ПРАКТИЧЕСКАЯ РАБОТА 3.

Тема: «Утилиты командной строки Windows для работы с сетью».

Цели работы «Утилиты командной строки» - формирование у студентов базовых знаний и компетенций в сфере организации и функционирования локальных информационно-вычислительных сетей и глобальной сети Интернет, необходимых для решения профессиональных задач, а также получение студентами практических умений и навыков построения, установки, конфигурирования, настройки, защиты, использования и сопровождения сетей в различных режимах функционирования.
Задачи работы:
научить студентов разбираться в базовых сетевых технологиях, принципах и протоколах маршрутизации, стеке TCP/IP, адресации в IP-сетях;

1. Подготовительная часть

Для проведения данной лабораторной работы необходим компьютер под управлением любой операционной системы семейства Microsoft Windows.
Все команды будут выполняться в командном интерпретаторе. Для его запуска необходимо нажать кнопку «Пуск» и выбрать раздел «Выполнить…». В строке ввода указать имя команды:
PowerShell или cmd
и нажать кнопку “Ok”. Откроется окно интерпретатора.
Команды вводятся с клавиатуры, завершаются вводом “Enter”.
Предыдущие команды можно вызвать для редактирования и последующего выполнения с помощью курсорной клавиши «Вверх».

2. Утилита ipconfig

Данная программа предназначена для получения информации о настройках протокола TCP/IP сетевых интерфейсов ОС Windows. Для получения краткой информации о настройках необходимо выполнить команду ipconfig без параметров.

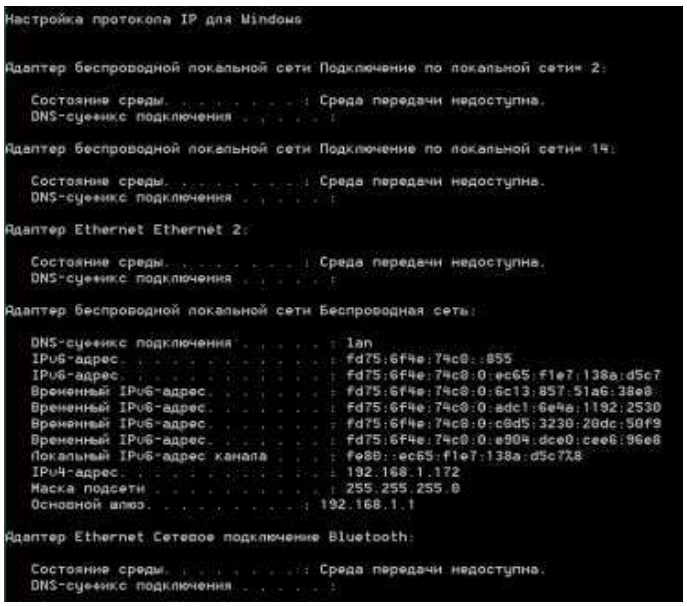


Рис.1 Результат выполнения команды `ipconfig`

Задание 1.

Выполните команду **`ipconfig`** и запишите информацию об IP-адресе, маске сети и шлюзе по умолчанию для сетевого адаптера.

Для получения подробной информации о настройках TCP/IP необходимо выполнить команду `ipconfig` с ключом `/all`:

```
ipconfig /all
```

С помощью команды ipconfig /all можно узнать MAC-адрес компьютера, а также ряд сведений об адресации уровня 3 для устройства.

```
Адаптер беспроводной покальной сети Беспроводная сеть:

   DNS-суффикс подключения . . . . . : lan
   Описание. . . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 7265
   Физический адрес. . . . . . . . . : 10-02-B5-F3-39-A0
   DHCP включен. . . . . . . . . . . : Да
   Автонастройка включена. . . . . . : Да
   IPv6-адрес. . . . . . . . . . . . : fd75:6f4e:74c0::855(Основной)
   Аренда получена. . . . . . . . . . : 6 ноября 2018 г. 10:08:14
   Срок аренды истекает. . . . . . . . . . : 14 декабря 2154 г. 21:30:36
   IPv6-адрес. . . . . . . . . . . . : fd75:6f4e:74c0:0:ec65:f1e7:138a:d5c7(Основной)
   Временный IPv6-адрес. . . . . . . : fd75:6f4e:74c0:0:6c13:857:51a6:38e8(Основной)
   Временный IPv6-адрес. . . . . . . : fd75:6f4e:74c0:0:adc1:6e4a:1192:2530(Устаревший)
   Временный IPv6-адрес. . . . . . . : fd75:6f4e:74c0:0:c0d5:3230:20dc:50f9(Устаревший)
   Временный IPv6-адрес. . . . . . . : fd75:6f4e:74c0:0:e904:dce0:cee6:96e8(Устаревший)
   Локальный IPv6-адрес канала . . . : fe80::ec65:f1e7:138a:d5c7%8(Основной)
   IPv4-адрес. . . . . . . . . . . . : 192.168.1.172(Основной)
   Маска подсети . . . . . . . . . . : 255.255.255.0
   Аренда получена. . . . . . . . . . : 7 ноября 2018 г. 13:03:52
   Срок аренды истекает. . . . . . . . . . : 8 ноября 2018 г. 1:03:51
   Основной шлюз. . . . . . . . . : 192.168.1.1
   DHCP-сервер. . . . . . . . . . . : 192.168.1.1
   IAID DHCPv6 . . . . . . . . . . . : 68158133
   DUID клиента DHCPv6 . . . . . . . : 00-01-00-01-1F-3B-CB-DA-10-02-B5-F3-39-A0
   DNS-серверы. . . . . . . . . . . : fe80::c24a:ff:fea4:7b6e%8
                                       192.168.1.1
   NetBios через TCP/IP. . . . . . . : Включен
   Список поиска DNS-суффиксов подключения :
                                       lan
```

