**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»**

**(СПбГУТ)**

**Кафедра безопасности информационных систем**

**ОТЧЁТ**

по лабораторная работе №2 на тему:   
**«Адресация в компьютерных сетях. Диагностика сетевых ресурсов»**

по дисциплине «Основы интернет-технологий»

Выполнил: студент группы ИСТ-331 Числова Е.В.

Принял: Павлович А.А.

Санкт-Петербург, 2024.

# Лабораторная работа №2.

# Цель работы:

В ходе практической работы закрепить знания о базовых понятиях адресации в компьютерных сетях. Ознакомиться и уметь применять набор инструментов для оптимизации и диагностики сетевых ресурсов.

# Вопросы для изучения:

1. Принципы адресации в компьютерных сетях.

2. Локальные адреса. MAC-адрес.

3. Сетевые адреса. IP-адрес.

4. Символьные имена. DNS, DHCP, Шлюзы.

5. Диагностика сетевых ресурсов. Протокол ICMP.

# Ход работы.

**Адресация в компьютерных сетях** – это процесс назначения и идентификации адресов для устройств и ресурсов в сети. Принципы адресации в компьютерных сетях включают в себя следующие основные аспекты:

1. **Уникальность:** Каждое устройство в сети должно иметь уникальный сетевой адрес, чтобы его можно было однозначно идентифицировать в сети.

2. **Иерархия**: Сетевые адреса могут быть организованы в иерархической структуре для упрощения маршрутизации и управления сетью. Обычно адресация основана на разделении сети на подсети (subnetting), что позволяет эффективно использовать адресное пространство.

3. **Масштабируемость:** Система адресации должна быть способна масштабироваться, чтобы поддерживать рост сети и добавление новых устройств без существенного изменения структуры сети.

4. **Идентификация сетевых служб и ресурсов**: В дополнение к идентификации устройств сетевая адресация может также использоваться для идентификации сетевых служб, приложений и других ресурсов.

5. **Распределение адресов**: Сетевые адреса могут распределяться как статически (вручную), так и динамически (автоматически с помощью протоколов, таких как DHCP), в зависимости от требований и конфигурации сети.

6. **IPv4 и IPv6**: в настоящее время наиболее распространенными стандартами адресации являются IPv4 (Internet Protocol version 4) и IPv6 (Internet Protocol version 6). IPv4 использует 32-битные адреса, в то время как IPv6 использует 128-битные адреса, что позволяет значительно расширить адресное пространство.

7. **Обеспечение безопасности**: Эффективная система адресации также способствует обеспечению безопасности сети, позволяя контролировать доступ к ресурсам и определять права доступа на уровне адресов.

**Локальный адрес** – это адрес, который применяется в рамках локальной сети или сети между устройствами, находящимися в близком географическом расположении, такими как домашняя сеть или офисная локальная сеть (LAN). Он обычно используется для идентификации конкретного устройства в этой сети. Локальные адреса могут быть присвоены как компьютерам, так и другим сетевым устройствам, таким как маршрутизаторы или принтеры.

**MAC-адрес** (Media Access Control address) – это уникальный идентификатор, присвоенный сетевому интерфейсу, обычно на уровне сетевой карты или адаптера. Каждое устройство в сети имеет свой собственный MAC-адрес, который используется для идентификации этого устройства в сети. MAC-адрес представлен в виде шестнадцатеричного числа, состоящего из шести групп по два символа, разделенных двоеточием (например, 00:1A:2B:3C:4D:5E).

MAC-адрес обычно физически записывается на сетевой карте или адаптере и остается неизменным для всей жизни устройства. Он используется на канальном уровне модели OSI (Data Link Layer) для управления доступом к среде передачи данных и идентификации устройства в локальной сети.

Сетевые адреса и IP-адрес (Internet Protocol address) – это ключевые концепции в сетевой технологии, которые позволяют устройствам обмениваться данными в сети.

**Сетевой адрес** – это адрес, который позволяет устройствам в сети идентифицировать друг друга и общаться между собой. Это может быть как локальная сеть (LAN), так и глобальная сеть, такая как Интернет. Сетевые адреса помогают маршрутизаторам и другим сетевым устройствам направлять пакеты данных к их конечному пункту назначения.

