Тема 1. Введение в веб-разработку. Инструменты веб-разработки

Практическая работа 1. Утилиты работы с сетью

Задание 1. Получение справочной информации по командам

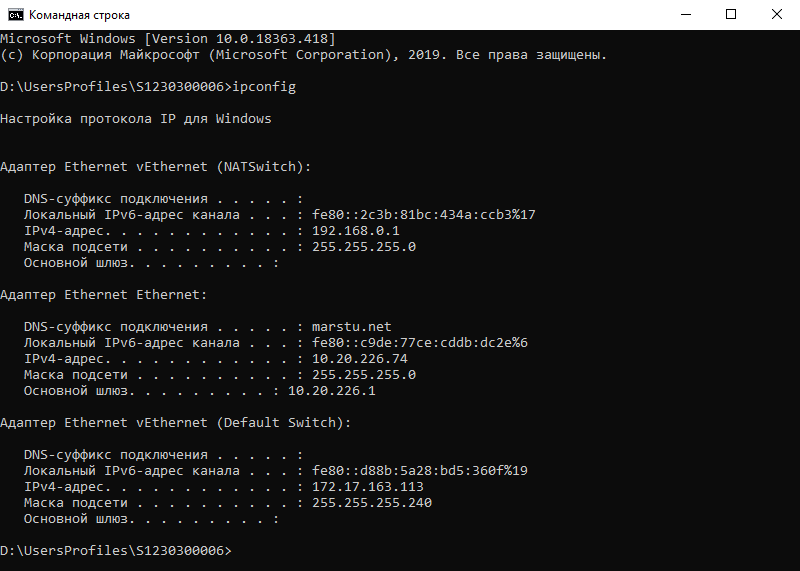


Рис. 1 команда ipconfig

Таким образом, утилита ipconfig позволяет выяснить, инициализирована ли конфигурация и не дублируются ли IP-адреса:

• если конфигурация инициализирована, то появляется IP-адрес, маска, шлюз;

• если IP-адреса дублируются, то маска сети будет 0.0.0.0;

• если при использовании DHCP компьютер не смог получить IP-адрес, то он будет равен 0.0.0.0

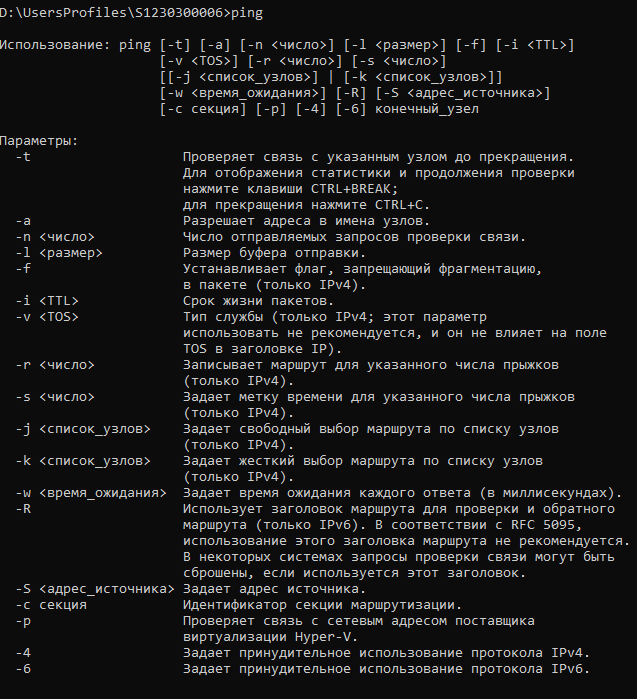


Рис. 2 команда просто ping

Это мы вывели информацию о команде

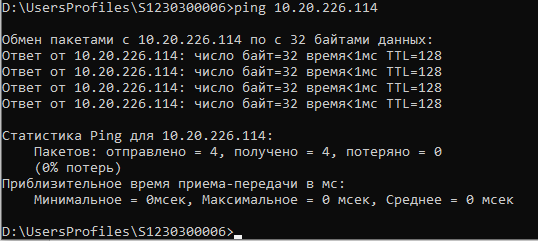


Рис. 3 команда ping

Мы пинганули соседний, локальный, ПК.

