МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ

УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра радиотехники и связи

**Отчет по практической работе №1**

«ДИАГНОСТИЧЕСКИЕ УТИЛИТЫ TCP/IP»

Выполнил: ст. группы ИСТ-33

Лебедева А. О.

Проверил: доцент, к.т.н

Чесноков С. Е.

Дата защиты \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Оценка  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Йошкар-Ола

2025

Оглавление

[Введение 3](#_Toc211813254)

[Задание 1 и 2. Получение справочной информации по командам и получение имени хоста. 4](#_Toc211813255)

[Задание 3. Изучение утилиты ipconfig 6](#_Toc211813256)

[Задание 4. Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP. 9](#_Toc211813257)

[Задание 5. Выбор ресурса для исследования доступа. 11](#_Toc211813258)

[Задание 6. Тестирование связи с помощью утилиты ping 12](#_Toc211813259)

[Задание 7. Определение пути IP-пакета 14](#_Toc211813260)

[Ответы на контрольные вопросы 15](#_Toc211813261)

# ****Введение****

Данная работа направлена на приобретение и закрепление практических навыков анализа сетевой инфраструктуры с помощью стандартного набора диагностических утилит операционных систем. В ходе выполнения работы будут решены следующие задачи:

* Изучение и применение основных утилит командной строки, таких как ping, traceroute (или tracert), netstat (и его современных аналогов ss), nslookup/dig и tcpdump.
* Проведение комплексного анализа сетевых соединений для определения их состояния, активности и производительности.
* Оценка доступности удаленных сетевых узлов и измерения ключевых метрик, таких как время отклика.
* Исследование маршрутов передачи данных через сеть для выявления «узких мест» и точек отказа.
* Изучение механизмов DNS — системы доменных имен, которая является основой удобного доступа к сетевым ресурсам.
* Освоение основ мониторинга сетевого трафика путем его захвата и последующего анализа для выявления аномалий и потенциальных угроз.
* Систематизация полученных данных и формирование отчетов, позволяющих делать обоснованные выводы о состоянии сети.

# Задание 1 и 2. Получение справочной информации по командам и получение имени хоста.

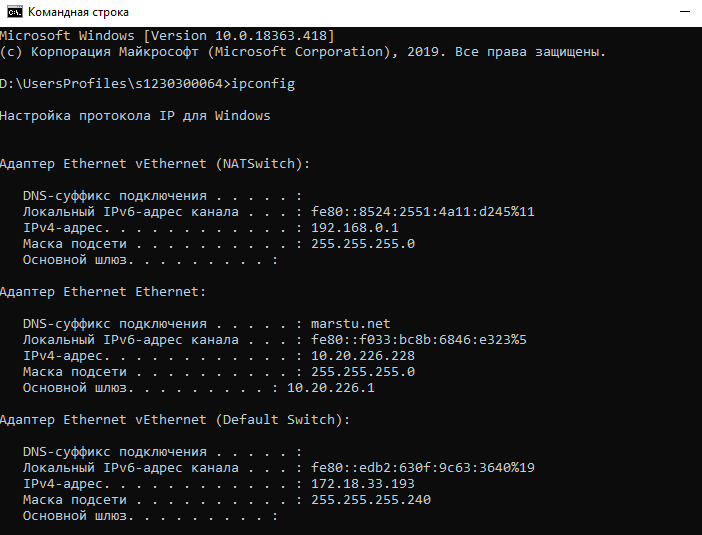


Рисунок 1. Результаты команды ipconfig

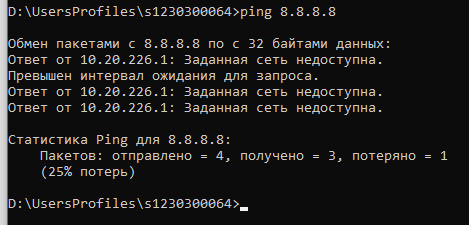


Рисунок 2. Результаты команды ping

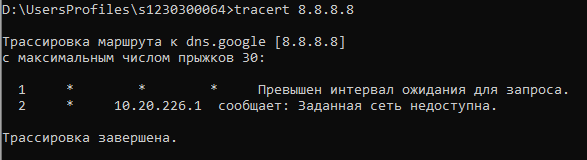


Рисунок 3. Результаты команды tracert



Рисунок 4. Результаты команды hostname

# Задание 3. Изучение утилиты ipconfig



Рисунок 5. Результаты команды ipconfig /?

