринбург (Яндекс)
* Оператор связи: не указан (МТС)

Разница в скорости связана в разных серверах для тестирования (в первом случае сервер от Ростелеком, во втором – от Яндекс).

* 1. Проведем 3 тестирования для разных городов с разными операторами связи, предоставляющими сервер для тестирования. Результат представлен в виде таблицы:

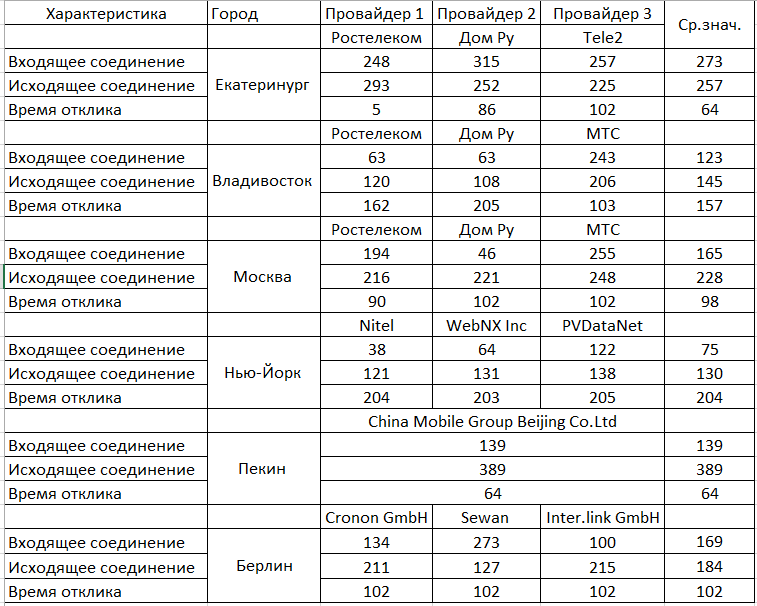


Рисунок 4. Таблица тестирования скорости в разных городах с разными провайдерами (снимок с Excel)

Корреляция скорости с расстоянием до города не явно выражена.

* 1. Запускаем тестирование через iperf3 (в роли клиента)

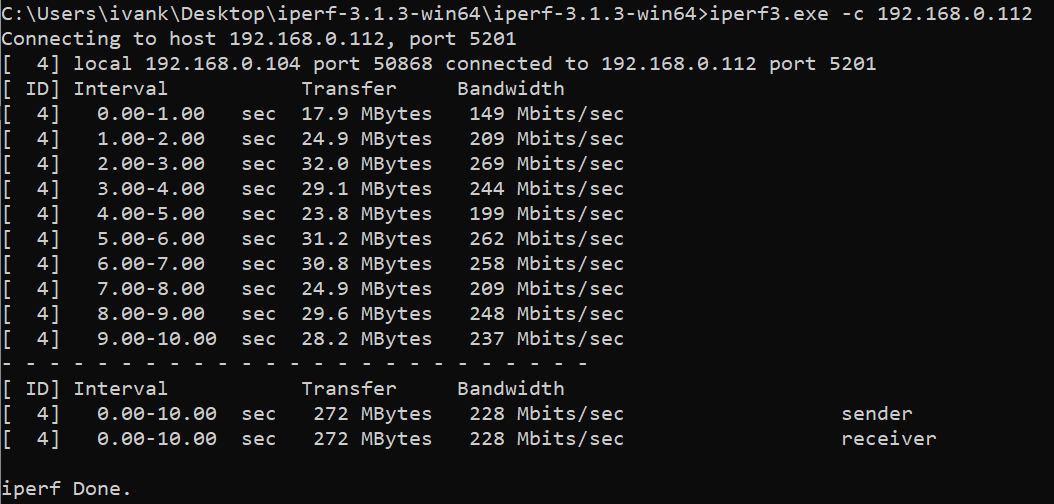


Рисунок 5. Первое тестирование

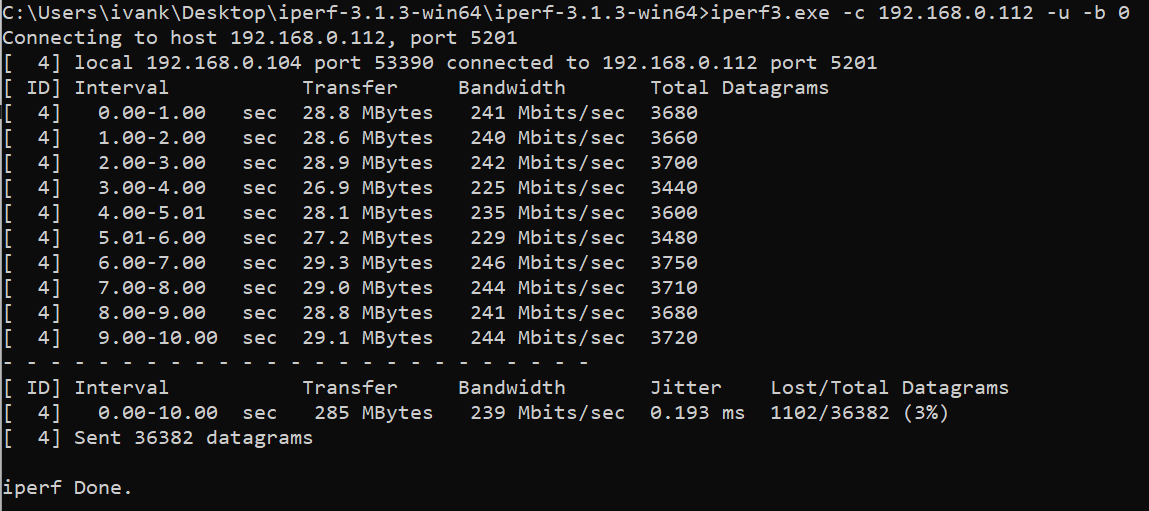


Рисунок 6. Второе тестирование (UDP)

При отправке пакетов наблюдается потеря пакетов 3 %. Джиттер – 0.193 мс. Скорость не изменилась.

