

Лабораторная работа № 1

Утилиты командной строки Windows для работы с сетью

Цель работы: научиться применять сетевые утилиты командной строки Windows

Теоретическая часть

Классификация систем подготовки текста

Утилитами называются сравнительно небольшие программы, предназначенные для решения каких-либо узкоспециализированных задач. В данной работе рассматриваются утилиты операционной системы Windows, используемые для диагностики сетевых подключений.

Утилита ipconfig

Для связи с сетью компьютеры оснащаются сетевыми интерфейсами, к которым относятся Ethernet платы, Wi-Fi и WiMAX модули. Указанные интерфейсы должны иметь IP адреса. Пример такого адреса – 192.168.0.1. Компьютер может иметь не одну плату, а две или три, и каждая из них будет иметь свой IP адрес. Если имеется WiMAX модуль, то и он будет иметь свой IP адрес. Таким образом, компьютер может иметь несколько адресов. Адреса необходимы для организации пересылки сообщений по сети. Адреса должны быть уникальными. Ведь если в сети находятся два компьютера с одинаковыми адресами, то кому из них будет адресовано сообщение с указанным адресом? IP адреса разбиты на две категории: приватные и публичные. Приватные адреса имеют силу лишь для своей локальной сети и в глобальной сети они не видны. Примером такого адреса является 192.168.0.1. Существуют сотни тысяч, а может быть, миллионы локальных сетей, в которых встречаются компьютеры с одинаковыми приватными адресами, и они никак не конфликтуют между собой из-за совпадения адресов. Публичные же адреса уникальны для всей глобальной сети.

Компьютеры образуют сети, которые также имеют свои адреса. Например, компьютер с адресом 192.168.0.1 находится в сети с адресом 192.168.0.0. У адреса сети и адреса компьютера, как видим, совпадают первые три числа. Сколько же на самом деле должно совпадать чисел определяет так называемая маска подсети. Для нашего примера эта маска имеет вид 255.255.255.0. Такое значение маски чаще всего и встречается в локальных сетях.

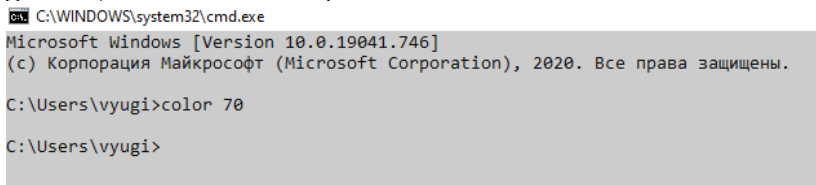
Сами компьютерные сети не изолированы друг от друга. Для связи их между собой используются специализированные компьютеры, называемые маршрутизаторами. Такие сетевые устройства имеют как минимум два сетевых интерфейса, один из которых принадлежит одной сети, другой же является частью второй сети. Маршрутизатор, перенаправляя сообщения с одного своего интерфейса на другой, обеспечивает межсетевой трафик. Если маршрутизатор имеет три платы, то он будет находиться на границе трех сетей. Широкое

распространение получили двухточечные сети, которые образуют два маршрутизатора, соединенные общим кабелем. Интерфейсы обеих маршрутизаторов, присоединенные к разным концам одного кабеля, должны иметь адреса, относящиеся к одной и той же сети. Более часто встречаются тупиковые сети. Такие сети связаны лишь с одним маршрутизатором (отсюда и название сети - тупиковая).

Компьютеры, находящиеся в такой сети, отправляют сообщения, адресованные в другие сети, на интерфейс этого маршрутизатора. Компьютеры, следовательно, должны знать адрес интерфейса маршрутизатора своей сети. Такой адрес носит название «основной шлюз». Маршрутизатор перенаправляет дальше, передавая их своим соседям-маршрутизаторам по двухточечным каналам связи. Таким образом, сообщение последовательно перемещается по следующим сетям: тупиковая сеть, двухточечная сеть 1, двухточечная сеть 2, ..., двухточечная сеть N, тупиковая сеть. Если же маршрут перемещения изучать по узлам, то он будет таким: компьютер (отправитель сообщения), маршрутизатор 1, маршрутизатор 2, ..., маршрутизатор N-1, компьютер (получатель сообщения).