**IP-адрес** – это числовой идентификатор, присваиваемый каждому устройству в сети, чтобы оно могло быть идентифицировано и общаться с другими устройствами в сети. IP-адрес используется на сетевом уровне модели OSI (Network Layer) для маршрутизации пакетов данных в сети. Он представлен в виде последовательности чисел, разделенных точками, например, 192.168.1.1.

IP-адресы могут быть присвоены как статически (вручную), так и динамически (автоматически) устройствам в сети. Статический IP-адрес остается постоянным и не изменяется с течением времени, в то время как динамический IP-адрес может изменяться автоматически в зависимости от настроек сети или протокола динамической настройки IP (DHCP).

**Символьные имена** – это человеко-читаемые идентификаторы, используемые для обозначения устройств, сервисов или ресурсов в компьютерной сети. Например, вместо использования числового IP-адреса для доступа к веб-сайту, можно использовать символьное имя, такое как "www.example.com". Символьные имена облегчают запоминание и обращение к ресурсам в сети.

**DNS** – это система, используемая для преобразования символьных имен в числовые IP-адреса и наоборот. Она работает как распределенная база данных, в которой хранятся записи, связывающие символьные имена с соответствующими IP-адресами. Когда пользователь вводит символьное имя в веб-браузере или другом сетевом приложении, компьютер использует DNS для определения соответствующего IP-адреса, по которому можно установить соединение.

**DHCP** – это протокол, используемый для динамической настройки IP-адресов и других сетевых параметров устройствам в сети. Он автоматически назначает IP-адрес, маску подсети, адрес шлюза (gateway) и другие параметры устройствам при их подключении к сети. DHCP упрощает процесс конфигурации сети, особенно в больших сетях, где ручное назначение IP-адресов может быть неэффективным.

**Шлюз** – это устройство или компьютер, которое соединяет разные сети и обеспечивает маршрутизацию данных между ними. Он является точкой входа или выхода для сети и обеспечивает доступ устройствам в сети к внешним сетям, таким как Интернет. Шлюз обычно имеет несколько сетевых интерфейсов и может выполнять функции маршрутизации, NAT (Network Address Translation) и другие.

**Диагностика сетевых ресурсов** – это процесс проверки доступности, работы и производительности сетевых устройств и сервисов. Один из наиболее распространенных инструментов для диагностики сетевых ресурсов – это протокол ICMP (Internet Control Message Protocol).

**Протокол ICMP** – это протокол управляющих сообщений Интернета, который используется для отправки управляющих сообщений и отчетов об ошибках в сети. Он часто используется для диагностики сетевых проблем и проверки доступности узлов в сети. Вот несколько основных видов ICMP-сообщений, используемых для диагностики сетевых ресурсов:

1. **Echo Request (Запрос эха):**

* ICMP-сообщение, отправляемое сетевым устройством для проверки доступности удаленного узла.
* Удаленный узел должен ответить на этот запрос ICMP-сообщением типа "Echo Reply" (Ответ эха), чтобы подтвердить свою доступность.

1. **Destination Unreachable (Недоступность назначения):**

* ICMP-сообщение, которое отправляется обратно отправителю, если маршрутизатор или узел не может доставить пакет до его назначения.
* Это может произойти, например, если маршрут до целевого узла отсутствует или если целевой узел не отвечает.