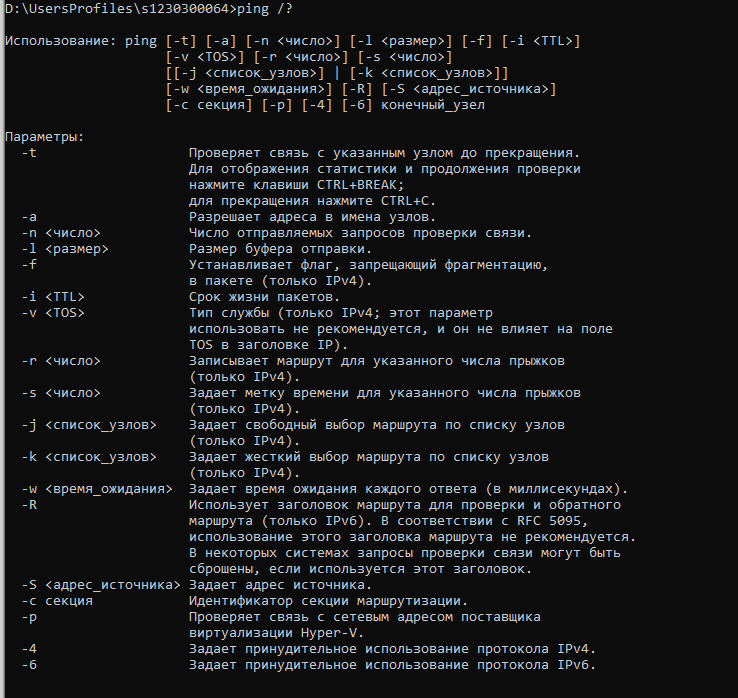


Рисунок 6. Результаты команды ping /?

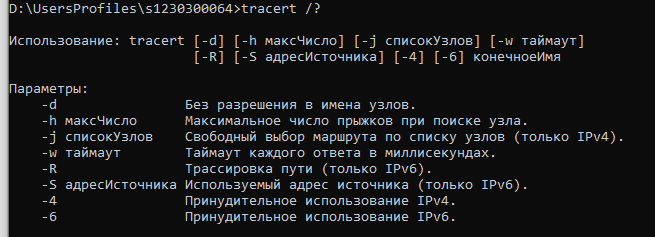


Рисунок 7. Результаты команды tracert /?

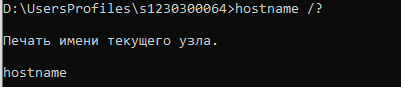


Рисунок 8. Результаты команды hostname /?

|  |  |
| --- | --- |
| Имя хоста | Ethernet Ethernet |
| IP-адрес | 10.20.226.246 |
| Маска подсети | 255.255.255.0 |
| Основной шлюз | 10.20.226.1 |
| Адрес DHCP сервера, если имеется | 10.0.0.2 |
| Описание адаптера | Realtek PCIe GbE Family Controller |
| Физический адрес сетевого адаптера | 70-85-C2-CF-7F-2F |
| Адрес DNS-сервера | 10.0.0.12  10.0.0.23 |
| Адрес WINS-сервера | Отсутствует |

Полезность информации для администратора сети и разработчика представлена ниже в виде таблицы.

