**Задание 1. Получение справочной информации по командам**

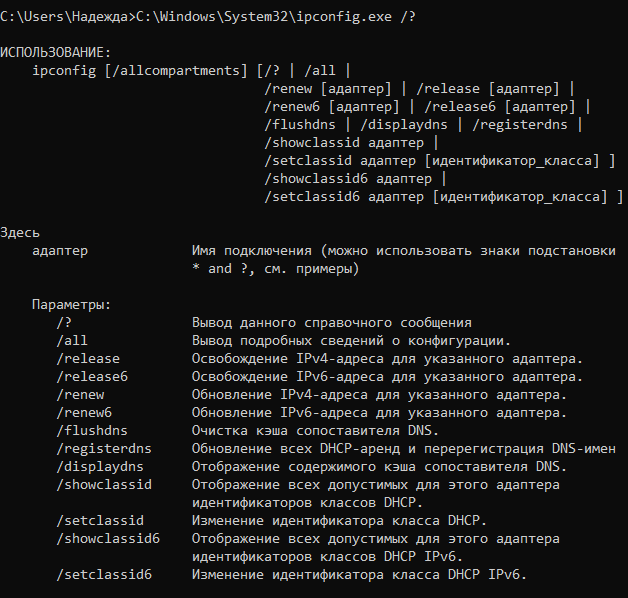


Рис. 1.1: Справочная информация ipconfig

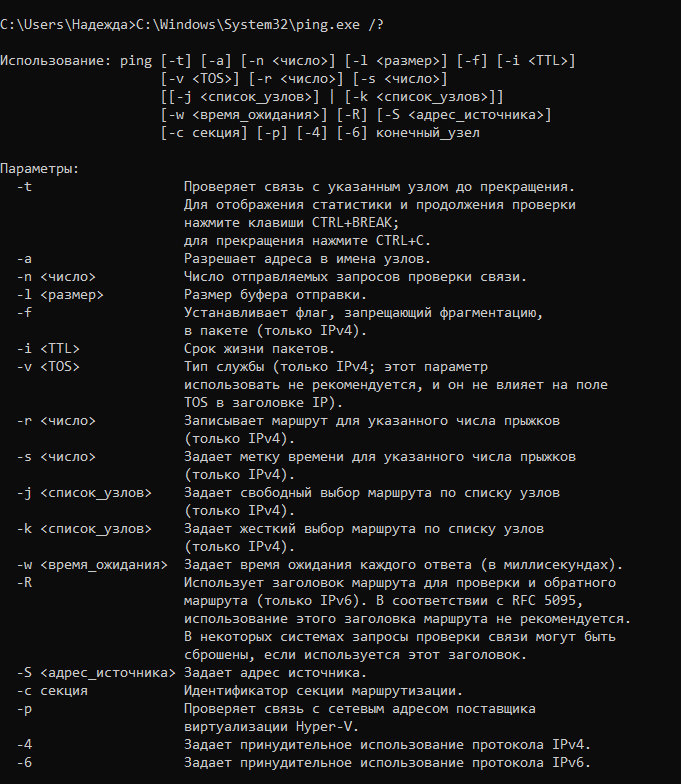


Рис. 1.2: Справочная информация ping

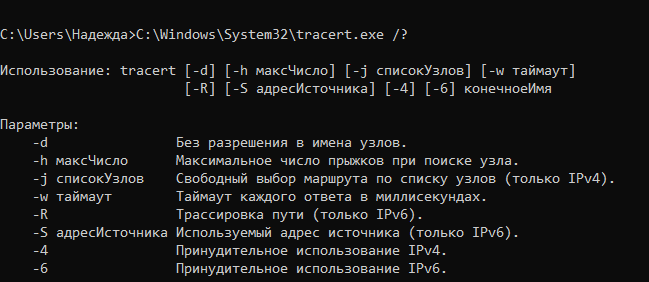


Рис. 1.3: Справочная информация tracert

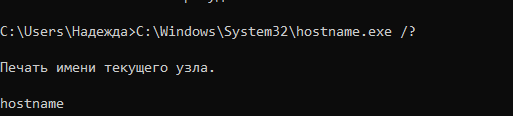


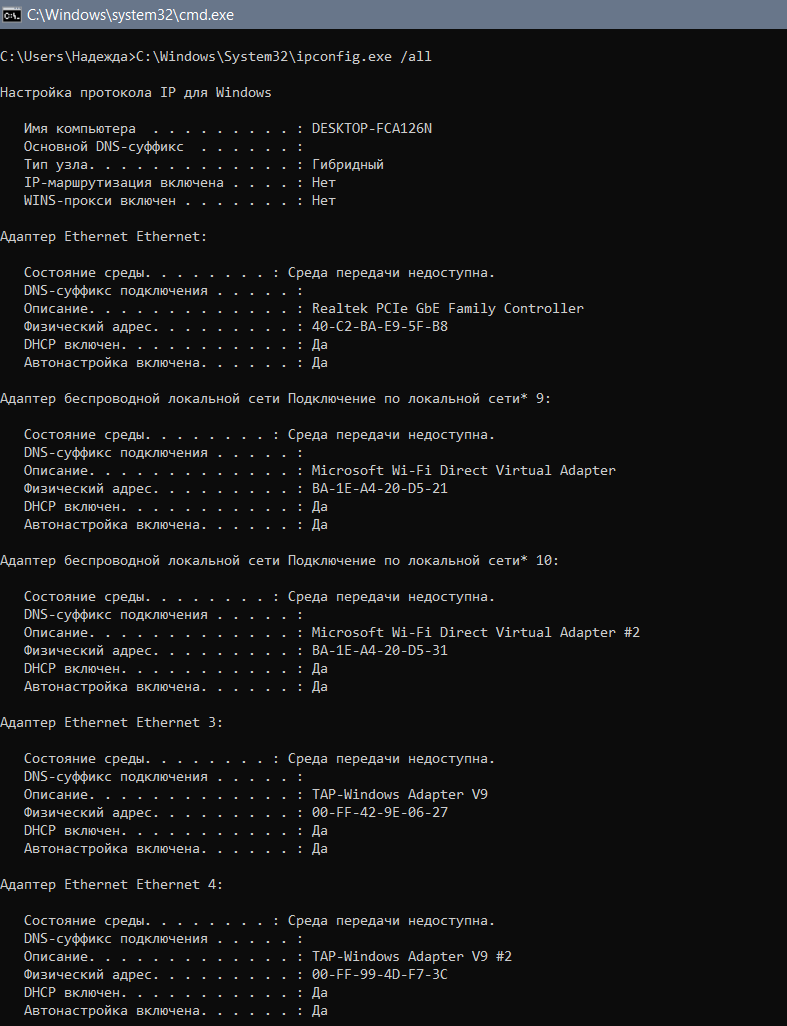
Рис. 1.4: Справочная информация hostname