Рис.2 Результат выполнения команды `ipconfig /all` для одного из интерфейсов

Задание 2.

Выполните команду **`ipcofig /all`** и запишите информацию об аппаратном адресе сетевой карты, списке DNS-серверов сетевого подключения.

3. Утилита `ping`

Данная программа предназначена для проверки доступности удаленного узла по сети. Для этого используется служебный протокол ICMP.

С локальной машины на удаленный узел посылается запрос с кодом “echo-request” (эхо-запрос) и в течение некоторого времени локальная машина ожидает ответа “echo-reply” (эхо-ответ). После получения каждого эхо-ответа служба эхо-тестирования предоставляет данные о времени, прошедшем между отправкой запроса и получением ответа. Это позволяет измерить производительность сети.

После отправки всех запросов утилита ping выдает отчет, содержащий уровень успешности запросов и среднее суммарное время доставки запросов и получения ответов.

У команды ping предусмотрен интервал ожидания ответа. Если в течение этого интервала ответ не получен, команда ping выдает сообщение об отсутствии ответа.

Причин может быть несколько:

– если получено диагностическое сообщение по протоколу ICMP, то необходимо проанализировать это сообщение (например, требуется фрагментация пакета);

– если ничего не получено, то удаленный узел не отвечает на запрос (не включен или на узле ответ блокирует брандмауэр), либо время прохождения пакетов по линии связи больше чем время ожидания ответа – в этом случае следует увеличить время ожидания.

В целом же результатом выполнения команды ping является одно из четырех возможных событий.

Во-первых, указанный узел может сгенерировать все четыре отклика. Это означает, что с указанным узлом возможно полноценное взаимодействие на уровне TCP/IP.

Второй вариант – для всех четырех запросов превышен интервал ожидания. Если время ожидания для всех четырех запросов превышается, это значит, что время TTL закончилось до получения ответа. Это может означать один вариант из трех возможных:

- Проблемы с соединением, которые не дают возможности передачи пакетов между двумя узлами и возникают из-за отключения кабеля, ошибок в таблице маршрутизации и тому подобных проблем.
- Передача информации есть, но она слишком медленная для получения ответа по команде ping. Это может происходить из-за перегрузки сети, неисправного сетевого оборудования или проводки.
- Передача информации идет, но брандмауэр блокирует ICMP трафик. В таких ситуациях опрос не работает, пока на

брандмауэре на целевой машине (а также на всех брандмауэрах на пути к ней) не будут разрешены ICMP эхо-сигналы

Третье, что может произойти при выполнении команды ping, - ситуация, когда некоторые отклики получены, а некоторые – нет. Это может указывать на неисправности в сетевых кабелях, сетевом оборудовании или на чрезмерную нагрузку сети.

И последний четвертый вариант: ошибка PING: Transmit Failed (передача не удалась) указывает на то, что TCP/IP неверно настроен на той машине, на которой вы пытаетесь выполнить команду ping. Эта ошибка специфична для Vista или более поздних версий. В более старых версиях Windows при неверной настройке TCP/IP ошибка также происходит, но сообщение в таком случае выглядит так: «Destination Host Unreachable» (Заданный узел недоступен)

В простейшем случае в качестве аргумента команде необходимо указать имя узла (DNS-имя или NetBIOS-имя) или IP-адрес узла, например:

```
ping 10.20.30.40
```

```
Обмен пакетами с 192.168.1.1 по с 32 байтами данных:
Ответ от 192.168.1.1: число байт=32 время=1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=10мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=1мс TTL=64

Статистика Ping для 192.168.1.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 10 мсек, Среднее = 3 мсек
```

Рис.3 Результат выполнения команды `ping` с параметрами по умолчанию

Задание 3.