Таким образом, для настройки сетевого интерфейса компьютера необходимо назначить ему IP адрес, маску подсети и основной шлюз.

Программа `ipconfig` предназначена для получения информации о настройках сетевых интерфейсов. Выполняется данная утилита в окне командной строки. Для этого необходимо нажать кнопку Пуск и выбрать пункт «Выполнить...». Далее следует ввести `cmd` и нажать Enter. В открывшемся окне командной строки (рис. 1) следует ввести команду `ipconfig` и нажать Enter. Пример результата выполнения данной утилиты показан на рис. 2.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19041.746]
(c) Корпорация Майкрософт (Microsoft Corporation), 2020. Все права защищены.

C:\Users\vyugi>color 70

C:\Users\vyugi>
```

Рис. 1. Окно командной строки

```

C:\Users\vyugi>ipconfig

Настройка протокола IP для Windows

Адаптер беспроводной локальной сети Подключение по локальной сети* 11:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Адаптер беспроводной локальной сети Подключение по локальной сети* 12:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Адаптер Ethernet Ethernet:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . . : fe80::64bb:f471:5743:c2f%9
    IPv4-адрес. . . . . : 192.168.3.107
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 192.168.3.10

Адаптер Ethernet Сетевое подключение Bluetooth:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Адаптер беспроводной локальной сети Беспроводная сеть:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

```

Рис. 2. Результат выполнения команды ipconfig

Утилита ping

Компьютеры и другие узлы сети помимо IP адресов имеют так называемые доменные адреса. Такие адреса удобны пользователям сети, так как они легче запоминаются. К примеру доменный адрес mail.ru запомнить намного проще чем его IP аналог в виде 94.100.180.70. За соответствие доменных и IP адресов отвечает DNS служба. Когда с компьютера исходит запрос на какой-либо сетевой ресурс по его доменному адресу, то DNS служба позволяет определить соответствующий этому ресурсу IP адрес.

Утилита ping позволяет проверить доступность какого-либо удаленного узла по сети. С этой целью на указанный узел отправляется сообщение в виде запроса, и утилита переходит в режим ожидания прихода ответного сообщения. По истечении некоторого времени посылается повторное сообщение. По результатам обмена сообщениями выводится статистика о качестве связи между двумя узлами. Для пингования удаленного узла можно использовать либо его IP адрес, либо его доменное имя.

Команда ping 127.0.0.1 позволяет проверить настройку самого сетевого интерфейса. Адрес 127.0.0.1 является служебным и узлам сети не назначается. Сетевой интерфейс при использовании данного адреса пингует сам себя. Доменное имя адреса 127.0.0.1 – localhost. Результат такой команды представлен на рис. 3.

```

C:\Users\vyugi>ping 127.0.0.1

Обмен пакетами с 127.0.0.1 по 32 байтами данных:
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128

Статистика Ping для 127.0.0.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

```

Рис. 3. Результат выполнения команды ping

В рассмотренном случае сетевой интерфейс настроен без ошибок, потери отсутствуют. Параметр TTL переводится как «время жизни» (time to life). Его создает узел, отправляющий в сеть свое сообщение. Маршрутизаторы, передавая данное сообщение из одной сети в другую, убавляют TTL на единицу. Если на каком-то маршрутизаторе TTL будет убавлено до нуля, то сообщение будет уничтожено. Маршрутизатор, удаливший из сети сообщение, извещает об этом отправителя, указывая свой адрес.

Второй вариант использования ping – это проверка состояния тупиковой сети, в которой находится сам узел. С этой целью пингуется основной шлюз (рис. 4):

