Сетевые утилиты (ping, netstat, route…)

Большинство рассматриваемых сетевых утилит для полноценной работы требуют наличия административных привилегий. Для операционных систем семейства Windows 2000/XP достаточно того, чтобы пользователь работал под учетной записью члена группы администраторов. Интерпретатор командной строки **cmd.exe** можно запустить с использованием меню **Пуск - Выполнить - cmd.exe**. В среде операционных систем Widows начиная с версии Vista интерпретатор **cmd.exe** должен быть запущен для выполнения с использованием пункта контекстного меню "Запустить от имени администратора". Командные файлы, в которых используются сетевые утилиты, также должны выполняться в контексте учетной записи с привилегиями 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 параметров.

Краткое описание и примеры использования сетевых утилит командной строки Windows:

ARP; IPCONFIG; GETMAC; NBTSTAT; NETSH; NETSTAT; NET; NSLOOKUP; PATHPING; PING; ROUTE; TELNET; TRACERT

Примеры практического использования.

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 (1) 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 на сетевом интерфейсе 192.168.1.1

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, 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 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. Применимо для Windows Vista/Windows 7 .

/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

/showclassid Adapter и **/setclassid Adapter[ClassID]** - эти параметры применимы для

Windows Vista / Windows 7 и используются для просмотра или изменения идентификатора Class ID, если он получен от DHCP - сервера при конфигурировании сетевых настроек.

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.

ipconfig /setclassid "Local Area Connection" TEST - установить для адаптера с именем "Local Area Connection" идентификатор класса DHCP "TEST". Если идентификатор класса DHCP не указан, то он будет удален.

Пример отображаемой конфигурации сетевого адаптера :

Ethernet adapter Подключение по локальной сети : - имя адаптера
DNS-суффикс подключения . . . . . : - DNS-суффикс из настроек сетевого подключения

Описание. . . . . : Realtek 8139d Adapter #2 - описание адаптера.
Физический адрес. . . . . : 00-14-02-7B-ED-67 - MAC- адрес данного адаптера.
DHCP включен. . . . . : Да - признак использования DHCP для конфигурирования сетевого адаптера
Автонастройка включена. . . . . : Да - признак автоматической настройки параметров адаптера с использованием функции автоматического назначения адресов (APIPA) при отсутствии сервера DHCP. Режим определяется значением ключа реестра

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\GUID адаптера\IPAutoconfigurationEnabled
Значение 0 (тип DWORD) параметра IPAutoconfigurationEnabled отключает APIPA. Если значение этого параметра равно 1 , или параметр отсутствует в реестре, APIPA активируется.

Автонастройка IPv4-адреса . . . . : 169.254.254.18(Основной) - автоматически полученный локальный адрес, если используется APIPA

Локальный IPv6-адрес канала . . . : fe80::7c22:e7f8:3a71:8249%16(Основной) - локальный IPv6 адрес, если используется адресация IPv6

IPv4-адрес. . . . . : 10.10.11.77(Основной) - используемый для данного адаптера IPv4 - адрес.

Маска подсети . . . . . : 255.255.224.0 - маска подсети.

Аренда получена. . . . . : 2 марта 2012 г. 22:44:48 - дата и время получения сетевой конфигурации от сервера DHCP

Срок аренды истекает. . . . . : 3 марта 2012 г. 2:31:27 - срок истечения аренды сетевых настроек. Определяется сервером DHCP.

Основной шлюз. . . . . : 10.10.11.1 - IP - адрес маршрутизатора, используемого в качестве шлюза по умолчанию.

Код класса DHCPv4. . . . . : TEST - код класса DHCP, если он существует.

DHCP-сервер. . . . . : 10.10.11.11 - - IP-адрес DHCP-сервера, от которого получена сетевая конфигурация.

Следующие 2 параметра (идентификатор участников DHCP - DUID и идентификатор арендованного адреса IAID) присутствуют при автоматическом конфигурировании настроек протокола IPv6 . В крупных сетях могут присутствовать несколько серверов DHCPv6. При автоматическом конфигурировании сетевого адаптера, все они получают от клиента специальный запрос **DHCP REQUEST**. Каждый из них проверяет, ему ли был направлен запрос. Сервер не приступает к обработке пакетов с DUID, отличающимся от его собственного. При совпадении DUID, сервер помечает адрес как присвоенный и возвращает ответ **DHCP REPLY**. На этом обработка запроса завершается.
IAID - это специальный идентификатор арендуемого IPv6-адреса длиной 4 байта. Клиенту выделяется адрес на время, определенное сервером (срок аренды). Когда предпочитаемый срок действия адреса заканчивается, клиент отправляет серверу пакет **DHCP RENEW** с запросом на продление этого срока. В сообщение включается идентификатор IAID, код которого также хранится в базе данных DHCP сервера. Если сервер готов продлить срок действия адреса, он отправляет ответ **DHCP REPLY** и клиент получает возможность использования арендованного адреса без повторного получения настроек.

IAID DHCPv6 . . . . . : 234890384 - идентификатор арендованного адреса IAID

DUID клиента DHCPv6 . . . . . : 00-01-00-01-14-E2-78-C0-00-0C-1E-7C-29-E3 - идентификатор участников DHCP

DNS-серверы. . . . . : 94.25.128.74
94.25.208.74 - адреса DNS - серверов, используемых для разрешения имен в IP-адреса узлов.

NetBios через TCP/IP. . . . . : Включен - режим использования NetBios через протокол TCP/IP.

Подробное описание команды IPCONFIG

Утилита GETMAC .

Утилита командной строки GETMAC присутствует в версиях Windows XP и старше. Используется для получения аппаратных адресов сетевых адаптеров (MAC-адресов) как на локальном, так и на удаленном компьютере.

Синтаксис:

GETMAC [/S <система> [/U <пользователь> [/P <пароль>]]] [/FO <формат>] [/NH] [/V]

Параметры:

/S <система> - имя или IP-адрес удаленного компьютера.

/U [<домен>\]<пользователь> Имя пользователя. Если не задано, то используется текущая учетная запись.

/P [<пароль>] - Пароль. Если задан параметр /U и не задан пароль, то он будет запрошен.

/FO <формат> - Формат, в котором следует отображать результаты запроса. Допустимые форматы: "TABLE" (таблица), "LIST" (список), "CSV" (разделяемые запятыми поля). Если параметр не задан, то используется вывод в виде таблицы (TABLE) .

/NH - Указывает, что строка заголовков столбцов не должна отображаться в результирующем файле. форматов TABLE и CSV.

/V - Отображение подробной информации. В отображаемой информации присутствует имя сетевого подключения и название сетевого адаптера.

/? - Вывод справки по использованию команды.

Примеры:

GETMAC /? - отобразить краткую справку об использовании GETMAC.
GETMAC /FO csv - выдать информации о MAC-адресах всех существующих на локальном компьютере сетевых адаптеров в формате CSV (полей с разделителями в виде запятой)
GETMAC /S COMPUTER /NH /V - получить MAC адреса сетевых адаптеров для удаленного компьютера COMPUTER, не отображать заголовки столбцов в таблице и использовать отображение подробной информации. Для подключения к удаленному компьютеру используется текущая учетная запись пользователя.
GETMAC /S 192.168.1.1 /NH /V - то же самое, но вместо имени компьютера задан его IP-

адрес.
GETMAC /S COMPUTER /U user /P password - получить MAC - адрес адаптеров удаленного компьютера COMPUTER. Для подключения к нему используется имя пользователя "user" и пароль "password"
GETMAC /S COMPUTER /U mydomain\user - для подключения к удаленному компьютеру используется учетная запись пользователя "user" в домене "mydomain". Пароль пользователя вводится по запросу.
GETMAC /S COMPUTER /U mydomain\user /P password - то же самое, что и в предыдущем случае, но пароль задан в командной строке.

Пример выводимой информации по GETMAC без параметров:

Физический адрес Имя транспорта
==========
==========
00-00-DB-CE-97-9C \Device\Tcpip_{85E2B831- 859B-45D4-9552-0E6DCFB57391}
00-2E-20-6B-0D-07 \Device\Tcpip_{158A50DF- F6F2-4909-8F15-DF94B51A81FF}

По имени транспорта можно найти в реестре записи, связанные с данным сетевым адаптером.

Утилита NBTSTAT .

Команда NBTSTAT позволяет получить статистику протокола NetBIOS over TCP/IP (NetBT), таблицу имен локальных и удаленных компьютеров и содержимое кэш NetBIOS имен. Применение NBTSTAT позволяет принудительно обновить кэш NetBIOS-имен компьютеров и имена, зарегистрированные с помощью серверов Windows Internet Name Service (WINS).