|  |  |  |
| --- | --- | --- |
| Параметр | Администратор | Разработчик |
| IP адрес и Маска | Контроль конфликтов, настройка подсетей | Привязка серверов, настройка подключений |
| Шлюз | Диагностика connectivity (пинг до шлюза) | Понимание маршрута запросов |
| DHCP сервер | Борьба с неавторизованными серверами, диагностика | Настройка тестовых сред, embedded |
| DNS сервер | Настройка фильтрации, внутренние имена | Отладка проблем с именами |
| MAC адрес | Фильтрация на портах, резервация IP | Привязка лицензий, низкоуровневая идентификация |
| WINS сервер | Поддержка legacy-систем | Совместимость со старым ПО (редко) |
| Имя хоста | Идентификация устройства в сети | Логирование, верификация сертификатов |

# Задание 4. Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP.

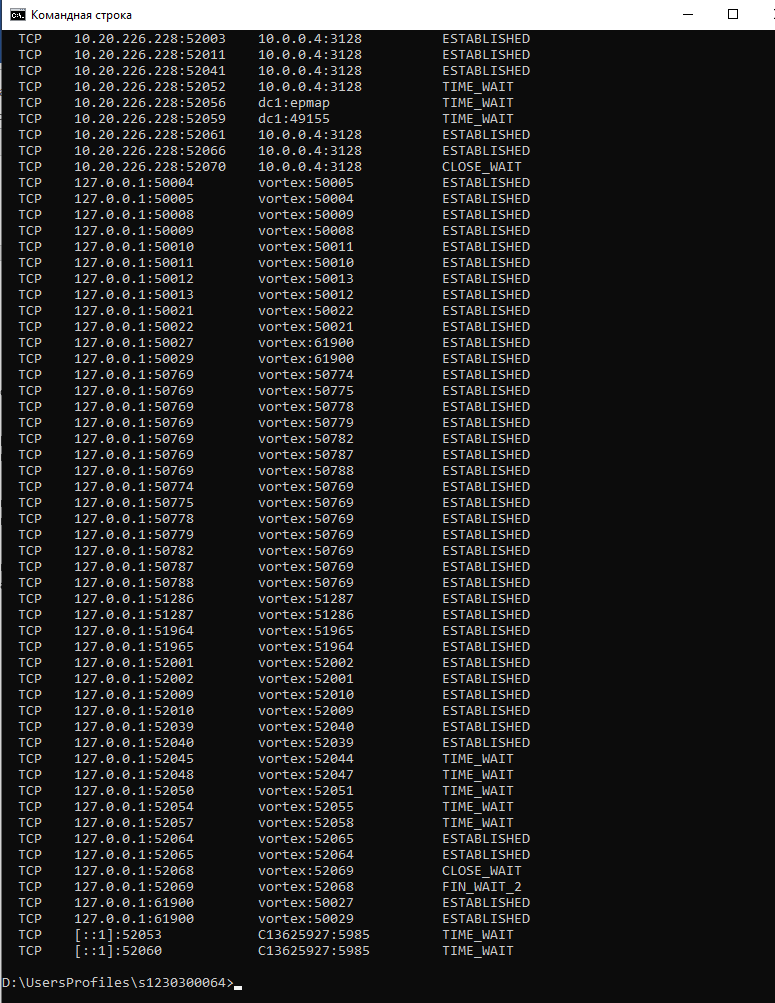


Рисунок 9. Результат команды netstat

Вывод о задании 4, практическая ценность команды netstat:

**Для Администратора/Сетевого инженера**: стетоскоп для прослушивания работы DNS. Основной инструмент для быстрой диагностики доступности ресурсов, проверки конфигурации и решения проблем пользователей.

**Для Разработчика (особенно Backend/DevOps):** способ проверить, видят ли внешние пользователи и другие сервисы вашу инфраструктуру так, как вы задумали. Критически важно для отладки взаимодействия микросервисов, работы API и настройки окружений.

**Для Специалиста по информационной безопасности**: Инструмент для расследования инцидентов: проверка, не ведёт ли подозрительное доменное имя на вредоносный IP, или для анализа фишинговых сайтов.

# Задание 5. Выбор ресурса для исследования доступа.

Выбрала вариант 1.