Проверьте доступность по сети шлюза по умолчанию и любого соседнего компьютера.

Среди дополнительных опций команда ping принимает флаг **`-f`**, который запрещает фрагментацию IP-пакетов. Так как сетевой уровень абстрагируется от используемой технологии канального уровня, то необходим механизм, с помощью которого можно передавать блоки данных произвольной длины через различные транспортные сети с их собственными технологиями канального уровня, которые имеют разные ограничения на размер кадра (MTU). В случае если пакет данных плюс служебные заголовки

превышает размер кадра, то пакет разбивается на фрагменты, которые уже могут быть переданы в кадрах канального уровня. На конечном узле фрагменты собираются в единый пакет данных.

Вторая опция команды – это флаг **`-l`**, после которого через пробел указывается цифра – размер буфера, который будет посылаться на удаленный узел в пакете ICMP. Используя совместно ключи `-l` и `-f` можно выяснить максимальный размер блока данных, помещенного в IP-пакет, который еще иначе называется MSS (максимальный размер сегмента). MSS будет равен длине блока данных + длина ICMP заголовка, который равен 8 байт в случае команды `ping`. Размер стандартного заголовка IP-пакета равен 20 байт. Таким образом MTU = "размер буфера команды `ping`" + 8 + 20.

Задание 4.

Экспериментально выясните максимальный размер кадра канального уровня (MTU) в сети. Для этого необходимо посылать пакеты различной длины при установленном флаге запрета фрагментации (MSS). В качестве удаленного узла можно выбрать адрес шлюза по умолчанию или адрес любого соседнего компьютера или сайт из варианта задания . Начните с начального значения размера буфера 1500.

Еще один флаг команды – это флаг **`-a`**, который позволяет получить имя DNS по адресу компьютера (как правило, IP-адресу).

```
C:\Users\opesk>ping -a 192.168.1.1

Обмен пакетами с OpenWrt.lan [192.168.1.1] с 32 байтами данных:
Ответ от 192.168.1.1: число байт=32 время=1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=1мс TTL=64

Статистика Ping для 192.168.1.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 1 мсек, Среднее = 0 мсек
```

Рис.4 Результат выполнения команды `ping` с параметром -a

Задание 5.

Определите DNS-имя любого соседнего компьютера по его IP-адресу.

Следующий флаг команды – это флаг **-i**, который позволяет задать TTL – «время жизни» посылаемых пакетов. Для решения проблем наличия петель в маршрутизации и, соответственно, бесконечной циркуляции IP-пакетов в сети, каждый посылаемый пакет имеет поле TTL, которое содержит некоторое целое число. Это число уменьшается на единицу при каждом прохождении пакета маршрутизаторов. В тот момент, когда значение TTL станет равным 0, такой пакет отбрасывается, а отправителю по протоколу ICMP отправляется уведомление о том, что пакет отброшен из-за нулевого TTL. По рекомендации RFC 1700 начальное значение TTL должно быть 64. Таким образом, это обеспечивает прохождение пакетом до 63 промежуточных маршрутизаторов. Различные операционные системы могут выбирать начальное значение TTL по-разному.

Приходящее уведомление о нулевом значении TTL, помимо всего прочего, содержит и IP-адрес маршрутизатора, на котором произошло обнуление TTL. Таким образом, посылая пакеты с начальным TTL = 1 и увеличивая TTL на единицу, можно получить список всех маршрутизаторов на пути следования пакета от отправителя к получателю.

```
C:\Users\opesk>ping -i 1 www.ya.ru

Обмен пакетами с ya.ru [87.250.250.242] с 32 байтами данных:
Ответ от 192.168.1.1: Превышен срок жизни (TTL) при передаче пакета.
Ответ от 192.168.1.1: Превышен срок жизни (TTL) при передаче пакета.
Ответ от 192.168.1.1: Превышен срок жизни (TTL) при передаче пакета.
Ответ от 192.168.1.1: Превышен срок жизни (TTL) при передаче пакета.

Статистика Ping для 87.250.250.242:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)

C:\Users\opesk>ping -i 2 www.ya.ru

Обмен пакетами с ya.ru [87.250.250.242] с 32 байтами данных:
Ответ от 10.10.133.1: Превышен срок жизни (TTL) при передаче пакета.
Ответ от 10.10.133.1: Превышен срок жизни (TTL) при передаче пакета.
Ответ от 10.10.133.1: Превышен срок жизни (TTL) при передаче пакета.
Ответ от 10.10.133.1: Превышен срок жизни (TTL) при передаче пакета.

Статистика Ping для 87.250.250.242:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)

C:\Users\opesk>ping -i 3 www.ya.ru

Обмен пакетами с ya.ru [87.250.250.242] с 32 байтами данных:
Ответ от 10.131.92.1: Превышен срок жизни (TTL) при передаче пакета.
Ответ от 10.131.92.1: Превышен срок жизни (TTL) при передаче пакета.
Ответ от 10.131.92.1: Превышен срок жизни (TTL) при передаче пакета.
Ответ от 10.131.92.1: Превышен срок жизни (TTL) при передаче пакета.

Статистика Ping для 87.250.250.242:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
```