Синтаксис:

nbtstat[-a RemoteName] [-A IPAddress] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [Interval]

Параметры командной строки:

-a RemoteName - отображает таблицу имен удаленного компьютера. NetBIOS-имена соответствуют перечню NetBIOS-приложений, выполняющихся на удаленном компьютере.

-A IPAddress - то же самое, что и в предыдущем случае, но вместо имени удаленного компьютера используется его IP-адрес.

-c - отображает кэш имен NetBIOS и соответствующих им IP-адресов.

-n - отображает таблицу NetBIOS-имен на локальном компьютере. Состояние "Зарегистрирован" означает, что имя зарегистрировано с использованием широковещательного запроса или с помощью сервера WINS.

-r - отображает статистику разрешения NetBIOS-имен. На компьютерах под управлением Windows XP и старше, выдается раздельная статистика о разрешении имен с помощью широковещательной рассылки и с помощью сервера имен WINS.

-R - очистка кэш NetBIOS-имен и загрузка данных из секции #PRE файла LMHOSTS.

-RR - очистка кэш NetBIOS - имен на локальном компьютере и их повторная регистрация с использованием сервера WINS.

-s - отображает статистику NetBIOS - сессий между клиентом и сервером и NetBIOS-имена удаленных узлов.

-S - отображает статистику сессий между клиентом и сервером и IP-адреса удаленных узлов.

Interval - интервал обновления отображаемых данных в секундах. Для прекращения автоматического обновления используется комбинация клавиш CTRL+C

/? - отобразить справку по использованию NBTSTAT.
Примеры использования: **nbtstat -n** - вывести список зарегистрированных NetBIOS-имен на локальном компьютере.
nbtstat -a SERVER - вывести список зарегистрированных NetBIOS-имен на компьютере SERVER.
nbtstat -A 192.168.1.1 - вывести список зарегистрированных NetBIOS-имен на удаленном компьютере с IP-адресом 192.168.1.1 .
nbtstat -RR - выполнить очистку и перерегистрацию NetBIOS-имен на локальном компьютере.

Утилита NETSH.EXE

Утилита сетевой оболочки NETSH (NETwork SHell) - наиболее полное и функциональное стандартное средство управления сетью с использованием командной строки в среде Windows XP и старше. Набор внутренних команд сетевой оболочки пополняется с появлением новых версий операционной системы, что необходимо учитывать при работе в локальной сети с различными ОС. Так, например, команда уровня wlan (netsh wlan - управление беспроводной сетью) может использоваться на компьютерах под управлением Windows Vista и старше и отсутствует в Widows XP. Синтаксис используемых команд и параметров также может различаться в разных операционных системах семейства Windows.

При запуске NETSH.EXE без параметров на экран выводится приглашение к вводу внутренних команд оболочки. Набор команд представляет собой многоуровневую структуру, позволяющую выполнять необходимые действия в выбранном контексте. При вводе знака вопроса **?** можно получить краткую справку по доступному перечню команд на данном уровне. Ввод команды данного уровня со знаком вопроса вызовет отображение справки по ее использованию. Аналогичную справку можно получить, введя определенную команду и, после перехода на уровень ее выполнения, ввести знак вопроса. При необходимости, можно выполнить нужное действие без использования интерактивного режима, указав в качестве параметров командной строки последовательный набор внутренних команд NETSH и необходимых параметров. Например:

netsh advfirewall show global последовательно выполняется команда первого уровня **advfirewall**, в ее контексте, команда следующего уровня **show** с параметром **global**

Команды NETSH можно выполнить и на удаленном компьютере с использованием подключения по локальной сети. Netsh также предоставляет возможность выполнения сценариев, представляющих собой группу команд в текстовом файле, выполняемых в режиме

очередности на определенном компьютере. В целом, возможности NETSH настолько обширны, что трудно найти сетевую задачу, которую невозможно было бы решить с использованием данной утилиты.

Синтаксис:

NETSH.EXE [-a AliasFile] [-c Context] [-r RemoteMachine] [-u [DomainName\]UserName] [-p Password | *] [Command | -f ScriptFile]

-a AliasFile - не завершать работу а перейти к приглашению ввода команд после выполнения AliasFile. AliasFile - имя текстового файла, в котором содержатся одна или несколько команд netsh .

-c Context - изменить контекст (уровень) команд netsh.

-r RemoteMachine - выполнять команды netsh на удаленном компьютере. В качестве RemoteMachine может использоваться имя или IP-адрес.

[-u DomainName\]UserName - имя пользователя для подключения к удаленному компьютеру. Если не задано, то используется текущее имя пользователя.

-p Password пароль для подключения к удаленному компьютеру.

Command - команда оболочки netsh , которую необходимо выполнить.

-f ScriptFile - аналогично ключу -a, но после выполнения команд файла сценария Scriptfile, работа netsh завершается.

Пример полученной справки об использовании по команде **netsh ?** или вводе знака вопроса на приглашение при запуске **netsh** без параметров в среде ОС Windows 7:

Применимы следующие команды:

Команды в этом контексте:
? - Отображение списка команд.
add - Добавление элемента конфигурации в список элементов.
advfirewall - Изменения в контексте 'netsh advfirewall'.
branchcache - Изменения в контексте 'netsh branchcache'.
bridge - Изменения в контексте 'netsh bridge'.
delete - Удаление элемента конфигурации из списка элементов.
dhcpclient - Изменения в контексте 'netsh dhcpclient'.
dnsclient - Изменения в контексте 'netsh dnsclient'.
dump - Отображение сценария конфигурации.
exec - Запуск файла сценария.
firewall - Изменения в контексте 'netsh firewall'.
help - Отображение списка команд.
http - Изменения в контексте 'netsh http'.
interface - Изменения в контексте 'netsh interface'.
ipsec - Изменения в контексте 'netsh ipsec'.
lan - Изменения в контексте 'netsh lan'.

mbn - Изменения в контексте 'netsh mbn'.
namespace - Изменения в контексте 'netsh namespace'.
nap - Изменения в контексте 'netsh nap'.
netio - Изменения в контексте 'netsh netio'.
p2p - Изменения в контексте 'netsh p2p'.
ras - Изменения в контексте 'netsh ras'.
rpc - Изменения в контексте 'netsh rpc'.
set - Обновление параметров конфигурации.
show - Отображение информации.
trace - Изменения в контексте 'netsh trace'.
wcn - Изменения в контексте 'netsh wcn'.
wfp - Изменения в контексте 'netsh wfp'.
winhttp - Изменения в контексте 'netsh winhttp'.
winsock - Изменения в контексте 'netsh winsock'.
wlan - Изменения в контексте 'netsh wlan'.

Доступны следующие дочерние контексты:
advfirewall branchcache bridge dhcpclient dnsclient firewall http interface ipsec lan mbn namespace nap netio p2p ras rpc trace wcn wfp winhttp winsock wlan

Чтобы получить справку по команде, введите эту команду, затем пробел и "?"

Примеры практического использования NETSH.

Как получить справку в виде текстового файла для выбранного контекста NETSH
Для примера, нужно получить справку в контексте работы с конфигурацией беспроводной сети **wlan** . Последовательно выполняем команды

netsh
wlan
set file open C:\wlanhelp.txt
?
set file close

В данном примере, команда **set file open C:\wlanhelp.txt** устанавливает режим вывода консольных сообщений в файл с именем C:\wlanhelp.txt. После установки данного режима, все, что вводится с клавиатуры и отображается на экране, будет записано в указанный текстовый файл. Таким образом, можно создавать файлы журналов отдельных сессий использования netsh . Вместо параметра **open** можно использовать **append** и имя уже существующего файла журнала. В таком режиме данные будут записываться в конец существующего текстового файла.

Как сохранить и восстановить сетевую конфигурацию

Команда **dump** создает сценарий, который содержит текущую конфигурацию. Если данные сценария сохранить в текстовый файл, то при необходимости, его можно будет использовать для восстановления измененных параметров с помощью команды загрузки и выполнения скриптов **exec**.

