

# «СЕТЕВЫЕ УТИЛИТЫ WINDOWS»

Составитель: Коробецкая А.А.

## ЗАДАНИЕ

В командной строке Windows выполнить:

1. Определить имя локального хоста с помощью утилиты `hostname`.
2. Определить MAC-адрес всех сетевых подключений (интерфейсов) с помощью утилиты `getmac`.
3. Проверить конфигурацию TCP/IP с помощью утилиты `ipconfig`. Записать в виде таблицы: логический и физический адреса основного сетевого интерфейса, маску подсети, DNS-сервер, используется ли DHCP.
4. Узнать ip-адрес произвольного сайта с помощью утилиты `nslookup`.
5. С помощью утилиты `ping`:
  - 1) проверить доступность DNS-сервера за 1 переход;
  - 2) (если выполняется **в классе**) проверить доступность трех соседних компьютеров в аудитории по ip-адресу и по доменному имени (спросить у одногруппников). На первый узел отправить 3 пакета, на второй 20 пакетов, на третий 7 пакетов;
  - 2) (если выполняется **дома**) проверить состояние связи с тремя произвольными узлами, находящимися в разных доменных зонах (например, .ru, .com и .uk). На первый узел отправить 3 пакета, на второй 20 пакетов, на третий 7 пакетов. Заполнить таблицу:

Доменное имя	IP-адрес	Общее число запросов	Число потерянных запросов	Процент потерянных запросов	Среднее время прохождения запроса

## Отчет

Отчет должен содержать:

- титульный лист;
- текст задания;
- скриншот или копия текста (шрифт Courier New) командной строки по каждому пункту задания;
- результаты по каждому пункту задания в виде текста или таблиц.

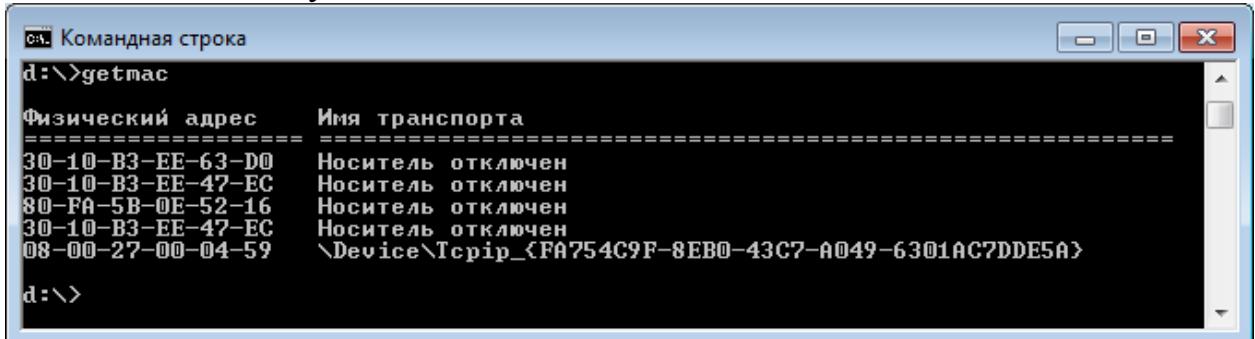
Пример:

1. Определить имя локального хоста с помощью утилиты `hostname`.

The screenshot shows a Windows Command Prompt window titled "Командная строка". The command `d:\>hostname` was entered, and the response "Анастасия-НБ" is displayed. The window has a standard Windows title bar and scroll bars on the right side.

Имя локального хоста: Анастасия-НБ

2. Определить MAC-адрес всех сетевых подключений (интерфейсов) с помощью утилиты getmac



Физический адрес	Имя транспорта
30-10-B3-EE-63-D0	Носитель отключен
30-10-B3-EE-47-EC	Носитель отключен
80-FA-5B-0E-52-16	Носитель отключен
30-10-B3-EE-47-EC	Носитель отключен
08-00-27-00-04-59	\Device\Tcpip_{FA754C9F-8EB0-43C7-A049-6301AC7DDE5A}

Системе известно 5 разных сетевых интерфейсов, но в данный момент активен только один с адресом 08-00-27-00-04-59.

