**Практическая работа № 1**

Изучение команд работы с сетью

1. ЦЕЛЬ РАБОТЫ

Целью работы является изучение команд работы с сетью в режиме командной строки Windows.

1. КОМАНДНАЯ СТРОКА WINDOWS

1.1. Окно Командная строка

Операционная система управляет аппаратурой компьютера и обеспечивает интерфейс между пользователем и компьютером.

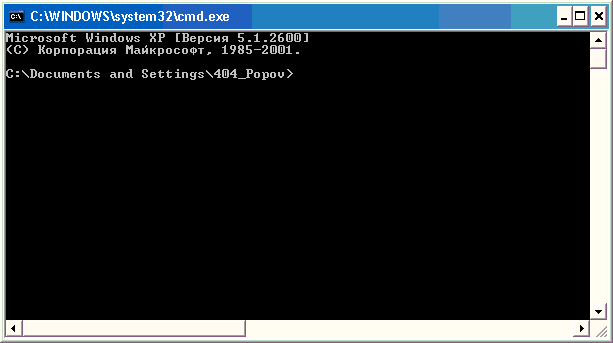
Этот интерфейс может быть реализован двумя способами – графический интерфейс (например, Проводник) и интерфейс командной строки, доставшийся Windows в наследство от операционной системы MS DOS.

При использовании интерфейса командной строки, пользователь набирает команды с клавиатуры, которые (обрабатываются) выполняются с помощью так называемого командного интерпретатора, иначе называемого командным процессором или оболочкой командной строки (command shell). Командный интерпретатор или оболочка командной строки — это программа, которая, находясь в оперативной памяти, считывает набираемые вами команды и обрабатывает их, обращаясь с помощью системных вызовов к функциям операционной системы.

Некоторые команды распознаются командным интерпретатором и выполняются операционной системой с помощью встроенных в нее команд — такие команды называются внутренними (например, COPY или DIR) Другие команды операционной системы представляют собой отдельные программы(утилиты), расположенные по умолчанию в том же каталоге, что и Cmd.exe, которые Windows загружает и выполняет аналогично другим программам. Такие команды называются внешними (например, MORE или XCOPY).

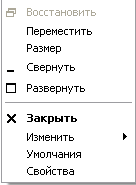
Файл Cmd.exe, как и другие исполняемые файлы, соответствующие внешним командам операционной системы, находятся в каталоге WINDOWS\system32\

Для работы в режиме командной строки надо выбрать в подменю Стандартные главного меню системное приложение Командная строка (значок ) или выбрать пункт Выполнить… (Run) в меню Пуск (Start), ввести имя файла Cmd.exe и нажать кнопку OK. В результате откроется новое окно, в котором можно запускать команды и видеть результат их работы.



Закрыть окно Командная строка можно щелчком по кнопке Закрыть ( ) или вводом в командной строке команды exit.

Окно Командная строка имеет специальный вид, отличный от других окон Windows. Управление размерами и местоположением окна, а также вывод в окне управляется с помощью меню. Это меню вызывается, если щелкнуть правой кнопкой мыши по строке заголовка:



Действия команд отменяются клавишей **Esc**

Команда Переместить позволяет перемещать окно по экрану, а команда Размер – изменить размер окна (только по вертикали). Команды Свернуть, Развернуть, Восстановить и Закрыть дублируют действие соответствующих кнопок строки заголовка окна.

Команда Изменить позволяет окну взаимодействовать с буфером обмена (только для текстовых данных), прокрутить содержимое окна (команда Прокрутить) или найти заданную строку текста в окне (команда Найти).

Взаимодействие с буфером обмена в окне командной строки выполняется с помощью команд Пометить, Копировать, Вставить и Выделить все.

Для копирования из окна командной строки необходимо выполнить следующие действия:

• вызвать контекстное меню для строки заголовка окна;

• в подменю команды Изменить контекстного меню выбрать команду Пометить;

• выделить фрагмент текста, который необходимо скопировать (сначала установить курсор мыши на первый символ копируемого фрагмента, затем нажать левую кнопку мыши и, не отпуская ее, установить курсор мыши на последний символ копируемого фрагмента);

• для выделения всего содержимого окна можно использовать команду Выделить все;

• опять вызвать контекстное меню и подменю команды Изменить контекстного меню выберите команду Копировать (можно также просто нажать клавишу Enter).

Скопированный фрагмент можно вставить в другое место окна или в любое приложение.

Для вставки текстовых данных в окно командной строки необходимо:

• установить курсор в то место, где будет производиться вставка;

• вызвать контекстное меню для строки заголовка окна;

• в подменю команды Изменить контекстного меню выбрать команду Вставить.

В диалоговом окне команды Свойства задаются параметры выводимого окна.

В закладке Общие этого окна можно выбрать размер курсора, режим вывода (окно или полноэкранный режим), количество запоминаемых команд, а также способ редактирования.

В закладке Шрифт можно выбрать шрифт для вывода текста в окне и, соответственно, горизонтальный размер окна, поскольку он зависит от величины выводимого шрифта.

В закладке Расположение задается размер буфера экрана и размер собственно экрана (ширина в символах, высота – в строках), а также положение верхнего левого угла окна относительно верхнего левого угла экрана (в пикселях).

В закладке Цвета можно выбрать цвета текста и фона для окон командной строки (основного и всплывающего).

Команда Умолчания окна Командная строка выводит закладку Расположение команды Свойства.

При возникновении проблем отображения букв русского алфавита в командной строке необходимо загрузить соответствующую таблицу Windows для этого необходимо набрать в командной строке команду

**chcp 1251**

Затем в свойствах командной строки установить шрифт **Lucida Console**/

1.2. Работа в режиме командной строки

Диалог пользователя в режиме командной строки осуществляется в форме команд, вводимых в ответ на приглашение и ответов операционной системы и пользовательской программы на введенные команды.

Приглашение по умолчанию содержит путь к текущей папке (папке, в которой в данный момент находится пользователь) и заканчивается символом '>'. Вид приглашения можно изменить с помощью команды prompt.

В момент загрузки окна Командная строка текущей является папка:

**C:\Documents and Settings\login-пользователя.**

Команда пользователя состоит из имени команды и, возможно, параметров. Параметры обычно задают объекты, над которыми выполняется действие команды. Кроме того, команда может содержать опции, задающие различные режимы выполнения команды. Первым символом опции является символ **"-"** или символ **"/"**. Имя команды и параметры могут набираться как прописными (заглавными), так и строчными латинскими буквами (все строчные буквы переводятся в Windows в прописные буквы). Имя команды, параметры и опции отделяются друг от друга пробелами. Если параметр (например, имя файла) содержит пробелы, он должен быть заключен в двойные апострофы (символ '"'). Ввод каждой команды заканчивается нажатием клавиши Enter (Return).

В качестве имени команды могут использоваться не только имена команд, но и имена программ (файлов с расширением .COM или .EXE), а также командных файлов с расширением .BAT (BatFileIcon)).

Если пользователь не указал, в каком каталоге следует искать программу, то поиск производится в текущем каталоге и в каталогах, заданных командой Path.

Для явного указания папки в команде следует в качестве имени команды использовать полное имя файла, включающее путь к той папке, в которой находится нужная программа или командный файл, например:

**c:\doc\prog\myprog**

До нажатия клавиши Enter можно редактировать строку вводимой команды, удаляя ранее введенные символы с помощью клавиш Backspace .

Кроме этого, можно вызвать предыдущую или следующую выполненную команду (если они есть) с помощью клавиш ↑ или ↓, а также подвести курсор в нужное место команды с помощью клавиш → или ← и выполнить корректировку команды в режиме вставки или замещения (переключение в режим вставки или замещения выполняется с помощью клавиши Ins).

Программы, но не команды, и командные файлы можно запустить, как и приложения Windows, с помощью команды Выполнить (где можно, при необходимости, указать параметры программы) или с помощью Проводника.

