

## Лабораторная работа №11 Использование сетевых утилит командной строки Windows.

Итак, мы хотим узнать IP-адрес страницы ssuedu.ru:



Открываем cmd и пингуем:

```
C:\Users\Пользователь>ping ssuedu.ru

Обмен пакетами с ssuedu.ru [141.8.194.122] с 32 байтами данных:
Ответ от 141.8.194.122: число байт=32 время=38мс TTL=55
Ответ от 141.8.194.122: число байт=32 время=38мс TTL=55
Ответ от 141.8.194.122: число байт=32 время=38мс TTL=55
Ответ от 141.8.194.122: число байт=32 время=38мс TTL=55

Статистика Ping для 141.8.194.122:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 38мсек, Максимальное = 38 мсек, Среднее = 38 мсек

C:\Users\Пользователь>_
```

Теперь найдём максимальный размер кадра в сети:

```
C:\Users\Пользователь>ping ssuedu.ru -f -l 1500

Обмен пакетами с ssuedu.ru [141.8.194.122] с 1500 байтами данных:
Требуется фрагментация пакета, но установлен запрещающий флаг.
Требуется фрагментация пакета, но установлен запрещающий флаг.
Требуется фрагментация пакета, но установлен запрещающий флаг.
Требуется фрагментация пакета, но установлен запрещающий флаг.

Статистика Ping для 141.8.194.122:
    Пакетов: отправлено = 4, получено = 0, потеряно = 4
    (100% потерь)

C:\Users\Пользователь>
```

Но успеха нет ☹

Тогда уменьшим размер передаваемой информации:

```
C:\Users\Пользователь>ping ssuedu.ru -f -l 1300

Обмен пакетами с ssuedu.ru [141.8.194.122] с 1300 байтами данных:
Ответ от 141.8.194.122: число байт=1300 время=39мс TTL=55
Ответ от 141.8.194.122: число байт=1300 время=70мс TTL=55
Ответ от 141.8.194.122: число байт=1300 время=39мс TTL=55
Ответ от 141.8.194.122: число байт=1300 время=102мс TTL=55

Статистика Ping для 141.8.194.122:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 39мсек, Максимальное = 102 мсек, Среднее = 62 мсек
```

Теперь всё гуд. Ну и «потолком» размера является 1472 и 1473 – выше уже не работает. **НО!** В моем случае это значение совершенно другое:

```
C:\Users\Пользователь>ping ssuedu.ru -f -l 1393

Обмен пакетами с ssuedu.ru [141.8.194.122] с 1393 байтами данных:
Требуется фрагментация пакета, но установлен запрещающий флаг.
Требуется фрагментация пакета, но установлен запрещающий флаг.
Требуется фрагментация пакета, но установлен запрещающий флаг.
Требуется фрагментация пакета, но установлен запрещающий флаг.

Статистика Ping для 141.8.194.122:
    Пакетов: отправлено = 4, получено = 0, потеряно = 4
    (100% потерь)

C:\Users\Пользователь>ping ssuedu.ru -f -l 1392

Обмен пакетами с ssuedu.ru [141.8.194.122] с 1392 байтами данных:
Ответ от 141.8.194.122: число байт=1392 время=39мс TTL=55
Ответ от 141.8.194.122: число байт=1392 время=39мс TTL=55
Ответ от 141.8.194.122: число байт=1392 время=39мс TTL=55
Ответ от 141.8.194.122: число байт=1392 время=39мс TTL=55


Статистика Ping для 141.8.194.122:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 39мсек, Максимальное = 39 мсек, Среднее = 39 мсек

C:\Users\Пользователь>
```

*1 В принципе я не удивлен...*

## TTL

Пингуем с TTL:

 C:\WINDOWS\system32\cmd.exe

```
C:\Users\Пользователь>ping ssuedu.ru -i 3

Обмен пакетами с ssuedu.ru [141.8.194.122] с 32 байтами данных:
Ответ от 46.150.128.29: Превышен срок жизни (TTL) при передаче пакета.
Ответ от 46.150.128.29: Превышен срок жизни (TTL) при передаче пакета.
Ответ от 46.150.128.29: Превышен срок жизни (TTL) при передаче пакета.
Ответ от 46.150.128.29: Превышен срок жизни (TTL) при передаче пакета.

Статистика Ping для 141.8.194.122:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)

C:\Users\Пользователь>
```

Пакет не дошел ☹ ну ничего, идем дальше!

Используем команду **tracert**:

```
Трассировка маршрута к ssuedu.ru [141.8.194.122]
с максимальным числом прыжков 30:

 1      1 ms      <1 мс      <1 мс      192.168.0.1
 2      <1 мс     <1 мс      <1 мс      80.82.174.9
 3       3 ms      <1 мс      <1 мс      46.150.128.29
 4      <1 мс     <1 мс      <1 мс      46.150.128.1
 5       1 ms       1 ms       1 ms      195.22.107.109
 6      30 ms      29 ms      31 ms      m9-r5.w-ix.ru [193.106.112.5]
 7      33 ms      32 ms      43 ms      mx480-mm11.as35000.msk-ix-m9.ptspb.net [195.208.208.119]
 8      33 ms      33 ms      33 ms      as35278.ix.dataix.ru [178.18.225.80]
 9       *         *         *          Превышен интервал ожидания для запроса.
10      38 ms      38 ms      41 ms      hrugnir.from.sh [141.8.194.122]

Трассировка завершена.
```

## Nslookup

По сути это утилита для работы(обращения) с DNS-сервером, введем ее:

```
C:\Users\Пользователь>nslookup
ТХЇТХЇ яю ёьюйрэш■: one.one.one.one
Address: 1.1.1.1
```

ВОТ ТАК ВОТ И ЖИВЕМ...

Запроим “А” запись домена ssuedu:

```
C:\Users\Пользователь>nslookup
ТхЁтхЁ ю ёыёурэш: one.one.one.one
Address: 1.1.1.1

> set type=a
> ssuedu.ru
ТхЁтхЁ: one.one.one.one
Address: 1.1.1.1

Не заслуживающий доверия ответ:
Ль : ssuedu.ru
Address: 141.8.194.122

>
```

Как видим, наш DNS сервер не отвечает за домен ssuedu, поэтому узнаем какой сервер отвечает за него:

```
> set type=cname
> ssuedu.ru
ТхЁтхЁ: one.one.one.one
Address: 1.1.1.1

ssuedu.ru
    primary name server = ns1.sprinthost.ru
    responsible mail addr = admin.sprinthost.ru
    serial = 2021042903
    refresh = 14400 (4 hours)
    retry = 7200 (2 hours)
    expire = 1209600 (14 days)
    default TTL = 86400 (1 day)

> _
```

Узнаем IP адрес этого сервера:

```
> set type=a
> ns1.sprinthost.ru
ТхЁтхЁ: one.one.one.one
Address: 1.1.1.1

Не заслуживающий доверия ответ:
Ль : ns1.sprinthost.ru
Addresses: 84.201.185.148
          141.8.196.224
```

Ну а дальше по стандарту: DNS-флуд, рекурсивные DNS-запросы, отраженные DNS-запросы и заполнение трафика мусором. **Но это совсем другая история...** 😊