Для сохранения используется команда:

dump Имя файла сценария

Для восстановления настроек из файла сценария используется команда:

exec Имя файла сценария

В некоторых версиях netsh команда dump с указанием имени файла почему-то не работает. Однако, для сохранения конфигурации можно воспользоваться способом, описанным выше - использовать запись в файл командой **set file open C:\mynet.sav** .

netsh
set file open C:\mynet.sav
dump
quit

Остается только слегка исправить полученный файл сценария C:\mynet.sav - удалить 1-ю строчку с командой **dump** и последние - с приглашением netsh и (или) командой **quit**

Второй способ - использовать netsh с перенаправлением вывода команды **dump** в файл:

netsh dump > C:\mynet.sav

Для сохранения отдельного контекста конфигурации можно воспользоваться командой dump на соответствующем уровне :

netsh interface dump > C:\myinterf.cnf - сохранить настройки сетевых интерфейсов в виде сценария netsh в файле C:\myinterf.cnf

Для восстановления сетевой конфигурации можно воспользоваться

netsh exec C:\mynet.sav

Обычно, после восстановления сетевых настроек из файла сценария , требуется перезапуск некоторых сетевых служб, а желательнее - выполнить перезагрузку Windows

Как выполнить переключение между контекстами netsh

Иногда требуется выполнить некоторые команды на одном уровне, перейти на другой, и снова вернуться на предыдущий. Для выполнения таких переходов используются команды **pushd** и **popd** . Принцип переключения между контекстами основан на обработке очереди в соответствии с правилом "первым вошел - последним вышел" или first-in-last-out (FILO) stack. Команда **pushd** запоминает текущий уровень (контекст) в стеке, а команда **popd** извлекает его из стека. Например:

netsh> - приглашение первого уровня команды nesh
pushd - введена команда запоминания контекста в стек
netsh> - приглашении netsh не меняется, контекст прежний.
interface ipv4 - переход на уровень interface и уровень ipv4
netsh interface ipv4> - соответственно, изменилась строка приглашения, отображая текущий контекст выполнения команды netsh

set address local static 192.168.1.9 255.255.255.0 192.168.1.1 1 - команда, меняющая настройки IP протокола.
netsh interface ip> - контекст выполнения команды, отображаемый в приглашении не изменяется.
popd - команда извлечения из стека запомненного контекста.
netsh > - строка приглашения изменилась, отображая текущий контекст выполнения команды netsh .

Без использования команд pushd и popd практически невозможно полноценное использование сценариев netsh.

Как найти примеры выполнения сетевых настроек с помощью netsh

Кроме сохранения и восстановления настроек использование команды **dump** позволяет получить примеры в виде сценария, соответствующего текущей конфигурации. Например, дамп секции interface дает пример выполнения команд netsh в контексте настроек сетевых интерфейсов. Пример сценария :

```
#========================
# Конфигурация интерфейса
#========================
pushd interface
reset all
popd
# Конец конфигурации интерфейса
. . .

# ----------------------------------------
# Настройка IP-интерфейсов
# ----------------------------------------
pushd interface ip
# Интерфейс настройки IP для "Подключение по локальной сети"

set address name=" Подключение по локальной сети " source=static addr=192.168.0.1
mask=255.255.255.0
set dns name="Подключение по локальной сети" source=static addr=192.168.0.2
mask=255.255.255.0
set wins name=" Подключение по локальной сети " source=static addr=192.168.0.9
```

Строки сценария, начинающиеся с символа #, являются комментариями. Команды pushd и popd позволяют определить контекст исполнения других команд netsh. Команды настроек конфигурации плюс справочная информация самой netsh позволяют довольно легко получить командную строку для выполнения отдельных сетевых настроек:

- Сменить IP-адрес в командной строке:

netsh interface ip set address name="Подключение по локальной сети" source=static addr=192.168.0.58 mask=255.255.255.0

name - имя сетевого подключения
source - static - статический IP-адрес. Возможно значение DHCP, если адрес назначается

автоматически сервером DHCP.
addr - значение IP-адреса
mask - значение маски сети.

Для получения сведений о дополнительных возможностях конфигурирования сетевых интерфейсов можно перейти на соответствующий контекст выполнения netsh, и выполнить интересующую команду с параметром **?** . Например:

netsh - старт NETSH
interface - перейти в контекст настройки сетевых интерфейсов **interface**
ip - перейти в контекст настройки протокола IP
set file open C:\setaddr.txt - записывать сессию в файл. Эта команда используется, если нужна справочная информация в виде текстового файла .
set address ? выдать справку по использованию **set address**
set file close - закрыть файл справки.
quit - завершить работу с netsh

Для Windows Windows 7 и старше, синтаксис будет немного отличаться, уровню **ip** будет соответствовать уровень **ipv4** или **ipv6**:

netch - старт NETSH
interface - перейти в контекст настройки сетевых интерфейсов **interface**
ipv4 - перейти в контекст настройки протокола IP v4
ipv6- перейти в контекст настройки протокола IP v6
set file open C:\setaddr.txt - записывать сессию в файл. Эта команда используется, если нужна справочная информация в виде текстового файла .
set address ? выдать справку по использованию **set address**
set file close
quit - завершить работу с netsh

Пример синтаксиса для смены адреса DNS-сервера в настройках сетевого подключения "Подключение по локальной сети 2" на адрес публичного DNS-сервера Googl в среде Windows 7:

netsh interface ipv4 set dnsservers name="Подключение по локальной сети 2" static 8.8.8.8 primary

Из информации файла справки следует, что возможно использование параметров командной строки netsh без указания ключевых слов:

netsh interface ipv4 set address name="Подключение по локальной сети" source=static addr=192.168.0.58 mask=255.255.255.0 gateway=192.168.0.1 gwmetric=1

Аналогично, без указания ключевых слов:

netsh interface ipv4 set address name="Подключение по локальной сети" static 192.168.0.58 255.255.255.0 192.168.0.1 1

При изменении одного из параметров настроек необходимо указывать и остальные. Например, только для изменения адреса шлюза по умолчанию недостаточно выполнить команду

netsh interface ipv4 set address name="Подключение по локальной сети" gateway=192.168.0.1 gwmetric=1

При ее выполнении отсутствующие параметры (IP-адрес и маска) будут сброшены. Для правильной смены шлюза по умолчанию команда должна быть следующей:

netsh interface ipv4 set address name="Подключение по локальной сети" source=static addr=192.168.0.58 mask=255.255.255.0 gateway=192.168.0.1 gwmetric=1

Результат применения команды **netsh** в некоторых случаях зависит от сетевой конфигурации системы. Например, для ”проброса портов” используется команда **netsh interface portproxy**, позволяющая реализовать перенаправление соединения на другой порт или узел. Напимер:

netsh interface portproxy add v4tov4 listenport=22 listenaddress=192.168.1.8 connectaddress=192.168.1.240 connectport=22 TCP

Команда создает правило, означающее, что подключение к узлу 192.168.1.8 по протоколу TCP на порт 22, будет перенаправлено на узел 192.168.1.240 TCP порт 22. Правила для проксирования портов можно посмотреть с помощью команды:

netsh interface portproxy show all

Результат выполнения команды будет выглядеть следующим образом:

Прослушивать ipv4:		**Подключиться к ipv4:**	
Адрес	**Порт**	**Адрес**	**Порт**
192.168.1.8	**22**	**192.168.1.240**	**22**

Правило присутствует, однако, перенаправление портов не будет работать, если на компьютере не запущена ”Вспомогательная служба IP” (iphlpsvc). Естественно, утилита **netsh** работоспособность службы не проверяет, поскольку это не входит в ее функционал. Это должен сделать сам пользователь, если обнаружилось, что на компьютере правила перенаправления портов не выполняются.

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] [-p Protocol] [-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. Данный параметр применим для операционных систем Widows XP и старше.

-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]
. . .

Имя - название протокола.

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 :

- Получить список слушаемых портов и связанных с ними программ:

netstat -a -b

netstat -ab - параметры командной строки можно объединять. Параметр **-ab** эквивалентен **-a -b**

netstat -a -n -b - отобразить список всех соединений с числовыми номерами портов

netstat -anb - аналогично предыдущей команде.

netstat -anbv - при использовании параметра **-v** отображается последовательность компонентов, участвующих в создании соединения или слушаемого порта.

 получить статистические данные:

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

netstat -e -v - кроме суммарных статистических данных для Ethernet, отображается статистика для каждого сетевого интерфейса.

netstat -e -s - дополнительно к статистике Ethernet, отображается статистика для протоколов IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP и UDPv6

netstat -s - получить статистику по протоколам IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP и UDPv6

netstat -s -p udp - получить статистику только по протоколу UDP

netstat -s -p icmp - получить статистику только по протоколу ICMP

Утилита NET.EXE

Утилита NET.EXE существует во всех версиях Windows и является одной из самых используемых в практической работе с сетевыми ресурсами. 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. Возможно использование только одного из элементов списка. Например, в соответствии с изложенными соглашениями, необходимо ввести NET COMMAND и один из переключателей - SWITCH1 или SWITCH2. Указанное в квадратных скобках имя [name] является необязательным параметром:
NET COMMAND [name] {SWITCH1 | SWITCH2}

- Запись [...] означает, что указанный элемент может повторяться. Повторяющиеся элементы должны быть разделены пробелом.

- Запись [,...] означает, что указанный элемент может повторяться, но повторяющиеся элементы должны быть разделены запятой или точкой с запятой, но не пробелом.

- 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.