Справка по команде Windows выводится либо с помощью команды

**имя-команды /?**

либо с помощью команды

**help имя-команды**

Например, справку по команде dir можно получить с помощью одной из команд:

**dir /? или help dir**

Для некоторых команд текст встроенной справки может быть довольно большим и не умещаться на одном экране. В этом случае помощь можно выводить последовательно по одному экрану с помощью команды MORE и символа конвейеризации |, например:

**XCOPY /? | MORE**

В этом случае после заполнения очередного экрана вывод помощи будет прерываться до нажатия любой клавиши. Кроме того, используя символы перенаправления вывода > и >>, можно текст, выводимый на экран, направить в текстовый файл для дальнейшего просмотра. Например, для вывода ipconfig в текстовый Seti.doc файл используется следующая команда:

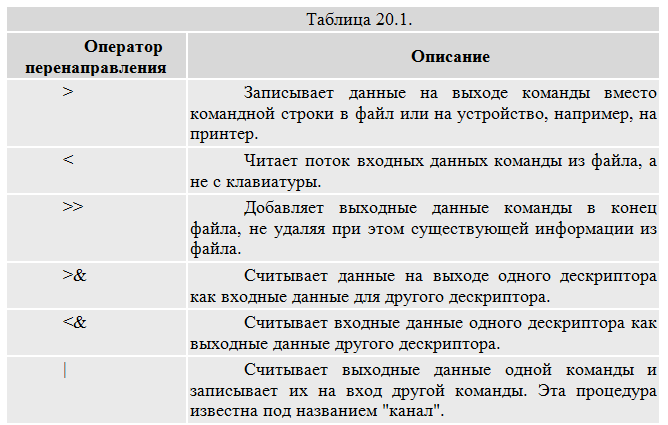
**ipconfig > D:\Seti.doc**

Для добавления выходных данных команды в конец файла, не удаляя при этом существующей информации из файла используется символ >>. Напрмер, чтобы добавить

результат выполнения команды arp -a в существующий файл Seti.doc надо набрать команду

**arp >> D:\Seti.doc**

В таблице описаны операторы перенаправления потоков ввода и вывода команд.



С помощью переназначения устройств ввода/вывода одна программа может направить свой вывод на вход другой или перехватить вывод другой программы, используя его в качестве своих входных данных. Таким образом, имеется возможность передавать информацию от процесса к процессу при минимальных программных издержках. Практически это означает, что для программ, которые используют стандартные входные и выходные устройства, операционная система позволяет:

• выводить сообщения программ не на экран (стандартный выходной поток), а в файл или на принтер (перенаправление вывода);

• читать входные данные не с клавиатуры (стандартный входной поток), а из заранее подготовленного файла (перенаправление ввода);

• передавать сообщения, выводимые одной программой, в качестве входных данных для другой программы (конвейеризация или композиция команд).

**2. КОМАНДЫ РАБОТЫ С СЕТЬЮ**

Краткое описание и примеры использования сетевых утилит командной строки Windows:

Большинство рассматриваемых сетевых утилит для полноценной работы требуют наличия административных привилегий. Для операционных систем семейства Windows 2000/XP достаточно того, чтобы пользователь являлся членом группы администраторов, для ОС Windows Vista и более поздних, требуется запуск команды от имени Администратора.

Интерпретатор командной строки cmd.exe может быть запущен несколькими способами. В среде операционных систем Widows Vista/Windows 7,8,10,11 cmd.exe должен быть запущен с использованием пункта контекстного меню, вызываемого правой кнопкой мышки - "Запустить от имени Администратора". Можно также в свойствах ярлыка CMD, установить флажок ”Запускать от имени Администратора”, использовать меню, вызываемое по комбинации клавиш Win+X - Командная строка (Администратор) или запуск из приложений уже выполняющихся в контексте учетной записи Администратора.

В списке представлены сетевые утилиты командной строки для получения информации о сетевых настройках, выполнения операций по конфигурированию и диагностике сети.

В описании команд используется

< текст > - текст в угловых скобках. Обязательный параметр

[ текст ] - текст в квадратных скобках. Необязательный параметр.

( текст ) - текст в круглых скобках. Необходимо выбрать один из параметров.

Вертикальная черта | - разделитель для взаимоисключающих параметров. Нужно выбрать один из них.

Многоточие ... - возможно повторение пара

Далее приведены команды работы с сетью. Более подробную информацию можно узнать по ссылке: [**https://ab57.ru/netcmd.html#id04**](https://ab57.ru/netcmd.html#id04)

[ARP](http://ab57.ru/netcmd.html#id01)

[IPCONFIG](http://ab57.ru/netcmd.html#id02)  
[GETMAC](http://ab57.ru/netcmd.html#id03)  
[NBTSTAT](http://ab57.ru/netcmd.html#id04)  
[NETSH](http://ab57.ru/netcmd.html#id05)  
[NETSTAT](http://ab57.ru/netcmd.html#id07)  
[NET](http://ab57.ru/netcmd.html#id08)  
[NSLOOKUP](http://ab57.ru/netcmd.html#id09)  
[PATHPING](http://ab57.ru/netcmd.html#id10)  
[PING](http://ab57.ru/netcmd.html#id11)  
[ROUTE](http://ab57.ru/netcmd.html#id12)  
[TELNET](http://ab57.ru/netcmd.html#id13)  
[TRACERT](http://ab57.ru/netcmd.html#id14)

Рассмотри некоторые основные команды работы с сетью.

**Утилита IPCONFIG .**

Утилита командной строки ipconfig присутствует во всех версиях Windows. Некоторые параметры командной строки не поддерживаются в версиях предшествующих Windows Vista/Windows 7.

Команда IPCONFIG используется для отображения текущих настроек протокола TCP/IP и для обновления некоторых параметров, задаваемых при автоматическом конфигурировании сетевых интерфейсов при использовании протокола Dynamic Host Configuration Protocol (DHCP).

**Синтаксис:**

*ipconfig [/allcompartments] [/all] [/renew[Adapter]] [/release[Adapter]] [/renew6[Adapter]] [/release6[Adapter]] [/flushdns] [/displaydns] [/registerdns] [/showclassidAdapter] [/setclassidAdapter [ClassID]]*

**Параметры:**

**/?** - отобразить справку по использованию IPCONFIG

**/all** - отобразить полную конфигурацию настроек TCP/IP для всех сетевых адаптеров. Отображение выполняется как для физических интерфейсов, так и для логических, как например, dialup или VPN подключения.

**/allcompartments** - вывести полную информацию о конфигурации TCP/IP для всех секций.

**/displaydns** - отобразить содержимое кэш службы DNS - клиент.

**/flushdns** - сбросить содержимое кэш службы DNS - клиент.

**/registerdns** - инициировать регистрацию записей ресурсов DNS для всех адаптеров данного компьютера. Этот параметр используется для изменения настроек DNS сетевых подключений без перезагрузки компьютера.

**/release[Adapter]** - используется для отмены автоматических настроек сетевого адаптера, полученных от сервера DHCP. Если имя адаптера не указано, то отмена настроек выполняется для всех адаптеров.

**/release6[Adapter]** - отмена автоматических настроек для протокола IPv6

**/renew[Adapter]** - обновить конфигурацию для сетевого адаптера настроенного на получение настроек от сервера DHCP. Если имя адаптера не указано, то обновление выполняется для всех адаптеров.

**/renew6[Adapter]** - как и в предыдущем случае, но для протокола IPv6

Изменение сетевых настроек с помощью команды IPCONFIG, в основном, применимо к тем сетевым адаптерам, которые настроены на автоматическое конфигурирование с использованием службы динамической настройки основных параметров на сетевом уровне DHCP (Dynamic Host Configuration Protocol) или службы автоматической настройки приватных IP - адресов APIPA (Automatic Private IP Addressing).