Рис.5 Результат выполнения команды `ping` с целью получения списка маршрутизаторов по пути следования

Задание 6.

Определите список маршрутизаторов на пути следования пакетов от локального компьютера до адреса из варианта задания.

4. Утилита tracert

Команда traceroute (tracert) — это утилита, позволяющая составить список переходов, по которым успешно проходит эхо-запрос на пути к узлу назначения.

Если запрос доходит до узла назначения, утилита trace заносит в список интерфейс каждого маршрутизатора на пути между узлами. Если на каком-то переходе на маршруте происходит сбой передачи данных, то адрес последнего маршрутизатора, ответившего на трассировку, может указать на место нахождения проблемы или ограничения системы безопасности.

Утилита traceroute определяет суммарное время прохождения сигнала в прямом и обратном направлениях (RTT) для каждого перехода на маршруте и сообщает о возможном отсутствии ответа на одном из переходов. RTT — это время, которое требуется на доставку пакета на удаленный узел и получения ответа это этого узла. Символ звездочки (*) используется для обозначения потерянного пакета или отсутствия ответа на пакет.

Данная утилита автоматизирует рассмотренный ранее процесс получения промежуточных маршрутизаторов с помощью утилиты `ping`. В простейшем случае в качестве аргумента команде необходимо указать имя узла (DNS-имя или NetBIOS-имя) или IP-адрес узла, например:

```
tracert 10.20.30.40
```

```
C:\Users\opesk>tracert ictis.sfedu.ru

Трассировка маршрута к ictis.sfedu.ru [195.208.245.251]
с максимальным числом прыжков 30:

  1     1 ms     1 ms     2 ms  OpenWrt.lan [192.168.1.1]
  2     1 ms     1 ms    <1 мс  10.10.133.1
  3     1 ms     1 ms     1 ms  10.131.92.1
  4     6 ms     3 ms     4 ms  uginfo-c1.r61.net [195.208.245.225]
  5     7 ms     6 ms     7 ms  hosting.r61.net [195.208.245.251]

Трассировка завершена.
```

Рис.6 Результат выполнения команды `tracert`

Задание 7.

Определите список маршрутизаторов на пути следования пакетов от локального компьютера до адреса из варианта задания.

По умолчанию `tracert` выполняет преобразование полученных IP-адресов маршрутизаторов в символьные имена DNS. Это замедляет работу `tracert`, поэтому, если преобразование не требуется, то можно указать ключ **`-d`**

```
C:\Users\opesk>tracert -d ictis.sfedu.ru

Трассировка маршрута к ictis.sfedu.ru [195.208.245.251]
с максимальным числом прыжков 30:

  1     1 ms     5 ms     8 ms  192.168.1.1
  2     1 ms    <1 мс    <1 мс  10.10.133.1
  3     1 ms     1 ms     1 ms  10.131.92.1
  4     4 ms     3 ms     3 ms  195.208.245.225
  5    14 ms     4 ms     4 ms  195.208.245.251

Трассировка завершена.
```

Рис.7 Результат выполнения команды `tracert` с параметром `-d`

Задание 8.

Определите список маршрутизаторов на пути следования пакетов от локального компьютера до адреса 178.248.237.68 и до адреса домена без преобразования IP-адресов в имена DNS. Адрес домена из варианта задания.

