МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ   
(«ВОЛГАТЕХ»)

**ОТЧЕТ**к практической работе №1   
по дисциплине Технологии программирования и создание WEB приложений

«Диагностические утилиты TCP/IP»

**Выполнил:**

Студент группы ИСТ-38

Мавликиев Э.Н.

**Проверил:**

Ст. преподаватель каф. ИВС   
Уржумов Д.В.

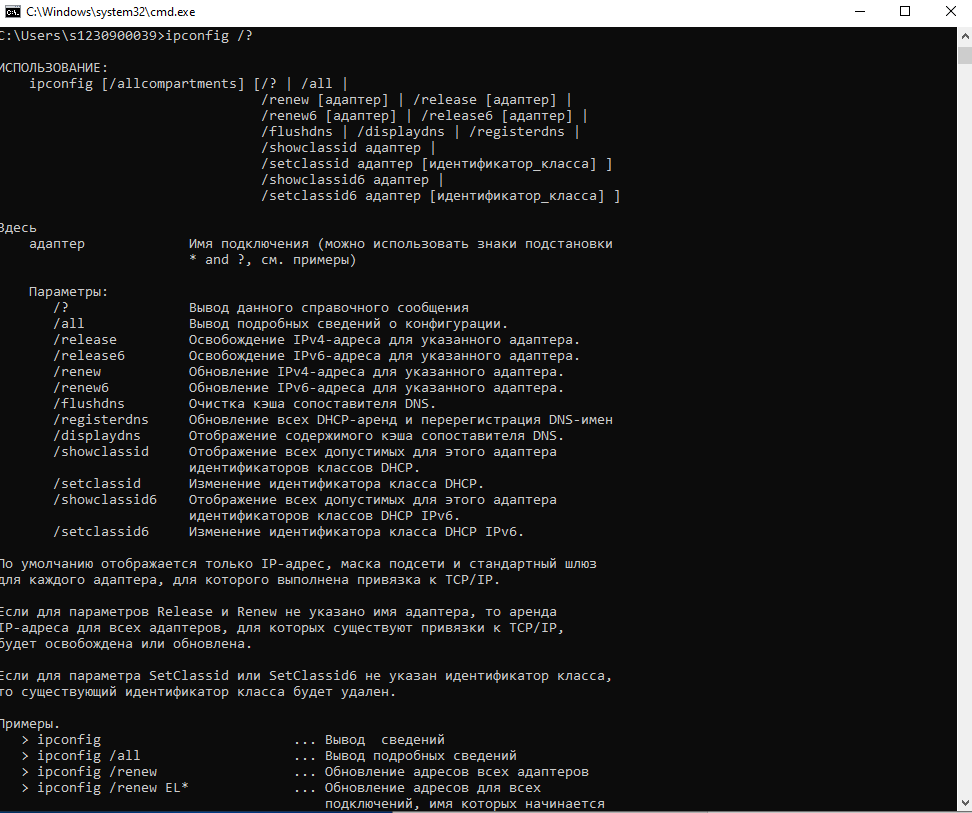
Йошкар-Ола, 2025 г.