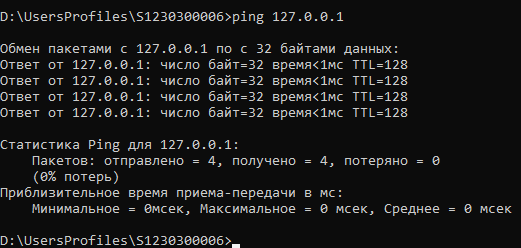


Рис. 4 команда ping

Для проверки того, что TCP/IP установлен и правильно сконфигурирован на локальном компьютере, в команде ping задается адрес петли обратной связи (loopback address):

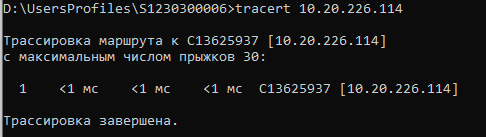


Рис. 5 команда tracert

Утилита tracert работает следующим образом: посылается по 3 пробных эхо - пакета на каждый хост, через который проходит маршрут до удаленного хоста. На экран при этом выводится время ожидания ответа на каждый пакет (Его можно изменить с помощью параметра - w). Пакеты посылаются с различными величинами времени жизни. Каждый маршрутизатор, встречающийся по пути, перед перенаправлением пакета уменьшает величину TTL на единицу. Таким образом, время жизни является счетчиком точек промежуточной доставки. Когда время жизни пакета достигнет нуля, предполагается, что маршрутизатор пошлет в компьютер - источник сообщение ICMP “Time Exeeded” (Время истекло). Маршрут определяется путем посылки первого эхо - пакета с TTL=1. Затем TTL увеличивается на 1 в каждом последующем пакете до тех пор, пока пакет не достигнет удаленного хоста, либо будет достигнута максимально возможная величина TTL (по умолчанию 30, задается с помощью параметра - h). Маршрут определяется путем изучения сообщений ICMP, которые присылаются обратно промежуточными маршрутизаторами. Примечание: некоторые маршрутизаторы просто молча уничтожаю т пакеты с истекшим TTL и не будут видны утилите tracert. Синтаксис: tracert [-d] [-h maximum\_hops] [-j host-list] [-w timeout] имя\_целевого\_хоста 46 Параметры: -d - указывает, что не нужно распознавать адреса для имен хостов; - h maximum\_hops - указывает максимальное число ходов для того, чтобы найти цель; - j host-list - указывает нежесткую статическую маршрутизацию в соответствии с host-list; - w timeout - указывает, что нужно ожидать ответ на каждый эхо-пакет заданное число мсек. Пример использования утилиты tracert:

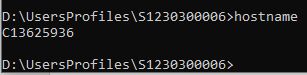


Рис. 6 команда hostname

Команда hostname - cетевая команда Windows HostName просто отображает текущее имя компьютера Windows. Это имя, по которому ваш компьютер идентифицируется другими устройствами и серверами в вашей локальной сети. Это имя также можно найти на странице сведений о системе графического интерфейса, однако эта команда быстрее.