Вариант задания взять из Пракической работы "Анализ Google Page Speed"

5. Утилита `route`

Утилита `route` позволяет получить/изменять таблицу маршрутизации локального компьютера. Для того чтобы получить таблицу маршрутизации, необходимо выполнить команду `route` с параметром `print`:

```
route print
```

Будут отображены следующие три раздела, относящиеся к текущим сетевым подключениям TCP/IP:

- Список интерфейса. Содержит адрес управления доступом к среде (MAC-адрес) и присвоенный номер интерфейса с поддержкой сети на узле, включая адаптеры Ethernet, Wi-Fi и Bluetooth.
- Таблица маршрутизации IPv4. Содержит все известные маршруты IPv4, включая прямые подключения, локальные сети и локальные маршруты, используемые по умолчанию.
- Таблица маршрутизации IPv6. Содержит все известные маршруты IPv6, включая прямые подключения, локальные сети и локальные маршруты, используемые по умолчанию.

```
===========================================================================
Список интерфейсов
 17...10 02 b5 f3 39 a1 ......Microsoft Wi-Fi Direct Virtual Adapter
 14...12 02 b5 f3 39 a0 ......Microsoft Wi-Fi Direct Virtual Adapter #3
  5...00 ff 13 44 e8 3f ......TAP-Windows Adapter V9
  8...10 02 b5 f3 39 a0 ......Intel(R) Dual Band Wireless-AC 7265
  2...10 02 b5 f3 39 a4 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 таблица маршрута
===========================================================================
Активные маршруты:
Сетевой адрес          Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.172     50
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.1.0    255.255.255.0         On-link     192.168.1.172    306
    192.168.1.172  255.255.255.255         On-link     192.168.1.172    306
    192.168.1.255  255.255.255.255         On-link     192.168.1.172    306
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link     192.168.1.172    306
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link     192.168.1.172    306
===========================================================================
Постоянные маршруты:
  Отсутствует
```

Рис.8. Часть вывода таблицы маршрутизации

Задание 9.
Получите таблицу маршрутизации локального компьютера.

Для внесения изменений в таблицу маршрутизации используются параметры **`add`** и **`delete`**.

6. Утилита `arp`

Данная утилита позволяет получить таблицу соответствия IP-адресов и MAC-адресов. В связи с тем, что сетевой уровень вводит свою систему адресов, уникальных в пределах все составной сети, то необходим механизм, с помощью которого можно преобразовывать IP-адреса в аппаратные адреса канального уровня, используемой транспортной сети.

В случае, если IP-адрес назначения находится в подсети, подключенной напрямую к одному из сетевых интерфейсов компьютера (т.е. не используя шлюз), то отправитель может отправить пакет данных «напрямую. Для этого отправитель посылает в соответствующий сетевой интерфейс (согласно таблице маршрутизации) широковещательный запрос по протоколу ARP, содержащий следующие данные:

- MAC-адрес источника
- IP-адрес источника
- искомый IP-адрес

Тот компьютер, который владеет искомым IP-адресом, отвечает на запрос. При этом результат опроса, т.е. MAC-адрес конечного компьютера, сохраняется в таблице ARP отправителя в течение некоторого времени, после которого запись удаляется. Конечный компьютер так же сохраняет в своей таблице ARP соответствие IP-адреса и MAC-адресе отправителя.

Если же удаленный узел достижим через шлюз, то пакет передается ему, и он принимает решение о методе доставке конечному узлу. В этом случае ARP запрос будет послан для выяснения аппаратного адреса шлюза.

Для получения таблицы ARP, необходимо запустить команду `arp` с ключом `-a`

```
arp -a
```

Команда `arp -a` позволяет получить список всех устройств, которые в данный момент представлены в ARP-кэше узла, а также IPv4-адрес, физический адрес и тип адресации (статическая/динамическая) для каждого из устройств.