1. **Time Exceeded (Время превышено):**

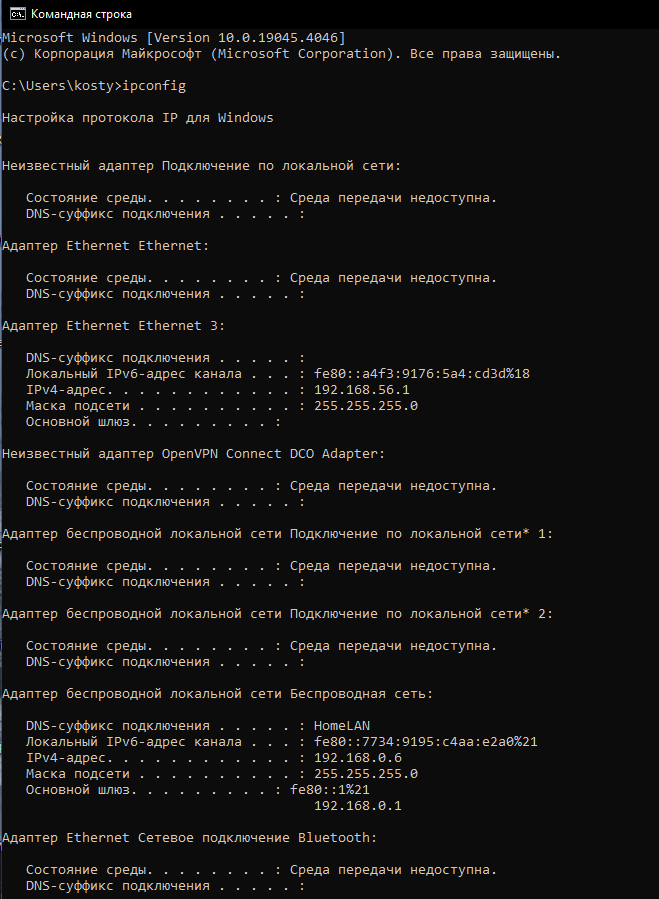
* ICMP-сообщение, которое отправляется обратно отправителю, если пакет не достигает своего пункта назначения в течение определенного времени.
* Это может произойти, если пакеты зацикливаются в сети или если они превышают максимальное количество прыжков (hop limit).