```

C:\Users\vyugi>ping 192.168.0.10

Обмен пакетами с 192.168.0.10 по 32 байтами данных:
Ответ от 192.168.0.10: число байт=32 время<1мс TTL=62
Ответ от 192.168.0.10: число байт=32 время=1мс TTL=62
Ответ от 192.168.0.10: число байт=32 время=1мс TTL=62
Ответ от 192.168.0.10: число байт=32 время<1мс TTL=62

Статистика Ping для 192.168.0.10:
    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

В данном примере маршрутизатор доступен. Он в свои ответные сообщения помещает TTL (62) отличное от TTL (128) сетевого интерфейса компьютера. Для проверки доступности удаленного хоста, как правило, применяются доменные адреса (рис. 5):

```
C:\Users\vyugi>ping yandex.ru
```

```
Обмен пакетами с yandex.ru [5.255.255.50] с 32 байтами данных:
```

```
Ответ от 5.255.255.50: число байт=32 время=8мс TTL=247
```

```
Ответ от 5.255.255.50: число байт=32 время=9мс TTL=247
```

```
Ответ от 5.255.255.50: число байт=32 время=11мс TTL=247
```

```
Ответ от 5.255.255.50: число байт=32 время=8мс TTL=247
```

```
Статистика Ping для 5.255.255.50:
```

```
Пакетов: отправлено = 4, получено = 4, потеряно = 0
```

```
(0% потерь)
```

```
Приблизительное время приема-передачи в мс:
```

```
Минимальное = 8мсек, Максимальное = 11 мсек, Среднее = 9 мсек
```

Рис. 5. Результат выполнения команды ping

Удаленный узел доступен. В данном случае мы видим, что DNS служба определила IP адрес узла в виде 5.255.255.50.

Утилита tracert

Эта утилита, последовательно применяя пинг с увеличивающимся TTL, позволяет получить список промежуточных маршрутизаторов (рис. 6):

```
C:\Users\vyugi>tracert yandex.ru
```

```
Трассировка маршрута к yandex.ru [77.88.55.50]
```

```
с максимальным числом прыжков 30:
```

1	<1 мс	<1 мс	<1 мс	192.168.3.10
2	<1 мс	<1 мс	<1 мс	proxy.rtu [192.168.200.3]
3	2 мс	2 мс	1 мс	172.31.2.1
4	2 мс	2 мс	1 мс	109x195x161x253.static-business.ryazan.ertelecom.ru [109.195.161.253]
5	2 мс	2 мс	2 мс	lag-3-438.bgu01.ryazan.ertelecom.ru [109.195.168.30]
6	5 мс	5 мс	5 мс	188.234.131.242
7	13 мс	7 мс	10 мс	net131.234.188-243.ertelecom.ru [188.234.131.243]
8	12 мс	11 мс	11 мс	yandex.ru [77.88.55.50]

```
Трассировка завершена.
```

Рис. 6. Результат выполнения команды tracert

Между двумя узлами в данном случае находится 7 маршрутизаторов.

Утилита pathping

Утилита pathping сочетает в себе черты команд ping и tracert, позволяя получить дополнительную информацию, которую не обеспечивают две последние. Команда определяет процент потерь сообщений на всех переходах, выявляя самые медленные и ненадежные участки маршрута.