Если в параметрах командной строки IPCONFIG используется имя адаптера, содержащее пробелы, то оно должно заключаться в двойные кавычки. Если имя содержит символы русского алфавита, то оно должно быть представлено в DOS-кодировке.

Для имен адаптеров применимо использование символа \* в качестве шаблона:

\* - любое имя

Локальн\* - имя адаптера начинается с " Локальн "

\* сети \* - имя адаптера содержит строку " сети "

Примеры использования:

**ipconfig** - отобразить базовые сетевые настройки для всех сетевых адаптеров.

**ipconfig /all** - отобразить все сетевые настройки для всех сетевых адаптеров.

**ipconfig /renew** "Подключение по локальной сети 2" - обновить сетевые настройки, полученные от DHCP - сервера только для адаптера с именем " Подключение по локальной сети 2"

**ipconfig /dysplaydns** - вывести на экран содержимое кэш службы разрешения имен DNS

ipconfig /showclassid "Подключение по локальной сети" - отобразить все допустимые для этого адаптера идентификаторы классов DHCP.

**Утилита PING.EXE**

PING.EXE - это, наверно, наиболее часто используемая сетевая утилита командной строки. Существует во всех версиях всех операционных систем с поддержкой сети и является простым и удобным средством опроса узла по имени или его IP-адресу.

Для обмена служебной и диагностической информацией в сети используется специальный протокол управляющих сообщений ICMP (Internet Control Message Protocol). Команда ping позволяет выполнить отправку управляющего сообщения типа Echo Request (тип равен 8 и указывается в заголовке сообщения) адресуемому узлу и интерпретировать полученный от него ответ в удобном для анализа виде. В поле данных отправляемого icmp-пакета обычно содержатся символы английского алфавита. В ответ на такой запрос, опрашиваемый узел дожжен отправить icmp-пакет с теми же данными, которые были приняты, и типом сообщения Echo Reply (код типа в заголовке равен 0) . Если при обмене icmp-сообщениями возникает какая-либо проблема, то утилита ping выведет информацию для ее диагностики.

Формат командной строки:

*ping [-t] [-a] [-n число] [-l размер] [-f] [-i TTL] [-v TOS] [-r число] [-s число] [[-j списокУзлов] | [-k списокУзлов]] [-w таймаут] конечное Имя*

Параметры:

**-t** - Непрерывная отправка пакетов. Для завершения и вывода статистики используются комбинации клавиш + (вывод статистики), и + (вывод статистики и завершение).

**-a** - Определение адресов по именам узлов.

**-n** число - Число отправляемых эхо-запросов.

**-l** размер - Размер поля данных в байтах отправляемого запроса.

**-f** - Установка флага, запрещающего фрагментацию пакета.

**-i** TTL - Задание срока жизни пакета (поле "Time To Live").

**-v TOS** - Задание типа службы (поле "Type Of Service").

**-r** число - Запись маршрута для указанного числа переходов.

**-s** число - Штамп времени для указанного числа переходов.

**-j** списокУзлов - Свободный выбор маршрута по списку узлов.

**-k** списокУзлов - Жесткий выбор маршрута по списку узлов.

**-w** таймаут - Максимальное время ожидания каждого ответа в миллисекундах.

Примеры использования:

**ping bsuir.by** - выполнить опрос узла с символьным адресом bsuir.by

**ping 8.8.8.8** - выполнить опрос узла с IP-адресом 8.8.8.8 с параметрами по умолчанию.

**ping -t yandex.ru** - выполнять ping до нажатия комбинации CTRL-C, При нажатии CTRL-Break - выдается статистика и опрос узла продолжается

**ping -n 1000 -l 500 192.168.1.1** - выполнить ping 1000 раз с использованием сообщений, длиной 500 байт.

**ping -a -n 1 -r 9 -w 1000 yandex.ru** - выполнить ping 1 раз (ключ -n 1), определять адрес по имени (ключ -a), выдавать маршрут для первых 9 переходов (-r 9), ожидать ответ 1 секунду (1000мсек)

Использование ключа -r позволяет получить трассировку маршрута, аналогичную получаемой с помощью команды tracert, но число промежуточных узлов не может превышать 9 .

**Утилита TRACERT.EXE**

Не смотря на появление утилиты PATHPIG, классическая утилита трассировки маршрута до заданного узла TRACERT , по-прежнему остается наиболее часто используемым инструментом сетевой диагностики. Утилита позволяет получить цепочку узлов, через которые проходит IP-пакет, адресованный конечному узлу. В основе трассировки заложен метод анализа ответов при последовательной отправке ICMP-пакетов на указанный адрес с увеличивающимся на 1 полем TTL. ("Время жизни" - Time To Live). На самом деле это поле не имеет отношения к времени, а является счетчиком числа возможных переходов при передаче маршрутизируемого пакета. Каждый маршрутизатор, получив пакет, вычитает из этого поля 1 и проверяет значение счетчика TTL. Если значение стало равным нулю, такой пакет отбрасывается и отправителю посылается ICMP-сообщение о превышении времени жизни ("Time Exceeded" - значение 11 в заголовке ICMP). Если бы не было предусмотрено включение поля TTL в IP пакеты, то при ошибках в маршрутах, могла бы возникнуть ситуация, когда пакет будет вечно циркулировать в сети, пересылаемый маршрутизаторами по кругу. При выполнении команды tracert.exe сначала выполняется отправка ICMP пакета с полем TTL равным 1 и первый в цепочке маршрутизатор (обычно это основной шлюз из настроек сетевого подключения) вычтя единицу из TTL получает его нулевое значение и сообщает о превышении времени жизни. Эта последовательность повторяется трижды, поэтому в строке результата, формируемой tracert.exe, после номера перехода отображаются три значения времени отклика:

1 1 ms <1 <1 192.168.1.1

1 - номер перехода (1 - первый маршрутизатор)

1 ms <1 <1 - время его ответа для 3-х попыток (1ms и 2 ответа менее чем 1 ms)

192.168.1.1 - его адрес (или имя)

Затем процедура повторяется, но TTL устанавливается равным 2 - первый маршрутизатор его уменьшит до 1 и отправит следующему в цепочке, который после вычитания 1 обнулит TTL и сообщит о превышении времени жизни. И так далее, пока не будет достигнут заданный узел, имя или адрес которого заданы в качестве параметра командной строки, например , tracert yandex.ru , или до обнаружения неисправности, не позволяющей доставить пакет узлу yandex.ru.

Пример результатов выполнения tracert google.com

**tracert google.com** - трассировка маршрута к узлу google.com

Результат:

Трассировка маршрута к google.com [74.125.45.100] с максимальным числом прыжков 30:

1 1 ms <1 <1 192.168.1.1

2 498 ms 444 ms 302 ms ppp83-237-220-1.pppoe.mtu-net.ru [83.237.220.1]

3 \* \* \* .

4 282 ms \* \* a197-crs-1-be1-53.msk.stream-internet.net [212.188.1.113]

5 518 ms 344 ms 382 ms ss-crs-1-be5.msk.stream-internet.net [195.34.59.105]

6 462 ms 440 ms 335 ms m9-cr01-po3.msk.stream-internet.net [195.34.53.85]

7 323 ms 389 ms 339 ms bor-cr01-po4.spb.stream-internet.net [195.34.53.126]

8 475 ms 302 ms 420 ms anc-cr01-po3.ff.stream-internet.net [195.34.53.102]

9 334 ms 408 ms 348 ms 74.125.50.57

10 451 ms 368 ms 524 ms 209.85.255.178

11 329 ms 542 ms 451 ms 209.85.250.140

12 616 ms 480 ms 645 ms 209.85.248.81

13 656 ms 549 ms 422 ms 216.239.43.192

14 378 ms 560 ms 534 ms 216.239.43.113

15 511 ms 566 ms 546 ms 209.85.251.9

16 543 ms 682 ms 523 ms 72.14.232.213

17 468 ms 557 ms 486 ms 209.85.253.141

18 593 ms 589 ms 575 ms yx-in-f100.google.com [74.125.45.100]

Трассировка завершена.