Задание 2. Получение имени хоста

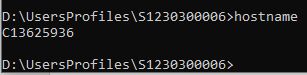


Рис. 7 команда hostname

C13625936 – Имя моего ПК

Задание 3. Изучение утилиты ipconfig

Таблица 1.3. Конфигурация TCP/IP

|  |  |
| --- | --- |
| Имя хоста | C13625936 |
| IP-адрес | 10.20.226.74 |
| Маска подсети | 255.255.255.0 |
| Основной шлюз | 10.20.226.1 |
| Используется ли DHCP (адрес DHCP-сервера) | 10.0.0.2 |
| Описание адаптера | Адаптер Ethernet Ethernet: |
| Физический адрес сетевого адаптера | 70-85-C2-D2-91-22 |
| Адрес DNS - сервера | 10.0.0.12 |
| Адрес WINS - сервера | 10.0.0.23 |

|  |  |
| --- | --- |
| Имя хоста | Уникальное имя, присвоенное устройству в сети для его идентификации. |
| IP-адрес | Уникальный числовой идентификатор устройства в сети, используемый для маршрутизации пакетов. |
| Маска подсети | Число, определяющее, какая часть IP-адреса относится к сети, а какая — к хосту. |
| Основной шлюз | IP-адрес маршрутизатора, через который устройство выходит в другие сети (например, в интернет). |
| Используется ли DHCP (адрес DHCP-сервера) | Протокол, автоматически назначающий IP-адреса и другие параметры сети. Здесь указан адрес сервера, который предоставляет эти настройки. |
| Описание адаптера | Название сетевого интерфейса (аппаратного или виртуального), через который устройство подключено к сети. |
| Физический адрес сетевого адаптера | Уникальный аппаратный идентификатор сетевой карты, используемый для идентификации устройства на канальном уровне. |
| Адрес DNS - сервера | IP-адрес сервера, который преобразует доменные имена (например, example.com) в IP-адреса. |
| Адрес WINS - сервера | IP-адрес сервера, который преобразует NetBIOS-имена в IP-адреса (используется в сетях Windows). |

**Диагностика сети** — Знание IP-адреса, маски подсети и шлюза позволяет быстро определить, к какой подсети принадлежит устройство, и проверить правильность маршрутизации.

**Устранение неполадок** — Если устройство не выходит в сеть, администратор может проверить, правильно ли настроены IP, шлюз, DNS и DHCP.

**Контроль безопасности** — MAC-адрес помогает идентифицировать устройство в сети, а знание DHCP-сервера — контролировать, какие устройства получают адреса автоматически.