Результат выполнения такой команды представлен на рисунке 7.

```

C:\Users\vyugi>pathping yandex.ru

Трассировка маршрута к yandex.ru [77.88.55.55]
с максимальным числом переходов 30:
 0 Angelina [192.168.3.107]
 1 192.168.3.10
 2 proxy.rtu [192.168.200.3]
 3 172.31.2.1
 4 109x195x161x253.static-business.ryazan.ertelecom.ru [109.195.161.253]
 5 lag-3-438.bgw01.ryazan.ertelecom.ru [109.195.168.30]
 6 188.234.131.242
 7 net131.234.188-243.ertelecom.ru [188.234.131.243]
 8 yandex.ru [77.88.55.55]

Подсчет статистики за: 200 сек. ...


| Прыжок | RTT  | Исходный узел |             | Маршрутный узел |   | Адрес                                                                 |
|--------|------|---------------|-------------|-----------------|---|-----------------------------------------------------------------------|
|        |      | Утер./Отпр.   | %           | Утер./Отпр.     | % |                                                                       |
| 0      |      |               |             |                 |   | Angelina [192.168.3.107]                                              |
| 1      | 0мс  | 0/ 100 = 0%   | 0/ 100 = 0% |                 |   | 192.168.3.10                                                          |
| 2      | 0мс  | 0/ 100 = 0%   | 0/ 100 = 0% |                 |   | proxy.rtu [192.168.200.3]                                             |
| 3      | 1мс  | 0/ 100 = 0%   | 0/ 100 = 0% |                 |   | 172.31.2.1                                                            |
| 4      | 2мс  | 0/ 100 = 0%   | 0/ 100 = 0% |                 |   | 109x195x161x253.static-business.ryazan.ertelecom.ru [109.195.161.253] |
| 5      | 3мс  | 0/ 100 = 0%   | 0/ 100 = 0% |                 |   | lag-3-438.bgw01.ryazan.ertelecom.ru [109.195.168.30]                  |
| 6      | 7мс  | 0/ 100 = 0%   | 0/ 100 = 0% |                 |   | 188.234.131.242                                                       |
| 7      | 6мс  | 0/ 100 = 0%   | 0/ 100 = 0% |                 |   | net131.234.188-243.ertelecom.ru [188.234.131.243]                     |
| 8      | 11мс | 1/ 100 = 1%   | 0/ 100 = 0% | 1/ 100 = 1%     |   | yandex.ru [77.88.55.55]                                               |


Трассировка завершена.

```

Рис. 7. Результат выполнения команды pathping

В настройках некоторых маршрутизаторов может стоять запрет на выдачу ответа на пришедший пинг.

Утилита arp

Сетевые интерфейсы, такие как Ethernet, Wi-Fi и WiMAX, имеют вшитые в их микросхемы адреса. Пример подобного адреса: 70-F3-95-A6-FE-0C. Эти адреса, называемые аппаратными, физическими или MAC, должны добавляться к сообщениям, прежде чем они будут переданы через сеть. Не все сети используют такие адреса, но в тупиковых они, как правило, применяются. Узел, собирающийся отправить сообщение другому узлу, должен предварительно узнать MAC адрес получателя сообщения. Для решения данной проблемы узел применяет технологию ARP, отправляя запрос другим узлам своей локальной сети. Данный ARP запрос содержит IP адрес получателя. Из всех узлов, получивших данный запрос, отвечает лишь тот, у кого требуемый IP адрес. В своем ответе (ARP отклике) тот узел сообщает свой MAC адрес. И лишь после этого первый узел ему сможет отправить свое сообщение. В тупиковых сетях компьютеры чаще всего отправляют свои сообщения маршрутизатору и, следовательно, в своих ARP запросах они указывают адрес основного шлюза. Для уменьшения ARP трафика компьютеры хранят в своей памяти таблицу с IP и MAC адресами тех устройств, с которыми они в последнее время обменивались сообщениями.

Утилита arp позволяет получить таблицу соответствия IP адресов и MAC адресов. На рис. 8 приведен вывод, полученный командой arp, выполненной с ключом -a

```
C:\Users\vyugi>arp -a
```