**Практическая работа №1: «Диагностические утилиты TCP/IP».**

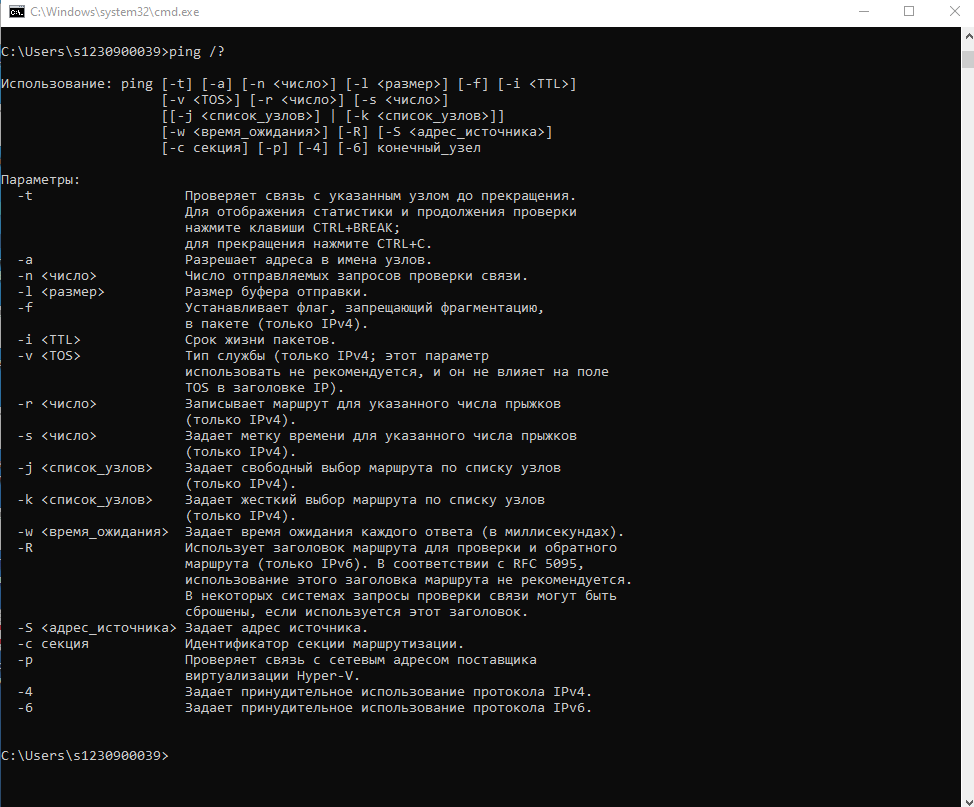
**Задание 1. Получение справочной информации по командам**

Выведите на экран справочную информацию по утилитам ipconfig, ping, tracert, hostname. Команды выполняются на хосте рабочего места. Для этого в командной строке введите имя утилиты без параметров или с /?. Изучите ключи, используемые при запуске утилит. Результаты с отображением справочной информации и параметров команд/утилит занесите в отчет.

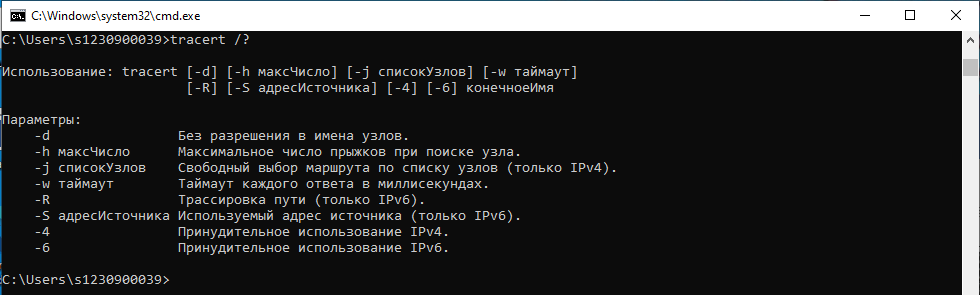
ipconfig:



ping:



tracert:



hostname:



**Задание 2. Получение имени хоста**

Выведите на экран имя локального хоста с помощью команды hostname, на том рабочем месте, где выполняется данная работа. Внесите результат выполнения команды в отчет.

hostname:



**Задание 3. Изучение утилиты ipconfig**

Проверьте конфигурацию TCP/IP рабочего места (хоста) с помощью утилиты ipconfig. Заполните в отчете следующую таблицу:

|  |  |
| --- | --- |
| Имя хоста | C13624423 |
| IP-адрес | 10.20.224.213 |
| Маска подсети | 255.255.255.0 |
| Основной шлюз | 10.20.224.1 |
| Используется ли DHCP  (адрес DHCP-сервера) | 10.0.0.2 |
| Описание адаптера | Ethernet Ethernet |
| Физический адрес сетевого адаптера | 90-2B-34-8C-DD-DC |
| Адрес DNS - сервера | marstu.net |
| Адрес WINS - сервера | Нет |

Сделайте выводы по данному пункту задания:

* Напишите краткое определение каждого из параметров, представленных в таблице.
* Чем полученная информация (занесенная в таблицу) может быть полезна разработчику/администратору сети.