В результатах трассировки могут присутствовать строки, где вместо адреса узла отображается звездочка (узел номер 3 в примере). Это не обязательно является признаком неисправности маршрутизатора, и чаще всего, говорит о том, что настройки данного узла запрещают ICMP-протокол из соображений безопасности или уменьшения нагрузки на канал .

Утилита PATHPING.EXE

Команда PATHPING выполняет трассировку маршрута к конечному узлу аналогично команде TRACERT , но дополнительно, выполняет отправку ICMP-эхо запросов на промежуточные узлы маршрута для сбора информации о задержках и потерях пакетов на каждом из них.

При запуске PATHPING без параметров, отображается краткая справка:

*pathping [-g Список] [-h Число\_прыжков] [-i Адрес] [-n] [-p Пауза] [-q Число\_запросов] [-w Таймаут] [-P] [-R] [-T] [-4] [-6] узел*

Параметры:

**-g** Список При прохождении по элементам списка узлов игнорировать предыдущий маршрут. Максимальное число адресов в списке равно 9 . Элементы списка помещаются в специальное поле заголовка отправляемых ICMP-пакетов.

**-h** Число\_прыжков - Максимальное число прыжков при поиске узла. Значение по умолчанию - 30

**-i** Адрес - Использовать указанный адрес источника в отправляемых ICMP-пакетах.

**-n** - Не разрешать адреса в имена узлов.

**-p** Пауза - Пауза между отправками (мсек) пакетов. Значение по умолчанию - 250.

**-q** Число\_запросов Число запросов для каждого узла. По умолчанию - 100

**-w** Таймаут - Время ожидания каждого ответа (мсек). Значение по умолчанию - 3000

**-R** - Тестировать возможность использования RSVP ( Reservation Protocol, протокола настройки резервирования ресурсов), который позволяет динамически выделять ресурсы для различных видов трафика.

**-T** - Тестировать на возможность использования QoS (Quality of Service - качество обслуживания) - системы обслуживания пакетов разного содержания с учетом их приоритетов доставки получателю.

**-4** - Принудительно использовать IPv4.

**-6** - Принудительно использовать IPv6.

Практически, PATHPING, запущенная на выполнение с параметрами по умолчанию, выполняет те же действия, что и команда TRACERT плюс команды PING для каждого промежуточного узла с указанием числа эхо-запросов, равным 100 (ping -n 100 . . . )

Пример результатов выполнения команды **pathping yandex.ru** :

Трассировка маршрута к yandex.ru [77.88.21.11] с максимальным числом прыжков 30:

1 192.168.1.1

2 180.84.250.11

3 180.84.250.53

4 80.184.112.25

5 msk-ix-m9.yandex.net [193.232.244.93]

6 l3-s900-dante.yandex.net [213.180.213.70]

7 s600-s900.yandex.net [213.180.213.54]

8 yandex.ru [77.88.21.11]

Подсчет статистики за: 200 сек. . . .

Исходный узел Маршрутный узел

Прыжок RTT Утер./Отпр. % Утер./Отпр. % Адрес

1 1мс 0/ 100 = 0% 0/ 100 = 0% 192.168.1.1

0/ 100 = 0% |

2 5мс 0/ 100 = 0% 0/ 100 = 0% 180.84.250.11

0/ 100 = 0% |

3 11мс 0/ 100 = 0% 3/ 100 = 3% 180.84.250.53

8/ 100 = 8% |

4 4мс 0/ 100 = 0% 0/ 100 = 0% 80.184.112.25

0/ 100 = 0% |

5 8мс 0/ 100 = 0% 0/ 100 = 0% msk-ix-m9.yandex.net [193.232.244.93]

0/ 100 = 0% |

6 12мс 0/ 100 = 0% 0/ 100 = 0% l3-s900-dante.yandex.net [213.180.213.70]

0/ 100 = 0% |

7 5мс 0/ 100 = 0% 0/ 100 = 0% s600-s900.yandex.net [213.180.213.54]

0/ 100 = 0% |

8 2мс 0/ 100 = 0% 0/ 100 = 0% yandex.ru [77.88.21.11]

В приведенном примере красным цветом выделен проблемный участок маршрута к конечному узлу с потерей 8% пакетов.

При интерпретации результатов выполнения pathping нужно учитывать тот факт, что некоторые маршрутизаторы могут быть настроены на блокировку icmp-трафика, что не позволяет правильно отработать трассировку, и получить по ним статистические данные.

**Утилита ARP.EXE**

Утилита командной строки ARP.EXE присутствует во всех версиях Windows и имеет один и тот же синтаксис.

Команда ARP позволяет просматривать и изменять записи в кэш ARP (Address Resolution Protocol - протокол разрешения адресов), который представляет собой таблицу соответствия IP-адресов аппаратным адресам сетевых устройств. Аппаратный адрес - это уникальный, присвоенный при изготовлении, 6-байтный адрес сетевого устройства, например сетевой карты. Этот адрес также часто называют MAC-адресом (Media Access Control - управление доступом к среде) или Ethernet-адресом. В сетях Ethernet передаваемые и принимаемые данные всегда содержат MAC-адрес источника (Source MAC) и MAC-адрес приемника (Destination MAC). Два старших бита MAC-адреса используются для идентификации типа адреса:

- первый бит - одиночный (0) или групповой (1) адрес.

- второй бит - признак универсального (0) или локально администрируемого адреса.

Следующие 22 бита адреса содержат специальный код производителя MFG или OUI - универсальный код организации.

Другими словами, любое сетевое устройство имеет аппаратный адрес, состоящий из 2- х частей. Старшую часть MAC - адреса, централизованно выделяемую по лицензии каждому производителю сетевого оборудования. Например, 00:E0:4C - для сетевых устройств REALTEK SEMICONDUCTOR CORP. Крупным производителям сетевого оборудования обычно принадлежит несколько диапазонов OUI .

И младшую часть MAC-адреса, которая формируется при производстве оборудования, и уникальна для каждого экземпляра устройства.

Отображение IP-адресов (формируемых программным путем), в аппаратные адреса, выполняется с помощью следующих действий:

- в сеть отправляется широковещательный запрос (ARP-request), принимаемый всеми сетевыми устройствами. Он содержит IP и Ethernet адреса отправителя, а также, целевой IP-адрес, для которого выполняется определение MAC-адреса.

- каждое устройство, принявшее запрос проверяет соответствие целевого IP-адреса, указанного в запросе, своему собственному IP-адресу. При совпадении, отправителю передается ARP-ответ (ARP-Reply), в котором содержатся IP и MAC адреса ответившего узла. Кадр с ARP-ответом содержит IP и MAC адреса как отправителя, так и получателя-составителя запроса.

- информация, полученная в ARP-ответе, заносится в ARP-кэш и может использоваться для обмена данными по IP-протоколу для данного узла. ARP-кэш представляет собой таблицу в оперативной памяти, каждая запись в которой содержит IP, MAC и возраст их разрешения. Возраст записи учитывается для того, чтобы обеспечить возможность повторного выполнения процедуры ARP при каком либо изменении соответствия адресов.

Синтаксис ARP.EXE:

*arp[-a [InetAddr] [-NIfaceAddr]] [-g [InetAddr] [-NIfaceAddr]] [-dInetAddr [IfaceAddr]] [-sInetAddr EtherAddr [IfaceAddr]]*

**-a[ InetAddr] [ -NIfaceAddr]** - ключ -a - отображает текущую таблицу ARP для всех интерфейсов. Для отображения записи конкретного IP-адреса используется ключ -a с параметром InetAdd , в качестве которого указывается IP-адрес. Если узел, отправляющий ARP-запрос имеет несколько сетевых интерфейсов, то для отображения таблицы ARP нужного интерфейса, можно использовать ключ -N с параметром IfaceAddr, в качестве которого используется IP-адрес интерфейса.