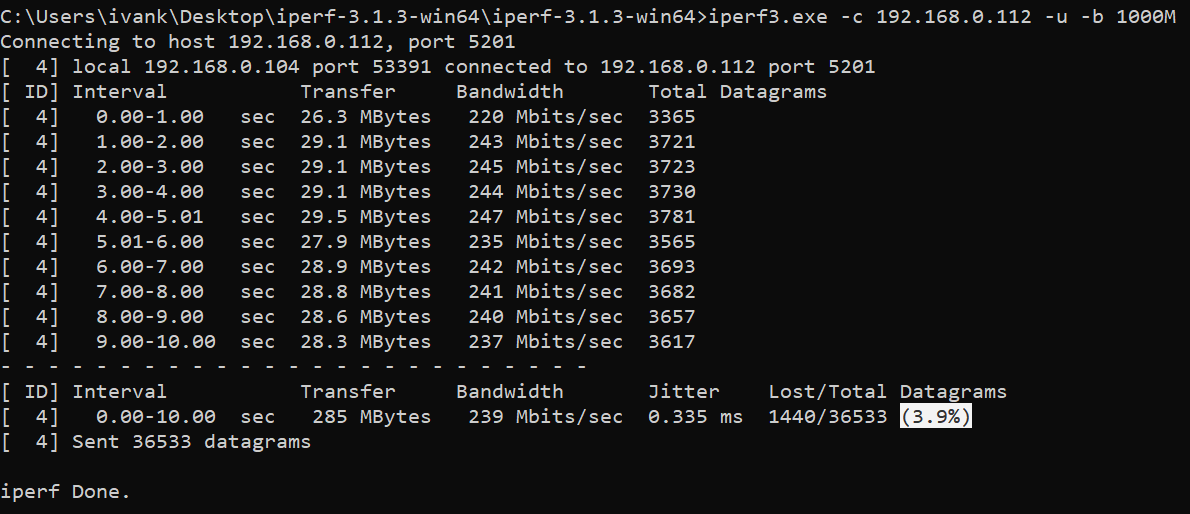


Рисунок 7. Третье тестирование (ограничение пропускной способности в 1000 Мбит/с)

Изменения не большие, потому что у обоих интерфейсов одинаковая пропускная способность в 1 Гиб/с. Джиттер – 0.335 мс.

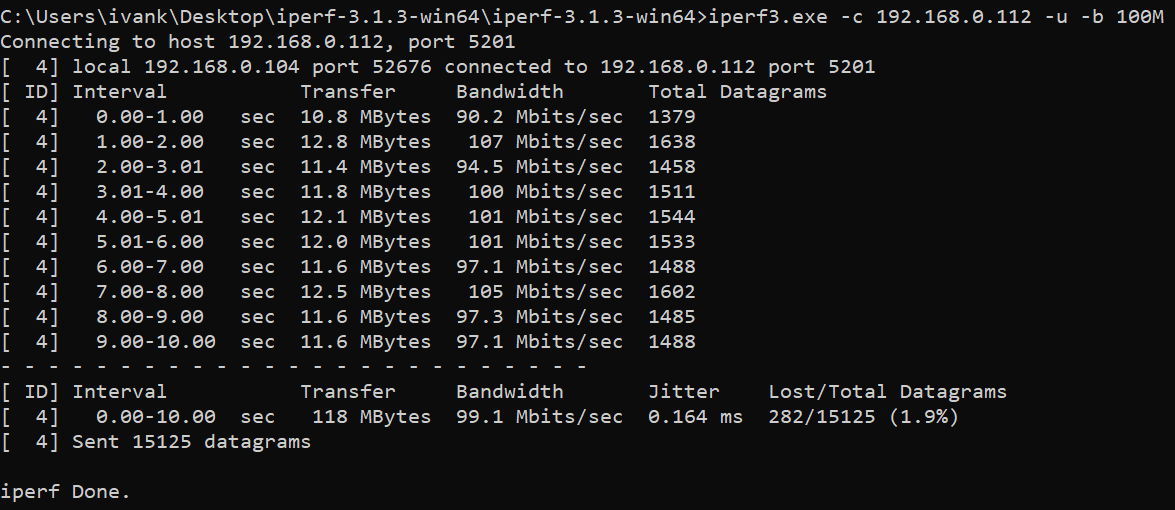


Рисунок 8. Четвертое тестирование (ограничение пропускной способности в 100 Мбит/с)

Скорость ниже, в силу того что искусственно уменьшена пропускная способность. Отсюда следует уменьшение размера переданных пакетов (за то же время при меньшей скорости передано меньше Мбайт пакетов). Процент потерянных пакетов – 1,9%. Джиттер – 0.164 мс.