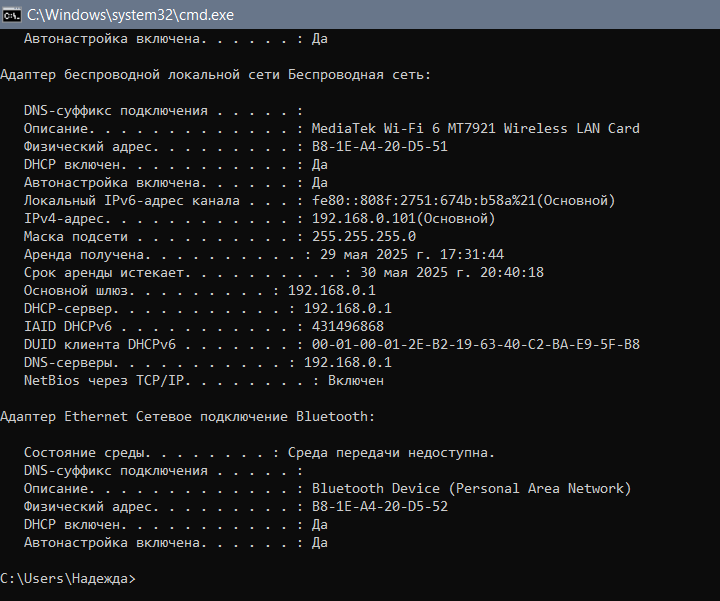
**Задание 2. Получение имени хоста**

****

Рис. 2: Справочная информация получения хоста

**Задание 3. Изучение утилиты ipconfig**

****

****

| **Параметр** | **Значение** |
| --- | --- |
| **Имя хоста** | DESKTOP-FCA126N |
| **IP-адрес** | 192.168.0.101 |
| **Маска подсети** | 255.255.255.0 |
| **Основной шлюз** | 192.168.0.1 |
| **Используется ли DHCP** | Да (DHCP-сервер: 192.168.0.1) |
| **Описание адаптера** | MediaTek Wi-Fi 6 MT7921 Wireless LAN Card |
| **Физический адрес (MAC)** | B8-1E-A4-20-D5-51 |
| **Адрес DNS-сервера** | 192.168.0.1 |
| **Адрес WINS-сервера** | Не используется (не указан в выводе) |