Интерфейс: 192.168.3.107 --- 0x9	адрес в Интернете	Физический адрес	Тип
192.168.3.10	98-da-c4-bf-96-b4	динамический	
192.168.3.50	00-25-90-d0-68-78	динамический	
192.168.3.99	20-cf-30-f1-32-8b	динамический	
192.168.3.171	24-be-05-15-21-b6	динамический	
192.168.3.250	3c-4a-92-c2-e3-74	динамический	
192.168.3.255	ff-ff-ff-ff-ff-ff	статический	
224.0.0.2	01-00-5e-00-00-02	статический	
224.0.0.22	01-00-5e-00-00-16	статический	
224.0.0.251	01-00-5e-00-00-fb	статический	
224.0.0.252	01-00-5e-00-00-fc	статический	
239.0.0.1	01-00-5e-00-00-01	статический	
239.255.255.250	01-00-5e-7f-ff-fa	статический	
255.255.255.255	ff-ff-ff-ff-ff-ff	статический	

Рис. 8. Результат выполнения команды arp

Утилита netstat

Когда мы говорим: «компьютеры обмениваются сообщениями», то это не совсем точное утверждение. На самом деле обмен происходит между сетевыми приложениями. В оперативной памяти компьютера одновременно могут находиться и выполняться несколько программ, получающих сообщения из сети или отправляющие их в сеть. Как же сообщения, приходящие из сети в компьютер, распределяются между этими приложениями? На этот случай в сообщениях предусмотрены дополнительные адреса, называемые портами. Здесь уместно привести аналогию с обычной почтовой корреспонденцией. Для того чтобы письмо было доставлено в многоквартирный дом (компьютер), на конверте письма указывается номер дома (IP адрес компьютера). Затем письма необходимо разложить по почтовым ящикам согласно номерам квартир. Номер квартиры, присутствующий на конверте письма, и есть аналог портов. Далее жильцы (т.е. сетевые приложения) забирают эти письма (сообщения). Когда приложение хочет обменяться сообщениями с другим удаленным приложением, оно должно знать не только IP адрес компьютера данного приложения, но и номер порта, которое то приложение использует. Эта связка из двух адресов (IP адрес и порт) называется сокетом. Как определяется номер порта, которое использует удаленное приложение - эта тема отдельного разговора. Оба приложения устанавливают между собой соединение, используя два сокета. Сокеты можно условно представить в виде двух разъемов (розеток), соединенных между собой неким виртуальным каналом связи. Когда одно приложение «помещает» в сокет свое сообщение, то оно доставляется на другой конец канала - на второй сокет, и попадает, таким образом, другому приложению. Команда netstat позволяет получить список сокетов. На рис. 9 приведен вывод, полученный с использованием опций a, n, и o.

```
C:\Users\vyugi>netstat -ano
```

Активные подключения

Имя	Локальный адрес	Внешний адрес	Состояние	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	900
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1536	0.0.0.0:0	LISTENING	824
TCP	0.0.0.0:1537	0.0.0.0:0	LISTENING	668
TCP	0.0.0.0:1538	0.0.0.0:0	LISTENING	1484
TCP	0.0.0.0:1539	0.0.0.0:0	LISTENING	1660
TCP	0.0.0.0:1540	0.0.0.0:0	LISTENING	2432
TCP	0.0.0.0:1542	0.0.0.0:0	LISTENING	3592
TCP	0.0.0.0:1546	0.0.0.0:0	LISTENING	808
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	6496
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING	6328
TCP	127.0.0.1:26443	127.0.0.1:49350	TIME_WAIT	0
TCP	127.0.0.1:26445	127.0.0.1:49350	TIME_WAIT	0
TCP	127.0.0.1:26446	127.0.0.1:49350	TIME_WAIT	0
TCP	127.0.0.1:26447	127.0.0.1:49350	TIME_WAIT	0
TCP	127.0.0.1:26448	127.0.0.1:49350	TIME_WAIT	0
TCP	127.0.0.1:26449	127.0.0.1:49350	TIME_WAIT	0
TCP	127.0.0.1:26451	127.0.0.1:49350	TIME_WAIT	0
TCP	127.0.0.1:28385	0.0.0.0:0	LISTENING	4
TCP	127.0.0.1:28390	0.0.0.0:0	LISTENING	4
TCP	127.0.0.1:49350	0.0.0.0:0	LISTENING	10356
TCP	127.0.0.1:49351	0.0.0.0:0	LISTENING	10864
TCP	192.168.3.107:139	0.0.0.0:0	LISTENING	4
TCP	192.168.3.107:10189	51.103.5.186:443	ESTABLISHED	4268
TCP	192.168.3.107:10251	77.88.55.50:443	ESTABLISHED	10500