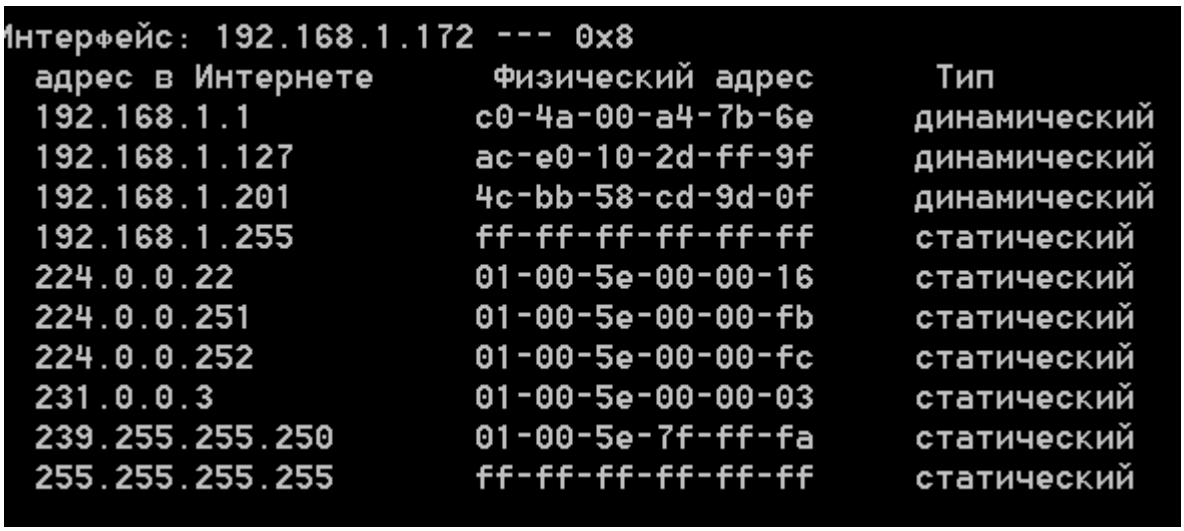


Рис.9 Результат выполнения команды `arp -a`

Задание 10.
Получите таблицу ARP локального компьютера.

Команда `arp` также позволяет выполнять модификацию таблицы маршрутизации с помощью ключей `-s` и `-d` (добавление и удаление соответственно).

В частности, если администратору сети необходимо повторно заполнить кэш обновленными данными, можно выполнить команду `arp -d*` для очистки кэша.

Кэш ARP содержит данные, полученные только от тех устройств, к которым недавно осуществлялся доступ. Чтобы проверить заполнение кэша ARP, следует выполнить команду `ping` для проверки связи с устройством, чтобы для него была создана запись в таблице ARP.

7. Утилита netstat

Команда `netstat` позволяет получить список используемых протоколов, локальных адресов и номеров портов, адрес и номер порта на удаленном узле, а также сообщает состояние соединений.

Если запустить команду `netstat` без параметров, то можно получить список активных TCP соединений между локальным и удаленными компьютерами. В колонке "состояние" отображается статус TCP-соединения.

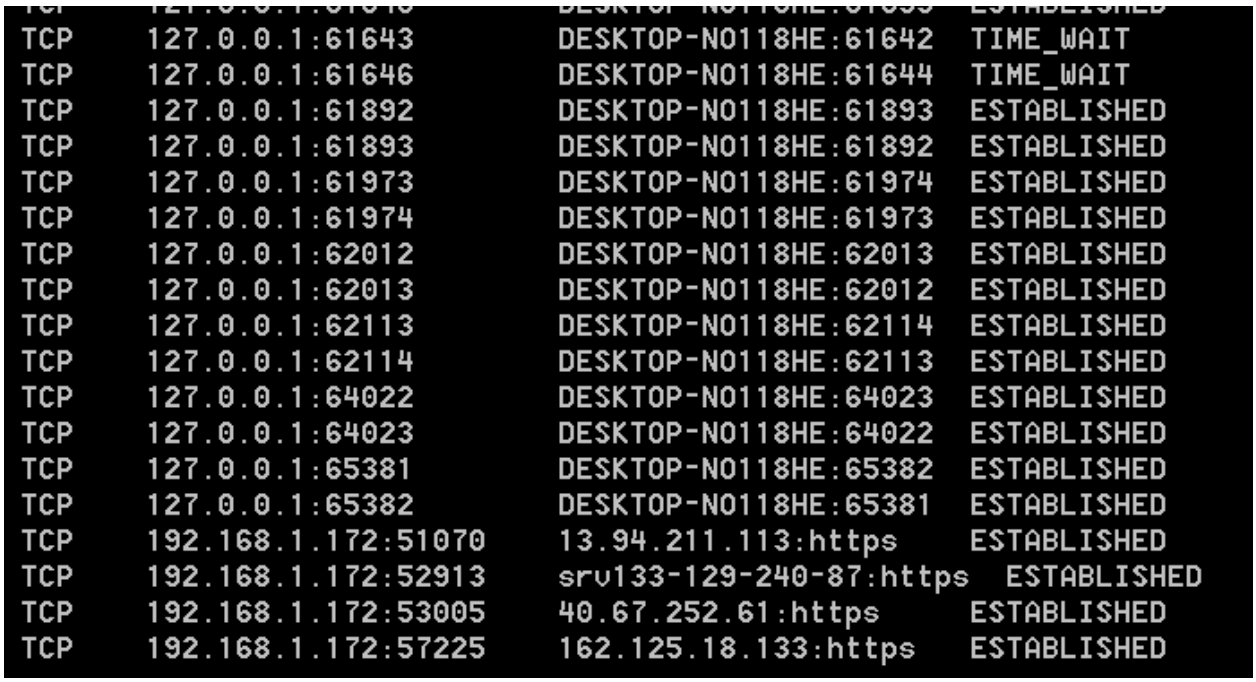


Рис.10. Результат работы команды `netstat`

Задание 11.
Получите список активных TCP-соединений локального компьютера.