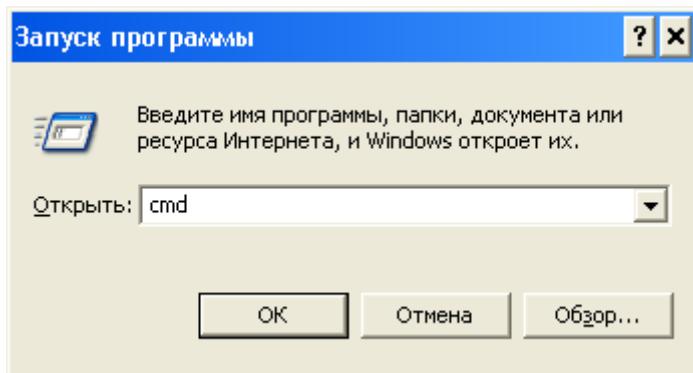
## УКАЗАНИЯ К ВЫПОЛНЕНИЮ

### Работа с командной строкой

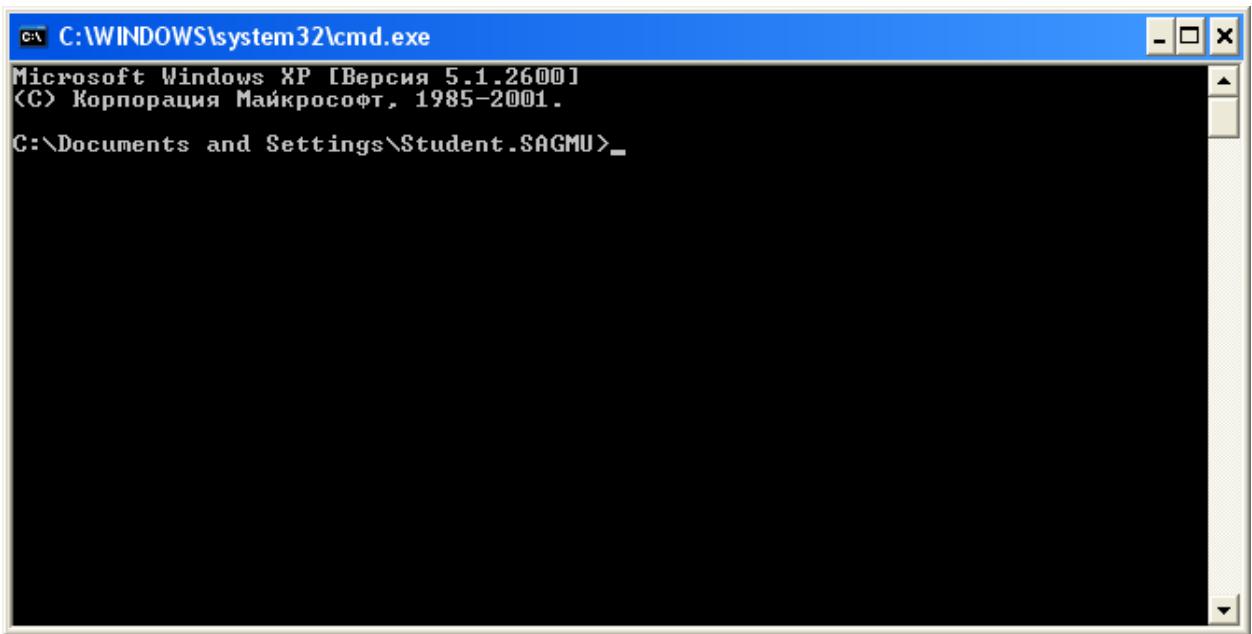
Командная строка позволяет вводить текстовые команды для операционной системы.

В Windows командную строку можно запустить двумя способами:

1. Пуск – Программы – Стандартные –  Командная строка
2. Пуск – Выполнить… – ввести cmd – OK