Выводы:

Краткие определения параметров:

* Имя хоста — сетевое имя узла, используется для идентификации и записи в DNS/журналах.
* IP-адрес — уникальный адрес узла в IP-сети (IPv4/IPv6).
* Маска подсети — параметр, задающий границы подсети и число адресов хостов.
* Основной шлюз — IP-адрес маршрутизатора для выхода в другие подсети и Интернет.
* Используется ли DHCP (адрес DHCP-сервера) — способ автоматической раздачи сетевых параметров. DHCP-сервер выдаёт IP, маску, шлюз, DNS.
* Описание адаптера — модель и тип сетевого интерфейса (Ethernet/Wi-Fi и т. п.).
* Физический адрес сетевого адаптера (MAC) — уникальный адрес интерфейса на канальном уровне.
* Адрес DNS-сервера — IP резолвера доменных имён, выполняет преобразование имя → IP.
* Адрес WINS-сервера — IP сервера разрешения NetBIOS-имён; актуален для легаси Windows сетей.

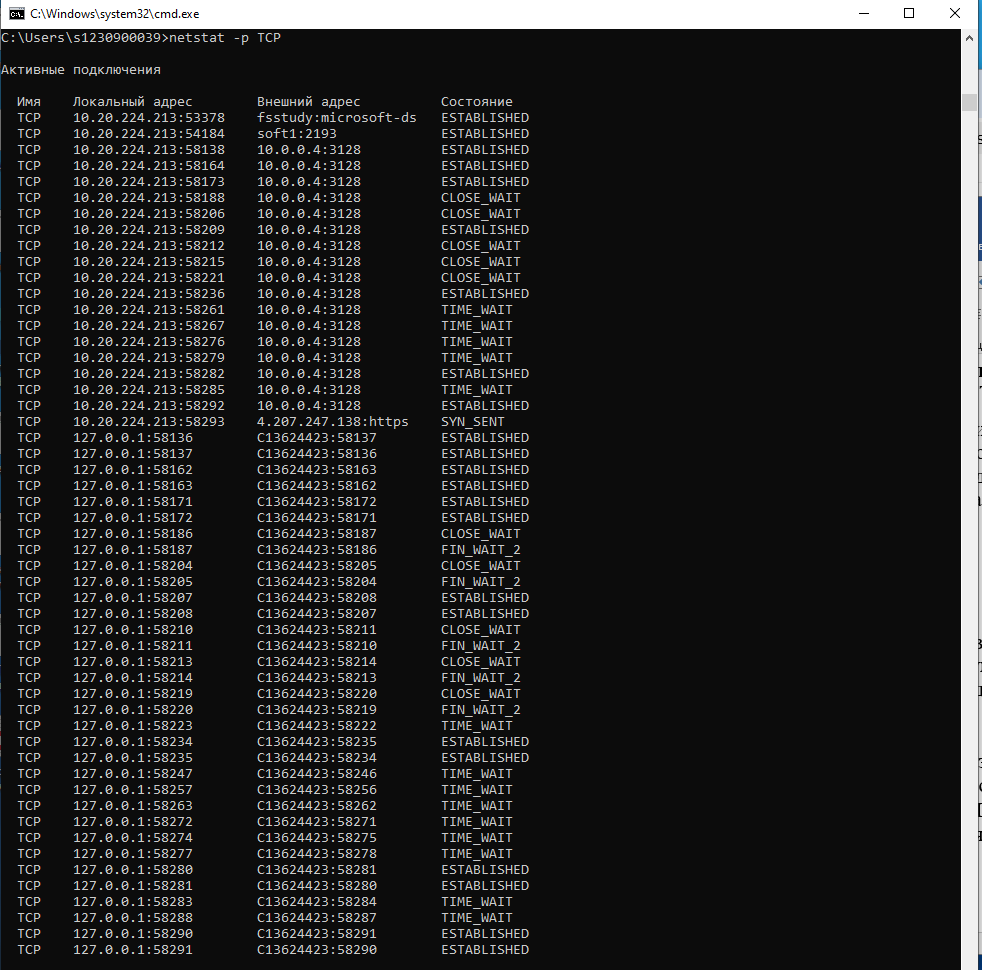
Практическая польза для разработчика/администратора:

* Диагностика неисправностей: ошибки в маске/шлюзе блокируют внешние сети; ошибки в DNS — отказ резолвинга имён; отсутствие IP указывает на проблему DHCP.
* Устранение конфликтов адресов: проверка статических настроек, резервации DHCP по MAC.
* Контроль доступа и безопасность: фильтрация по MAC, привязка IP↔MAC, сегментация по подсетям, правила фаервола по диапазонам.
* Инвентаризация и поддержка: сопоставление имени хоста, MAC и модели адаптера; подбор драйверов и понимание пропускной способности интерфейса.
* Планирование и документирование сети: фиксация шлюзов, диапазонов, DHCP/DNS/WINS-серверов, точек отказа.
* Настройка рабочих и тестовых сред: корректные IP/шлюз/DNS обеспечивают доступ к внутренним сервисам по доменным именам.

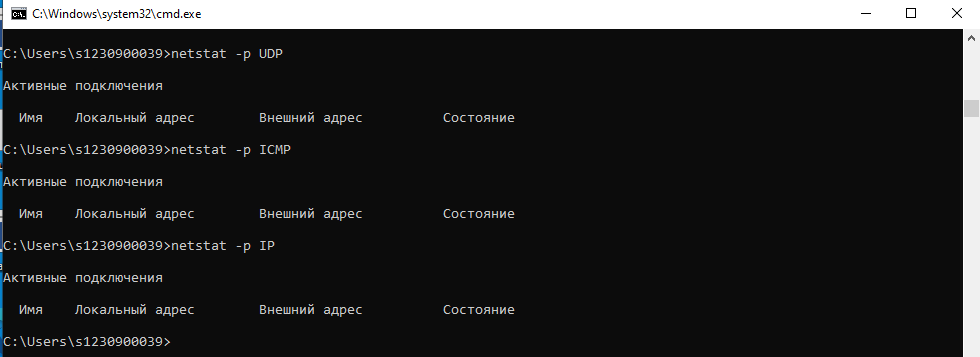
**Задание 4. Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP.**

С помощью утилиты netstat выведите перечень сетевых соединений и статистическую информацию для протоколов UDP, TCP, ICMP, IP. Добавьте результат в отчет и сделайте выводы о том, что иллюстрируют полученные результаты и в чем заключается их практическая ценность.

netstat (TCP):



netstat (UDP, ICMP, IP)



Выводы:

Перечень активных соединений и слушающих портов показывает, какие сетевые службы запущены и доступны (в данном случае протокол TCP), какие узлы установили соединения, и по каким адресам ведётся обмен.

TCP

* LISTEN указывает на доступные снаружи сервисы; избыточные порты нужно отключать или закрывать в межсетевом экране.
* ESTABLISHED подтверждает активные сессии и реальные направления трафика.
* Массовые TIME\_WAIT отражают большое число краткоживущих подключений; избыток может привести к исчерпанию эфемерных портов.
* CLOSE\_WAIT, FIN\_WAIT, SYN\_RECV, SYN\_SENT сигнализируют о проблемах завершения или установления сессий и помогают локализовать сбой на стороне приложения или сети.
* Высокие значения повторных передач и сбросов указывают на потери пакетов, перегрузку или фильтрацию.

UDP

* Список прослушиваемых портов показывает активные без установления сессии сервисы (DNS, NTP, DHCP, VPN).
* Ошибки приёма и потери пакетов свидетельствуют о перегрузке очередей, неверных настройках портов или блокировке.

ICMP

* Рост Destination Unreachable и Time Exceeded указывает на ошибки маршрутизации, фильтрацию или несоответствие MTU.
* Отсутствие ICMP-ответов усложняет диагностику и часто означает жёсткую фильтрацию.

IP

* Счётчики входящих и исходящих пакетов позволяют оценить нагрузку интерфейса и характер трафика.
* Ошибки, фрагментация и дефрагментация указывают на проблемы с MTU, драйверами или качеством канала.