По умолчанию `netstat` выполняет преобразование полученных IP-адресов в символьные имена DNS и номера портов в название сетевых служб. Это замедляет работу netstat, поэтому если преобразование не требуется, то можно указать ключ **`-n`**

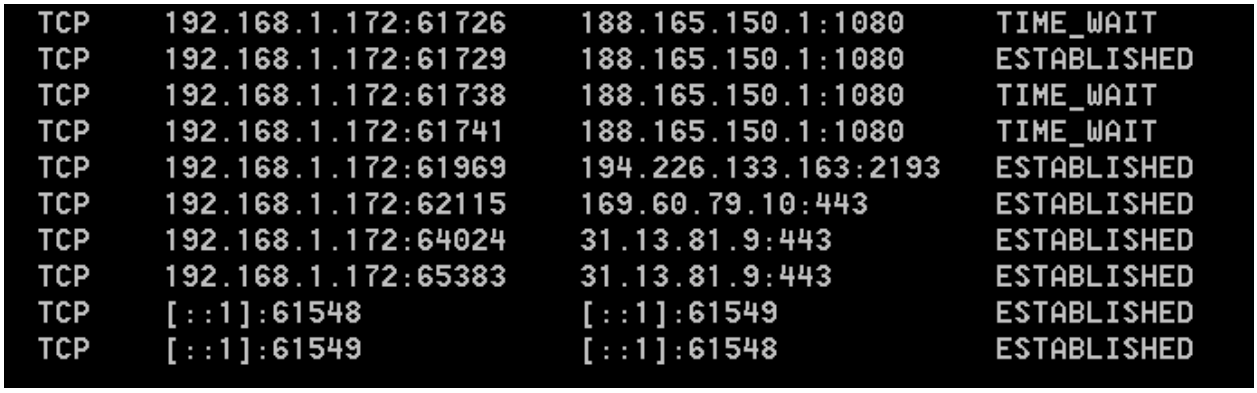
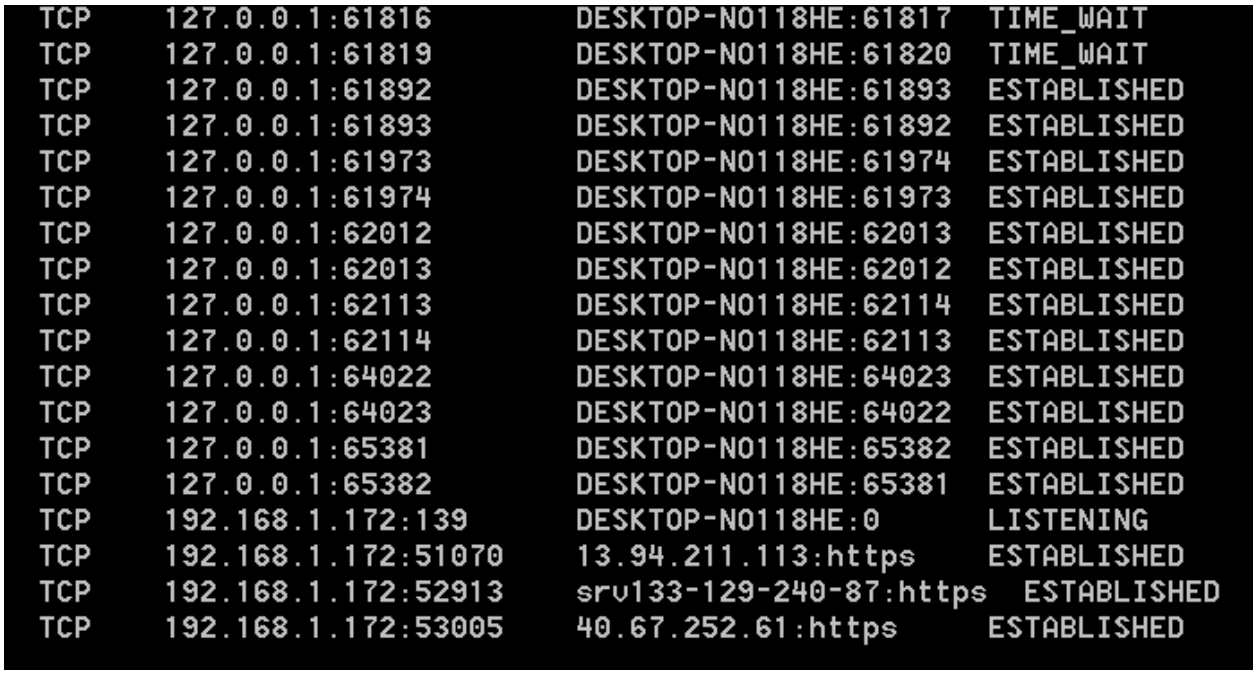


Рис.11. Результат работы команды `netstat -n`

Задание 12.
Получите список активных TCP-соединений локального компьютера без преобразования IP-адресов в символьные имена DNS.