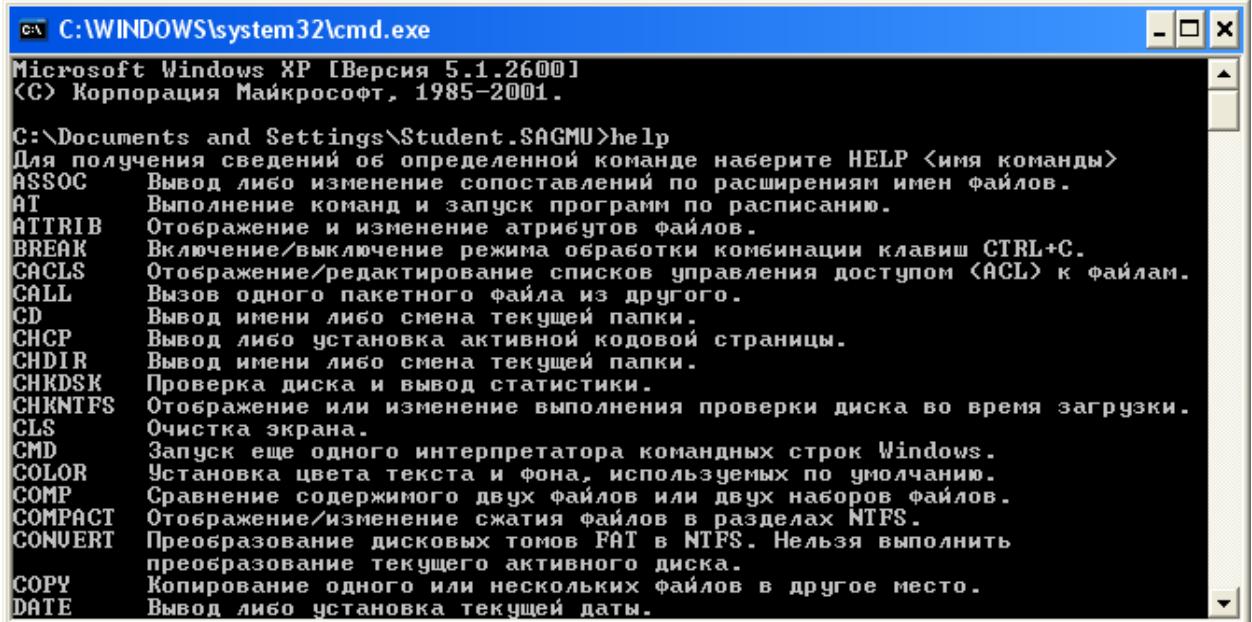


В результате запустится окно командной строки с возможностью ввода различных команд в виде текста.



Каждая команда – это имя программы, выполняющей эту команду, плюс некоторый набор параметров, определяющих, что именно нужно сделать.

Набор стандартных команд можно посмотреть с помощью команды `help`:



`help <имя команды>` выводит справку по конкретной команде и ее параметрам.

```

C:\WINDOWS\system32\cmd.exe - help copy
C:\Documents and Settings\Student.SAGMU>help copy
Копирование одного или нескольких файлов в другое место.

COPY [/D] [/U] [/N] [/Y | /-Y] [/Z] [/A | /B] источник [/A | /B]
      [+ источник [/A | /B] [+ ...]] [результат [/A | /B]]

источник      Имена одного или нескольких копируемых файлов.
/A             Файл является текстовым файлом ASCII.
/B             Файл является двоичным файлом.
/D             Указывает на возможность создания зашифрованного файла
результат     Каталог и/или имя для конечных файлов.
/U             Проверка правильности копирования файлов.
/N             Использование, если возможно, коротких имен при копировании
файлов, чьи имена не удовлетворяют стандарту 8.3.
/Y             Подавление запроса подтверждения на перезапись существующего
конечного файла.
/-Y            Обязательный запрос подтверждения на перезапись существующего
конечного файла.
/Z             Копирование сетевых файлов с возобновлением.

Ключ /Y можно установить через переменную среды COPYCMD.
Ключ /-Y командной строки переопределяет такую установку.
По умолчанию требуется подтверждение, если только команда COPY
не выполняется в пакетном файле.
Для продолжения нажмите любую клавишу . . .

```

В данной работе будут использоваться различные команды, не входящие в перечень стандартных.

Примечание Здесь показаны примеры выполнения команд в ОС Windows 7. Для других версий результаты могут иметь немного другой вид, но вся необходимая в заданиях информация будет доступна.