**-g[ InetAddr] [ -NIfaceAddr]** ключ -g идентичен ключу -a.

**-d InetAddr[ IfaceAddr]** - используется для удаления записей из ARP-кэш. Возможно удаление по выбранному IP или полная очистка ARP кэш. Для удаления всех записей, вместо адреса используется символ \* Если имеется несколько сетевых интерфейсов, то очистку можно выполнить для одного из них, указав в поле IfaceAddr его IP .

**-s InetAddr EtherAddr [ IfaceAddr]** - используется для добавления статических записей в таблицу ARP. Статические записи хранятся в ARP-кэш постоянно. Обычно, добавление статических записей используется для сетевых устройств, не поддерживающих протокол ARP или не имеющих возможности ответить на ARP- запрос.

**/?** - получение справки по использованию arp.exe. Аналогично - запуск arp.exe без параметров.

**Примеры использования ARP:**

**arp -a** - отобразить все записи таблицы ARP.

**arp -a 192.168.0.9)**- отобразить запись, соответствующую IP-адресу 192.168.0.9

**arp -a** 192.168.1.158 -N 192.168.1.1 - отобразить таблицу ARP для адреса 192.168.1.158((здесь задается IP адрес из ARP - таблицы) на сетевом интерфейсе 192.168.1.1(здесь IP - адрес своего компьютера)

**arp -a -N** 10.164.250.148 - отобразить все записи таблицы ARP на сетевом интерфейсе 10.164.250.148 .

**arp -s** 192.168.0.1 00-22-15-15-88-15 - добавить в таблицу ARP статическую запись, задающую соответствие IP - адреса 192.168.0.1 и MAC-адреса 00-22-15-15-88-15

**arp -s** 192.168.0.1 00-22-15-15-88-15 192.168.0.56 - то же самое, что и в предыдущем случае, но с указанием сетевого интерфейса, для которого выполняется добавление статической записи.

**arp -d** 192.168.1.1 192.168.1.56 удаление записи из таблицы ARP для IP-адреса 192.168.1.1 на сетевом интерфейсе 192.168.1.56

**arp -d \*** - полная очистка таблицы ARP. Аналогично - arp -d без параметров. Если имеется несколько сетевых интерфейсов, то очистка может быть выполнена только для одного из них - arp -d \* 192.168.0.56.

Некоторые замечания по практическому использованию команды ARP:

- разрешение адресов по протоколу ARP выполняется только при операциях передачи данных по протоколу IP .

- время жизни записей в таблице ARP ограничено, поэтому, перед просмотром ее содержимого для конкретного адреса нужно выполнить ping на этот адрес.

- если ответ на ping не приходит, а запись для данного IP-адреса присутствует в таблице ARP, то этот факт можно интерпретировать как блокировку ICMP-пакетов брандмауэром пингуемого узла.

- невозможность подключения к удаленному узлу по протоколам TCP или UDP при наличии записей в таблице ARP для целевого IP, может служить признаком отсутствия служб обрабатывающих входящие подключения, или их блокировки брандмауэром (закрытые порты).

- ARP протокол работает в пределах локального сегмента сети. Поэтому, если выполнить ping на внешний узел ( например ping yandex.ru ), то в таблице ARP будет присутствовать запись для IP - адреса маршрутизатора (шлюза), через который выполняется отправка пакета во внешнюю сеть.

При использовании команды ARP для отображения таблицы, не помещающейся на экране, удобно пользоваться командой постраничного вывода more или перенаправлением стандартного вывода в файл:

arp -a | more

arp -a > C:\myarp.txt

**Утилита ROUTE.EXE**

Утилита ROUTE.EXE используется для просмотра и модификации таблицы маршрутов на локальном компьютере. При запуске без параметров, на экран выводится подсказка по использованию route:

*route [-f] [-p] [команда [конечная\_точка] [mask маска\_сети] [шлюз] [metric метрика]] [if интерфейс]]*

**-f** - используется для сброса таблицы маршрутизации. При выполнении команды route -f из таблицы удаляются все маршруты, которые не относятся к петлевому интерфейсу (IP 127.0.0.1 маска -255.0.0.0), не являются маршрутами для многоадресной (multicast) рассылки (IP 224.0.0.1 маска 255.0.0.0) и не являются узловыми маршрутами (маска равна 255.255.255.255) .

**-p** - используется для добавления в таблицу постоянного маршрута. Если маршрут добавлен без использования параметра -p то он сохраняется только до перезагрузки системы (до перезапуска сетевого системного программного обеспечения). Если же, при добавлении маршрута использовался данный параметр, то информация о маршруте записывается в реестр Windows (раздел HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PersistentRoutes ) и будет использоваться постоянно при активации сетевых интерфейсов.

**команда** - козможно использование команд **add** - добавление маршрута, **change** - изменение существующего маршрута, **delete** - удаление маршрута или маршрутов, print - отображение текущей таблицы маршрутов

**конечная\_точка** - IP-адрес - **адрес сети** назначения или адрес 0.0.0.0 для шлюза по умолчанию.

**mask маска\_сети** - маска сети назначения.

**шлюз - IP-адрес шлюза**, через который будет выполняться отправка пакета для достижения конечной точки.

**metric число** - значение метрики (1-9999). Метрика представляет собой числовое значение, позволяющее оптимизировать доставку пакета получателю, если конечная точка маршрута может быть достижима по нескольким разным маршрутам. Чем меньше значение метрики, тем выше приоритет маршрута.

**if интерфейс** - идентификатор сетевого интерфейса. Может задаваться в виде десятичного или шестнадцатеричного числа. Посмотреть идентификаторы можно с помщью команды **route print**

Примеры :

**route print -** отобразить текущую таблицу маршрутов

**route print 192.\*** - отобразить таблицу маршрутов только для адресов, начинающихся с 192.

**route add** 0.0.0.0 mask 0.0.0.0 192.168.1.1 - установить в качестве шлюза по умолчанию (основного шлюза) адрес 192.168.1.1

route -p add 10.0.0.0 mask 255.0.0.0 10.0.0.1 - добавить маршрут для подсети 10.0.0.0/255.0.0.0 и запомнить его в реестре . Постоянный статический маршрут.

**route delete** 10.0.0.0 mask 255.0.0.0 - удалить маршрут для подсети 10.0.0.0/255.0.0.0 .

route add 10.10.10.10 192.168.1.158 - добавить маршрут для узла с IP-адресом 10.10.10.10 . Если маска в команде не задана, то подразумевается ее значение равное 255.255.255.255 , т.е конечная точка назначения является одиночным IP-адресом узла.

**route delete 10.10.10.10** - удалить маршрут созданный предыдущей командой

route change 10.0.0.0 mask 255.0.0.0 10.10.10.1 - изменить адрес перехода для существующего маршрута к сети 10.0.0.0/255.0.0.0 на значение 10.10.10.1

route -f - очистить таблицу маршрутов. После перезагрузки системы, или при перезапуске сетевых подключений таблица маршрутов будет восстановлена исходя из текущей сетевой конфигурации компьютера.

**Утилита NET.EXE**

Утилита NET.EXE существует во всех версиях Windows. Позволяет подключать и отключать сетевые диски, запускать и останавливать системные службы, добавлять и удалять пользователей, управлять совместно используемыми ресурсами, устанавливать системное время, отображать статистические и справочные данные об использовании ресурсов и многое другое.