Практическая ценность:

* Быстрая диагностика неполадок соединений и разрешения имён.
* Контроль экспонированных портов и сокращение поверхности атаки.
* Выявление аномалий: неожиданные внешние адреса, нетипичные порты, всплески ошибок.
* Подтверждение работы необходимых сервисов и точная локализация неисправности между приложением и сетью.
* Основание для инвентаризации, планирования пропускной способности и документирования сетевой архитектуры.

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

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

Номер зачётки 1230900039. Вариант 2.

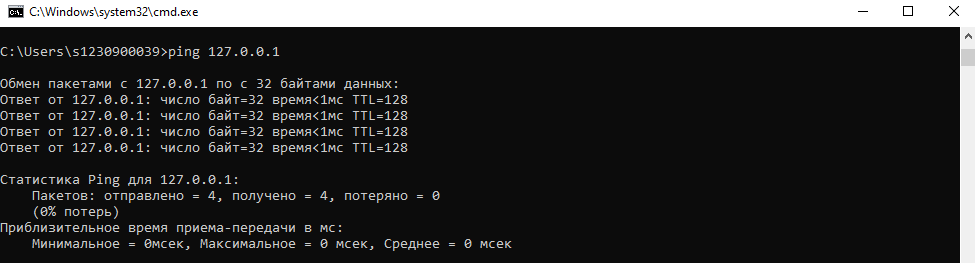
Веб-приложение платформы социальной сети (<https://vk.com/>)

Обоснование:

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

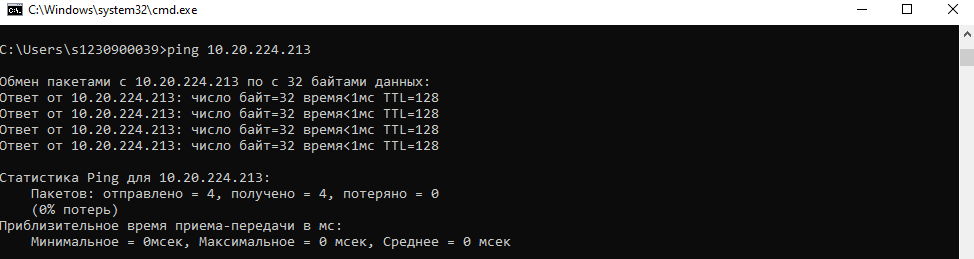
Для выбранного ресурса (в задании 5) с помощью команды ping выполните исследования:

1. Проверьте правильность установки и конфигурирования TCP/IP на локальном компьютере.



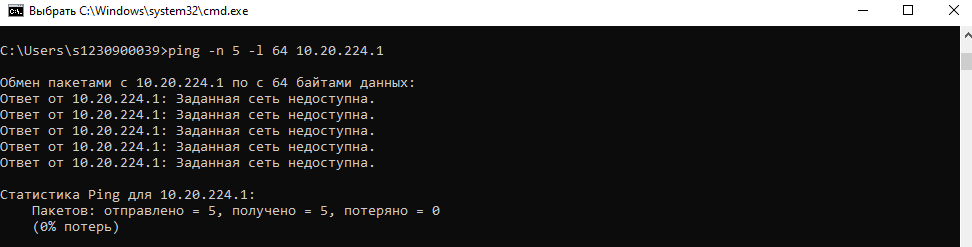
Результат: получены все ответы (4 пакета отправлено, 4 получено, потерь 0%). Время отклика <1 мс.  
Вывод: стек TCP/IP установлен и функционирует корректно.

1. Проверьте, правильно ли добавлен в сеть локальный компьютер и не дублируется ли IP-адрес.