Справочная система NET.EXE, пожалуй, является одной из лучших в семействе операционных систем Windows. 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 системными службами

Данный режим использования **NET.EXE** , в некоторой степени, является не характерным для основного предназначения утилиты, и начиная с Windows XP, для управления системными службами используется специальная утилита командной строки **SC.EXE**. Тем не менее, NET.EXE в среде любой версии операционных систем Windows может быть использована для запуска и остановки системных служб (сервисов). Согласно справочной информации, список служб, которыми можно управлять с помощью **net.exe** можно получить используя следующую команду:

net help services

Но это не совсем верно, и на самом деле, с помощью **net.exe** можно запустить или остановить практически любую системную службу, и в том числе, не представленную в списке , отображаемом при выполнении данной команды . Для остановки используется параметр **stop**, а для запуска - параметр **start**:

net stop dnscache - остановить службу **dnscache**
net start dnscache - запустить службу **dnscache**

Возможно использование как короткого, так и полного имени ("Dnscache" - короткое, "DNS-клиент" - полное имя службы). Имя службы, содержащее символы русского алфавита и пробелы заключается в двойные кавычки.

net stop "DNS-клиент" - остановить службу **DNS-клиент** .

Полное имя службы можно скопировать из "Панель управления" - "Администрирование" - "Службы" - Имя службы - "Свойства" - "Выводимое имя".

Для приостановки некоторых системных служб или продолжения работы ранее приостановленной службы используются команды **NET PAUSE** и **NET CONTINUE** :

net pause "Планировщик заданий" - приостановить службу "Планировщик заданий"
net continue schedule - продолжить работу службы "Планировщик заданий" . Имя службы задано в коротком формате.

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

В операционных системах семейства Windows, если в конце имени разделяемого ресурса используется знак **$** то такой ресурс является скрытым и не отображается в проводнике при просмотре сетевого окружения. Это правило относится не только к автоматически создаваемым ресурсам для системного администрирования (C$, D$, ADMIN$ и т.п.), но и для любого пользовательского разделяемого ресурса. Если, например, для сетевого доступа выделена папка под именем "movies", то она будет видна в сетевом окружении, а если - под именем "movies$" - то нет.
Для того, чтобы скрыть в сетевом окружении отдельный компьютер используется команда:
NET config server /hidden:yes
Чтобы вернуть отображение компьютера в сетевом окружении
NET config server /hidden:no

UNC-пути можно использовать и для локальной машины, только в этом случае вместо имени "Сервер" нужно подставлять знак "?" или ".", а путь к файлу указывать вместе с буквой диска. Например так: "\\?\C:\Windows\System32\file.exe" .

Для отключения сетевого диска или устройства используется команда **net use** с ключом **/DELETE**

net use X: /delete - отключить сетевой диск X:

Регистр букв в данном ключе не имеет значения и можно использовать сокращения:

net use Y: /del

Примеры выполнения команды **NET USE** для подключения сетевых дисков:

net use X: \\server\shares - подключить сетевой диск X: которому соответствует разделяемый сетевой каталог с именем **shares** на компьютере с именем **server**

net use Y:\C$ /USER:Администратор admpass - подключить сетевой диск Y: которому соответствует скрытый ресурс C$ (корневой каталог диска C:) . При подключении к удаленному компьютеру используется имя пользователя **Администратор** и пароль **admpass**

То же самое, но с использованием учетной записи в домене **mydomain net use Y:\C$ /USER:mydomain\Администратор admpass**

net use Y:\C$ /USER:Администратор@mydomain admpass

Если в командной строке пароль не задан, то он будет запрошен при подключении к сетевому ресурсу. Если ключ **/USER** не задан, то для авторизации на удаленном компьютере используется текущая учетная запись.

net use Y:\C$ /SAVECRED - выполнить подключение с запоминанием полномочий (credentials) пользователя. При первом подключении, будет выдан запрос на ввод имени пользователя и пароля , которые будут запомнены и не будут запрашиваться при последующих подключениях. Параметр **/savecred** не работает в версиях Домашняя и Начальная Windows 7 / Windpws XP

Для изменения режима запоминания подключенных сетевых дисков используется ключ **/PERSISTENT**

net use /PERSISTENT:NO - не запоминать сетевые подключения.
net use /PERSISTENT:YES - запоминать сетевые подключения.

Необходимо учитывать, что режим, определяемый значением ключа /PERSISTENT, относится к вновь создаваемым подключениям. Если, например, сетевой диск X: был создан при установленном режиме запоминания (PERSISTENT:YES), а затем вы выполнили смену режима командой **net use /PERSISTENT:NO** и подключили сетевой диск Y: , то после перезагрузки системы, не будет восстановлено подключение диска Y: , но будет восстановлено подключение диска X:

Подробное описание команд NET

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 обновременоо подключающихся пользователей равным 5 .

Кроме этого, при создании разделяемого ресурса можно указать краткое его описание (заметку) с помощью параметра /REMARK и режим кэширования файлов с помощью параметра /CACHE .

NET SHARE имя_ресурса=диск:путь [/USERS:число | /UNLIMITED] [/REMARK:"текст"] [/CACHE:Manual | Automatic | No] [/CACHE:Manual | Documents| Programs | None]

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 .

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 с 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 .

Работа с пользователями и компьютерами.

Утилита NET.EXE позволяет отобразить данные об учетных записях пользователей и групп, добавлять новые записи, удалять существующие, отображать параметры безопасности, связанные с авторизацией пользователей и некоторые другие операции по администрированию на локальном компьютере или контроллере домена.

NET ACCOUNTS - эта команда используется для обновления базы данных регистрационных записей и изменения параметров входа в сеть (LOGON) . При использовании этой команды без указания параметров, выводятся текущие значения параметров, определяющих требования к паролям и входу в сеть, - время принудительного завершения сессии, минимальную длину пароля, максимальное и минимальное время действия пароля и его уникальность.

Синтаксис данной команды:

NET ACCOUNTS [/FORCELOGOFF:{минуты | NO}] [/MINPWLEN:длина] [/MAXPWAGE:{дни | UNLIMITED}] [/MINPWAGE:дни] [/UNIQUEPW:число] [/DOMAIN]

Пример отображаемой информации по команде NET ACCOUNTS :

Принудительный выход по истечении времени через: Никогда
Минимальный срок действия пароля (дней): 0
Максимальный срок действия пароля (дней): 42
Минимальная длина пароля: 0
Хранение неповторяющихся паролей: Нет
Блокировка после ошибок ввода пароля: Никогда
Длительность блокировки (минут): 30
Сброс счетчика блокировок через (минут): 30
Роль компьютера: РАБОЧАЯ СТАНЦИЯ

При использовании в локальной сети, каждый компьютер может выполнять как роль сервера (server), предоставляющего свои ресурсы для совместного использования, так и рабочей станции (workstation), использующей разделяемые сетевые ресурсы. Основные

настройки сетевых служб сервера и рабочих станций можно отобразить с помощью команд:

net config server - настройки сетевых служб для роли сервера.
net config workstation - настройки сетевых служб для роли рабочей станции.

Настройки служб сервера можно изменить с использованием параметров:

/AUTODISCONNECT:минуты - максимальное время, в течение которого сеанс пользователя может быть не активен, прежде чем соединение будет отключено. Можно использовать значение -1, которое означает, что отключение вообще не производится. Допустимый диапазон значений: от -1 до 65535; по умолчанию используется 15.
/SRVCOMMENT:"текст"
Добавляет текст комментария для сервера, который отображается на экране Windows и при выполнении команды NET VIEW. Максимальная длина этого текста составляет 48 знаков. Текст должен быть заключен в кавычки.
/HIDDEN:{YES | NO} Указывает, должно ли выводиться имя данного сервера в списке серверов. Учтите, что "скрытие" сервера не изменяет параметров доступа к этому серверу. По умолчанию используется значение NO.
net config server /SRVCOMMENT:"Игровой сервер" /AUTODISCONNECT:5 - автоотключение при неактивности пользователя - 5 минут..
net config server /HIDDEN:YES>/AUTODISCONNECT:-1 - автоотключение при неактивности пользователя не выполняется, сервер не отображается в сетевом окружении.

При выполнении на контроллере домена, утилита net.exe позволяет добавлять новые компьютеры в базу данных Active Directory (AD) или удалять существующие компьютеры из нее.

net computer \\notebook /add - добавить в домен компьютер notebook .
net computer \\notebook /del - удалить из домена компьютер notebook .

Для просмотра списка групп пользователей и изменения их состава, а также добавления новых или удаления существующих групп используются команды **NET GROUP** и **NET LOCALGROUP**. Первая из них используется только на контроллерах домена и предназначена для работы с группами пользователей в домене.

net group - отобразить список групп пользователей в текущем домене.

net localgroup - отобразить список групп пользователей данного компьютера.
Синтаксис и назначение параметров этих команд практически не отличаются.