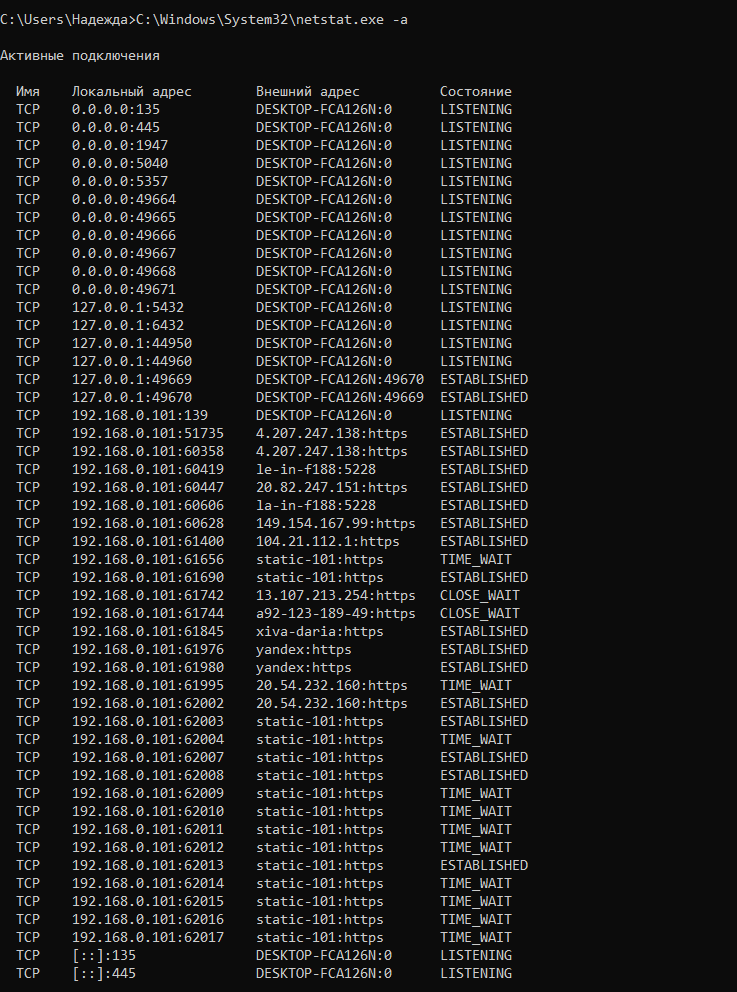
**1. Краткие определения параметров:**

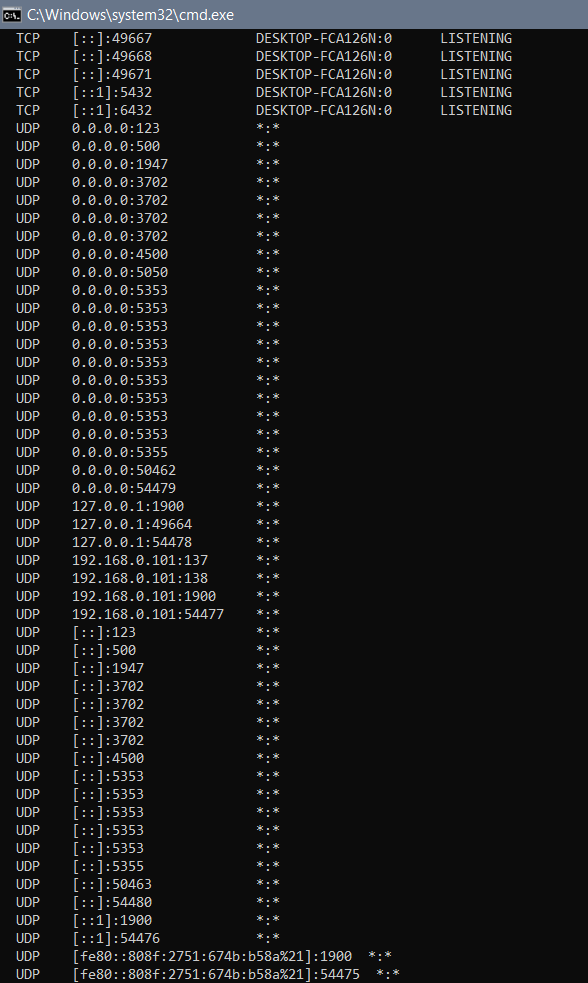
* **Имя хоста**: Уникальное сетевое имя компьютера в локальной сети (DESKTOP-FCA126N)
* **IP-адрес**: Логический адрес устройства в сети IPv4 (192.168.0.101)
* **Маска подсети**: Определяет границы сети (255.255.255.0 = сеть 192.168.0.0, доступно 254 хоста)
* **Основной шлюз**: IP-адрес маршрутизатора, связывающего локальную сеть с внешними сетями (192.168.0.1)
* **DHCP**: Протокол автоматической выдачи IP-адресов (сервер: 192.168.0.1)
* **MAC-адрес**: Физический идентификатор сетевого адаптера (B8-1E-A4-20-D5-51)
* **DNS-сервер**: Сервер для преобразования доменных имён в IP-адреса (192.168.0.1)