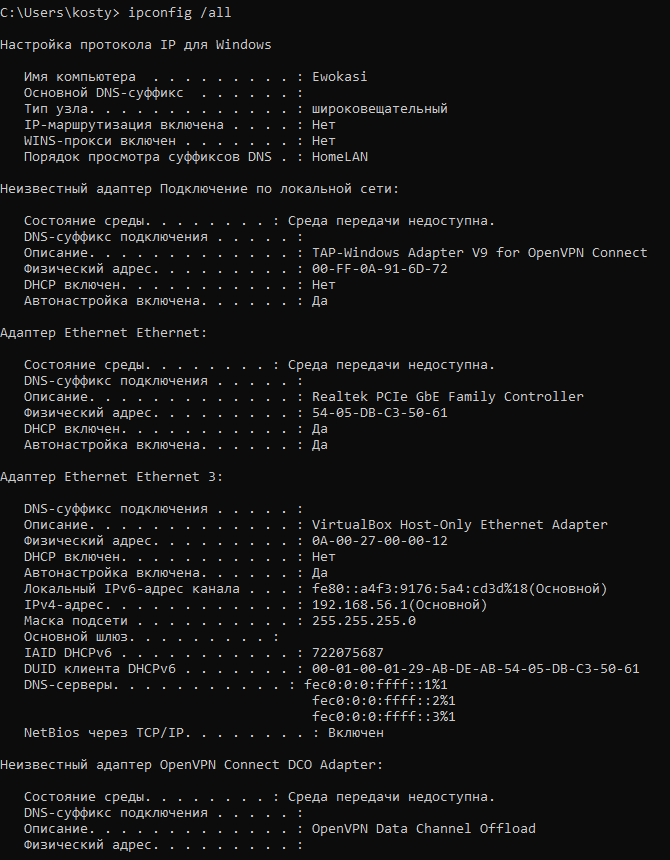
1. **Redirect (Перенаправление):**

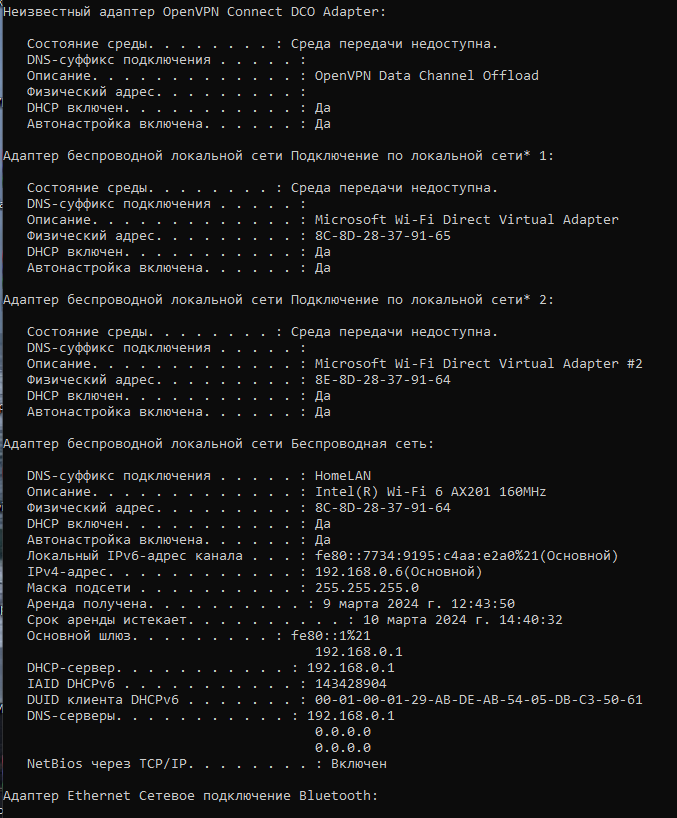
* ICMP-сообщение, которое отправляется маршрутизатором, чтобы указать отправителю более оптимальный путь к целевому узлу.
* Это используется для улучшения маршрутизации в сети.

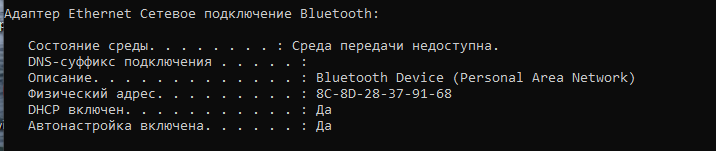
Протокол ICMP широко используется различными средствами диагностики сети, такими как утилита ping, tracert (traceroute) и другие, для проверки доступности узлов, определения проблем маршрутизации и оценки производительности сети.

* Ipconfig / ipconfig /all









Описание:

1. Неизвестный адаптер Подключение по локальной сети: Этот адаптер не используется или не настроен. DHCP выключен.

2. Адаптер Ethernet Ethernet: Описание указывает на Realtek PCIe GbE Family Controller. DHCP включен.

3. Адаптер Ethernet Ethernet 3 VirtualBox Host-Only Ethernet Adapter. DHCP выключен. У адаптера есть IPv4-адрес, который используется для виртуальной среды VirtualBox.

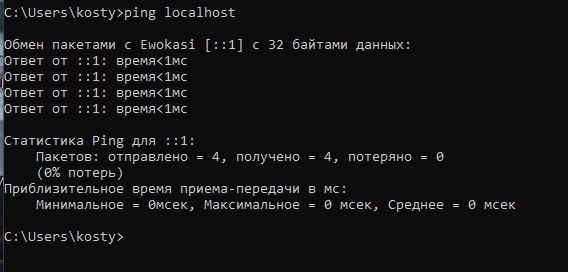
4. Неизвестный адаптер OpenVPN Connect DCO Adapter: Этот адаптер используется для подключения к VPN через OpenVPN. DHCP включен.

5. Адаптеры беспроводной локальной сети Подключение по локальной сети 1 и Подключение по локальной сети 2: Эти адаптеры также не используются. DHCP включен.

6. Адаптер беспроводной локальной сети Беспроводная сеть: Описание указывает на Intel(R) Wi-Fi 6 AX201 160MHz. DHCP включен. Этот адаптер подключен к сети HomeLAN с IPv4-адресом 192.168.0.6 и шлюзом 192.168.0.1.

7. Адаптер Ethernet Сетевое подключение Bluetooth: Этот адаптер используется для соединения с устройствами Bluetooth. DHCP включен.

Физический адрес 00-FF-0A-91-6D-72 – уникальный адрес сетевого оборудования на ПК.