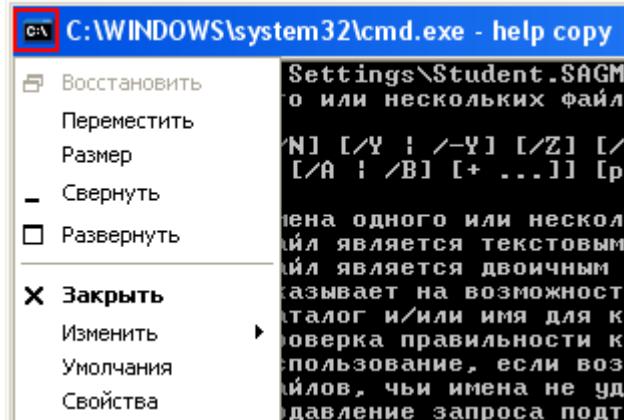
### **Как скопировать текст из командной строки?**

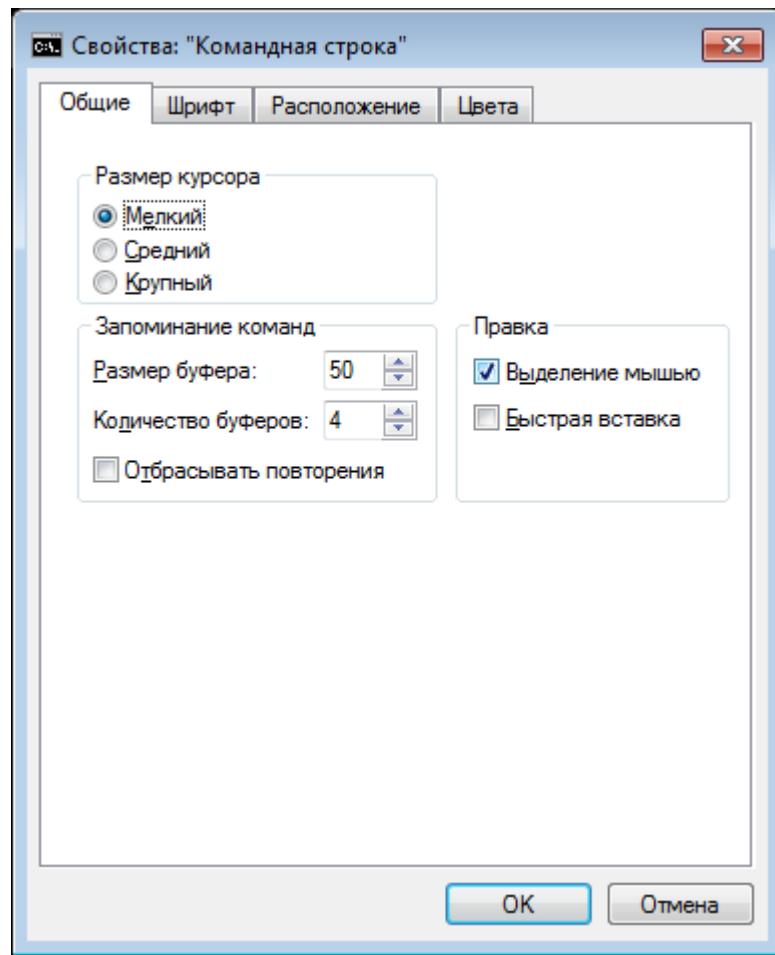
Комбинация Ctrl+C для копирования в командной строке не работает (точнее, она не копирует текст, а отменяет текущее действие).

1. Правый клик – Пометка
2. Выделить копируемый текст
3. Правый клик или Enter

После этого текст будет скопирован в буфер обмена.

Если нужно часто копировать текст из командной строки, можно включить постоянное выделение. Правый клик по иконке командной строки в верхнем левом углу – Свойства – включить галочку Выделение мышью.





### *Как быстро повторить предыдущую команду?*

Клавиши навигации (стрелки вверх-вниз, Home, End, PageUp, PageDown) позволяют пролистывать все ранее введенные команды, стрелки вправо-влево позволяют перемещаться в пределах команды и редактировать ее.

Нажатие Enter в любом месте команды приведет к ее выполнению.

### *«Кракозябры» вместо русских букв*

Командная строка изначально предназначена для работы с латиницей и русский текст может отображаться некорректно.