## Эхо-тестирование

* 1. Воспользуемся утилитой *ping* для эхо тестирования узла *yandex.ru*:

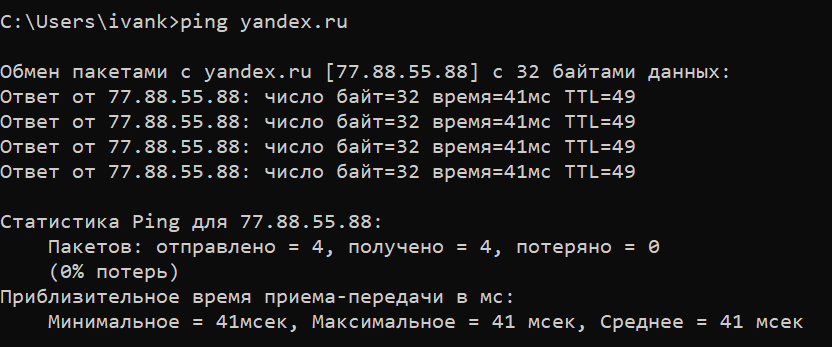


Рисунок 9. Использование утилиты ping

* 1. Повторим тестирование, указав параметр -t, в течение 5 минут:

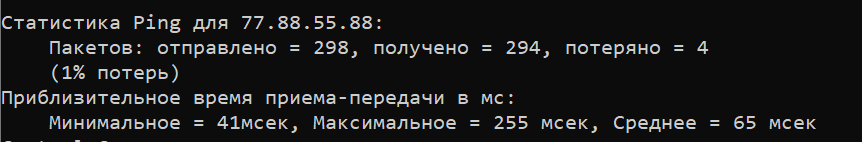


Рисунок 10. Тестирование в течение 5 минут

Разница небольшая. Во втором случае время задержки изменялось и временно стабилизировались. Возможно, это связано с тем, что параллельно с проведением тестирования были открыты несколько вкладок в браузере, что влияло на стабильность соединения и пропускную способность.

* 1. Зададим установленное количество тестов (10) при одном запуске утилиты ping (команда *ping -n 10 example.com*):
* google.com: средний RTT – 127 мс
* ya.ru: средний RTT – 101 мс
* baidu.ru: средний RTT – 99 мс
* urfu.ru: не получилось провести тест (Превышен интервал ожидания для запроса). Возможно, это произошло из-за того, что urfu.ru не принимает ICMP пакеты.
* ripe.net: не получилось провести тестирование по причине ошибки (Заданная сеть доступна). Возможно, та же причина, что и с urfu.ru.
  1. Проведем тестирование с увеличением размера пакета (команда *ping -l <size> ya.ru*). Узел перестает отвечать при размере пакета 4432 байт.
  2. Проведем тестирование с установленным флагом DF. Максимально возможный размер пакета при запрете на фрагментацию пакета – 1472 байта.

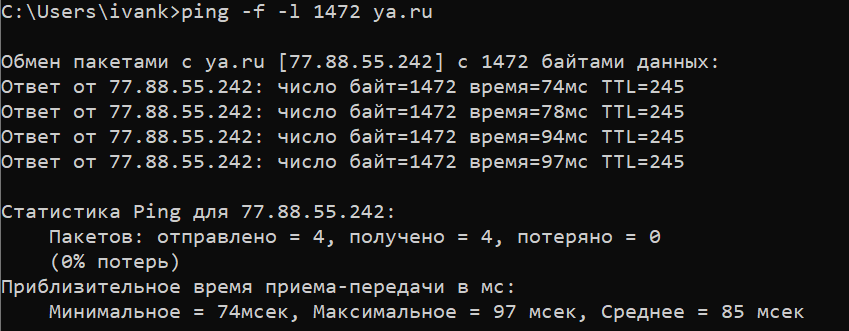


Рисунок 11. Максимальный размер пакета

Минимальный размер пакета – 0 байт. При этом ошибки при тестировании не возникает. Таким образом PMTU = 1472 + 8 + 20 = 1500 байт.

* 1. Результат работы команды *arp -a:*

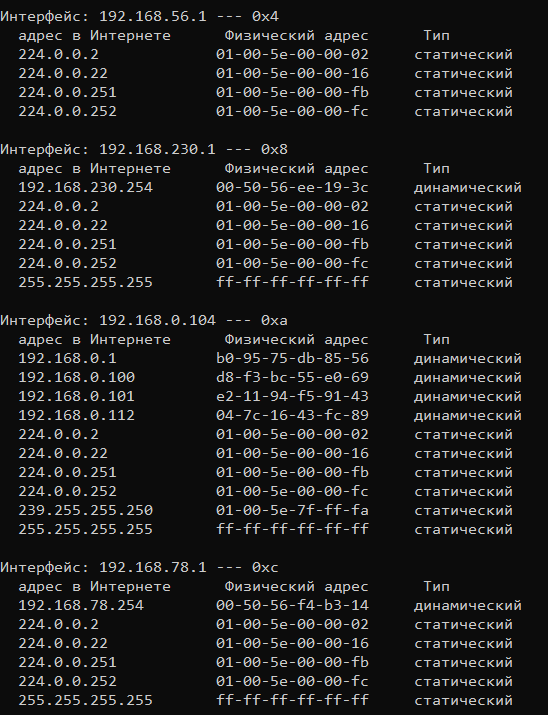


Рисунок 12. ARP-таблица

* 1. Повторяем сканирование (предварительно выполнив команду *ping* устройства, для занесения устройства в *arp*-таблицу).