**Настройка сетевых служб** — Информация о DNS и WINS позволяет настроить корректное разрешение имен в сети.

**Документирование сети** — Все параметры важны для ведения актуальной документации по сетевой инфраструктуре.

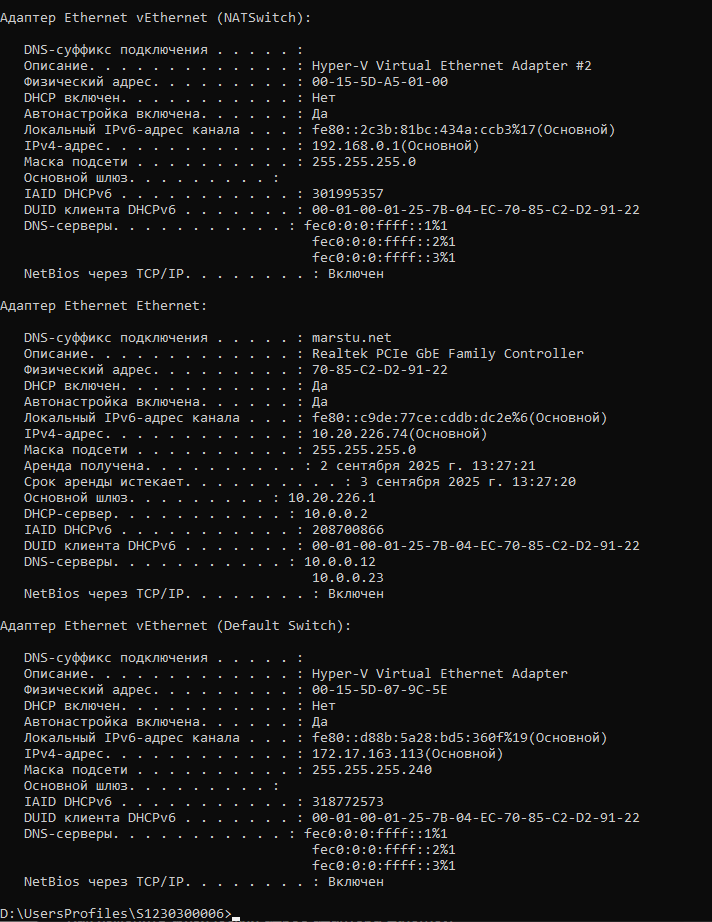


Рис. 8 команда ipconfig/all

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

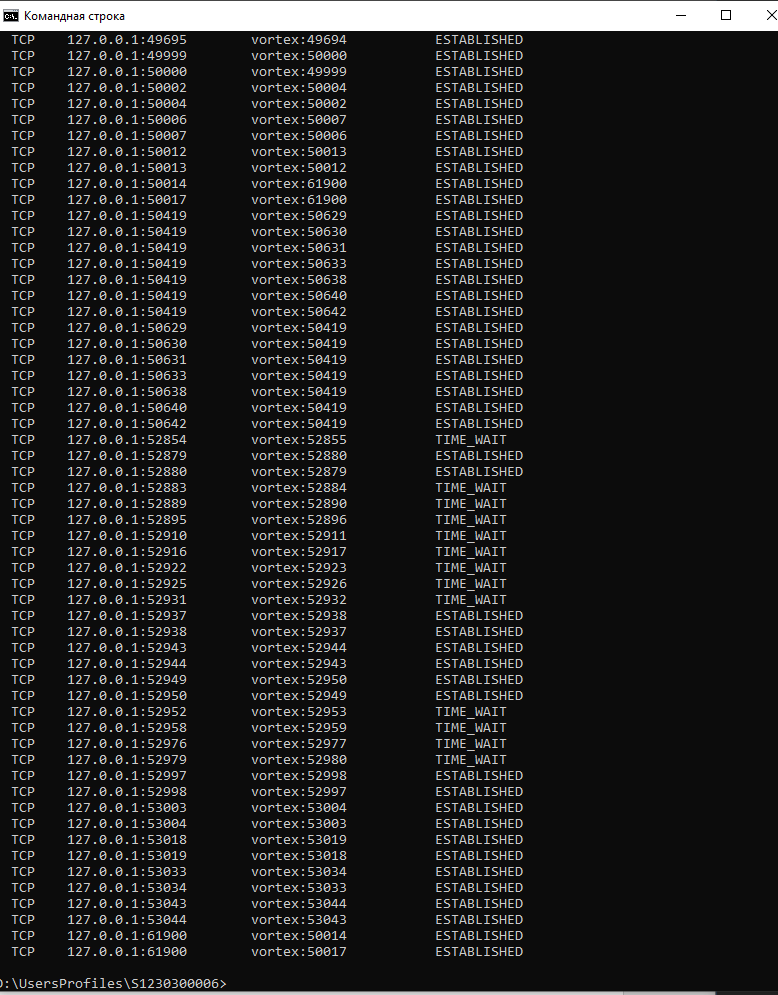


Рис. 9 команда netstat

Задание 5. Выбор ресурса для исследования доступа.

Таблица 1.4. Исследование сетевого ресурса

По предоставленному преподавателем варианту подберите сетевой ресурс для дальнейшего исследования согласно таблице 1.4:

|  |  |
| --- | --- |
| Номер варианта | Класс сетевого ресурса |
| 1 | Веб-приложение электронной коммерции |

Для выбранного ресурса, в отчет внесите обоснование того, согласно каким критериям, был сделан выбор в пользу сетевого ресурса.