NET LOCALGROUP [имя_группы [/COMMENT:"текст"]] [/DOMAIN] имя_группы {/ADD /COMMENT:"текст"] | /DELETE} [/DOMAIN] имя_группы имя [...] {/ADD | /DELETE} [/DOMAIN]

имя_группы - имя локальной группы, которую необходимо добавить, изменить или удалить. Если указать только имя группы, то будет выведен список пользователей или глобальных групп, являющихся членами этой локальной группы.
/COMMENT:"текст" - комментарий для новой или существующей группы. Текст должен быть заключен в кавычки.
/DOMAIN - Команда выполняется на основном контроллере домена в текущем домене. В

противном случае операция выполняется на локальном компьютере.
имя [...] - Список из одного или нескольких имен пользователей, которые необходимо добавить или удалить из локальной группы. Имена разделяются пробелом. Эти имена могут быть именами пользователей или глобальных групп, но не именами других локальных групп. Если пользователь зарегистрирован в другом домене, его имени должно предшествовать имя домена (например, SALES\RALPHR).
/ADD - Добавляет имя группы или имя пользователя в локальную группу. Регистрационная запись для добавляемых пользователей или глобальных групп должна быть создана заранее.
/DELETE - Удаляет имя группы или пользователя из локальной группы.

net localgroup Администраторы - отобразить список пользователей локальной группы **Администраторы** данного компьютера.
net localgroup Администраторы testuser /add - добавление в группу **Администраторы** нового пользователя с именем **testuser**
net localgroup Администраторы testuser /delete - удалить пользователя **testuser** из группы **Администраторы** .

Для работы с учетными записями пользователей используется команда **net user**

NET USER [имя_пользователя [пароль | *] [параметры]] [/DOMAIN] имя_пользователя {пароль | *} /ADD [параметры] [/DOMAIN] имя_пользователя [/DELETE] [/DOMAIN]

имя_пользователя - имя пользователя, которое необходимо добавить, удалить, изменить или вывести на экран. Длина имени пользователя не должна превосходить 20 знаков.
пароль - пароль для учетной записи пользователя. Пароль должен отвечать установленным требованиям на длину - быть не короче, чем значение, установленное параметром /MINPWLEN в команде NET ACCOUNTS, и в то же время не длиннее 14 знаков.
***** - Вызывает открытие специальной строки ввода пароля. Пароль не выводится на экран во время его ввода в этой строке.
/DOMAIN команда будет выполняться на контроллере домена в текущем домене.
/ADD - добавление нового пользователя.
/DELETE - удаление пользователя.
Параметры - Допустимые параметры :
/ACTIVE:{YES | NO} - Активизирует учетную запись или делает ее не активной. Если учетная запись не активна, пользователь не может получить доступ к серверу. По умолчанию используется значение YES (т.е. учетная запись активна).
/COMMENT:"текст" - Добавляет описательный комментарий об учетной записи (длиной не более 48 знаков). Текст должен быть заключен в кавычки.
/COUNTRYCODE:nnn - Использует кодовую страницу нужного языка для вывода справки и сообщений об ошибках. Значение 0 означает выбор кодовой страницы по умолчанию.
/EXPIRES:{дата | NEVER} - Устанавливает дату истечения срока действия ученой записи. Если используется значение NEVER, то время действия учетной записи не ограничено. Дата истечения срока действия задается в формате дд/мм/гг или мм/дд/гг, в зависимости от того, какая кодовая страница используется. Месяц может быть указан цифрами, названием месяца или трехбуквенным его сокращением. В качестве разделителя полей должен использоваться знак косой черты (/).
/FULLNAME:"имя" - Указывает настоящее имя пользователя (а не кодовое имя, заданное параметром имя_пользователя). Настоящее имя следует заключить в кавычки.
/HOMEDIR:путь Указывает путь к домашнему каталогу пользователя. Этот каталог должен существовать.

/PASSWORDCHG:{YES | NO} Определяет, может ли пользователь изменять свой пароль. По умолчанию используется значение YES (т.е. изменение пароля разрешено).
/PASSWORDREQ:{YES | NO} Определяет, является ли указание пароля обязательным. По умолчанию используется значение YES (т.е. пароль обязателен).
/PROFILEPATH[:путь] Устанавливает путь к профилю пользователя.
/SCRIPTPATH:путь Устанавливает расположение пользовательского сценария для входа в систему.
/TIMES:{промежуток | ALL} - Устанавливает промежуток времени, во время которого пользователю разрешен вход в систему. Этот параметр задается в следующем формате: день[-день][,день[-день]],время[-время][,время[-время]]
Время указывается с точностью до одного часа. Дни являются днями недели и могут указываться как в полном, так и в сокращенном виде. Время можно указывать в 12- и 24-часовом формате. Если используется 12-часовой формат, то можно использовать am, pm, a.m. или p.m. Значение ALL указывает, что пользователь может войти в систему в любое время, а пустое значение указывает, что пользователь не может войти в систему никогда.
Разделителем полей указания дней недели и времени является запятая, разделителем при использовании нескольких частей является точка с запятой.
/USERCOMMENT:"текст" - Позволяет администратору добавлять или изменять текст комментария к учетной записи. **/WORKSTATIONS:{имя_компьютера[,...] | *}** - Перечисляет до восьми различных компьютеров, с которых пользователь может войти в сеть. Если данный параметр имеет пустой список или указано значение *, пользователь может войти в сеть с любого компьютера.

Примеры использования:

net user - отобразить список пользователей
net user /DOMAIN - отобразить список пользователей текущего домена
net user VASYA /USERCOMMENT:"Тестовый пользователь " /add - добавить пользователя с именем **VASYA**
net user VASYA /delete - удалить созданного пользователя.
net user VASYA password /USERCOMMENT:"Тестовый пользователь " /add - создать учетную запись нового пользователя VASYA с паролем password .
net user VASYA * /USERCOMMENT:"Тестовый пользователь " /add - то же, что и в предыдущей команде, но пароь будет запрошен при создании новой учетной записи.
net user VASYA * - изменить пароль существующего пользователя VASYA. Новый пароль будет запрошен при выполнении команды.
net user VASYA Boss - изменить пароль пользователя VASYA на новое значение Boss

Пример последовательности команд для создания нового пользователя с правами локального администратора:BR>
net user VASYA Boss /ADD
- создание учетной записи.
net localgroup Администраторы VASYA /ADD - добавление пользователя в группу "Администраторы"

Отправка сообщений по локальной сети

Для отправки сообщений в Windows XP используется команда **NET SEND**

NET SEND {имя | * | /DOMAIN[:имя] | /USERS} сообщение имя - имя пользователя, компьютера или имя для получения сообщений, на которое отправляется данное сообщение.

Если это имя содержит пробелы, то оно должно быть заключено в кавычки (" ").
***** - отправка сообщения по всем именам, которые доступны в данный момент.
/DOMAIN[:имя домена] - сообщение будет отправлено по всем именам домена данной рабочей станции. Если указано имя домена, то сообщение отправляется по всем именам указанного домена или рабочей группы.
/USERS - сообщение будет отправлено всем пользователям, подключенным в настоящий момент к серверу.
сообщение - текст отправляемого сообщения.

Для того, чтобы получить сообщение, должна быть запущена "Служба сообщений" (MESSENGER). Имена пользователей, компьютеров и текст сообщений на русском языке должны быть в DOS-кодировке.
Перечень доступных активных имен на данном компьютере и состояние службы сообщений можно получить с использованием команды **net name** без параметров. По всему списку имен, отображаемому в результате выполнения данной команды возможна отправка сообщений.
Примеры использования:

net send VASYA привет! - отправка сообщения на имя VASYA .
net send * привет! - отправка сообщения всем пользователям локальной сети, имена которых можно определить.
net send /DOMAIN:mydomain Привет - отправка сообщения всем пользователям в домене mydomain
net send /USERS Привет! - отправка сообщений всем пользователям, зарегистрированным службой сервера данного компьютера.

В операционных системах Windows 7/Windows 8 команда **net send** не реализована и для обмена сообщениями в локальной сети используется команда **msg**. Такая же команда существует и в операционных системах WindowsXP/Server 2003, но используется в них только для обмена сообщениями с пользователями терминальных сессий. Тем не менее, при определенных настройках службы сервера **Terminal Server** команда **msg** может использоваться для обмена сообщениями между пользователями Windows XP и более поздних версий Windows. Для этого необходимо на каждом компьютере, которому будут отправляться сообщения, разрешить удаленный вызов процедур для службы сервера терминалов, добавив в раздел
реестра **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server** параметр **AllowRemoteRPC** типа REG_DWORD и равный **1** . Для вступления данного значения в силу, требуется перезагрузка. После чего команду **msg** можно будет использовать как альтернативу **net send** на компьютерах с любой версией Windows. Необходимо также учитывать тот факт, что потребуются настройки брандмауэров, поскольку по умолчанию, передача и прием сообщений по сети, как правило, блокируются.