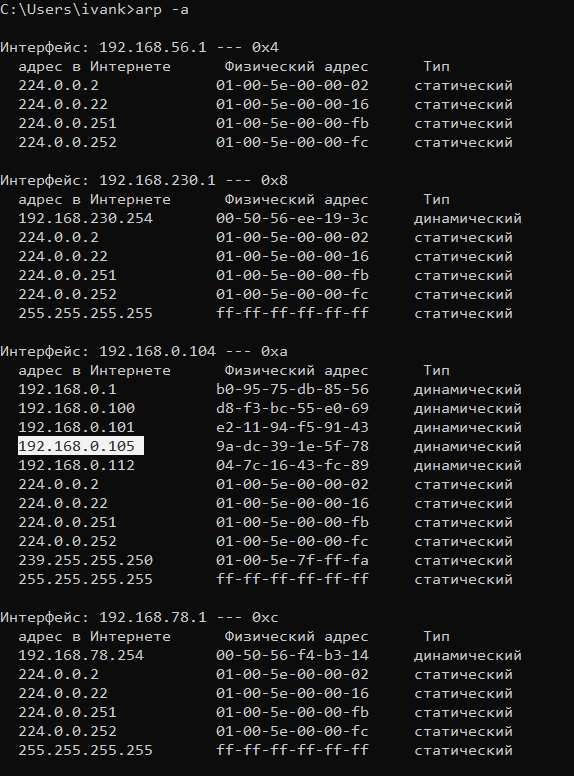


Рисунок 13. Добавление устройства в arp-таблицу

* 1. Посмотрим IPv6 соседей:

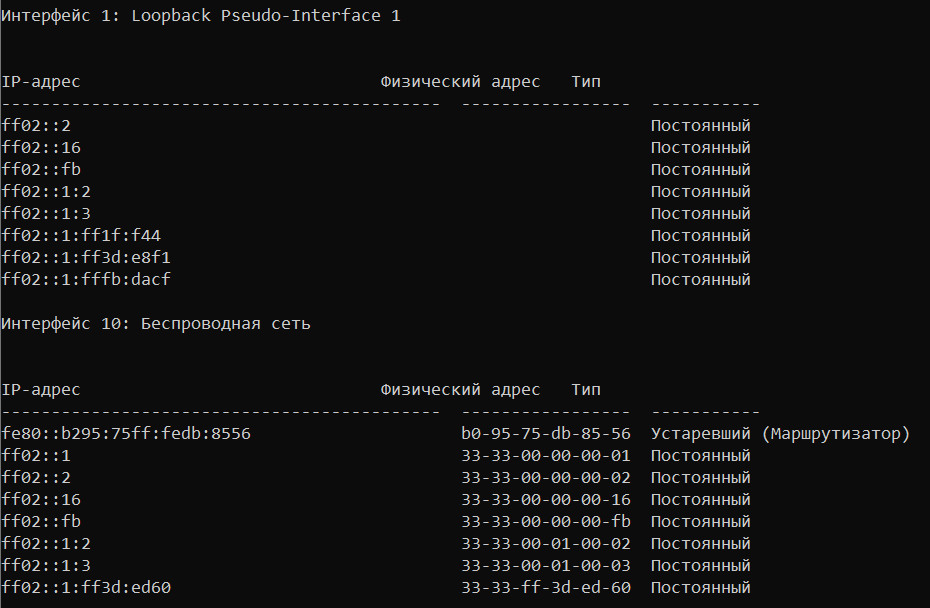


Рисунок 14. ipv6 соседи (1)

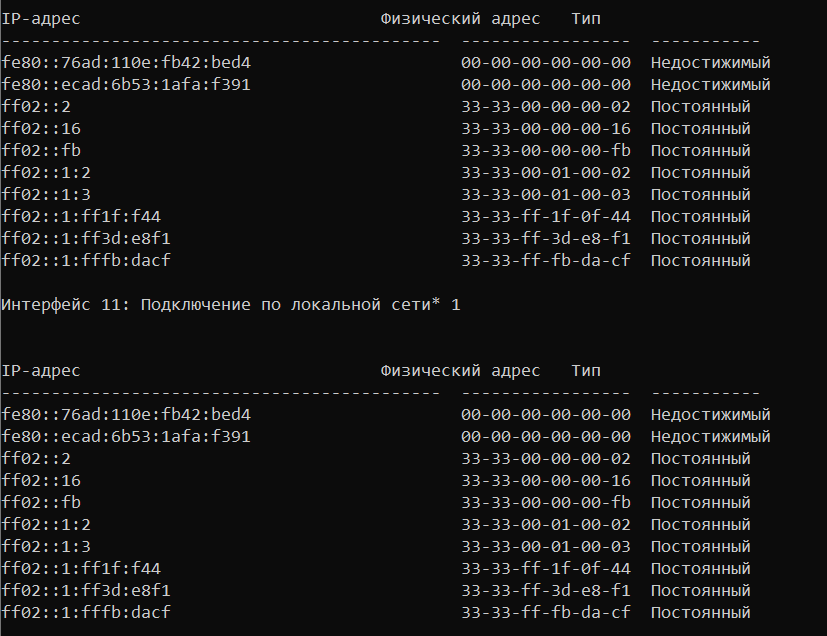


Рисунок 15. ipv6 соседи (2)

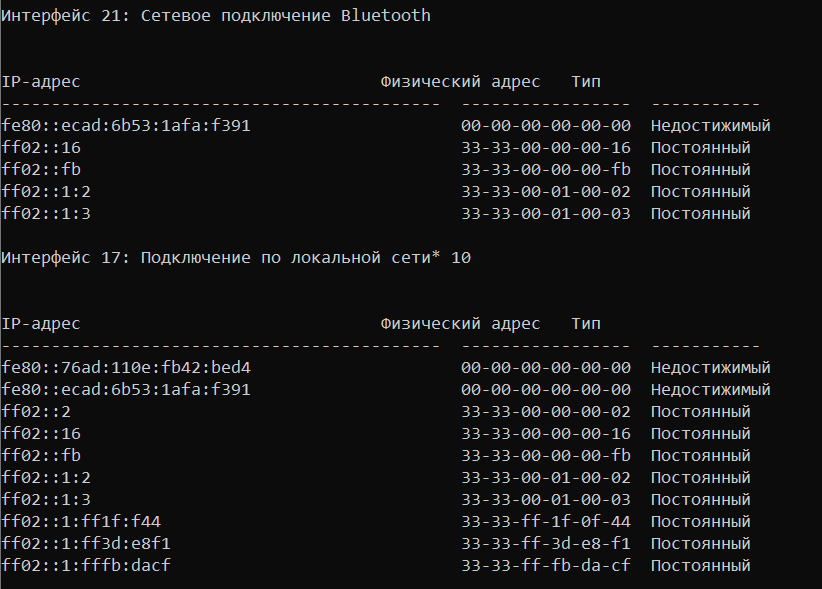


Рисунок 16. ipv6 соседи (3)