Выбор в пользу веб-приложения электронной коммерции **Ozon** был сделан на основании следующих критериев:

1. **Функциональное назначение:**  
   Онлайн-магазин представляет собой многофункциональную платформу, предназначенную для продажи товаров и услуг через интернет. Ресурс позволяет пользователю выполнять широкий спектр действий: искать товары, добавлять их в корзину, оформлять заказы, отслеживать доставку и управлять своим профилем.
2. **Критерий интерактивности:**  
   Сайт активно взаимодействует с пользователем, предоставляя возможность персонализации (например, рекомендации по истории покупок), авторизации, обратной связи и работы с базой данных заказов.
3. **Критерий динамичности:**  
   Ресурс динамически обновляет информацию (наличие товаров, цены, акции) и использует серверные технологии (например, API, базы данных, обработку запросов) для формирования контента в реальном времени.
4. **Критерий архитектуры и технологий:**  
   Ozon реализован как клиент-серверное веб-приложение с разделением фронтенд- и бэкенд-компонентов. Используются современные технологии веб-разработки — HTML5, CSS3, JavaScript, а также серверные языки и базы данных для обработки заказов и хранения информации о пользователях.
5. **Критерий значимости и актуальности:**  
   Электронная коммерция является одним из наиболее активно развивающихся направлений ИТ. Исследование такого ресурса позволяет изучить вопросы безопасности, аутентификации, обработки персональных данных и защиты финансовых транзакций.
6. **Критерий доступности для исследования:**  
   Ресурс общедоступен, не требует специальных разрешений для анализа интерфейса, структуры и механизма взаимодействия клиента с сервером.

# Задание 6. Тестирование связи с помощью утилиты ping

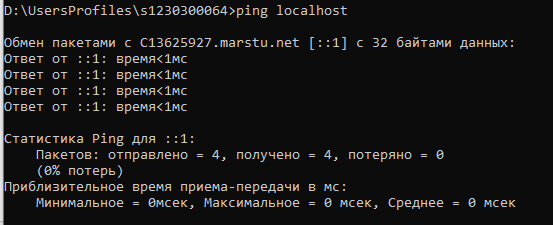


Рисунок 10. Результат команды ping localhost

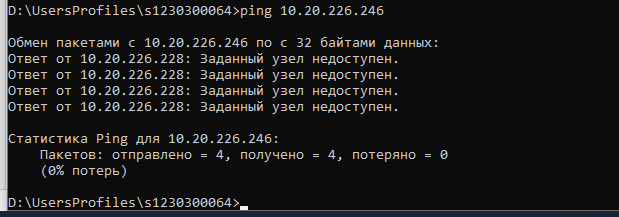


Рисунок 11. Результат команды ping 10.20.226.246

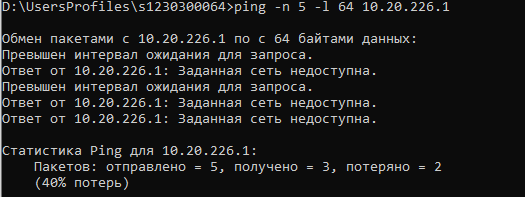


Рисунок 12. Результат команды ping -n 5 -l 64 10.20.226.1

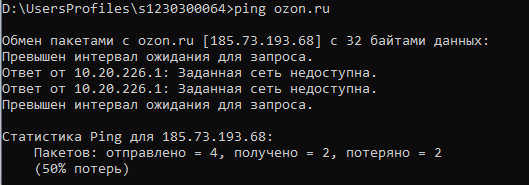


Рисунок 13. Результат команды ping ozon.ru

|  |  |  |  |
| --- | --- | --- | --- |
| Пункт | Команда | Ожидаемый результат | Что означает результат |
| A | Ping localhost | Ответ от С13625927.marstu.net | Стек TCP/IP работает корректно |
| B | Ping 10.20.226.246 | Ответ от 10.20.226.246 | Конфликта IP-адресов в сети нет. |
| C | ping -n 5 -l 64 10.20.226.1 | 5 ответов от шлюза, пинг 1-5мс | Связь с роутером стабильна. |
| D | ping ozon.ru | Ответ от IP-адреса Ozon | Сайт доступен, интернет работает. |

# Задание 7. Определение пути IP-пакета

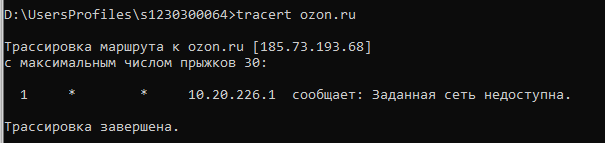


Рисунок 14. Результат команды tracert ozon.ru

tracert - определяет путь прохождения пакетов через сеть, отправляя эхо-запросы с возрастающим TTL.