Справку по работе с командой **msg**. можно получить введя **/?** в качестве параметра:

MSG {<пользователь> | <имя сеанса> | | @<имя файла> | *}
[/SERVER:<сервер>] [/TIME:<секунд>] [/V] [/W] [<сообщение>]

<пользователь> Имя пользователя.
<имя сеанса> Имя сеанса.
Идентификатор сеанса.
@<имя файла> Файл, содержащий список имен пользователей, сеансов или

идентификаторов сеансов, которым отправляется сообщение.
***** Отправить сообщение всем сеансам на указанном сервере.
/SERVER:<сервер> Сервер (по умолчанию - текущий).
/TIME:<секунд> Интервал ожидания подтверждения от получателя.
/V Отображение информации о выполненных действиях.
/W Ожидание ответа от пользователя, полезно вместе с /V.
<сообщение> Отправляемое сообщение. Если не указано, выдается запрос или принимается ввод из STDIN.

Примеры использования:

msg * /server:TSServer "Тестовое сообщение " - отправить тестовое сообщение всем пользователям компьютера **TSServet**

msg RDP-Tcp#0 /server:TSServer "Тестовое сообщение" - отправить тестовое сообщение пользователю терминальной сессии с именем RDP-Tcp#0 на компьютере **TSServer**

msg console /server:Windows7 "Тестовое сообщение" - отправить тестовое сообщение текущему локальному пользователю компьютера **Windows7**

msg console "Тестовое сообщение" - отправка тестового сообщения от пользователя сеанса RDP локальному пользователю

Статистика и синхронизация часов .

Утилита NET.EXE позволяет получить статистические данные по использованию служб сервера и рабочей станции. Статистика содержит информацию о сеансах, доступе к сетевым устройствам, объемах принятых и переданных данных, отказах в доступе и ошибках, обнаруженных в процессе сетевого обмена.

net statistics server - отобразить статистические данные для службы сервера

net statistics workstation - отобразить статистические данные для службы рабочей станции

Для изменения системного времени компьютера используется команда **NET TIME** :

NET TIME [\\компьютер | /DOMAIN[:домен]| /RTSDOMAIN[:домен]] [/SET] [\\компьютер] /QUERYSNTP [\\компьютер] /SETSNTP[:список серверов NTP]

NET TIME синхронизирует показания часов компьютера с другим компьютером или доменом. Если используется без параметров в домене Windows Server, выводит текущую дату и время дня, установленные на компьютере, который назначен сервером времени для данного домена. Эта команда позволяет задать сервер времени NTP для компьютера. **\\компьютер** - имя компьютера, который нужно проверить или с которым нужно синхронизировать показания часов.
/DOMAIN[:домен] Задает домен, с которым нужно синхронизировать показания часов.
/RTSDOMAIN[:домен] - выполняет синхронизацию времени с сервером времени (Reliable Time Server) из указанного домена.
/SET - Синхронизирует показания часов компьютера со временем указанного компьютера или домена.
/QUERYSNTP - Отображает назначенный этому компьютеру сервер NTP (только Windows

XP)
/SETSNTP[:ntp server list] - задать список серверов времени NTP для этого компьютера (только Windows XP).
Это может быть список IP-адресов или DNS-имен, разделенных пробелами. Если задано несколько серверов, список должен быть заключен в кавычки.

Параметры /QUERYSNTP и /SETSNTP не поддерживаются в операционных системах Windows 7 и более поздних. Для настройки службы времени в этих ОС используется утилита **w32tm.exe**

net time \\COMPUTER - отобразить время на компьютере COMPUTER. Вместо имени компьютера можно использовать его IP-адрес.
net time \\COMPUTER /SET - установить часы текущего компьютера по значению часов компьютера COMPUTER

net time \\COMPUTER /SET /YES - установить часы текущего компьютера по значению часов компьютера COMPUTER без запроса подтверждения. Обычно ключ /YES используется в командных файлах, выполняющихся без участия пользователя.

net time /QUERYSNTP - отобразить сервер времени, определенный для данного компьютера.
net time \\COMPUTER /QUERYSNTP - отобразить сервер времени, определенный для указанного компьютера.
net time /SETSNTP:"1.ru.pool.ntp.org time.windows.com" - задать в качестве NTP-серверов узлы **1.ru.pool.ntp.org** и **time.windows.com**

Утилита NSLOOKUP.EXE

Утилита **NSLOOKUP** присутствует во всех версиях операционных систем Windows и является классическим средством диагностики сетевых проблем, связанных с разрешением доменных имен в IP-адреса. NSLOOKUP предоставляет пользователю возможность просмотра базы данных DNS-сервера и построения определенные запросов, для поиска нужных ресурсов DNS. Практически, утилита выполняет функции службы DNS-клиент в командной строке Windows.

После запуска, утилита переходит в режим ожидания ввода. Ввод символа **?** или команды **help** позволяет получить подсказку по использованию утилиты.

Примеры использования:

nslookup - запуск утилиты
yandex.ru. - отобразить IP-адрес (а) узла с именем yandex.ru . Точка в конце имени желательна для минимизации числа запросов на разрешение имени к серверу DNS. Если завершающей точки нет, то NSLOOKUP сначала попытается разрешить указанное имя как часть доменного имени компьютера, на котором она запущена.
server 8.8.4.4 - установить в качестве сервера имен DNS-сервер Google с IP-адресом 8.8.4.4
yandex.ru. - повторить запрос с использованием разрешения имени DNS-сервером Google.
set type=MX - установить тип записи MX
yandex.ru. - отобразить MX-запись для домена yandex.ru - В примере узел обмена почтой для домена - mx.yandex.ru
mx.yandex.ru. - отобразить информацию по mx.yandex.ru
set type=A - установить тип записи в **A**

mx.yandex.ru - получить IP-адреса для mx.yandex.ru .
exit - завершить работу с nslookup

Возможно использование утилиты NSLOOKUP не в интерактивном режиме:

nslookup odnoklassniki.ru - определить IP-адрес узла odnokassniki.ru с использованием сервера DNS, заданного настройками сетевого подключения.
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)
nslookup 8.8.8.8 - определить имя узла, IP-адрес которого равен 8.8.8.8 с использованием DNS-сервера, заданного настройками сетевого подключения.

Команда nslookup - отдельная статья с описанием команды NSLOOKUP.

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 PING.EXE

PING.EXE - это, 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] конечноеИмя

Параметры:

-t - Непрерывная отправка пакетов. Для завершения и вывода статистики используются комбинации клавиш **Ctrl + Break** (вывод статистики), и **Ctrl + C** (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 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 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 искользовался 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 или адрес 0.0.0.0 для шлюза по умолчанию.

mask маска_сети - маска сети.

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 TELNET.EXE

На заре развития сети Интернет, сервис TELNET был основным средством удаленной работы пользователей, реализующим взаимодействие терминала с процессом на удаленном компьютере. На сегодняшний день, TELNET, в основном, используется как средство удаленного администрирования специализированных сетевых устройств. Сервис TELNET входит в состав практически всех сетевых операционных систем и реализован в виде программного обеспечения сервера Telnet и клиентской оболочки с текстовым или графическим интерфейсом. Подключившись к серверу, удаленный пользователь получает доступ к командной строке, поддерживаемой сервером, таким же образом, как если-бы он работал с локальным терминалом. Утилита TELNET работает поверх протокола TCP и позволяет пользователю подключиться к удаленному узлу не только на стандартный порт 23, но и на любой другой TCP-порт, тем самым, позволяя взаимодействовать с любым приложением, управляемым командной строкой. Так, например, с использованием утилиты **telnet** можно подключиться к серверам, поддерживающим текстовый (telnet-like) ввод команд и данных - SMTP, POP3, IMAP и т.п. Кроме этого, утилиту можно использовать в качестве средства грубой проверки возможности подключения на любой TCP-порт (проверки слушается ли определенный порт TCP).