Выполнение команды net без параметров вызывает краткую справку со списком возможных уровней использования, запуск с параметром help позволяет получить более подробную информацию об использовании net.exe:

Синтаксис данной команды:

NET HELP

имя\_команды

-или-

NET имя\_команды /HELP

Можно использовать следующие имена команд:

NET ACCOUNTS NET HELP NET SHARE

NET COMPUTER NET HELPMSG NET START

NET CONFIG NET LOCALGROUP NET STATISTICS

NET CONFIG SERVER NET NAME NET STOP

NET CONFIG WORKSTATION NET PAUSE NET TIME

NET CONTINUE NET PRINT NET USE

NET FILE NET SEND NET USER

NET GROUP NET SESSION NET VIEW

NET HELP SERVICES - эта команда выводит список служб, которые можно запустить.

NET HELP SYNTAX - эта команда выводит объяснения синтаксических правил, используемых при описании команд в Справке.

NET HELP имя\_команды | MORE - просмотр справки по одному экрану за раз.

При описании команды NET используются следующие синтаксические соглашения:

- Заглавными буквами набраны слова, которые должны быть введены без изменений, строчными буквами набраны имена и параметры, которые могут изменяться, например, имена файлов.

- Необязательные параметры заключены в квадратные скобки - [ ].

- Списки допустимых параметров заключены в фигурные скобки - { }. Необходимо использовать один из элементов такого списка.

- Символ | (вертикальная черта) используется в качестве разделителя элементов списка. - При вводе в командной строке можно использовать русские названия служб, при этом они должны быть заключены в кавычки и не допускается изменение прописных букв на строчные и наоборот. Например, команда

NET START "Обозреватель сети"

запускает службу обозревателя сети.

Подробную справку по использованию нужной команды, например use , можно получить несколькими способами:

net use ? - справка о синтаксисе команды

net use /help - подробная справка по использованию команды с описанием используемых ключей.

net help use - аналогично предыдущей форме вызова справки.

net help use | more - отобразить справку в постраничном режиме выдачи на экран. Удобно пользоваться в тех случаях, когда тест не помещается на экране. Нажатие Enter перемещает текст на одну строку, нажатие пробела - на один экран.

net help use > C:\helpuse.txt - создать текстовый файл справки C:\helpuse.txt

• Работа с сетевыми дисками

net use - отобразить список сетевых дисков, подключенных на данном компьютере.

Состояние Локальный Удаленный Сеть

-------------------------------------------------------------------------------

Отсоединен X: \\SERVER\movies Microsoft Windows Network

OK Y: \\SERVER\shares Microsoft Windows Network

В колонке "Локальный" отображается буква сетевого диска, а в колонке "Удаленный" - имя удаленного сетевого ресурса в формате UNC

UNC - это Общее соглашение об именах (Uniform Naming Convention) или универсальное соглашение об именовании (universal naming convention), соглашение об именовании файлов и других ресурсов, дающее определение местоположения ресурса .

Имя, соответствующее UNC - полное имя ресурса в сети, включающее имя сервера и имя совместно используемого (разделяемого, сетевого ) ресурса (принтера, каталога или файла). Синтаксис UNC-пути к каталогу или файлу следующий:

\\Сервер\СетевойКаталог[\ОтносительныйПуть]

Сервер - сетевое имя компьютера, СетевойКаталог - это сетевое имя общего каталога на этом компьютере, а необязательный ОтносительныйПуть - путь к каталогу или файлу из общего каталога.

СетевойКаталог не обязательно называется так же, как ассоциированный с ним каталог на сервере, имя даётся в ходе открытия общего доступа к каталогу в файловой системе компьютера

• Работа с файлами и каталогами

NET SHARE - эта команда позволяет выделить ресурсы системы для сетевого доступа . При запуске без других параметров, выводит информацию обо всех ресурсах данного компьютера, которые могут быть совместно использованы . Для каждого ресурса выводится имя устройства или путь и соответствующий комментарий.

net share - получить список разделяемых в локальной сети ресурсов данного компьютера. Пример списка:

Общее имя Ресурс Заметки

------------------------------------------------------------------------------

G$ G:\ Стандартный общий ресурс

E$ E:\ Стандартный общий ресурс

IPC$ Удаленный IPC

ADMIN$ C:\WINDOWS Удаленный Admin

INSTALL C:\INSTALL Дистрибутивы и обновления

net share INSTALL - получить информацию о разделяемом ресурсе с именем INSTALL .

Имя общего ресурса INSTALL

Путь C:\INSTALL

Заметки Дистрибутивы и обновления

Макс. число пользователей Не ограничен

Пользователи Administrator

Кэширование Вручную

Для добавления нового разделяемого по сети ресурса используется параметр **/ADD**

net share TEMP="C:\Documents And Settings\LocalSettings\games" - добавить новый разделяемый каталог под именем TEMP

net share TEMP="C:\Documents And Settings\LocalSettings\games" /users:5 - добавить новый разделяемый каталог под именем TEMP с максимальным числом обновременно подключающихся пользователей равным 5 .

Для удаления существующего разделяемого ресурса используется параметр /DELETE:

net share TEMP /DELETE - удалить разделяемый ресурс под именем TEMP

Удаление выполняется только для имени разделяемого ресурса и не затрагивает каталог локального диска, связанный с данным именем.

Для работы с файлами, открытыми по сети на данном компьютере, используется команда NET FILE . По каждому открытому ресурсу выводится идентификационный номер, путь файла, имя пользователя, которым используется файл, и количество блокировок при совместном использовании. Кроме того, команда NET FILE позволяет закрыть совместно используемый файл и снять блокировки .

net file - получить список открытых по сети файлов (если есть).

net file 4050 /close - принудительно закрыть файл, идентификатор которого равен 4050

Для получения списка компьютеров рабочей группы или домена с разделяемыми ресурсами используется команда

net view - отобразить список компьютеров в сетевом окружении.

net view | more - отобразить список компьютеров в постраничном режиме вывода на экран.

net view > C:\computers.txt - отобразить список компьютеров c записью результатов в текстовый файл.

Синтаксис данной команды:

NET VIEW [\\имя\_компьютера [/CACHE] | /DOMAIN[:имя\_домена]]

NET VIEW /NETWORK:NW [\\имя\_компьютера]

net view \\server - отобразить список сетевых ресурсов компьютера server

net view /DOMAIN:mydomain - отобразить список компьютеров с разделяемыми ресурсами в домене mydomain Если имя домена не указано, то выводится список всех доступных компьютеров локальной сети.

net view /NETWORK:NW - отобразить список серверов Novell Netware, доступных в данной локальной сети.

net view /NETWORK:NW \\NWServer - отобразить списков сетевых ресурсов сервера Netware с именем NWServer .

Утилита NETSTAT.EXE

Утилита netstat.exe присутствует во всех версиях Windows, однако, существуют некоторые отличия используемых параметров командной строки и результатов ее выполнения, в зависимости от операционной системы. Используется для отображения TCP и UDP -соединений, слушаемых портов, таблицы маршрутизации, статистических данных для различных протоколов.

Синтаксис:

*netstat[-a] [-e] [-n] [-o] [-pProtocol] [-r] [-s] [Interval]*

**-a** - отображение всех активных соединений по протоколам TCP и UDP, а также, списка портов, которые ожидают входящие соединения (слушаемых портов).

**-b** - отображение всех активных соединений по протоколам TCP и UDP, а также, списка портов, которые ожидают входящие соединения (слушаемых портов) с информацией об именах исполняемых файлов.

**-e** - отображение статистики Ethernet в виде счетчиков принятых и отправленных байт и пакетов.

**-n** - отображение номеров портов в виде десятичных чисел.

**-o** - отображение соединений, включая идентификатор процесса (PID) для каждого соединения.

**-p** Protocol - отображение соединений для заданного протокола. Протокол может принимать значения tcp, udp, tcpv6, udpv6 . При использовании совместно с параметром -s в качестве протокола можно задавать tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6, ipv6.