Объяснение полученных результатов на рисунке 14:   
1. Превышен интервал ожидания для запроса.

Команда tracert отправила ему (Наш Wi-Fi роутер или маршрутизатор провайдера) запросы, но не получила ни одного ответа.

2. 10.20.226.1 сообщает: Заданная сеть недоступна.

Это ключевая ошибка. Она говорит о том, что у компьютера полностью отсутствует маршрут для доступа в любую внешнюю сеть, включая интернет.

Адрес 10.20.226.1 — это адрес какого-то внутреннего интерфейса роутера или сервера в локальной сети. Но система не знает, как через него выходить наружу.

# Ответы на контрольные вопросы

**1. Что такое IP-адрес и какую роль он играет в сети?**

IP-адрес (Internet Protocol Address) - это уникальный числовой идентификатор устройства в компьютерной сети, работающей по протоколу TCP/IP.

Он играет роль "почтового адреса" для вашего устройства (компьютера, телефона, принтера и т.д.) в сети. Когда одно устройство хочет отправить данные другому, оно указывает в пакете IP-адрес получателя. Это позволяет маршрутизаторам понять, куда нужно доставить этот пакет данных.

**2. Какое значение имеет маска подсети и как она используется?**

Маска подсети - это 32-битное число, определяющее структуру IP-адреса

Маска подсети определяет, какая часть IP-адреса относится к адресу сети, а какая -к адресу конкретного хоста (устройства) в этой сети.

Значение: Она позволяет разделить большую сеть на меньшие, логические подсети. Это повышает безопасность, упрощает управление трафиком и уменьшает "шум" в сети (широковещательный трафик).

Маска применяется к IP-адресу с помощью побитовой операции AND. Результат этой операции — адрес сети.

Пример: Устройство с IP `192.168.1.10` и маской `255.255.255.0` находится в сети `192.168.1.0`. Адрес хоста в этой сети - `.10`.

**3. Что такое DNS и какова его функция в сети?**

DNS (Domain Name System) - распределенная база данных для преобразования имен в IP-адреса.

DNS преобразует удобные для человека доменные имена (например, `google.com`) в понятные компьютерам IP-адреса (например, `142.251.209.14`), которые используются для маршрутизации пакетов данных. Без DNS нам пришлось бы запоминать числовые IP-адреса всех сайтов.

**4. Объясните разницу между статическим и динамическим IP-адресом.**

Статический IP:

* Назначается вручную администратором
* Постоянный, не изменяется со временем
* Используется для серверов, принтеров, сетевого оборудования
* Преимущества: стабильность, предсказуемость
* Недостатки: требует ручного управления

Динамический IP:

* Назначается автоматически сервером DHCP
* Временный, может изменяться
* Используется для рабочих станций, мобильных устройств
* Преимущества: автоматизация, экономия адресов
* Недостатки: возможны конфликты, нестабильность

**5. Что такое утилита ping и как она работает?**

Ping - это утилита для проверки достижимости узла в сети и измерения времени задержки (latency).

Как работает: Она отправляет на целевой узел пакеты по протоколу ICMP (Echo-Request) и ждет ответа (Echo-Reply). На основе полученных ответов она вычисляет время прохождения пакета туда и обратно и показывает потери пакетов.

**6. Какую информацию можно получить с помощью команды traceroute?**

Traceroute (или `tracert` в Windows) - это сетевая утилита для отслеживания пути, который проходят пакеты данных от исходного устройства до целевого узла через сеть Интернет.