При запуске TELNET.EXE без параметров, программа переходит в интерактивный режим, ожидая ввода команд пользователем. Для получения списка доступных команд используется ввод знака вопроса или **/h** . Набор доступных команд может отличаться для разных версий **telnet**, но всегда будут присутствовать команды подключения к удаленному узлу (**open**), закрытия существующего подключения (**close**), установки (**set**) и сброса (**unset** параметров.

set ? - отобразить текущие параметры сессии. Отображаются параметры, связанные с эмуляцией терминала, режима отображения вводимых символов (локального эха), интерпретацией управляющих последовательностей символов, способа аутентификации.

open 192.168.1.1 - подключиться к серверу TELNET узла 192.168.1.1

open 192.168.1.1 25 - подключиться к серверу, слушающему порт 25/TCP узла 192.168.1.1

После подключения к удаленному серверу, вводимые с клавиатуры символы будут передаваться на обработку удаленной системе и, для возврата в командную строку **telnet** , требуется ввод специальной комбинации клавиш переключения режима (Escape character) - по умолчанию это **CTRL-]** . Для выхода из telnet используется команда **quit**.

На практике, как правило, используется запуск telnet с параметрами по умолчанию и с указанием имени или IP-адреса и номера порта TCP удаленной системы.

telnet 192.168.1.1 - подключиться к серверу telnet узла 192.168.1.1

telnet yandex.ru 80 - подключиться к серверу HTTP (TCP порт 80) узла yandex.ru

Если подключение невозможно, то утилита **telnet** завершится сообщением:

Не удалось открыть подключение к этому узлу на порт . . . Сбой подключения.

Если имя или IP-адрес в командной строке достижимы, то такое сообщение говорит о том, что заданный порт не слушается удаленной системой (или закрыт брандмауэром) . Если же удаленная система не поддерживает текстовое (telnet-like) управление, то, как правило, соединение устанавливается, экран терминала остается пустым, и после нажатия любой клавиши, сессия может завершиться, но сообщения о сбое соединения не будет. В некоторых случаях, удаленный сервер, не поддерживающий телнетоподобный протокол может выдать баннер, отображая информацию о себе, как например, это делают серверы VNC, отбражая версию протокола RFB.
В операционных системах Windows 7, Windows Server 2008,Windows Server 2008 R2, для управления службой TELNET на локальном или удаленном компьютере можно воспользоваться специальной утилитой tlntadmn, позволяющей запустить, приостановить, остановить или продолжить работу сервера TELNET, а также настроить некоторые параметры его конфигурации.

В Windows 7 и более поздних версиях, сервер и клиент **telnet** при установке системы не инсталлируются. Для того, чтобы воспользоваться утилитой **telnet.exe**, нужно добавить ее в систему используя "Панель управления" – "Программы и компоненты" – "Включение или отключение компонентов Windows" – установить галочку на "Клиент Telnet". При необходимости, можно таким же образом установить и сервер Telnet.

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 пакетах, 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 . Подобные же настройки используются в сетях корпорации Microsoft . Для проверки, попробуйте выполнить трассировку маршрута к узлу microsoft.com .

□ Определение подмены адреса узла в файле hosts

Одним из последствий вирусного заражения довольно часто является блокировка доступа к сайтам антивирусных компаний, поисковым системам, популярным социальным сетям

(Vkontakte, Odnoklassniki, Facebook, Twitter и т.п.). Подобный же прием используется для кражи учетных данных пользователей путем перенаправления на вредоносный сайт, адрес которого берется из зараженного файла **hosts**.

Порядок преобразования доменных имен в IP-адреса следующий:

- проверяется наличие данных об имени в кэш службы разрешения имен (процедура определения IP по имени уже выполнялась, и в памяти есть актуальные результаты). Если запись есть, то будут использованы ее данные.

- проверяется наличие записи об имени и адресе в файле **hosts**. Если запись есть, то будут использованы ее данные.

- для разрешения доменного имени в IP-адрес выполняется запрос к серверу DNS, заданному в настройках сетевого подключения.

Файл **hosts** при настройках по умолчанию, находится в каталоге \Windows\system32\drivers\etc\ и обычно содержит строки, начинающиеся с символа # , являющиеся комментариями, и одну запись для определения имени узла петлевого интерфейса:

127.0.0.1 localhost

127.0.0.1 - IP-адрес, localhost - имя. Если добавить запись **127.0.0.1 odnoklassniki.ru**, то для имени odnoklassniki.ru будет использоваться адрес 127.0.0.1, который не предназначен для выполнения реальной передачи данных, и сервер с указанным именем станет недоступен. Если же вместо адреса 127.0.0.1 использовать адрес поддельного сервера, созданного злоумышленниками, то вместо реального сайта, соответствующего доменному имени, посетитель перейдет на поддельную страницу.
Структура записей файла **hosts** предполагает, что между адресом и соответствующим ему именем должен быть хотя бы один символ табуляции (пробел). Каждой записи отводится одна строка в файле **hosts**. Иногда, вредоносная программа выполняет смещение записей относительно отображаемой на экране части файла, заполняя видимую часть пробелами, а в непомещающейся в области просмотра части, могут присутствовать записи, например

31.214.145.172 odnoklassniki.ru
31.214.145.172 www.facebook.com
31.214.145.172 www.vk.com
31.214.145.172 www.vkontakte.ru

Данный адрес взят из реально зараженного файла **hosts** и принадлежит сети одного из провайдеров Германии. Сейчас он безопасен, и не занят обслуживанием вредоносного сервера.
На зараженном компьютере, в файл **hosts** было добавлено множество пустых строк, и поддельные записи располагались с разным смещением относительно начала строки, что могло затруднить ручной поиск. Кроме того, вредоносные программы могут использовать и некоторые другие способы подмены содержимого **hosts** - изменение местоположения самого файла, использование атрибута "скрытый" и имени с подменой символа на похожий по написанию символ национального алфавита - "о" и т.п. Другими словами, достоверно

определить сам факт подмены адреса с помощью файла **hosts**, путем прямого анализа содержимого реестра, системных каталогов и самого файла занимает довольно длительное время и не всегда позволяет исключить ошибку поиска вредоносных записей. А, тем временем, задача легко решается с использованием всего лишь 2-х команд из рассмотренных выше - **ping** и **nslookup** .

ping odnoklassniki.ru - в ответе на пинг будет отображаться адрес, соответствующий имени **odnoklassniki.ru** при определении IP-адреса на данном компьютере

nslookup odnoklassniki.ru - получить IP-адрес, соответствующий имени odnoklassniki.ru от сервера DNS.

Если адрес по результатам пинга отличается от адреса, полученного от DNS-сервера, то присутствует факт подмены содержимого файла **hosts**. Для некоторых крупных доменов утилита **nslookup** может выдавать список из нескольких IP. Тогда IP-адрес, полученный в результатах пинга, должен присутствовать в списке адресов от nslookup.

Иногда, в качестве способа блокировки определенных сайтов, используется добавление несуществующих статических маршрутов для соответствующих IP-адресов или подсетей, что легко отследить с помощью утилиты **tracert**

□ Как открыть порт в брандмауэре Windows 7-10

Разрешить входящие соединения через брандмауэр Windows (открыть порт) можно с использованием контекста **firewall** утилиты **netsh**

netsh firewall set portopening protocol=TCP port=27015 name=MyServer mode=ENABLE scope=ALL
или
netsh firewall set portopening TCP 27015 MyServer ENABLE ALL
protocol - Протокол порта. TCP (Transmission Control Protocol), UDP (User Datagram Protocol), ALL - Все протоколы.
port - Номер порта.
name - Имя порта (необязательно)
mode - Режим порта. ENABLE - Пропускать через брандмауэр (по умолчанию). DISABLE - Не пропускать через брандмауэр.
scope - Область порта (необязательно). ALL - Пропускать через брандмауэр весь трафик (по умолчанию). SUBNET - Пропускать через брандмауэр только трафик локальной сети (подсети). CUSTOM - Пропускать через брандмауэр только указанный трафик.

С учетом значений по умолчанию и необязательных параметров открыть TCP порт 27015 в брандмауэре Windows можно командой

netsh firewall set portopening TCP 27015

В Windows Vista/Windows7 пока поддерживается синтаксис приведенный в примере выше, однако в последующих версиях операционных систем он будет полностью заменен на контекст **netsh advfirewall** - управление улучшенным брандмауэром. Подсказку по использованию можно получить при вводе команды с параметром **?** (знак вопроса) :

netsh advfirewall ?

В контексте правил для брандмауэра:

netsh advfirewall firewall ?