* **Ping Localhost**

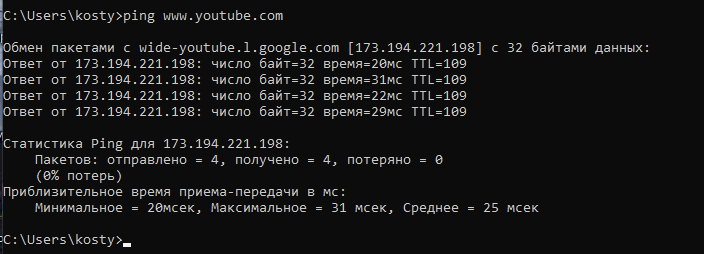
Описание:

ping localhost проверяет связь с собственным компьютером через локальный адрес. Вывод показывает, что обмен пакетами происходит успешно без потерь данных:

* Пакеты: отправлено = 4, получено = 4, потеряно = 0 (0% потерь)
* Приблизительное время приема-передачи в мс:
* Минимальное = 0мсек,
* Максимальное = 0 мсек,
* Среднее = 0 мсек.

Это говорит о том, что соединение через локальный хост стабильно, и время отклика минимально, что ожидаемо, так как данные не проходят реальное сетевое соединение и маршрутизацию, а просто возвращаются обратно к самому компьютеру.

* **Ping youtube**



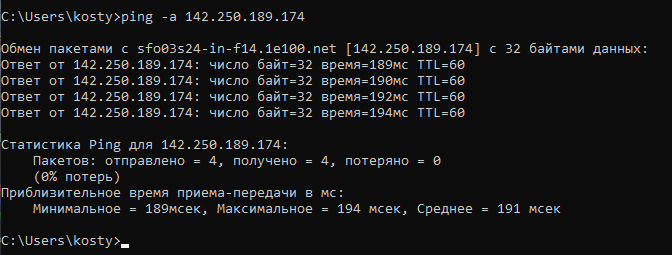
Описание:

ping www.youtube.com проверяет доступность и задержку при обмене пакетами с веб-сайтом www.youtube.com. Вывод показывает успешный обмен пакетами без потерь данных:

* Пакеты: отправлено = 4, получено = 4, потеряно = 0 (0% потерь)
* Приблизительное время приема-передачи в мс:
* Минимальное = 20мсек,
* Максимальное = 31 мсек,
* Среднее = 25 мсек.

Эти значения времени представляют задержку (ping) между компьютером и сервером www.youtube.com (с адресом 173.194.221.198). Минимальное время показывает самую быструю задержку в получении ответа от сервера, максимальное - самую долгую, а среднее время - среднюю задержку.

* **Ping -a ip**



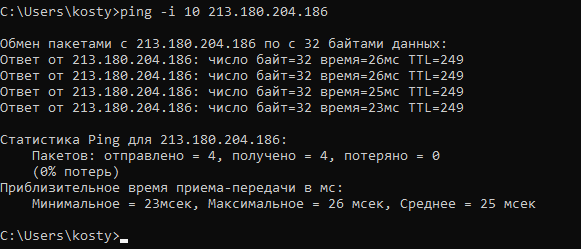
Описание:

ping -a 142.250.189.174 пытается определить имя хоста для IP-адреса 142.250.189.174. Полученное имя хоста - sfo03s24-in-f14.1e100.net. Затем осуществляется обмен пакетами с этим хостом. Вывод показывает успешный обмен пакетами без потерь данных:

* Пакеты: отправлено = 4, получено = 4, потеряно = 0 (0% потерь)
* Приблизительное время приема-передачи в мс:
* Минимальное = 189мсек,
* Максимальное = 194 мсек,
* Среднее = 191 мсек.

Это показывает, что связь с хостом sfo03s24-in-f14.1e100.net с IP-адресом 142.250.189.174 стабильна, и время отклика в пределах нормы.

* **Ping -I**



Описание:

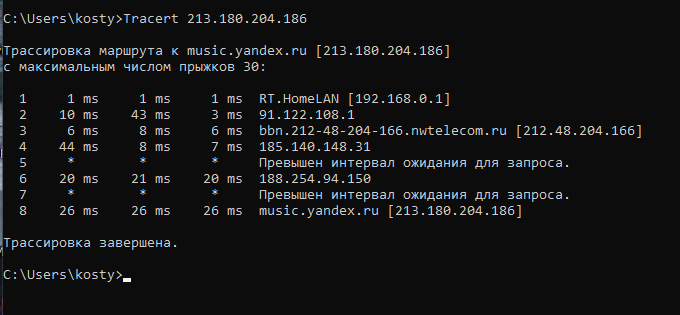
ping -i 10 213.180.204.186 позволяет задать интервал между отправкой пакетов. В данном случае, интервал установлен на 10 миллисекунд.