Пример: Wildberries, Ozon, Amazon

|  |  |
| --- | --- |
| Критерий | Обоснование |
| **Актуальность** | Электронная коммерция — одна из самых динамично развивающихся отраслей, особенно в России и мире. Исследование таких ресурсов позволяет изучать современные тренды в IT, безопасности, пользовательском опыте и масштабируемости систем. |
| **Пользовательский опыт (UX/UI)** | Успех платформы зависит от удобства интерфейса, скорости загрузки, адаптивности под разные устройства. Исследование позволяет анализировать лучшие практики дизайна и оптимизации производительности. |
| **Безопасность** | Такие ресурсы обрабатывают большое количество личных данных пользователей и платежную информацию, что требует высокого уровня защиты. Исследование позволяет анализировать методы аутентификации, шифрования, защиты от мошенничества и DDoS-атак. |
| **Масштабируемость** | Популярные платформы электронной коммерции должны выдерживать высокую нагрузку, особенно во время распродаж. Исследование таких систем помогает понять, как реализованы балансировка нагрузки, кэширование, резервное копирование и восстановление после сбоев. |
| **Доступность для исследования** | Многие крупные платформы предоставляют публичные API, документацию, а также имеют открытые вакансии и кейсы, что облегчает сбор информации для анализа. |
| **Интеграция с внешними сервисами** | Веб-приложения электронной коммерции часто интегрируются с платежными системами, службами доставки, CRM, аналитическими инструментами. Это позволяет изучать API, протоколы обмена данными, стандарты безопасности. |
| **Сложность и функциональность** | Веб-приложения электронной коммерции включают в себя множество компонентов: каталог товаров, корзину, систему оплаты, личный кабинет, отзывы, рекомендательные системы, логистику. Это позволяет изучать взаимодействие фронтенда и бэкенда, работу с базами данных, API, микросервисами. |

* **Для студентов/разработчиков:** Понимание архитектуры высоконагруженных систем, современных технологий и подходов к разработке.
* **Для администраторов:** Анализ методов обеспечения безопасности, мониторинга и оптимизации производительности.
* **Для бизнеса:** Выявление лучших практик для повышения конверсии, удержания клиентов и защиты данных.

Задание 6. Тестирование связи с помощью утилиты ping

**Выбранный ресурс:** [Wildberries](https://www.wildberries.ru) (IP-адрес: 95.108.211.11)

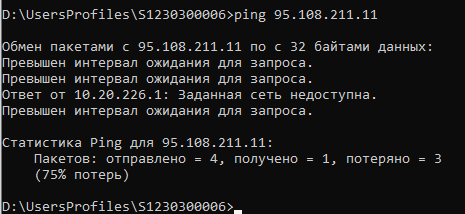


Рис. 10 команда ping 95.108.211.11

А. Пинг идёт

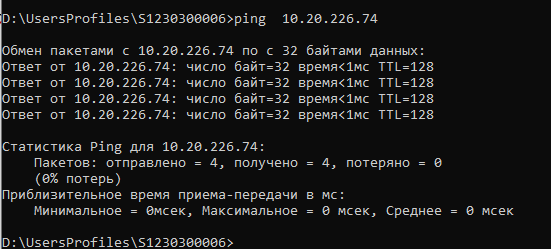


Рис. 11 команда ping 10.20.226.74

**b. Ответ от локального IP без потерь пакетов подтверждает, что компьютер правильно подключен к сети и его IP-адрес не конфликтует с другими устройствами.**

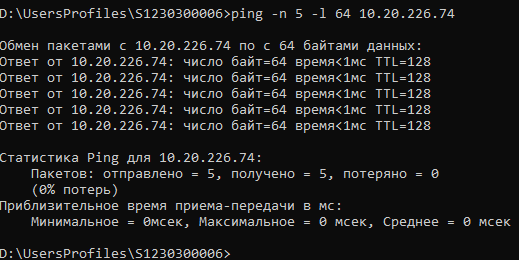


Рис. 12 команда ping -n 5 -l 64 10.20.226.74

ping -n 5 -l 64 10.20.226.74

**c. Проверка функционирования шлюза по умолчанию (5 эхо-пакетов длиной 64 байта)**

Ответ от шлюза без потерь пакетов и с малым временем отклика (1 мс) означает, что шлюз по умолчанию работает корректно и маршрутизирует трафик.