**-s** - отображение статистических данных по протоколам TCP, UDP, ICMP, IP , TCP over IPv6, UDP over IPv6, ICMPv6, и IPv6 . Если задан параметр -p , то статистика будет отбражатися только для выбранных протоколов.

**-r** - отображение таблицы маршрутов. Эквивалент команды **route print**

**-Interval** - интервал обновления отображаемой информации в секундах.

**-v** - отображать подробную информацию.

**/?** - отобразить справку по использованию netstat

При использовании утилиты netstat.exe удобно пользоваться командами постраничного вывода (more), перенаправления стандартного вывода в файл ( > ) и поиска текста в результатах (find).

**netstat -a | more** - отобразить все соединения в постраничном режиме вывода на экран.

netstat -a > C:\netstatall.txt - отобразить все соединения с записью результатов в файл C:\netstatall.txt.

**netstat -a | find /I "LISTENING"** - отобразить все соединения со статусом LISTENING. Ключ /I в команде find указывает, что при поиске текста не нужно учитывать регистр символов.

netstat -a | find /I "listening" > C:\listening.txt - отобразить все соединения со статусом LISTENING с записью результатов в файл C:\listening.txt.

Пример отображаемой информации:

Активные подключения

Имя Локальный адрес Внешний адрес Состояние

TCP 0.0.0.0:80 0.0.0.0:0 LISTENING

[ httpd.exe]

TCP 0.0.0.0:445 0.0.0.0:0 LISTENING

Не удается получить сведения о владельце

TCP 0.0.0.0:5800 0.0.0.0:0 LISTENING

[WinVNC.exe]

TCP 127.0.0.1:50197 127.0.0.1:50198 ESTABLISHED

[firefox.exe]

UDP 192.168.0.107:1900 \*:\*

SSDPSRV [svchost.exe]

. . .

Локальный адрес - локальный IP-адрес участвующий в соединении или связанный со службой, ожидающей входящие соединения (слушающей порт). Если в качестве адреса отображается 0.0.0.0 , то это означает - "любой адрес", т.е в соединении могут использоваться все IP-адреса существующие на данном компьютере. Адрес 127.0.0.1 - это петлевой интерфейс, используемый в качестве средства IP протокола для взаимодействия между процессами без реальной передачи данных.

Внешний адрес Внешний IP-адрес, участвующий в создании соединения.

Состояние - состояние соединения. Состояние Listening говорит о том, что строка состояния отображает информацию о сетевой службе, которая ожидает входящие соединения по соответствующему протоколу на адрес и порт, отображаемые в колонке "Локальный адрес ". Состояние ESTABLISHED указывает на активное соединение. В колонке "Состояние" для соединений по протоколу TCP может отображаться текущий этап TCP-сессии определяемый по обработке значений флагов в заголовке TCP - пакета (Syn, Ask, Fin ... ). Возможные состояния:

CLOSE\_WAIT - ожидание закрытия соединения.

CLOSED - соединение закрыто.

ESTABLISHED - соединение установлено.

LISTENING - ожидается соединение (слушается порт)

TIME\_WAIT - превышение времени ответа.

Имя программного модуля, связанного с данным соединением отображается, если задан параметр -b в командной строке при запуске netstat.exe.

**Примеры использования :**

**netstat -a** получить список слушаемых портов и связанных с ними программ:

**•**  получить статистические данные:

**netstat -e** - получить статистические данные для Ethernet. Отображается суммарные значения принятых и полученных байт для всех сетевых адаптеров.

**netstat -e -s** - дополнительно к статистике Ethernet, отображается статистика для протоколов IP , ICMP , TCP , UDP

**Утилита NSLOOKUP**

Утилита NSLOOKUP присутствует в операционных системах Windows, начиная с Windows NT , и предназначена для формирования запросов к серверам DNS из командной строки. Фактически, утилита является аналогом службы DNS-клиент и позволяет диагностировать проблемы с разрешением имен в системе DNS. По умолчанию, все запросы отправляются на DNS-сервер, адрес которого задан настройками сетевого подключения. В терминах утилиты такой сервер является сервером по умолчанию (default server). Команда ipconfig /all позволяет получить информацию о настройках протокола IP и, в том числе, о серверах DNS, используемых в системе.

При запуске nslookup без параметров, утилита переходит в интерактивный режим, ожидая ввод команд пользователя. Ввод знака вопроса или help позволяет отобразить справку о внутренних командах и опциях nslookup:

Команды:

(идентификаторы отображаются в верхнем регистре, квадратные скобки "[]" обозначают необязательные параметры)

**NAME**  - печать сведений об узле или домене NAME с помощью сервера по умолчанию

**NAME1 NAME2** - та же операция, но в качестве сервера используется NAME2

**help или ?** - печать сведений о стандартных командах

set OPTION - установить параметр

**al**l - печать параметров, текущего сервера и узла

**[no]debug** - печать отладочных сведений

**[no]d2**  - печать полных отладочных сведений

**[no]defname** - добавить имя домена ко всем запросам

**[no]recurse** - запрос рекурсивного ответа на запрос

**[no]search** - использовать список поиска доменов

**[no]vc** - всегда использовать виртуальную схему

**domain=NAME** - установить имя домена по умолчанию NAME

**srchlist=N1[/N2/.../N6]** - установить домен N1 и список поиска N1,N2 и т.д.

**root=NAME** - установить корневой сервер NAME

**retry=X** - установить число повторов X

timeout=X - установить интервал времени ожидания в X секунд

**type=X установить тип запроса (пр. A,AAAA, A+AAAA, ANY, CNAME, MX, NS, PTR, SOA, SRV)**

**querytype=X** - то же, что и type

**class=X** - установить класс запроса ( IN (Internet), ANY)

**[no]msxfr** - использовать быструю зону MS для передачи

**ixfrver=X** - текущая версия, использующаяся в передаче запросов IXFR

**server NAME** - установить сервер по умолчанию NAME, используя текущий сервер по умолчанию

**lserver NAME** - установить сервер по умолчанию NAME, используя первоначальный сервер

root - сделать текущий сервер по умолчанию корневым сервером

ls [opt] DOMAIN [> FILE] - перечисление адресов в домене DOMAIN (необязательно:вывод в файл FILE)

**-a** - перечисление канонических имен и псевдонимов

**-d** - перечисление всех записей

-t TYPE - перечисление записей указанного типа RFC (пр. A,CNAME,MX,NS,PTR etc.)

**view FILE** - сортировка файла "ls" и его просмотр с помощью pg

**exit** - выход из программы

При запуске с некоторыми из перечисленных параметров, команда nslookup выполняется в не интерактивном режиме без диалога с пользователем:

**nslookup yandex.ru.** - выполнить запрос к DNS-серверу, заданному по умолчанию, на разрешение доменного имени yandex.ru. Для уменьшения количества ненужных запросов к серверам имен, имя домена нужно вводить в виде полностью определенного имени (fully qualified domain name) , т.е. с точкой в конце. Если этого не делать, то nslookup будет сначала выполнять запрос на разрешение имени относительно домена того компьютера, на котором она выполняется, т.е. yandex.ru.mydomain.ru если имя локального домена mydomain.ru.

**nslookup -type=mx yandex.ru** - то же, что и в предыдущем примере, но с указанием типа запрашиваемой записи -type=mx. Сервер DNS ответит на запрос утилиты nslookup перечислением почтовых серверов, обслуживающих домен yandex.ru

**nslookup odnoklassniki.ru 8.8.8.8** - определить IP-адрес узла odnokassniki.ru с использованием DNS-сервера 8.8.8.8 (публичный DNS-сервер Google), вместо DNS-сервера, заданного в настройках сетевого подключения.

**nslookup -type=mx -timeout=8 vk.com 208.67.220.220** - отобразить запись MX для домена vk.com из базы данных сервера с IP-адресом 208.67.220.220 (сервер OpenDNS). При выполнении команды, максимальное время ожидания ответа сервера - 8 секунд.