Информация:

1. Список всех промежуточных маршрутизаторов (хостов) на пути.

2. Время отклика каждого из них (обычно отправляется 3 пакета).

3. Проблемные узлы, где пакеты теряются (обозначаются ``).

**7. Что такое NAT и как он используется в сетях?**

NAT (Network Address Translation) — это механизм, преобразующий частные (внутренние) IP-адреса в один публичный (внешний) IP-адрес при выходе в интернет, и наоборот.

Как используется: Это основа работы домашних и корпоративных сетей. Ваш роутер имеет один "белый" IP-адрес от провайдера, но раздает устройствам в локальной сети "серые" адреса (например, `192.168.1.x`). Когда вы заходите на сайт, роутер подменяет ваш внутренний адрес на свой внешний, а получив ответ, перенаправляет его нужному устройству. NAT решает проблему нехватки IPv4-адресов и повышает безопасность.

**8. Какова функция утилиты netstat?**

Netstat показывает статистику и информацию о сетевых соединениях, таблице маршрутизации и интерфейсах компьютера.

Функции. Позволяет увидеть:

Все установленные соединения (какие программы с какими адресами соединены).

Какие порты прослушиваются на компьютере (что может указывать на сервисы или malware).

Статистику по сетевым интерфейсам.

**9. Что такое DHCP и как он работает?**

DHCP (Dynamic Host Configuration Protocol) — это протокол, который автоматически назначает устройствам в сети IP-адреса и другие параметры (маску, шлюз, DNS-серверы).

Как работает (упрощенно):

1. Устройство подключается к сети и отправляет запрос `DHCP Discover`.

2. DHCP-сервер отвечает предложением `DHCP Offer` с набором параметров.

3. Устройство выбирает предложение и запрашивает его `DHCP Request`.

4. Сервер подтверждает выделение адреса пакетом `DHCP Ack`.

**10. Каковы основные команды для диагностики сетевых подключений в Windows?**

`ipconfig` – Показывает IP-адреса, шлюзы, маски для всех сетевых адаптеров.

`ipconfig /all` – Показывает всю информацию, включая DNS и MAC-адрес.

`ipconfig /release` – Освобождает текущий IP-адрес.

`ipconfig /renew` – Запрашивает новый IP-адрес у DHCP-сервера.

`ping` – Проверяет доступность узла.

`tracert` – Определяет путь к узлу.

`nslookup` – Проверяет работу DNS, запрашивает IP по имени и наоборот.

`netstat` – Показывает сетевые соединения и порты.

`getmac` – Показывает MAC-адреса сетевых адаптеров.

**11. Что такое TCP и UDP, и в чем их основные различия?**

Это транспортные протоколы, которые работают поверх IP.

|  |  |  |
| --- | --- | --- |
| Функция | TCP | UDP |
| Установление соединения | С установлением соединения (handshake). | Без установления соединения. |
| Надежность | Гарантированная доставка. Потерянные пакеты пересылаются | Пакеты могут быть потеряны. |
| Порядок доставки | Пакеты прибывают в правильном порядке. | Порядок не гарантируется. |
| Контроль перегрузки | Есть | Контроля перегрузки нет. |
| Примеры | Веб-браузинг (HTTP/S), email (SMTP), передача файлов (FTP). | Видеостриминг, онлайн-игры, VoIP(Skype, Zoom), DNS-запросы. |

**12. Как использовать утилиту nslookup для проверки DNS?**

Прямой запрос (имя -> IP): `nslookup google.com`

Обратный запрос (IP -> имя): `nslookup 8.8.8.8`

Запрос к конкретному DNS-серверу: `nslookup google.com 8.8.8.8` (спросит у Google DNS, а не у вашего провайдера)

Просмотр всех доступных DNS-записей (MX, TXT и т.д.): `nslookup -type=any google.com`

**13. Что такое MAC-адрес и где он используется?**

MAC-адрес (Media Access Control) — это физический и уникальный идентификатор сетевого адаптера (Wi-Fi, Ethernet), «прошитый» на заводе.