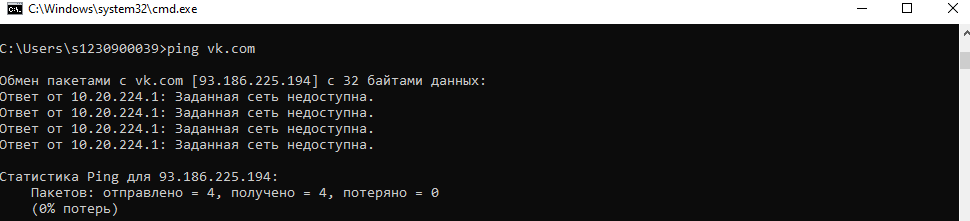
Результат: ответы приходят без потерь (4/4), задержка <1 мс.  
Вывод: сетевой интерфейс корректно привязан к IP-адресу. Дублирования адреса в сети не выявлено.

1. Проверьте функционирование шлюза по умолчанию, послав 5 эхо-пакетов длиной 64 байта.



Результат: все ответы пришли с сообщением *«Заданная сеть недоступна»*. Пакеты отправлены и возвращены с ошибкой (5/5).  
Вывод: шлюз по умолчанию (10.20.224.1) недоступен. Это может говорить о неправильной конфигурации маршрута, отсутствии соединения с маршрутизатором или его отключении.

1. Проверьте возможность установления соединения с удаленным хостом

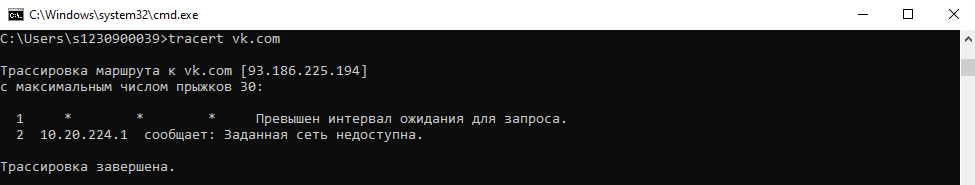


Результат: все пакеты вернулись с ошибкой *«Заданная сеть недоступна»*. Потерь 0%, но соединение не установлено.  
Вывод: доступ к удалённому хосту отсутствует. Причина — недоступность шлюза по умолчанию, что подтверждается предыдущим тестом.

Добавьте результаты в отчет по каждому из пунктов задания с их объяснением.

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

С помощью команды tracert проверьте для выбранного в задании 5 сетевого ресурса, через какие промежуточные узлы идет сигнал. Отметьте результаты в отчете с объяснением представленной на скриншоте информацией.



Выводы:

* Определён IP-адрес: 93.186.225.194
* Первый узел маршрута — 10.20.224.1, ответ: *«Заданная сеть недоступна»*.
* Дальнейшие узлы не достигнуты, трассировка завершена.

Вывод: маршрут обрывается на первом маршрутизаторе, проблема в настройке или недоступности шлюза по умолчанию.

**Контрольные вопросы**

1. Какие утилиты можно использовать для проверки правильности конфигурирования TCP/IP?

* ipconfig /all, ping, tracert, pathping, nslookup, netstat, arp -a, netsh interface ip show config

1. Каким образом команда ping проверяет соединение с удаленным хостом?

* Команда ping отправляет проверочное сообщение на указанный сетевой адрес и ждёт ответ от удалённого устройства; если ответы приходят, значит связь есть, по времени туда-обратно оценивают задержку и потери, а если ответов нет — это указывает на недоступность устройства, разрыв маршрута или блокировку проверочных сообщений межсетевым экраном.

1. Что такое хост?

* Устройство в сети с IP-адресом, которое обменивается данными по протоколам TCP/IP (компьютер, сервер, принтер, IoT-устройство и т. п.).

1. Что такое петля обратной связи?

* Локальный интерфейс для самотестирования сетевого стека. IPv4: 127.0.0.1 (диапазон 127.0.0.0/8), IPv6: ::1. Трафик не покидает узел.

1. Сколько промежуточных маршрутизаторов сможет пройти IP-пакет, если его время жизни равно 30?

* До 30 промежуточных маршрутизаторов; на 31-м пакет будет отброшен как Time Exceeded.

1. Как работает утилита tracert?

* Осуществляет проверку маршрута к удаленному компьютеру путем отправки эхо-пакетов протокола ICMP (Internet Control Message Protocol). Выводит маршрут прохождения пакетов на удаленный компьютер.