# Использование сетевых утилит командной строки Windows

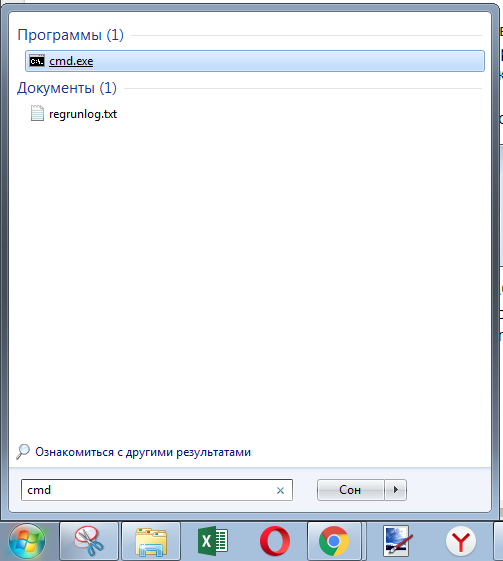
**ping** - это утилита сетевого администрирования, используемая для проверки доступности достижимости хоста и измерению времени доставки сообщений. Команда ping отправляет эхо-сигнал ICMP запрашивая пакеты и ожидая ответа ICMP.

**traceroute** - это диагностический инструмент компьютерной сети для отображения пути пакета и измерение его транзитных задержек по пути к хосту.

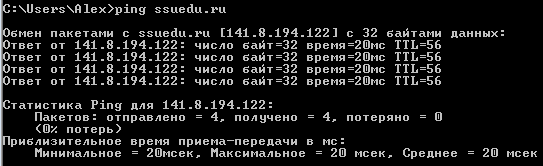
**nslookup** - это средство командной строки сетевого администрирования, обычно используемое для запросов к системе доменных имен (DNS) для получения имени домена или отображения IP-адреса или для получения любой DNS записи.

## Практическая часть

1. Найдите IP address сайта ssuedu.ru.
2. Для этого запустите командную строку Windows.

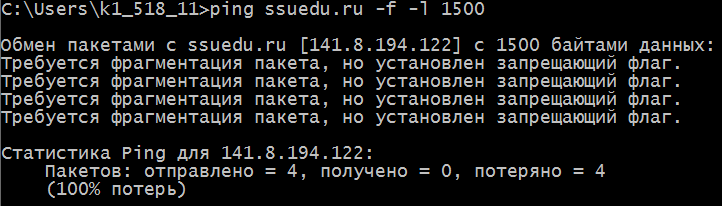


3. В командной строке введите команду **ping ssuedu.ru**



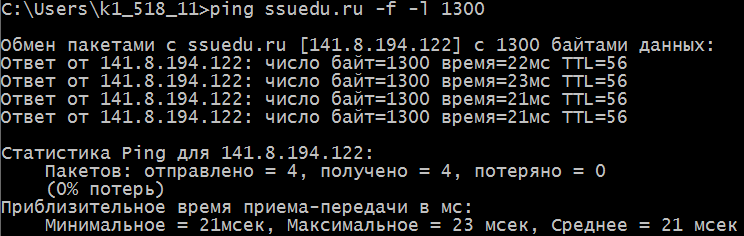
4. Мы видим что IP адресом домена является адрес **141.8.194.122**. Кроме адреса мы видим информацию об отправленных (и потерянных) пакетах, а также время прохождения пакета с момента отправки сообщения до момента получения ответа.

5. Теперь давайте найдём максимальный размер кадра в сети, в командной строке введите: **ping ssuedu.ru -f -l 1500**

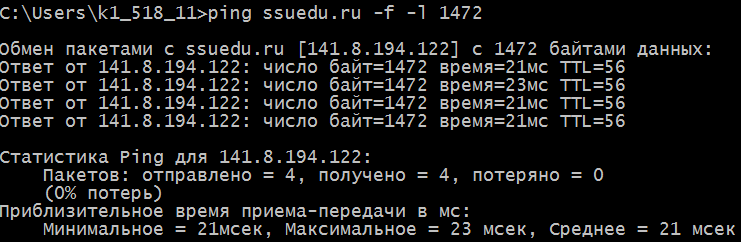
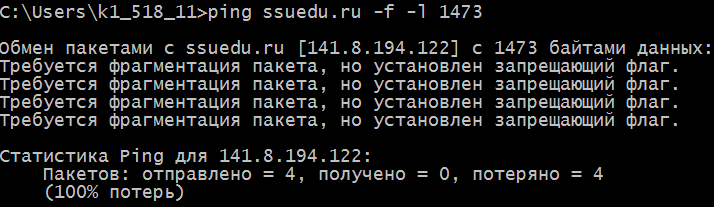
****

6. Мы видим что все наши пакеты были потеряны, это связано с размером фрейма, который мы установили в байтах. Это значит что размер информации которую мы хотели поместить в фрейм был слишком велик и нам нужно было это информацию фрагментировать перед отправкой. Это происходит автоматически, но мы указали ключ -f который запрещает фрагментацию. Более подробно о ключах читайте [тут](https://ab57.ru/cmdlist/ping.html).

7. Теперь давайте уменьшим размер передаваемой информации в фрейме, отправим команду **ping ssuedu.ru -f -l 1300**

****

8. Здорово, теперь всё работает, значит минимальный фрагмент данных который можно отправить в фрейме находится между значениями 1300 и 1500. Не будем долго вас томить, попробуйте отправить ping c **-l 1472** и **-l 1473.**

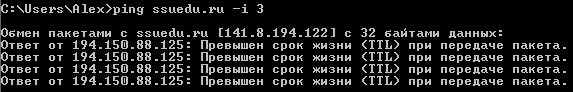
****

9. Значит мы можем отправить максимум 1472 байт данных в одном фрейме (кадре). Но почему так? Ведь размер блока передаваемых данных в фрейме должен быть равен 1500 ([согласно RFC](https://habr.com/post/227729/)). Дело в том что нужно учитывать, что 8 байт уйдёт на ICMP заголовок и ещё 20 байт IP. По этому мы имеем в распоряжении всего 1472 байта.