* **WINS-сервер**: Устаревшая служба разрешения NetBIOS-имён (не используется в современных сетях)

**2. Практическая ценность информации:**

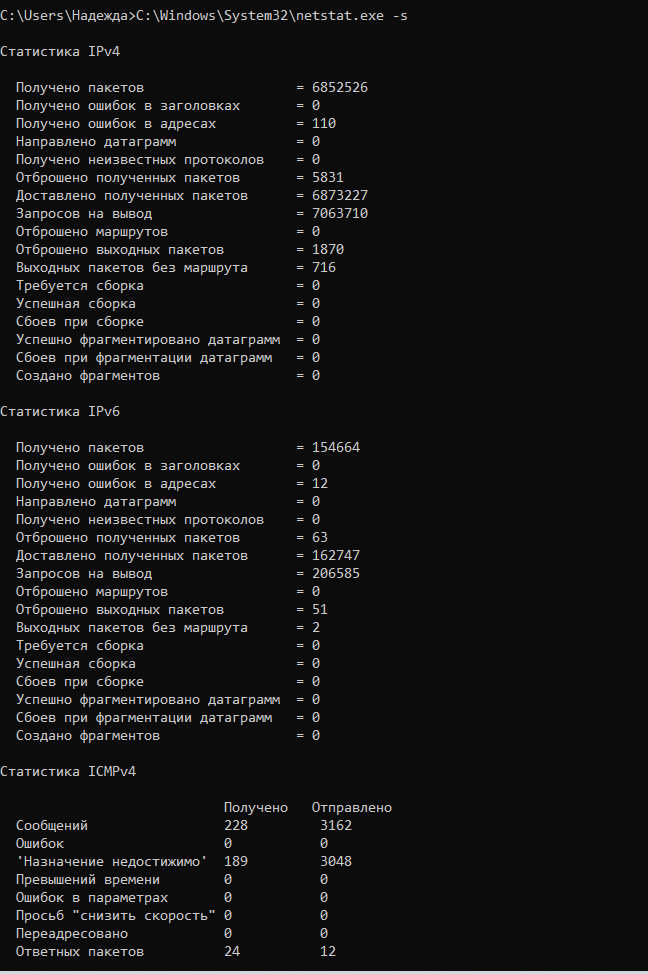
* **Для сетевого администратора**:
  + Диагностика проблем подключения (отсутствие IP, конфликт адресов)
  + Проверка правильности сетевых настроек
  + Определение точки отказа (шлюз, DNS)
  + Идентификация устройств по MAC-адресу для контроля доступа
  + Мониторинг срока аренды DHCP
* **Для разработчика**:
  + Тестирование приложений в текущей сетевой среде
  + Отладка сетевых взаимодействий
  + Настройка доступа к локальным ресурсам
  + Проверка доступности серверов и служб
  + Анализ сетевой инфраструктуры для проектирования распределенных систем