С: Командная строка

SHUTDOWN	пъорыНэюх шыш сферыхээюх тчыншхэшх ююяНШхБр.
SORT	тюЕсшБютр ттиоф.
START	тчяюызхэшх яБюуБрьц шыш ююрэф т юСфхыНэю юэх.
SUBST	тчэрүхэшх чрфээюе яе8ш шыхкш фшёбр.
SYSTEMINFO	тчтиоф ётхфхэшх ю ёшё8хх ш ююштшум ююяНШхБр.
TASKLIST	тчюсБрхэшх тэх1 тчяюы хьц1 чрфру, тчынш ёыецс.
TASKKILL	тчхБрхэшх шыш юёБрэютр яБю9хеёр шыш яБшынхэш .
TIME	тчтиоф ш ёёБрэютр ёшё8хээюю тБххэш.
TITLE	тчэрүхэшх чркуюютр юээр фы 8хье-хую ёхрээр шэ8хЯяExБрСюБр ююрэфэц1 ё8Бю CMD.EXE.
TREE	тчришхэшх ююсБрхэшх ё8Ее8еEJ трБрыюют фшёбр шыш яряш.
TYPE	тчтиоф эр хъБрэ ёюфхБщьюю 8хъё8иотц1 Уршыют.
VER	тчтиоф ётхфхэшх тхБёши Windows.
VERIFY	тёБрэютр 8хщир яБютхБеш яБртшыНэюё8 чряшёш Уршыют эр фшёв.
VOL	тчтиоф 8х8и ю ёхБщьюю эюхБр 8и8р фы фшёбр.
XCOPY	8ояшБютрэшх Уршыют ш фхБхтнхт трБрыюют.
WMIC	тчтиоф ётхфхэшх WMI т шэ8хБр8штэю ё8хфх.

—ююяюыз8хыНэжх ётхфхэш ю яБюуБрьц яБштхфх т юяшёрэшх яБюуБрьц ююрэфэю ё8Е юш т ёяБртх.

D:\>\_

В этом случае необходимо сменить кодировку или перейти на английский язык. К сожалению, угадать нужную кодировку в каждом случае невозможно, поэтому необходимо попробовать следующие команды:

```
chcp 866  
chcp 1251  
chcp 65001  
chcp 1252
```

### Утилита hostname

Простейшая утилита, выводит имя локального хоста. Используется без параметров.

В Windows имя локального хоста задается настройках системы (правый клик по ярлыку «Мой компьютер» – Свойства, либо Пуск – Панель управления – Система,

С: Командная строка

```
D:\>hostname  
Анастасия-НБ  
D:\>
```

В отчете необходимо показать командную строку и написать, какое доменное имя использует ваш компьютер.

### Утилита getmac

Позволяет узнать МАС-адреса всех устройств, которые подключены (или были когда-то подключены) в системе.

```
cmd Командная строка
D:\>getmac
Физический адрес      Имя транспорта
=====
30-10-B3-EE-63-D0      Носитель отключен
30-10-B3-EE-47-EC      Носитель отключен
80-FA-5B-0E-52-16      \Device\Tcpip_{7E0FC114-9A58-4A81-837A-6C9CC9CAEF4A}
30-10-B3-EE-47-EC      Носитель отключен
08-00-27-00-04-59      \Device\Tcpip_{FA754C9F-8EB0-43C7-A049-6301AC7DDE5A}

D:\>
```

В отчете необходимо показать командную строку и написать, сколько и каких MAC-адресов использует ваш компьютер (обычно их 1 или 2).

### Утилита ipconfig

Выводит текущие сетевые настройки для всех сетевых подключений: IP-адрес, маску подсети, адрес шлюза по умолчанию, адреса DNS (Domain Name System) и др.

```
cmd Командная строка
D:\>ipconfig
Настройка протокола IP для Windows

Адаптер PPP АИСТ:
DNS-суффикс подключения . . . . . : 37.9.148.66
IPv4-адрес . . . . . : 255.255.255.255
Маска подсети . . . . . : 0.0.0.0

Адаптер беспроводной локальной сети Беспроводное сетевое соединение 2:
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :

Адаптер беспроводной локальной сети Беспроводное сетевое соединение:
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :

Ethernet adapter Подключение по локальной сети:
DNS-суффикс подключения . . . . . : aistnet.autograd.ru
Локальный IPv6-адрес канала . . . . . : fe80::a5b0:7185:26ed:99c6%12
IPv4-адрес . . . . . : 10.240.5.4
Маска подсети . . . . . : 255.255.255.192
Основной шлюз. . . . . : 10.240.5.1

Ethernet adapter Сетевое подключение Bluetooth:
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
```

Как видите, ipconfig показывает множество соединений, в том числе неактивных (для них указано «Среда передачи недоступна»).

Нас интересует «Подключение по локальной сети» (через сетевой кабель) и PPP АИСТ (подключение к провайдеру для доступа в Интернет). Другие подключения (на скриншоте лишь часть из них) – это различные службы.