Для открытия порта 27015 в Windows 7 с учетом нового синтаксиса правильнее использовать команду:

netsh advfirewall firewall add rule name="Open Port 27015" dir=in action=allow protocol=TCP localport=27015

add rule - добавить правило
name - название правила. Название может быть произвольным, и если текст содержит пробелы - заключаться в двойные кавычки. Имя правила не должно принимать значение **all**
dir - направление обмена данными (in-входящий трафик, out- исходящий)
action - действие по отношению к попадающему под правило соединению (allow - разрешить, block - запретить)
protocol - разновидность протокола. (TCP - протокол TCP, UDP - протокол UDP, ANY - любой протокол). Если параметр **protocol** не указан, то используется значение по умолчанию - ANY)
localport - номер порта на локальном компьютере. Можно указывать диапазон портов 0 - 65535 или any - любой порт или номера через запятую - 67,69 .
Примеры правил брандмауэра Windows 7-10

По сравнению с предыдущими версиями Windows синтаксис правил стал немного сложнее, но и возможности брандмауэра значительно расширились.
Краткий список возможных параметров правил :

add rule name=<строка>
dir=in|out
action=allow|block|bypass
[program=<путь к программе>]
[service=<краткое имя службы>|any]
[description=<строка>]
[enable=yes|no (по умолчанию - yes)]
[profile=public|private|domain|any[,...]]
[localip=any|||<подсеть>|<диапазон>|<список>]
[remoteip=any|localsubnet|dns|dhcp|wins|defaultgateway| ||<подсеть>|<диапазон>|<список>]
[localport=0-65535||<диапазон портов>[,...]|RPC|RPC-EPMap|IPHTTPS|any (по умолчанию - any)]
[remoteport=0-65535|<диапазон портов>[,...]|any (по умолчанию - any)]
[protocol=0-255|icmpv4|icmpv6|icmpv4:тип,код|icmpv6:тип,код| tcp|udp|any (по умолчанию - any)]
[interfacetype=wireless|lan|ras|any]
[rmtcomputergrp=<строка SDDL>]
[rmtusrgrp=<строка SDDL>]
[edge=yes|deferapp|deferuser|no (по умолчанию - no)]
[security=authenticate|authenc|authdynenc|authnoencap|notrequired (по умолчанию - notrequired)]

Некоторые правила применения параметров:

Параметры могут следовать в произвольном порядке - **dir=in action=allow** и **action=allow dir=in** являются допустимыми значениями.
Если указана удаленная группа пользователей или компьютеров, для параметра **security** необходимо установить значение **authenticate, authenc, authdynenc** или **authnoencap**.
Установка authdynenc в качестве значения параметра security позволяет системам динамически согласовывать использование шифрования трафика, соответствующего данному правилу брандмауэра Windows. Шифрование согласуется в соответствии со свойствами существующего правила безопасности соединения. Этот параметр позволяет компьютеру принять первый пакет TCP или UDP входящего соединения IPsec, при условии, что он защищен, но не зашифрован, с помощью IPsec. Как только первый пакет будет обработан, сервер повторно согласует соединение и обновит его, чтобы все последующие соединения были полностью зашифрованы.

Если action=bypass, должна быть указана группа удаленных компьютеров, если dir=in.

Короткое имя службы можно посмотреть в ее свойствах, в поле **Имя службы**. Так, для службы "DNS-клиент" короткое имя - Dnscache . Если service=any, правило действует только для служб.

Значением кода или типа ICMP может быть **any** - любой ICMP трафик.

Параметр **edge** можно указывать только для правил входящего трафика (dir=in) .

AuthEnc и **authnoencap** нельзя использовать вместе. Если задан параметр authnoencap, то параметр security=authenticate задавать необязательно.

Параметр **Authdynenc** допустим только в том случае, если значение dir равно in.

Примеры:

Добавление правила для входящего трафика для программы qip.exe:

netsh advfirewall firewall add rule name="allow QIP" dir=in program="c:\programfiles\qip\qip.exe" action=allow

Добавление правила, запрещающего исходящий трафик для TCP порта 80:

netsh advfirewall firewall add rule name="allow80" protocol=TCP dir=out localport=80 action=block

Добавление правила входящего трафика с требованием безопасности и шифрования для трафика через TCP-порт 80:

netsh advfirewall firewall add rule name="Require Encryption for Inbound TCP/80" protocol=TCP dir=in localport=80 security=authdynenc action=allow

Добавление правила входящего трафика для messenger.exe с требованием безопасности:

netsh advfirewall firewall add rule name="allow messenger" dir=in program="c:\program files\messenger\msmsgs.exe" security=authenticate action=allow

Добавление правила обхода брандмауэра с проверкой подлинности для группы acmedomain\scanners, определяемой строкой SDDL:

netsh advfirewall firewall add rule name="allow scanners" dir=in rmtcomputergrp=<строка SDDL> action=bypass security=authenticate

Добавление правила разрешения исходящего трафика для локальных портов 5000-5010 для udp:

netsh advfirewall firewall add rule name="Allow port range" dir=out protocol=udp localport=5000-5010 action=allow

Для просмотра всех правил брандмауэра используется команда:

netsh advfirewall firewall show rule name=all
netsh advfirewall firewall show rule name=all | more - с выдачей результатов на экран в постраничном режиме
netsh advfirewall firewall show rule name=all > C:\firewallrues.txt - с выдачей результатов в файл

Для просмотра конкретного правила указывается его имя. Для удаления правила используется параметр **delete**:

netsh advfirewall firewall show rule name=TEST просмотр правила с именем **TEST**
netsh advfirewall firewall delete rule name=test - удаление правила с именем **TEST**

Для изменения значений в существующих правилах используется параметр **set** и **new** перед изменяемым значением:

netsh advfirewall firewall set rule name="Allow port range" new localport=5000-6000 изменить диапазон портов для правила "Allow port range"

Настройками по умолчанию, в режиме повышенной безопасности брандмауэр Windows 7 блокирует все входящие подключения, не соответствующие ни одному правилу и разрешает исходящие.

Wi-Fi точка доступа стандартными средствами Windows 7-10

В операционной системе Windows 7 реализована технология **Virtual WiFi**, позволяющая легко создавать **программную точку доступа (Software Access Point - SoftAP)** . В отличие от полноценных беспроводных точек доступа, реализуемая таким образом SoftAP, позволяет создать только один виртуальный адаптер, который будет работать только в режиме точки доступа, и может быть использовано шифрование только по WPA2-PSK/AES. Тем не менее, этого вполне достаточно для создания функциональной беспроводной сети без реально существующей точки доступа. Такая сеть, обозначается как **Wireless Hosted Network**, или просто **Hosted Network** (**Размещенная Сеть**).

Для создания размещенной сети используется команды сетевой оболочки **netsh.exe** в

контексте **wlan**:

netsh wlan set hostednetwork [mode=]allow|disallow - разрешить или запретить использование размещенной сети.
netsh wlan set hostednetwork [ssid=]<идентификатор_SSID> [key=]<парольная_фраза> [keyUsage=]persistent|temporary - задать параметры размещённой сети.
ssid - идентификатор SSID сети, другими словами - имя беспроводной сети;
key - ключ безопасности, используемый в данной сети, т.е. парольная фраза, используемая при подключении клиентов к виртуальной точке доступа. Ключ должен быть строкой символов ASCII длиной от 8 до 63 знаков.
keyUsage - указывает, является ключ безопасности постоянным или временным. По умолчанию, ключ является постоянным (**persistent**) и используется при каждом включении размещенной сети.

Примеры:
set hostednetwork mode=allow
set hostednetwork ssid=ssid1
set hostednetwork key=passphrase keyUsage=persistent
set hostednetwork mode=allow ssid=MyWiFi key=MyPassWord
Или - одной командной строкой:

netsh wlan set hostednetwork mode=allow ssid=MyWiFi key=MyPassWord - создать виртуальную точку доступа Wi-Fi с именем **MyWiFi** и паролем **MyPassWord**

Созданная программная точка доступа не будет запущена автоматически. Для запуска потребуется выполнить команду :

netsh wlan start hostednetwork
Для остановки - **netsh wlan stop hostednetwork**

При использовании команд управления размещенной сетью требуются права администратора. Для организации доступа в Интернет с использованием размещенной сети можно воспользоваться совместным подключением через, созданный после выполнения команды создания размещенной сети , виртуальный сетевой адаптер - **Адаптер мини-порта виртуального WiFi Microsoft (Microsoft Virtual WiFi miniport adapter)** . Если же данный адаптер не обнаруживается в диспетчере учтройств и отсутствует в списке сетевых адаптеров, то наиболее вероятно, что драйвер реального Wi-Fi устройства не сертифицирован для использования в операционной системе Windows 7 и не поддерживает технологию **Virtual WiFi**.

Как получить список беспроводных сетей стандартными средствами Windows 7-10

Ниже приведено содержимое командного файла, который позволяет собрать список беспроводных сетей, включая имя, уровень сигнала, BSSID. Информация записывается в файл **wlans.txt** каталога временных файлов и открывается для просмотра с помощью редактора **wordpad**

```
chcp 1251
netsh wlan show networks mode=bssid > %TEMP%\wlans.txt
start "LIST" "%ProgramFiles%\Windows NT\Accessories\wordpad.exe"
%TEMP%\wlans.txt
```