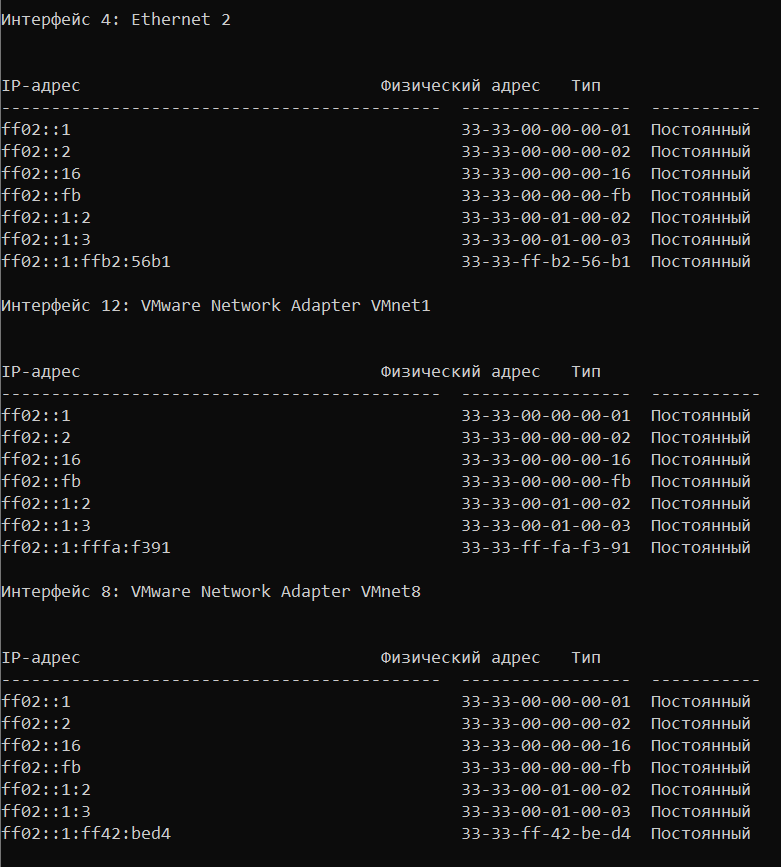


Рисунок 17. ipv6 соседи (4)

После соотнесения MAC-адресов получаем соответствие (192.168.0.1 (IPv4) - b0-95-75-db-85-56 (MAC) - fe80::b295:75ff:fedb:8556 (IPv6)).

* 1. Проводим тестирование ping с IPv6 адресом через 10 интерфейс (интерфейс беспроводной сети):

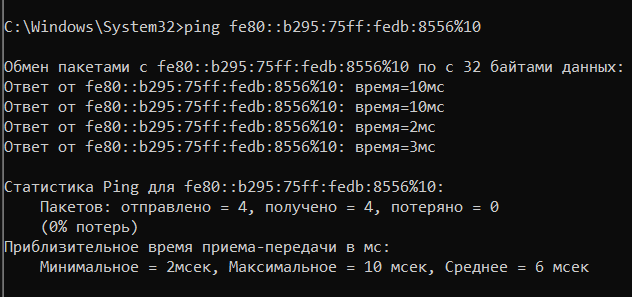


Рисунок 18. Тестирование ping через ipv6 адрес

## Трассировка маршрута

* 1. При помощи утилиты *tracert* выполняем трассировку маршрута до узла *google.com*:

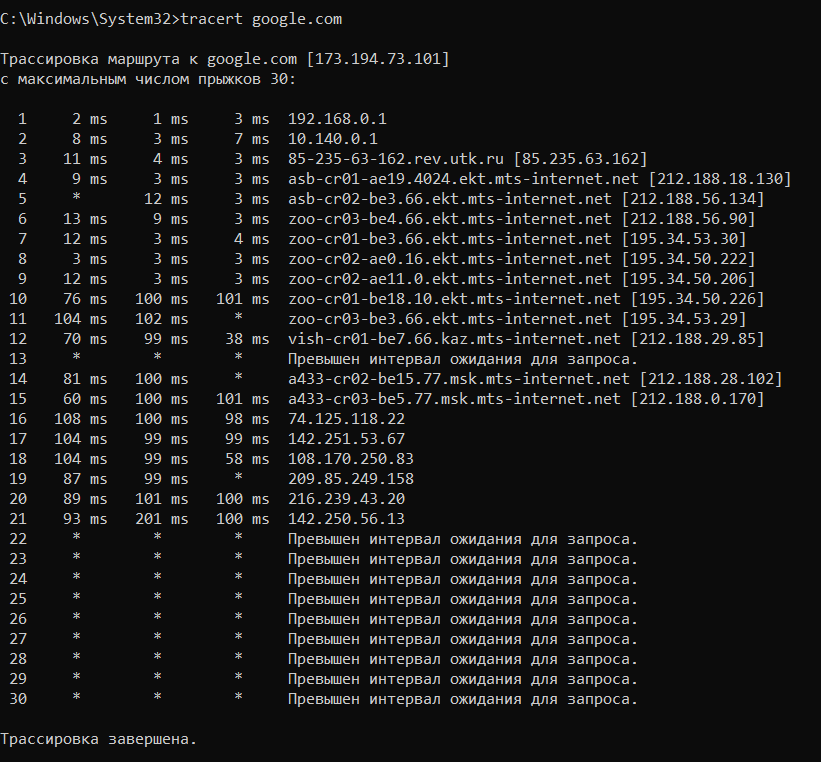


Рисунок 19. Трассировка маршрута до google.com

* 1. Укажем владельца для каждого найденного IP-адреса:
     1. Локальная сеть
     2. Локальная сеть
     3. Екатеринбург (UTC-IFST)
     4. Москва (MTS PJSC)
     5. Москва (MTS PJSC)
     6. Москва (MTS PJSC)
     7. Москва (MTS PJSC)
     8. Москва (MTS PJSC)
     9. Москва (MTS PJSC)
     10. Москва (MTS PJSC)
     11. Москва (MTS PJSC)
     12. Москва (MTS PJSC)
     13. Москва (MTS PJSC)
     14. Москва (MTS PJSC)
     15. Москва (MTS PJSC)
     16. Google (до конца)
  2. Повторим трассировку для узлов *ya.ru*, *e1.ru*, *urfu.ru*, *baidu.com*:

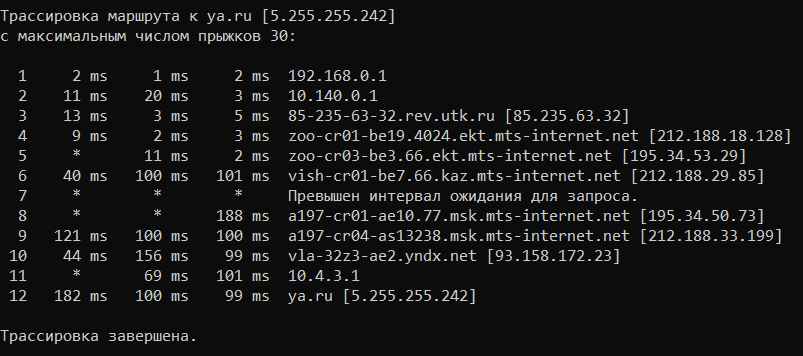


Рисунок 20. Трассировка ya.ru

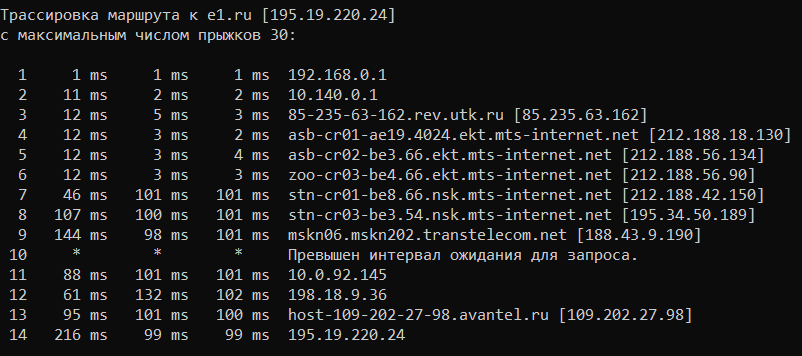


Рисунок 21. Трассировка e1.ru

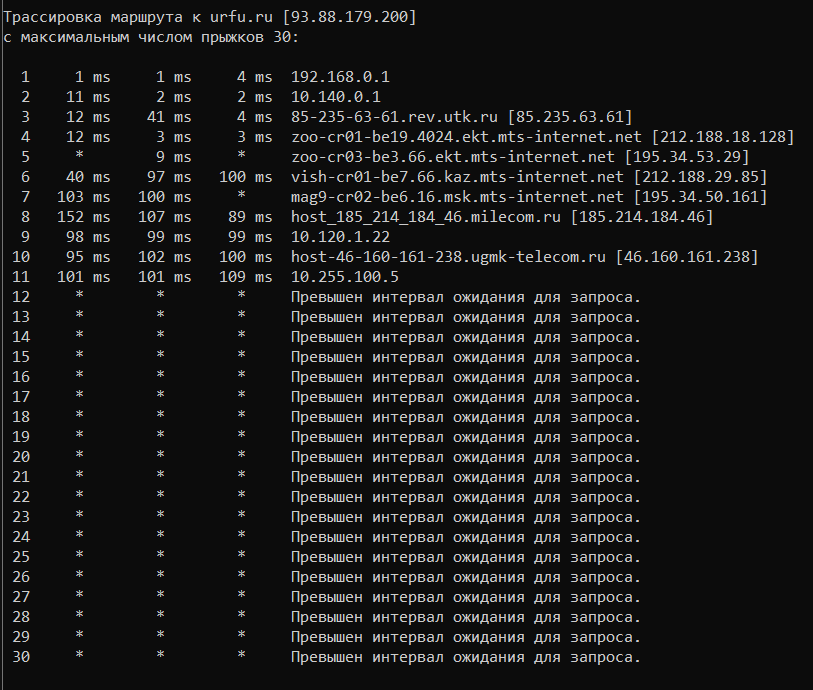


Рисунок 22. Трассировка urfu.ru

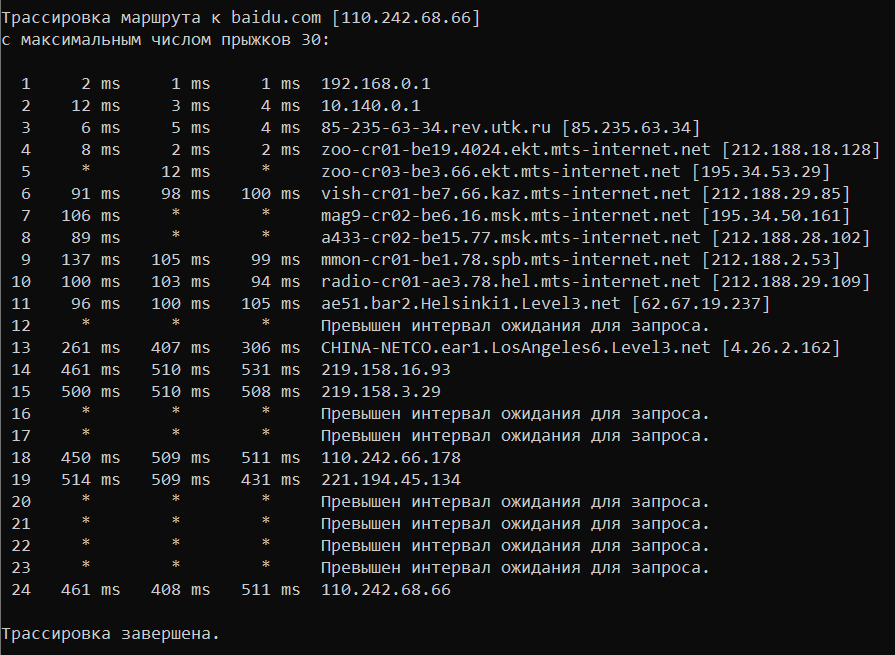


Рисунок 23. Трассировка baidu.com

Первые 2 шага трассировок совпадают (1 – «квартира», 2 – «дом»).

* 1. Адреса из префикса 195.85.107.0/24 в трассировке не присутствуют.
  2. Выбран сервер: ТрансТелеКом, AS20485: <http://lg.ttk.ru/>.

Проведем трассировку публичного IP-адреса, полученного в п.1.4.:

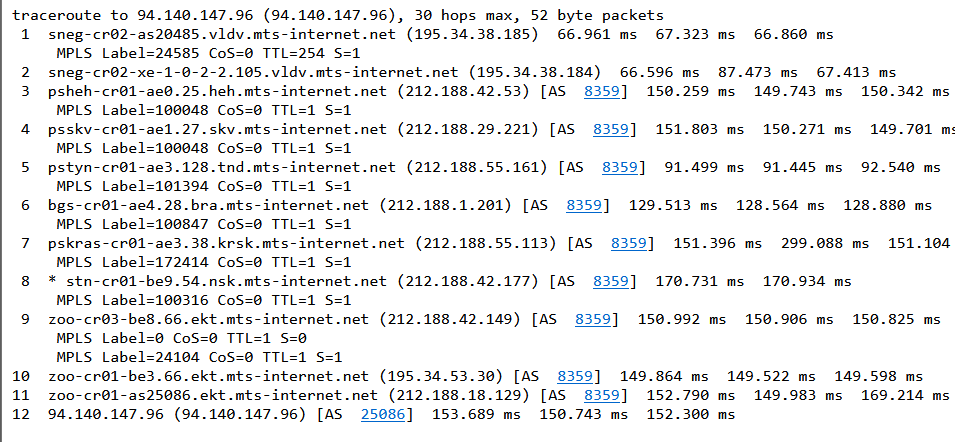


Рисунок 24. Трассировка личного публичного IP-адреса

Трассировка проходит через провайдеров:

* MTS PJSC
* Digital One LLC
* MTS PJSC
  1. Выполним трассировку от рабочего места до первого публичного адреса в трассировке из предыдущего пункта (212.188.18.129):

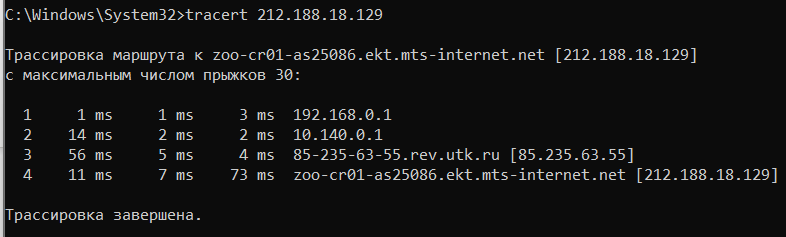


Рисунок 25. Трассировка до первого публичного IP-адреса

Провайдер: MTS PJSC.

* 1. Сравним маршруты, полученные в пунктах 4.5 и 4.6 по транзитным адресам и по владельцам транзитных автономных систем. Отличаются владельцы транзитных автономных систем.
  2. Используем другой LG сервер (потому что он умеет строить BGP графы) <http://lg.comfortel.pro/>. Путей до искомого адреса (AS-Path): 4. Существует ASN, с которым уже сталкивались? - нет.