***Важно!*** *Максимальный размер кадра будет отличаться в зависимости от целевой сети.*

10. Давайте разберёмся что такое TTL (Time to Live). Каждый пакет в сети имеет TTL - время жизни пакета. При прохождении 1 сетевого оборудования из этого значения вычитается 1 пункт. Если TTL достигнет 0, маршрутизатор уничтожает (отбрасывает) фрейм. Этот механизм предотвращает [петли маршрутизации](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%BD%D0%B0%D1%8F_%D0%BF%D0%B5%D1%82%D0%BB%D1%8F).

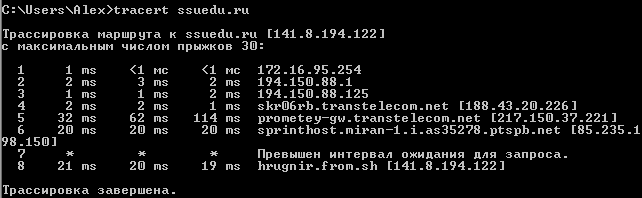
11. Давайте попробуем отправить **ping** с **TTL=3**, посмотрим, дойдет ли наш пакет.



12. Пакет не дошел, это связано с тем что количество сетевых устройств между нами и запрашиваемым сайтов больше 3х.

***Важно!*** *Максимальный размер TTL= 255!*

13. Для того чтобы понять, какое количество сетевого оборудования проходит наш ICMP пакет (ping), перед тем как добраться до целевого хоста (ssuedu.ru), мы будем использовать команду [Traceroute](https://ru.wikipedia.org/wiki/Traceroute), введите в командной строке **tracert ssuedu.ru**.



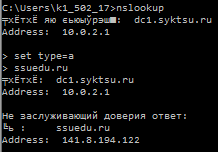
14. Как работает данная команда:

1. Отправляет 3 ICMP пакета (ping) с TTL=1. Это значит что пакет будет откинут (уничтожен) на первом хосте, который встретится по пути. Об этом мы получим сообщение от хоста. Тем самым мы узнаем 1) адрес хоста 2) время которое прошло с момента отправки до момента получения ответа об уничтожении пакета.
2. Дальше опять отправляется 3 ICMP пакета (ping) но уже с TTL=2. Пакет будет откинут на 2м хосте. И так далее, TTL увеличивается на 1, пока мы не достигнем нашего целевого хоста.
3. Отправление 3х ICMP пакетов, помогает нам понять, включена ли балансировка, т.е. возможно есть несколько маршрутов по которым мы можем добраться до хоста, если это так, то мы увидим существенные различия во временных затратах на отправку и получение сообщения.

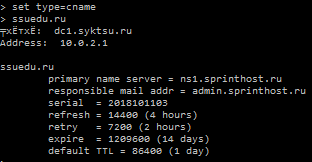
15. Давайте познакомимся с еще одно командой [nslookup](https://ru.wikipedia.org/wiki/Nslookup). При вводе данной команды, вы получите ответ от вашего DNS сервера, который обслуживает вашу сеть и его адреса.



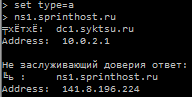
16. Теперь вы можете отправлять различные запросы на данный [DNS сервер](https://ru.wikipedia.org/wiki/DNS-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80). Давайте запросим [A запись](https://ru.wikipedia.org/wiki/%D0%A2%D0%B8%D0%BF%D1%8B_%D1%80%D0%B5%D1%81%D1%83%D1%80%D1%81%D0%BD%D1%8B%D1%85_%D0%B7%D0%B0%D0%BF%D0%B8%D1%81%D0%B5%D0%B9_DNS) для домена ssuedu.ru. Для этого введем **set type=a** ,а затем домен **ssuedu.ru**. Ответ не заслуживает доверия, потому что наш DNS сервер не отвечает за данный домен, не является первичным. Т.е. для того чтобы ответить нам, DNS сервер сначала сделал запрос до [первичного DNS сервера](http://www.opennet.ru/docs/dns/dns.html#hier), и перенаправил нам его ответ.



17. Давайте узнаем, какой DNS-сервер отвечает за домен ssuedu.ru. Для этого введем запрос **set type=cname** ,а затем домен **ssuedu.ru**.



18. Отлично! Мы видим **primary name server** ([первичный DNS-сервер](http://www.opennet.ru/docs/dns/dns.html#hier)), им является **ns1.sprinthost.ru**. Теперь давайте узнаем IP адрес данного сервера. Запросим **set type=a** ,а затем домен **ns1.sprinthost.ru**. В итоге мы получили IP адрес первичного DNS-сервера домена **ssuedu.ru**.



19. Злоумышленник может использовать эту информацию для проведения атаки на первичный DNS-сервер, с целью подмены данных или блокирования работы сервера.

**В данной лабораторной работе мы узнали:**

1. Как узнать **IP адрес** сайта;
2. Как узнать через какое сетевое оборудование проходит пакет, на пути к сайту и сколько времени это занимает;
3. Узнали что такое **фрейм (кадр)**, какой его размер и предназначение.
4. Узнали что такое **TTL** и для чего используется этот параметр;
5. Как узнать свой **DNS-сервер** и его адрес, а также **первичный DNS-сервер** любого домена и его адрес.