**d. Проверка возможности установления соединения с удаленным хостом**

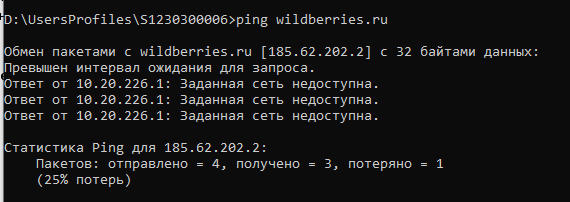


Рис. 13 команда ping wildberries.ru

Имеются проблемы в маршрутизации.

Задание 7. Определение пути IP-пакета

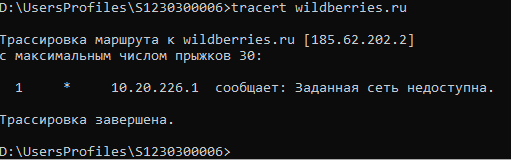


Рис. 14 команда tracert wildberries.ru

* **10.20.226.1** — это ваш **основной шлюз** (маршрутизатор).
* **Сообщение "Заданная сеть недоступна"** означает, что ваш шлюз **не знает маршрута** до сети, в которой находится адрес 185.62.202.2, или **нет подключения к интернету**.
* **Звёздочка (\*)** — отсутствие ответа от первого узла (возможно, шлюз блокирует ICMP-пакеты или не отвечает на tracert).

Задание 8. Сохранение отчета и отправка на проверку

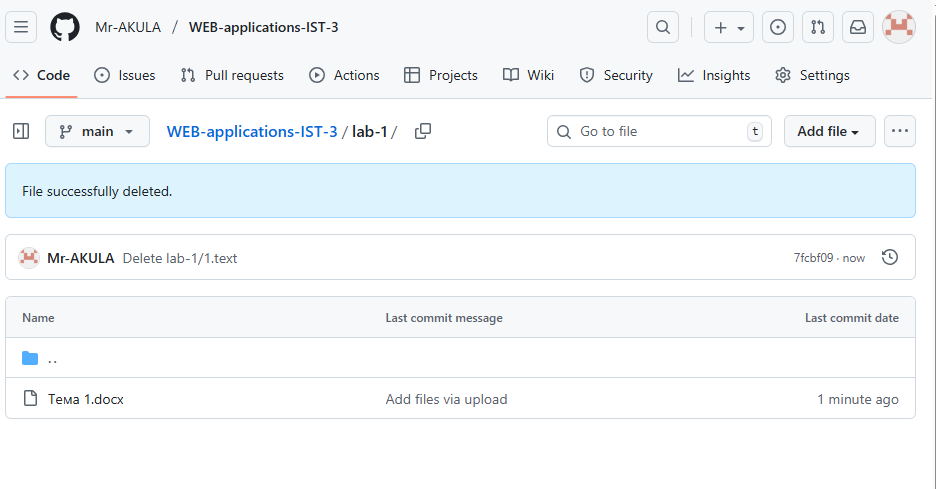


Рис. 15 git

Контрольные вопросы

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

IP-адрес — уникальный числовой идентификатор устройства в сети, используемый для маршрутизации пакетов данных. Обеспечивает доставку информации от отправителя к получателю.

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

Маска подсети определяет, какая часть IP-адреса относится к сети, а какая — к хосту. Используется для разделения сети на подсети и определения, какие устройства находятся в одной локальной сети.

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

DNS (Domain Name System) — система, преобразующая доменные имена (например, wildberries.ru) в IP-адреса. Обеспечивает удобство использования сети, позволяя обращаться к ресурсам по именам, а не по числовым адресам.