У вас могут быть другие варианты подключения, но чаще всего используется подключение по локальной сети или беспроводное подключение.

В локальной сети провайдера компьютер имеет адрес 10.250.5.4 с маской 255.255.255.192.

Во внешней сети (Интернете) компьютер имеет адрес 37.9.148.66.

Более подробную информацию можно получить с помощью ipconfig /all:

Командная строка

Ethernet adapter Подключение по локальной сети:

DNS-суффикс подключения . . . . .	:	aistnet.autograd.ru
Описание . . . . .	:	Realtek PCIe GBE Family Controller
Физический адрес . . . . .	:	80-FA-5B-0E-52-16
DHCP включен . . . . .	:	Да
Автонастройка включена . . . . .	:	Да
Локальный IPv6-адрес канала . . . . .	:	fe80::a5b0:7185:26ed:99c6%12(Основной)
IPv4-адрес . . . . .	:	10.240.5.4(Основной)
Маска подсети . . . . .	:	255.255.255.192
Аренда получена . . . . .	:	30 марта 2016 г. 11:08:51
Срок аренды истекает . . . . .	:	3 апреля 2016 г. 11:08:51
Основной шлюз . . . . .	:	10.240.5.1
DHCP-сервер . . . . .	:	10.240.5.1
IAID DHCPv6 . . . . .	:	293665371
DUID клиента DHCPv6 . . . . .	:	00-01-00-01-1C-8B-0F-65-80-FA-5B-0E-52-16
DNS-серверы . . . . .	:	62.106.124.111 62.106.124.1
NetBIOS через TCP/IP . . . . .	:	Включен

Сведения о конфигурации сети в виде таблицы:

MAC-адрес	00-1D-60-74-8B-E8
IP-адрес	10.254.1.130
Маска подсети	255.255.255.192
Адрес шлюза по умолчанию (через какой роутер подключаемся к сети)	10.254.1.129
DNS-серверы (кто преобразует DNS-имена в IP-адреса)	62.106.124.111, 62.106.124.1
DHCP (кто выдал нам IP-адрес)	вкл., сервер 10.254.1.129, адрес был получен 29.102014 в 16:00

В отчете необходимо показать командную строку и заполнить аналогичную таблицу для основного сетевого подключения.

### Утилита nslookup

Утилита nslookup позволяет узнать ip-адрес(-а), связанные с доменным именем, а также, от какого DNS-сервера получена эта информация.

```
с:\ Командная строка
D:\>nslookup vk.com
>xÈtxÈ: ns2.smr.aist.net.ru
Address: 62.106.124.111

Не заслуживающий доверия ответ:
Цъ : vk.com
Addresses: 2a00:bdc0:3:103:1:0:403:902
            2a00:bdc0:3:103:1:0:403:900
            2a00:bdc0:3:103:1:0:403:901
            87.240.131.118
            87.240.131.119
            87.240.131.120

D:\>
```

\*в данном примере «столкнулись» две разных кодировки, поэтому половина текста написана по-русски, а половина – «кракозябрами»

Таким образом, для vk.com на сервере ns2.smr.aist.net.ru удалось узнать 6 разных IP-адресов: три адреса IPv6 и три адреса IPv4.

В отчете необходимо узнать IP-адреса любого другого узла, показать командную строку и записать, какой сервер сообщил IP-адреса и сколько их.

### Утилита ping

Утилита ping служит для проверки доступности узла с заданным именем или IP-адресом. Работает путем отправки последовательности эхо-запросов. Если хост доступен, он должен отправить эхо-ответ.

По умолчанию отправляется 4 пакета, в результате работы выводятся результаты доставки каждого пакета и общая статистика.

```
с:\ Командная строка
D:\>ping sagmu.ru

Обмен пакетами с sagmu.ru [46.20.71.172] с 32 байтами данных:
Ответ от 46.20.71.172: число байт=32 время=1мс TTL=61

Статистика Ping для 46.20.71.172:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
        <0% потеря>
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 1 мсек, Среднее = 1 мсек

D:\>
```

В первую очередь, ping выводит *IP-адрес* для запрашиваемого узла.

*Задержка* – время, за которое пакет дошел до узла и вернулся обратно. Зачастую это время называют «пингом», хотя по сути это неверно. Пинг – это сама программа, отправляющая запросы.