Где используется: На канальном уровне (L2) модели OSI. Он используется для коммутации фреймов в пределах одной локальной сети (LAN). Коммутаторы (switches) используют MAC-адреса, чтобы понять, на какой порт отправить фрейм. В интернете работают IP-адреса, а MAC-адреса меняются на каждом «прыжке» между маршрутизаторами.

**14. Как работает утилита whois и для чего она применяется?**

Whois — это протокол и утилита для запроса информации о доменных именах и IP-адресах.

Как работает: Она отправляет запрос к WHOIS-базам данных регистраторов (для доменов) или RIR (Regional Internet Registries, для IP).

Применение: Узнать:

Владельца домена (часто скрыто приватностью).

Дату регистрации и окончания срока действия домена.

Контактные данные администратора.

Принадлежность IP-адреса какому провайдеру.

**15. Что такое маршрутизация и как она осуществляется в сети?**

Маршрутизация — это процесс определения оптимального пути для передачи сетевого пакета от отправителя к получателю через промежуточные сети.

Как осуществляется: Специальные устройства — маршрутизаторы (роутеры) — имеют таблицы маршрутизации. Эти таблицы содержат правила, куда направить пакет с тем или иным адресом назначения. Маршрутизаторы обмениваются информацией друг с другом с помощью специальных протоколов маршрутизации (BGP, OSPF), чтобы строить и поддерживать актуальные таблицы.

**16. Каковы основные типы сетевых протоколов? Приведите примеры.**

Прикладного уровня (Application): HTTP, HTTPS, FTP, SMTP, POP3, IMAP, DNS, DHCP.

Транспортного уровня (Transport): TCP, UDP.

Сетевого уровня (Network): IP, ICMP, ARP.

Канального уровня (Data Link): Ethernet, Wi-Fi (IEEE 802.11), PPP.

Физического уровня (Physical): Витая пара (Ethernet), оптоволокно, радиоволны (Wi-Fi).

**17. Что такое "шум" в контексте сетевой передачи данных?**

"Шум" (или широковещательный трафик, broadcast) — это сетевые пакеты, которые адресованы не конкретному устройству, а всем устройствам в сети. Например, ARP-запросы ("У кого такой IP-адрес? Ответьте мне!") или DHCP-запросы. Избыточный "шум" может загружать сеть и снижать ее производительность.

**18. Какова роль сетевых интерфейсов в компьютере?**

Сетевой интерфейс — это точка соединения между компьютером и сетью. Это может быть физическое устройство (сетевая карта, Wi-Fi адаптер) или виртуальное (VPN-адаптер, адаптер виртуальной машины).

Роль: Предоставить операционной системе аппаратные средства и драйверы для отправки и приема данных по сети. Каждому интерфейсу присваивается свой MAC- и IP-адрес.

**19. Что такое "ping" и как его можно использовать для проверки доступности узла в сети?**

Ping — основной инструмент проверки доступности. Если вы пингуете узел (например, `ping ya.ru`) и получаете ответы, это означает:

1. Ваш компьютер имеет рабочее сетевое подключение.

2. Ваш DNS-сервер работает (преобразовал `ya.ru` в IP).

3. Между вами и целевым узлом есть сетевая связь.

4. Сам целевой узел работает и отвечает.

**20. Какова разница между локальной и глобальной адресацией в сети Интернет?**

|  |  |
| --- | --- |
| Локальная (частная) адресация (Private IP) | Глобальная (публичная) адресация (Public IP) |
| Используется внутри частных сетей (дома, офиса) | Используется для идентификации устройств в глобальной сети Интернет |
| Адреса не маршрутизируются в интернете. | Адреса уникальны и маршрутизируются по всему интернету |
| Диапазоны: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255,  192.168.0.0 – 192.168.255.255 | Все остальные адреса, не входящие в частные диапазоны |
| Могут повторяться в разных частных сетях | Не могут повторяться |
| Доступ в интернет через NAT | Прямой доступ в интернет |