Рис. 8. Результат выполнения команды netstat

Данный вывод показывает, что сокеты обозначаются в виде пары IP_адрес:порт (с двоеточием между адресами). Например, 192.168.3.107:10189. Виртуальный канал связи, существующий между двумя сетевыми приложениями, обозначен парой сокетов. Например, 192.168.3.107:10189 и 51.103.5.186:443. Первый сокет открыт на компьютере, другой на удаленном узле. Адрес в виде 0.0.0.0 означает любые IP адреса. Если в качестве номера порта присутствует 0, то это означает любые значения портов. В колонке "Состояние" отображается состояние соединения:

- LISTENING – ожидание подключения;
- ESTABLISHED – соединение установлено, идет обмен сообщениями;
- TIME_WAIT – время ответа превышено.

Первый тип состояния (LISTENING) означает, что сетевое приложение ждет установления соединения по определенному порту. Например, сокет 0.0.0.0:445 означает, что какое-то удаленное приложение может отправить на компьютер сообщение на порт 445 с целью установить виртуальное соединение.

В последней колонке (PID) выводятся номера процессов. Под процессами понимаются приложения. Из вывода мы видим, что процесс 4 ждет подключения по портам 445, 5357 и 7680. Как выше было сказано, какая-то программа с другого узла может отправить запрос на установление соединения с процессом 2944. Такая

программа свое сообщение может адресовать на любой из указанных трех портов. Чтобы выяснить, какая программа запущена под видом процесса 2944, вызовем диспетчер задач. В окне диспетчера перейдем на вкладку Процессы и войдем в меню Вид. Далее выберем строчку «Выбрать столбцы» и активируем чекбокс ИД процесса (PID). Щелкнем по ОК. Затем отсортируем таблицу по столбцу ИД процесса (PID), щелкнув по его названию. Находим запись, соответствующую процессу 2944.

Практическая часть

1. В окне командной строки выполните команду `ipconfig`. Запишите в отчет информацию об IP адресе сетевого адаптера, маске сети и шлюзе по умолчанию.

2. Для получения более подробной информации о настройках адаптера запустите в окне командной строки утилиту `ipconfig` с ключом `/all`.

3. Повторите команду `ipconfig /all` с выводом в текстовый файл и запишите в отчет информацию о физическом адресе сетевой платы.

4. Применив команду `ping`, проверьте настройку платы, доступность основного шлюза и доступность удаленного узла. Адреса удаленных узлов выбирайте по своему варианту (см. Варианты).

5. Используя опцию `-i` команды `ping` определите адреса первых трех маршрутизаторов, находящихся между вашим компьютером и удаленным узлом.

6. Применив команду `tracert`, получите список роутеров на маршруте от вашего компьютера до удаленного узла. Адреса поместите в отчет.

7. Используя `pathping`, изучите состояние линков на маршруте от вашего компьютера до удаленного узла и определите самые «узкие места» (т.е. самые медленные участки).

8. Получите таблицу ARP вашего компьютера. Выпишите в отчет MAC адрес основного шлюза.

9. Командой `netstat`, выполненной с ключами `-a`, `-n` и `-o`, получите список соединений, действующих на Вашем компьютере.

10. Определите имя любого приложения, установившего соединение с удаленной программой. Обоснуйте свой вывод.

Варианты по бригадам:

1. infpol.ru
2. vk.com
3. skype.com
4. yandex.ru
5. ok.ru
6. mail.ru
7. rambler.ru
8. wikipedia.org
9. youtube.com
10. facebook.com