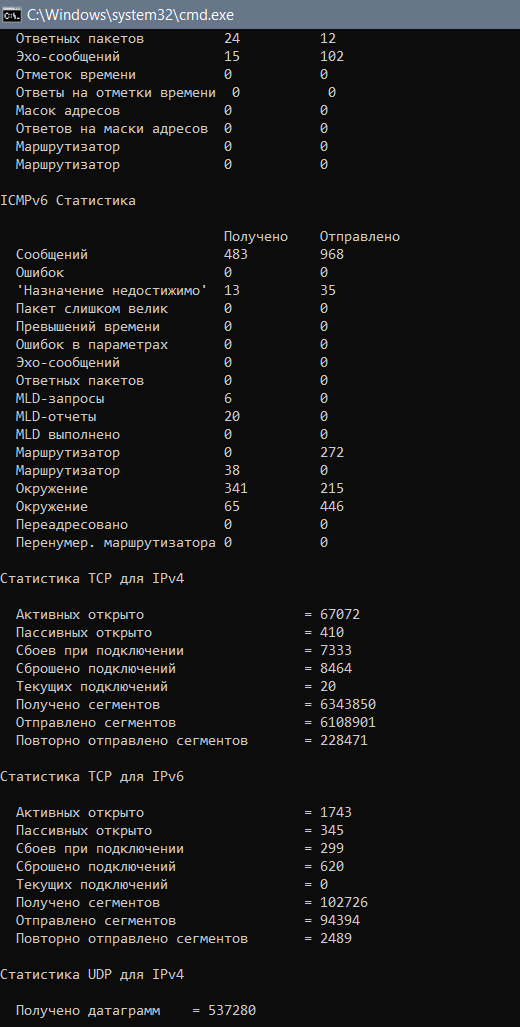
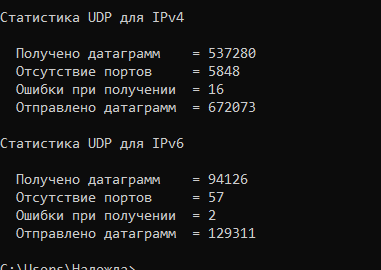
**Задание 4. Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP**

**netstat -a (фрагмент)**

****

**netstat -s (фрагмент)**

****

** **

1. **Что иллюстрируют результаты:**
   * netstat -a показывает:
     + Все активные сетевые соединения (ESTABLISHED)
     + Прослушиваемые порты (LISTENING)
     + Тип протокола (TCP/UDP)
     + Локальные и удалённые адреса с портами
   * netstat -s предоставляет:
     + Статистику по пакетам для IPv4/IPv6
     + Данные по ошибкам передачи
     + Количество активных/закрытых TCP-соединений
     + Статистику по UDP-пакетам
2. **Практическая ценность для администратора:**
   * **Безопасность**: Выявление неавторизованных соединений
     + Пример: Неизвестные ESTABLISHED-подключения к подозрительным IP
     + Прослушивание нестандартных портов
   * **Диагностика проблем**:
     + Большое количество "TIME\_WAIT" соединений → Проблемы с закрытием сокетов
     + Рост ошибок в статистике → Проблемы с сетевой картой или драйверами
   * **Оптимизация ресурсов**:
     + Анализ загрузки портов
     + Выявление неиспользуемых служб
3. **Практическая ценность для разработчика:**
   * **Отладка приложений**:
     + Проверка открытых портов серверного приложения
     + Выявление утечек сокетов (растущее число соединений)
   * **Анализ сетевого взаимодействия**:
     + Мониторинг активности приложения в реальном времени
     + Проверка установленных соединений с БД, API и др.
   * **Тестирование производительности**:
     + Оценка количества обрабатываемых соединений
     + Анализ потерь пакетов (через статистику ошибок)