**nslookup -type=any -timeout=8 vk.com 208.67.220.220** - то же, что и в предыдущем примере, но выполняется запрос на отображение любых типов записей.

Пример отображаемых данных:

Сервер: 208.67.220.220

Не заслуживающий доверия ответ:

vk.com internet address = 87.240.131.119

vk.com internet address = 87.240.131.99

vk.com nameserver = ns2.vkontakte.ru

vk.com nameserver = ns4.vkontakte.ru

vk.com nameserver = ns1.vkontakte.ru

vk.com nameserver = ns4.vkontakte.ru

vk.com nameserver = ns2.vkontakte.ru

vk.com nameserver = ns1.vkontakte.ru

ns1.vkontakte.ru internet address = 93.186.237.2

ns2.vkontakte.ru internet address = 93.186.224.100

Для разных версий nslookup и разных DNS-серверов, обслуживающих запрос, отображаемая информация может незначительно отличаться. Тот же запрос, сформированный англоязычной версией утилиты nslookup.exe и направленный на обработку DNS-серверу компании Google приведет к отображению следующих данных:

Address: 8.8.8.8

Non-authoritative answer:

vk.com internet address = 87.240.131.120

vk.com internet address = 87.240.143.244

vk.com

primary name server = ns1.vkontakte.ru

responsible mail addr = ncc.vkontakte.ru

serial = 2013100501

refresh = 3600 (1 hour)

retry = 900 (15 mins)

expire = 604800 (7 days)

default TTL = 900 (15 mins)

vk.com AAAA IPv6 address = 2a00:bdc0:3:103:1:0:403:901

vk.com AAAA IPv6 address = 2a00:bdc0:3:103:1:0:403:902

vk.com AAAA IPv6 address = 2a00:bdc0:3:103:1:0:403:903

vk.com nameserver = ns1.vkontakte.ru

vk.com nameserver = ns2.vkontakte.ru

vk.com nameserver = ns4.vkontakte.ru

vk.com MX preference = 10, mail exchanger = mail.vk.com

vk.com text =

"v=spf1 ip4:93.186.224.0/20 ip4:87.240.128.0/18 mx include:aspmx.googlem

ail.com ~all"

Сообщение **"Не заслуживающий доверия ответ:"** (Non-authoritative answer: ) говорит о том, что выполняющий запрос DNS-сервер, не является владельцем зоны vk.com т.е. записи для узла vk.com в его базе отсутствуют, и для разрешения имени использовался рекурсивный запрос к другому DNS-серверу. Если отправить запрос DNS-серверу ns1.vkontakte.ru, то будет получен авторитетный ответ (authoritative answer) :

Server: ns1.vkontakte.ru

Address: 93.186.237.2

vk.com

primary name server = ns1.vkontakte.ru

responsible mail addr = ncc.vkontakte.ru

serial = 2013100501

refresh = 3600 (1 hour)

retry = 900 (15 mins)

expire = 604800 (7 days)

default TTL = 900 (15 mins)

vk.com internet address = 87.240.131.118

vk.com AAAA IPv6 address = 2a00:bdc0:3:103:1:0:403:904

vk.com AAAA IPv6 address = 2a00:bdc0:3:103:1:0:403:905

vk.com AAAA IPv6 address = 2a00:bdc0:3:103:1:0:403:906

vk.com nameserver = ns4.vkontakte.ru

vk.com nameserver = ns1.vkontakte.ru

vk.com nameserver = ns2.vkontakte.ru

vk.com MX preference = 10, mail exchanger = mail.vk.com

vk.com text =

"v=spf1 ip4:93.186.224.0/20 ip4:87.240.128.0/18 mx include:aspmx.googlem

ail.com ~all"

ns4.vkontakte.ru internet address = 93.186.239.253

ns4.vkontakte.ru AAAA IPv6 address = 2a00:bdc0:ff:4::2

ns1.vkontakte.ru internet address = 93.186.237.2

ns1.vkontakte.ru AAAA IPv6 address = 2a00:bdc0:ff:1::2

ns2.vkontakte.ru internet address = 93.186.224.100

ns2.vkontakte.ru AAAA IPv6 address = 2a00:bdc0:ff:2::2

mail.vk.com internet address = 93.186.236.94

nslookup 8.8.4.4 - отобразить имя узла, соответствующее IP-адресу 8.8.4.4

nslookup -ls -d mydomain.ru. > listdns.txt - отобразить все записи для домена mydomain.ru, обслуживаемого текущим DNS-сервером. Вывод направляется в файл listdns.txt текущего каталога. Задавать абсолютный путь к файлу не следует, поскольку все существующие на данный момент версии nslookup.exe успешно перенаправляют стандартный вывод в файл, только если он располагается в текущем каталоге.

При работе в интерактивном режиме, после старта на экран выводится приглашение к вводу команд - символ ">" . При вводе команд необходимо учитывать регистр символов, например, LS -d mydomain.ru. будет воспринята как ошибочна команда, а ls -D mydomain.ru. - как команда с ошибочной опцией.

**Задание к лабораторной работе:**

1. Изучить правила работы с командной строкой Windows

2. Изучить команды работы с сетью.

3. Для каждой команды выполнить те ключи (пункты), помеченные красным цветом.

4. Результаты выполнения соответствующей команды с различными ключами сначала вывести на экран, потом при необходимости вывести в отдельный файл с именем команды и расширением doc(например команда ping>>D:\ping.doc выведет результаты выполнения команды в файл ping.doc)

5. Выполнить индивидуальные задания согласно варианта с обязательным сохранением результата работы в отдельном текстовом файле.

6. Утилиты, выделенные желтым цветом, желательно проанализировать с помощью программы Wireshark.

**Задания**

1. Зациклить команду ping к любому компьютеру (например bsuir.by):

2. Выдать команду о настройке стека ТСP/IP вашего компьютера(IP - адрес, МАС - адрес, адрес шлюза, IP - адрес DNS - сервера по умолчанию);

3. Определить МАС - адрес шлюза;

4. Вывести состояние портов протокола TCP и UDP;

5. Проследить маршрут следования пакетов к заданному узлу(например к bsuir.by);

6. Определить символьное (DNS ) имя DNS - сервера своего домена;

7. Вывести таблицу маршрутизации своего компьютера;

8. Вывести DNS - кэш своего компьютера;

9. Вывести информацию о имеющихся сетевых дисках (если есть);

10. Вывести статистику Ethernet по протоколам IP, ICMP, TCP,UDP;

11. Вывести информацию о разделяемых ресурсах вашего компьютера в локальной сети;

12. Используя команду nslookup с ключом –type=ns (name server – сервер имен) вывести имена и IP-вдреса DNS-серверов корневой зоны доменных имен и зоны BY.

13. Определить МАС - адреса узлов всех компьютеров локальной сети с которыми соединялся ваш компьютер.

Варианты индивидуальных заданий.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Задание1 | Задание2 | Задание3 | Задание4 |
| 1 | 1 | 2 | 7 | 12 |
| 2 | 2 | 3 | 8 | 11 |
| 3 | 4 | 9 | 2 | 6 |
| 4 | 5 | 2 | 10 | 4 |
| 5 | 12 | 3 | 9 | 2 |
| 6 | 2 | 6 | 1 | 11 |
| 7 | 3 | 2 | 12 | 7 |
| 8 | 10 | 6 | 2 | 4 |
| 9 | 11 | 9 | 5 | 2 |
| 10 | 8 | 4 | 10 | 13 |
| 11 | 2 | 7 | 9 | 3 |
| 12 | 6 | 5 | 2 | 11 |
| 13 | 1 | 7 | 8 | 2 |
| 14 | 9 | 13 | 2 | 5 |
| 15 | 1 | 2 | 3 | 4 |