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

Статический IP назначается вручную и не изменяется. Используется для серверов и устройств, к которым нужен постоянный доступ.

Динамический IP назначается автоматически (например, через DHCP) и может изменяться при каждом подключении. Удобен для обычных пользователей.

5. Что такое утилита ping и как она работает?

Ping — утилита для проверки доступности узла в сети. Отправляет ICMP-эхо-запросы и ждёт ответов. Позволяет оценить время отклика и потери пакетов.

6. Какую информацию можно получить с помощью команды traceroute?

Traceroute (или tracert в Windows) показывает путь пакетов до целевого узла, выводит IP-адреса и время отклика всех промежуточных маршрутизаторов. Помогает диагностировать проблемы маршрутизации.

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

NAT (Network Address Translation) — технология, позволяющая нескольким устройствам в локальной сети использовать один внешний IP-адрес для доступа в интернет. Экономит IPv4-адреса и повышает безопасность.

8. Какова функция утилиты netstat?

Netstat отображает активные сетевые соединения, порты, статистику по протоколам (TCP, UDP, ICMP, IP). Используется для мониторинга и диагностики сетевой активности.

9. Что такое DHCP и как он работает?

DHCP (Dynamic Host Configuration Protocol) автоматически назначает IP-адреса и другие параметры сети (маска, шлюз, DNS) устройствам. Упрощает администрирование сети.

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

ping — проверка доступности узла.

tracert — трассировка маршрута.

ipconfig — просмотр сетевых настроек.

netstat — просмотр активных соединений.

nslookup — проверка DNS.

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

TCP — надёжный, ориентированный на соединение протокол (гарантирует доставку пакетов, контроль ошибок).

UDP — ненадёжный, без установки соединения (быстрее, но не гарантирует доставку).

Примеры: TCP — веб-сайты, email; UDP — потоковое видео, онлайн-игры.

12. Как использовать утилиту nslookup для проверки DNS?

Nslookup позволяет вручную отправлять запросы к DNS-серверам для получения IP-адреса по доменному имени и наоборот.

Пример:

Copynslookup wildberries.ru

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

MAC-адрес — уникальный аппаратный идентификатор сетевого адаптера. Используется на канальном уровне для идентификации устройств в локальной сети.

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

Whois — утилита для получения информации о владельце домена или IP-адреса (регистратор, контакты, даты регистрации). Используется для проверки прав на домен и диагностики сетевых проблем.

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

Маршрутизация — процесс выбора пути для передачи пакетов данных от отправителя к получателю через промежуточные узлы (маршрутизаторы). Осуществляется на основе таблиц маршрутизации.

16. Каковы основные типы сетевых протоколов? Приведите примеры.

Протоколы маршрутизации: RIP, OSPF, BGP.

Транспортные протоколы: TCP, UDP.

Протоколы приложений: HTTP, FTP, DNS, SMTP.

Протоколы канального уровня: Ethernet, PPP.

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

Шум — помехи, искажающие сигнал при передаче данных по физическим каналам (кабели, радиочастоты). Может приводить к ошибкам и потере пакетов.

18. Какова роль сетевых интерфейсов в компьютере?

Сетевые интерфейсы (сетевые карты, Wi-Fi адаптеры) обеспечивают физическое и логическое подключение компьютера к сети, преобразуют данные для передачи по каналам связи.

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

Ping — утилита для проверки доступности узла путём отправки ICMP-эхо-запросов. Позволяет оценить время отклика и потери пакетов, что помогает диагностировать проблемы с подключением.

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

Локальная адресация — используется внутри частной сети (например, 192.168.x.x, 10.x.x.x). Не маршрутизируется в интернете.

Глобальная адресация — уникальные публичные IP-адреса, маршрутизируемые в интернете (например, 8.8.8.8).