Необходимо помнить, что задержка включает не только время прохождения запроса по сети, но и время его обработки получателем. Т.е. большое значение задержки может быть вызвано как загруженностью сети, так и загруженностью самого узла.

Ping также позволяет проверить *TTL*, т.е. число переходов (прыжков, хопов), которые остались у пакета при возвращении. При прохождении каждого маршрутизатора (роутера) в сети TTL уменьшается на 1. Зная его

значение у отвечающего узла (обычно это 32, 64, 128, 256), можно вычислить число пройденных маршрутизаторов.

В нашем примере  $TTL = 61 = 64 - 3$ , т.е., скорее всего, по пути до sagmu.ru было пройдено 3 маршрутизатора.

Число отправляемых пакетов, TTL отправителя и другие настройки задаются в параметрах.

Некоторые параметры утилиты ping:

-t	выполняет команду ping бесконечно до прерывания (Ctrl+Break – пауза, Ctrl+C – прервать);
-a	позволяет определить доменное имя узла по его IP-адресу;
-n count	посыпает количество пакетов ECHO, указанное параметром count;
-i ttl	устанавливает время жизни пакета в величину ttl (каждый маршрутизатор уменьшает ttl на единицу);
-w timeout	указывает время ожидания (timeout) ответа от удаленного хоста в миллисекундах (по умолчанию – 1сек).

Примечание: поскольку с утилиты ping зачастую начинается хакерская атака, некоторые серверы в целях безопасности могут не посыпать эхо-ответы (например, www.microsoft.com).

Проверим доступность шлюза по умолчанию (ближайшего роутера), полученного в ipconfig.

Адрес шлюза по умолчанию (через какой роутер подключаемся к сети)	10.254.1.129
---	--------------

Поскольку это ближайший роутер, он обязан быть доступным ровно за один прыжок, т.е. без промежуточных соединений (параметр -i 1):

```
D:\>ping -i 1 10.254.1.129

Обмен пакетами с 10.254.1.129 по с 32 байтами данных:
Ответ от 10.254.1.129: число байт=32 время=2мс TTL=255

Статистика Ping для 10.254.1.129:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
        <0% потеря>
Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 2 мсек, Среднее = 2 мсек
```

Проверим доступность серверов sagmu.ru, google.com и bundesbank.de, отправив на них 3, 20 и 7 запросов соответственно:

```
D:\>ping -n 3 sagmu.ru

Обмен пакетами с sagmu.ru [46.20.71.172] по с 32 байтами данных:
Ответ от 46.20.71.172: число байт=32 время=1мс TTL=61
Ответ от 46.20.71.172: число байт=32 время=1мс TTL=61
Ответ от 46.20.71.172: число байт=32 время=1мс TTL=61

Статистика Ping для 46.20.71.172:
    Пакетов: отправлено = 3, получено = 3, потеряно = 0
        <0% потеря>
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 1 мсек, Среднее = 1 мсек
```

```

см. Командная строка
D:\>ping -n 20 google.com

Обмен пакетами с google.com [37.29.1.30] с 32 байтами данных:
Ответ от 37.29.1.30: число байт=32 время=1мс TTL=57
Статистика Ping для 37.29.1.30:
    Пакетов: отправлено = 20, получено = 20, потеряно = 0
        <0% потеря>
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 1 мсек, Среднее = 1 мсек
D:\>

```

```

см. Командная строка
D:\>ping -n 7 bundesbank.de

Обмен пакетами с bundesbank.de [217.110.59.166] с 32 байтами данных:
Превышен интервал ожидания для запроса.

Статистика Ping для 217.110.59.166:
    Пакетов: отправлено = 7, получено = 0, потеряно = 7
        <100% потеря>

```

Последний узел, видимо, закрыт для пинга в целях безопасности. Через браузер сайт загружается без сбоев.

Доменное имя	IP-адрес	Общее число запросов	Число потерянных запросов	Процент потерянных запросов	Среднее время прохождения запроса
sagmu.ru	46.20.71.172	3	0	0	1
google.com	37.29.1.30	20	0	0	1
bundesbank.de	217.110.59.166	7	7	100	-

Для выполнения задания выберите три других узла. В отчет вставьте содержимое командной строки и заполните таблицу из задания. Если какой-то адрес недоступен через пинг, проверьте, загружается ли он через браузер и укажите это в отчете.