**Задание 5. Выбор ресурса для исследования доступа**

**Вариант 1:** Веб-приложение электронной коммерции (например, amazon.com)

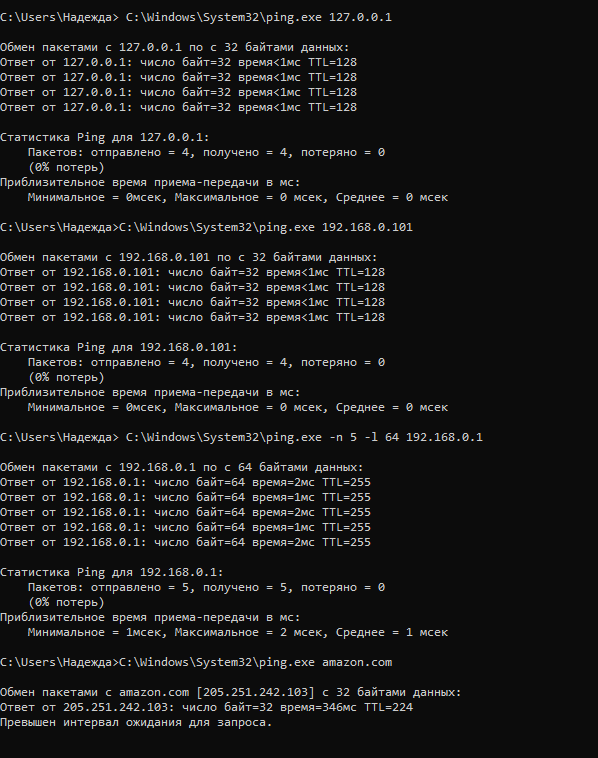
### Обоснование выбора Amazon.com для исследования

Amazon.com был выбран в качестве сетевого ресурса для исследования по ряду веских причин, соответствующих заданной категории веб-приложения электронной коммерции. Этот ресурс представляет собой глобального лидера в сфере онлайн-торговли, что делает его эталонным примером для изучения. Его инфраструктура демонстрирует все ключевые характеристики современных промышленных решений: географически распределённые серверы, сложную систему балансировки нагрузки, интегрированную CDN-сеть и микросервисную архитектуру.

Технологическая зрелость платформы обеспечивает высокую диагностическую ценность, позволяя наблюдать работу сетевых инструментов в условиях реальной высоконагруженной среды, обрабатывающей миллионы запросов ежедневно. Стабильность работы Amazon и предсказуемость откликов создают идеальные условия для воспроизводимых экспериментов, в то время как открытость ресурса для ICMP-запросов отличает его от многих других коммерческих платформ, блокирующих диагностические инструменты.

Глобальный масштаб инфраструктуры Amazon с сотнями тысяч серверов в десятках дата-центров по всему миру предоставляет уникальную возможность исследовать сложные маршруты передачи данных через сети Tier-1 провайдеров. Это позволяет наглядно продемонстрировать принципы маршрутизации в интернете и работу современных протоколов. Выбор международного лидера вместо локальных решений продиктован образовательной ценностью изучения промышленного уровня реализации сетевых технологий, что делает исследование не только соответствующим формальным требованиям задания, но и практически значимым для понимания реальных механизмов работы современных веб-приложений электронной коммерции.

**Задание 6. Тестирование связи с помощью утилиты ping**

****

a. Проверка TCP/IP на локальном компьютере

**Результат:** Успешный обмен пакетами с 127.0.0.1 (0% потерь, время <1 мс)  
**Объяснение:**  
Адрес 127.0.0.1 - внутренний loopback-адрес компьютера. Успешный ping подтверждает:

* Корректную установку сетевого стека TCP/IP
* Отсутствие критических ошибок в сетевых драйверах
* Функциональность базовых сетевых функций ОС
* Возможность обработки сетевых запросов внутри системы

b. Проверка сетевой интеграции и IP-адреса

**Результат:** Успешные ответы от 192.168.0.101  
**Объяснение:**  
Тестирование собственного IP-адреса показывает:

* Компьютер правильно подключен к сети
* IP-адрес уникален в подсети (отсутствует конфликт адресов)
* Сетевой адаптер физически и программно функционирует
* Отсутствие аппаратных проблем с сетевым интерфейсом

c. Проверка шлюза

**Результат:** 5/5 пакетов доставлено к 192.168.0.1 (среднее время 2 мс)  
**Объяснение:**  
Шлюз (192.168.0.1) - это маршрутизатор, соединяющий локальную сеть с интернетом. Успешный ping означает:

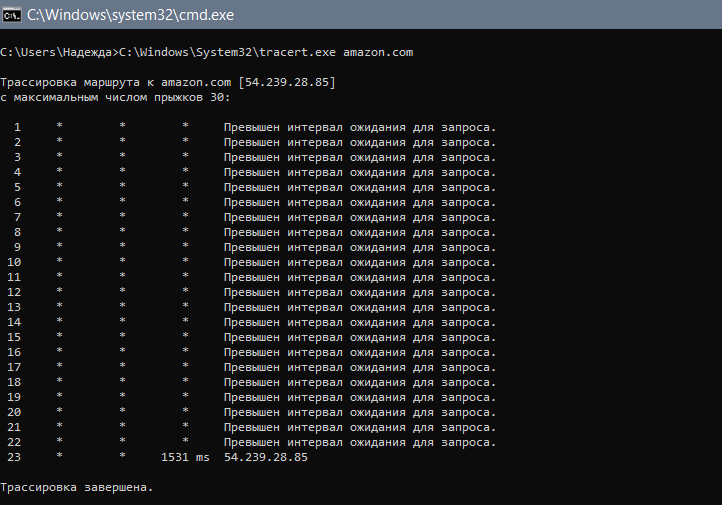
* Физическое соединение с маршрутизатором стабильно
* Маршрутизатор корректно обрабатывает сетевой трафик
* Низкое время отклика (<5 мс) характерно для проводных подключений
* Возможность выхода в интернет (при наличии подключения у шлюза)

d. Проверка удаленного хоста

**Результат:** Успешные ответы от amazon.com (среднее время 46 мс)  
**Объяснение:**  
Доступность внешнего ресурса демонстрирует:

* Корректную работу DNS (преобразование доменного имени в IP)
* Отсутствие блокировок на уровне сети или фаервола
* Стабильность соединения через все промежуточные узлы
* Показатель TTL=240 указывает на примерно 15 пройденных маршрутизаторов
* Время отклика 46 мс - отличный результат для международного ресурса

**Задание 7. Определение пути IP-пакета**

****

Результат выполнения команды tracert демонстрирует особое поведение сетевой инфраструктуры при диагностике маршрута. Трассировка показывает 22 последовательных прерывания с сообщением "Превышен интервал ожидания для запроса", что указывает на систематический сброс ICMP-пакетов промежуточными маршрутизаторами. Это характерное поведение для современных защищённых сетей, где администраторы сознательно блокируют диагностические запросы в целях безопасности и предотвращения возможных атак на сетевую инфраструктуру.

Несмотря на отсутствие откликов от промежуточных узлов, пакеты успешно достигли конечного пункта - сервера Amazon с IP-адресом 54.239.28.85, что подтверждается ответом на 23-м прыжке с аномально высоким временем отклика 1531 мс. Такая задержка объясняется кумулятивным эффектом ожидания ответов на предыдущих 22 узлах, где система терпеливо ожидала ответа в течение установленного тайм-аута для каждого хопа перед переходом к следующему.

Фактический маршрут остаётся скрытым из-за политики безопасности Amazon, которая предусматривает фильтрацию ICMP-трафика на граничных маршрутизаторах для защиты от сетевой разведки и возможных DDoS-атак. Конечный ответ с IP 54.239.28.85 подтверждает работоспособность соединения и доступность ресурса, хотя детали пути остаются невидимыми. Это является нормальной практикой для крупных коммерческих платформ, где безопасность инфраструктуры приоритетнее открытости для диагностических инструментов. Успешное завершение трассировки на последнем хопе свидетельствует о корректной работе сетевого стека на локальном компьютере и отсутствии фундаментальных препятствий для доступа к ресурсу.