Если указать ключ **-a**, то в списке соединений будут указаны также и прослушиваемые компьютером порты TCP и UDP.



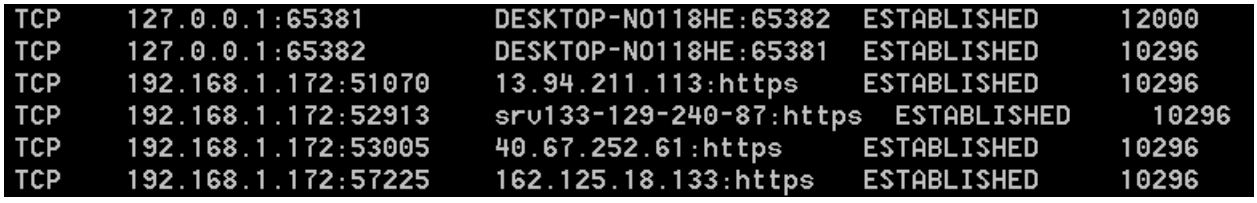
```
  TCP    127.0.0.1:61816        DESKTOP-NO118HE:61817  TIME_WAIT
  TCP    127.0.0.1:61819        DESKTOP-NO118HE:61820  TIME_WAIT
  TCP    127.0.0.1:61892        DESKTOP-NO118HE:61893  ESTABLISHED
  TCP    127.0.0.1:61893        DESKTOP-NO118HE:61892  ESTABLISHED
  TCP    127.0.0.1:61973        DESKTOP-NO118HE:61974  ESTABLISHED
  TCP    127.0.0.1:61974        DESKTOP-NO118HE:61973  ESTABLISHED
  TCP    127.0.0.1:62012        DESKTOP-NO118HE:62013  ESTABLISHED
  TCP    127.0.0.1:62013        DESKTOP-NO118HE:62012  ESTABLISHED
  TCP    127.0.0.1:62113        DESKTOP-NO118HE:62114  ESTABLISHED
  TCP    127.0.0.1:62114        DESKTOP-NO118HE:62113  ESTABLISHED
  TCP    127.0.0.1:64022        DESKTOP-NO118HE:64023  ESTABLISHED
  TCP    127.0.0.1:64023        DESKTOP-NO118HE:64022  ESTABLISHED
  TCP    127.0.0.1:65381        DESKTOP-NO118HE:65382  ESTABLISHED
  TCP    127.0.0.1:65382        DESKTOP-NO118HE:65381  ESTABLISHED
  TCP    192.168.1.172:139      DESKTOP-NO118HE:0      LISTENING
  TCP    192.168.1.172:51070    13.94.211.113:https    ESTABLISHED
  TCP    192.168.1.172:52913    srv133-129-240-87:https  ESTABLISHED
  TCP    192.168.1.172:53005    40.67.252.61:https     ESTABLISHED
```

Рис.12. Результат работы команды `netstat -n`

Задание13.

Получите список прослушиваемых компьютером портов TCP и UDP с и без преобразования IP-адресов в символьные имена DNS.

Утилита `netstat` в операционной системе Windows поддерживает ключ **-o**, с помощью которого можно получить название/идентификатор процесса, создавшего/прослушивающего соединение.



```
TCP    127.0.0.1:65381        DESKTOP-NO118HE:65382  ESTABLISHED     12000
TCP    127.0.0.1:65382        DESKTOP-NO118HE:65381  ESTABLISHED     10296
TCP    192.168.1.172:51070    13.94.211.113:https    ESTABLISHED     10296
TCP    192.168.1.172:52913    srv133-129-240-87:https  ESTABLISHED     10296
TCP    192.168.1.172:53005    40.67.252.61:https     ESTABLISHED     10296
TCP    192.168.1.172:57225    162.125.18.133:https   ESTABLISHED     10296
```

Рис.13. Результат работы команды `netstat -o`

Результат выполнения Заданий 1-13 оформить скриншотами и разместить в файле отчета по Практической работе 3.

Над каждым размещенным скриншотом указать название вводимой команды.

Скриншоты должны быть читаемыми, аналогично представленных в данном файле.