Результаты показывают успешный обмен пакетами с IP-адресом 213.180.204.186:

* Пакеты: отправлено = 4, получено = 4, потеряно = 0 (0% потерь)
* Приблизительное время приема-передачи в мс:
* Минимальное = 23 мсек,
* Максимальное = 26 мсек,
* Среднее = 25 мсек.

Это показывает стабильное соединение с указанным хостом, и время отклика остается в пределах нормы.

* **Tracert**



Описание:

tracert 213.180.204.186 отображает маршрут следования пакетов к указанному IP-адресу (в данном случае, к music.yandex.ru - 213.180.204.186).

Вывод показывает последовательные прыжки через различные узлы сети, каждый из которых представлен IP-адресом и временем задержки (в миллисекундах) до этого узла.

Основные моменты:

1. Первый прыжок (hop) отправляет пакеты на маршрутизатор вашей локальной сети с адресом 192.168.0.1, который является маршрутизатором домашней сети.

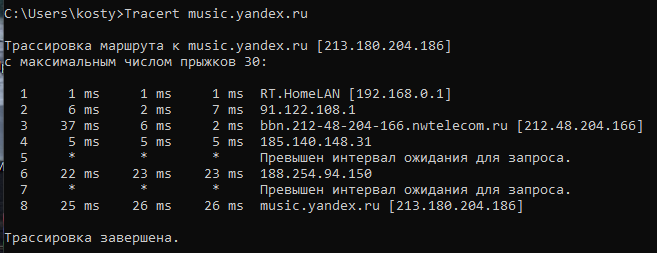
2. После этого, маршрутизатор пересылает пакеты по цепочке других узлов (hop), преодолевая различные сегменты сети, включая провайдеров интернета и другие маршрутизаторы.

3. На пятом и седьмом прыжке отображаются звездочки (), что означает, что превышен интервал ожидания для запроса. Это может быть связано с тем, что маршрутизаторы не отвечают на запросы, либо они принимают дольше, чем установленный таймаут.

4. Затем, на восьмом прыжке, пакеты успешно достигают music.yandex.ru с IP-адресом 213.180.204.186.

Это дает общее представление о пути, который пакеты проходят для достижения указанного хоста.

* **Tracert Yandex.music.ru**



Описание:

tracert music.yandex.ru отображает маршрут следования пакетов к указанному доменному имени (в данном случае, к music.yandex.ru), а затем к соответствующему IP-адресу (213.180.204.186).

Основные моменты:

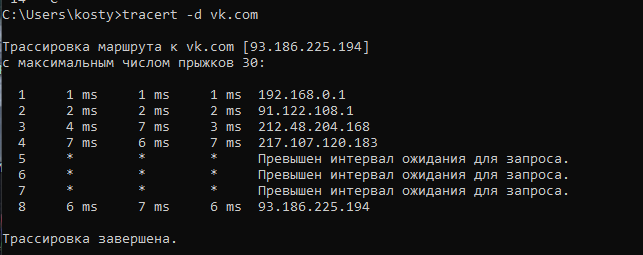
1. Первый прыжок (hop) отправляет пакеты на маршрутизатор вашей локальной сети с адресом 192.168.0.1, который является маршрутизатором домашней сети.

2. После этого, пакеты проходят через несколько промежуточных узлов (hops), включая маршрутизаторы провайдеров интернета, и достигают конечного узла music.yandex.ru.

3. На пятом и седьмом прыжке отображаются звездочки (), что означает, что превышен интервал ожидания для запроса. Это может быть связано с тем, что маршрутизаторы не отвечают на запросы, либо они принимают дольше, чем установленный таймаут.

4. На восьмом прыжке пакеты успешно достигают music.yandex.ru с IP-адресом 213.180.204.186.

Это дает общее представление о пути, который пакеты проходят для достижения указанного домена music.yandex.ru.

* **Tracert -d vk.com**

Описание:

tracert -d vk.com пытается отследить маршрут к доменному имени vk.com, указав при этом опцию -d, чтобы не выполнять обратное DNS-разрешение для каждого узла.