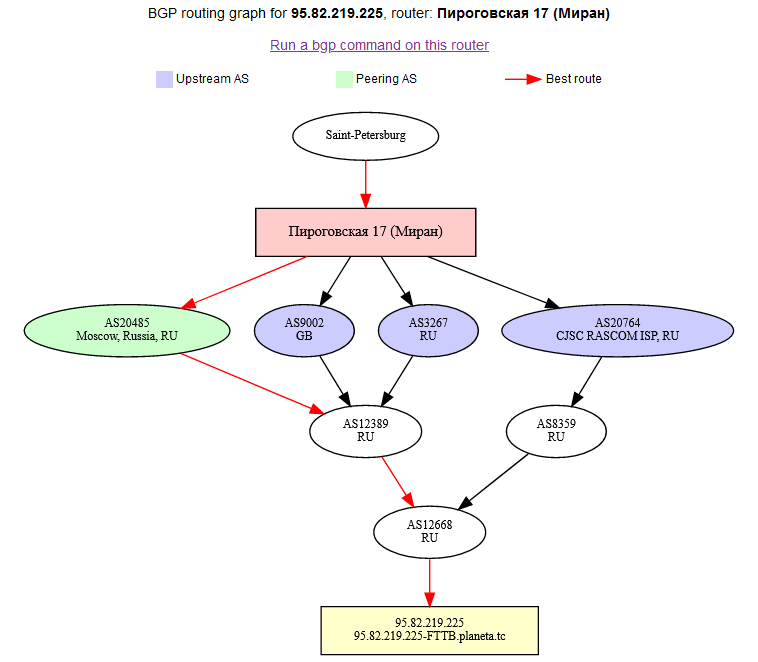


Рисунок 26. BGP граф

* 1. При помощи утилиты *pathping* выполним трассировку маршрута до узла *google.com*:

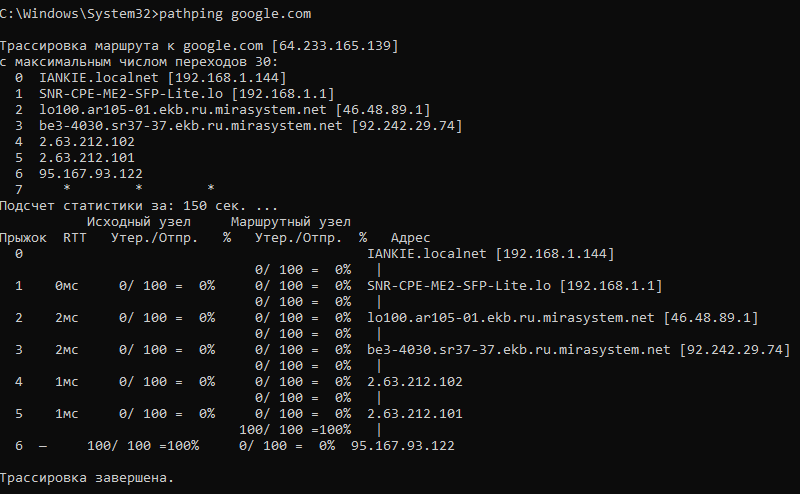


Рисунок 27. Выполнение команды pathping google.com

Особенность работы этой команды заключается в том, что она комбинирует функционал команды ping и tracert и позволяет получить более полную картину сетевой топологии. Также эта команда проводит серию ping-запросов и отображает статистику потери пакетов на каждом узле – полезно при диагностике сетевых неполадок. Еще одна функция – измерение задержек на каждом узле. Весь отчет работы этой команды можно записать в отдельный файл – удобно.

## Работа с DNS

1. 1. При помощи утилиты *nslookup* запросим адреса ресурсов ya.ru, yandex.ru, www.yandex.ru, google.com, e1.ru и urfu.ru.

ya.ru: 3 адреса (один из них IPv6)

yandex.ru: 5 адресов (один IPv6)

www.yandex.ru: 5 адресов (один IPv6)

google.com: 7 адресов (один IPv6)

e1.ru: 1 адрес IPv4

urfu.ru: 1 адрес IPv4

Адреса были получены итеративным способом, так как в выводе был указан DNS сервер, который предоставил информацию о ресурсе и список его IP адресов.

* 1. При помощи базы whois определим владельцев исследуемых доменных имен и время их первой регистрации.

ya.ru: YANDEX, LLC; 12.07.1999

yandex.ru: YANDEX, LLC; 23.09.1997

www.yandex.ru: YANDEX, LLC; 23.09.1997

google.com: MarkMonitor Inc.; 15.09.1997

e1.ru: INTERNET TEHNOLOGII LLC; 22.02.2000

urfu.ru: Ural Federal University; 16.12.2008

* 1. Выполним запросы к ресурсу urfu.ru вызывая утилиту nslookup с ключами «-type=MX», «-type=TXT», «-type=A», «-type=AAAA».

У всех команд одно общее начало вывода:

Server: SNR-CPE-ME2-SFP-Lite.lo

Address: 192.168.1.1

Вывод первой команды (-type=MX):

urfu.ru MX preference = 100, mail exchanger = ironport10.urfu.ru

urfu.ru nameserver = ns1.urfu.ru

urfu.ru nameserver = ns3.urfu.ru

urfu.ru nameserver = ns2.urfu.ru

ironport10.urfu.ru internet address = 93.88.176.6

ns1.urfu.ru internet address = 212.193.66.21

ns2.urfu.ru internet address = 93.88.176.11

ns3.urfu.ru internet address = 212.193.72.21

Вывод второй команды (-type=TXT):

\*\*\* No text (TXT) records available for urfu.ru

Вывод третьей команды (-type=A):

Non-authoritative answer:

Name: urfu.ru

Address: 93.88.179.200

Вывод четвертой команды (-type=AAAA):

Name: urfu.ru

Ключ -type нужен для указания типа запрашиваемой записи:

* MX – адрес почтового сервера
* TXT – тестовая запись
* A – адрес (IPv4)
* AAAA – адрес IPv6
  1. Ознакомимся с кэшем DNS запросов в системе с помощью команды ipconfig /displaydns.

В выводе есть адреса, с которыми ранее не сталкивались, например: [www.asus.com](http://www.asus.com). То, что мы ранее не сталкивались с этим адресом, связано с обращением к DNS именам приложений, которые работают на компьютере. В нашем случае это приложение ASUS, которое периодически проверят обновления для устройства, за этим обращается к домену www.asus.com. Мы при этом работали с доменными именами в браузере.