Основные моменты:

1. Первый прыжок (hop) отправляет пакеты на маршрутизатор вашей локальной сети с адресом 192.168.0.1, что, вероятно, является вашим маршрутизатором домашней сети.

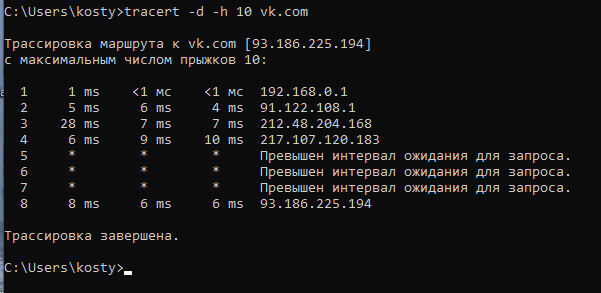
2. После этого пакеты проходят через несколько промежуточных узлов (hops), включая маршрутизаторы провайдеров интернета.

3. На пятом и шестом прыжке, а также на седьмом превышен интервал ожидания для запроса, что может быть связано с тем, что эти маршрутизаторы не отвечают на запросы или они принимают слишком долго, чем установленный таймаут.

4. Восьмой прыжок успешно достигает конечного узла с IP-адресом 93.186.225.194, который соответствует vk.com.

Это дает общее представление о маршруте, который пакеты проходят, чтобы достичь сайта vk.com.

* **Tracert -d -h 10 vk.com**



Описание:

tracert -d -h 10 vk.com, которая пытается отследить маршрут к доменному имени vk.com с ограничением на максимальное число прыжков до 10 (указано опцией -h). Опция -d используется для того, чтобы не выполнять обратное DNS-разрешение для каждого узла.

Основные моменты:

1. Первый прыжок (hop) отправляет пакеты на маршрутизатор вашей локальной сети с адресом 192.168.0.1 является маршрутизатором домашней сети.

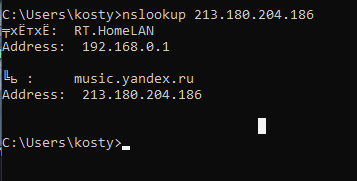
2. После этого пакеты проходят через несколько промежуточных узлов (hops), включая маршрутизаторы провайдеров интернета.

3. На пятом и шестом прыжке, а также на седьмом превышен интервал ожидания для запроса, что может быть связано с тем, что эти маршрутизаторы не отвечают на запросы или они принимают слишком долго, чем установленный таймаут.

4. Восьмой прыжок успешно достигает конечного узла с IP-адресом 93.186.225.194, который соответствует vk.com.

Это дает общее представление о маршруте, который пакеты проходят, чтобы достичь сайта vk.com, с ограничением числа прыжков до 10.

* **Nslookup ip**



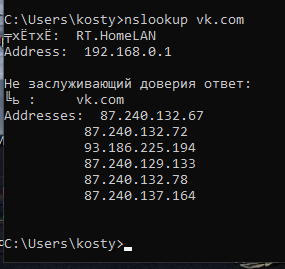
Описание:

По результатам команды nslookup 213.180.204.186, система возвращает следующую информацию:

* Сервер: RT.HomeLAN
* Address: 192.168.0.1
* Name: music.yandex.ru
* Address: 213.180.204.186

Эта информация говорит о том, что IP-адрес 213.180.204.186 соответствует доменному имени music.yandex.ru. Таким образом, запрос был успешно разрешен, и установлено соответствие между указанным IP-адресом и доменным именем.

* **Nslookup domain**



Описание:

Этот ответ указывает на несколько IP-адресов, которые связаны с доменным именем vk.com. Однако, в сообщении указано, что ответ "не заслуживает доверия". Это может быть связано с тем, что полученные данные не прошли аутентификацию или не подтверждены авторитетным источником.

В любом случае, IP-адреса, перечисленные в ответе, представляют собой адреса, которые могут использоваться для доступа к ресурсу vk.com.  
**Выводы:**

Я закрепила знания о базовых понятиях адресации в сетях, ознакомилась и научилась применять набор инструментов для оптимизации и диагностики сетевых ресурсов.