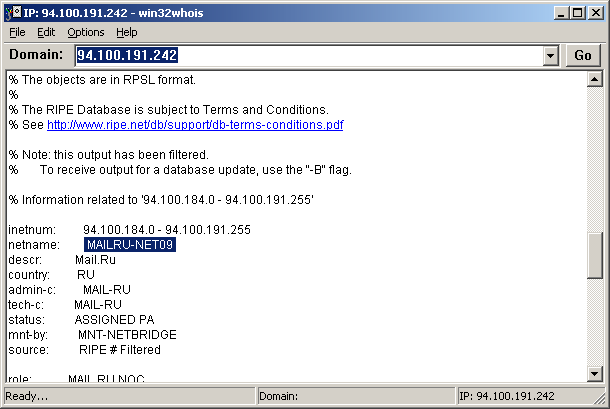
**Что делать, если причиной недоступности сайта является неправильное разрешение доменного имени.**

Определение IP-адреса по доменному имени (разрешение DNS-имени) выполняется в следующем порядке:  
  
- просматривается содержимое кэш службы разрешения имен. Если адрес уже разрешался раньше и в кэш данной службы присутствует соответствующая запись - будет использован IP-адрес из кэш . Данные в кэш хранятся определенное время и удаляются по мере старения или при перезапуске службы.  
  
- просматривается содержимое файла **hosts**, и если в нем имеется запись для данного имени, - используется заданный в ней IP-адрес. Этот файл обычно хранится в папке \windows\system32\drivers\etc\  
  
- выполняется запрос на разрешение доменного имени к серверу DNS, задаваемому в настройках сетевого подключения. Соединение выполняется по протоколу UDP на порт 53 сервера. Используется IP-адрес из ответа DNS - сервера.  
  
В первую очередь нужно определить, какому IP-адресу соответствует доменное имя сайта, который не открывается на данном компьютере. Самый простой способ - выполнить команду, например, для узла **mail.ru**:  
  
**ping mail.ru**  
  
Результат выполнения **ping**:  
  
**Обмен пакетами с mail.ru [94.100.191.242] по 32 байт:  
  
Ответ от 94.100.191.242: число байт=32 время=38мс TTL=54  
Ответ от 94.100.191.242: число байт=32 время=29мс TTL=54  
Ответ от 94.100.191.242: число байт=32 время=30мс TTL=54  
Ответ от 94.100.191.242: число байт=32 время=29мс TTL=54  
  
Статистика Ping для 94.100.191.242:   
Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),   
Приблизительное время передачи и приема:   
наименьшее = 29мс, наибольшее = 38мс, среднее = 31мс***На заметку. Некоторые узлы настроены таким образом, что блокируют протокол****ICMP****и не отвечают на эхо-запрос. В результатах выполнения команды будет сообщение об ошибке ("превышен интервал ожидания ответа" . . . ) Кроме того, довольно часто подобные настройки используются брандмауэрами на клиентских компьютерах, в сетях небольших провайдеров и т.п. Отсутствие ответа в результатах выполнения****ping****совсем не означает недоступность сайта.*  
  
Как видно из результатов выполнения **ping.exe**, доменному имени **mail.ru**, разрешенному на данном компьютере, соответствует IP-адрес = **94.100.191.242**. На следующем шаге нужно определить реальную принадлежность данного адреса домену **mail.ru** . Для этого можно воспользоваться онлайн - сервисами **Whois**, которые можно найти на сайтах интернет-провайдеров, хостинговых компаний, регистраторов доменных имен и т.п., или специальными программами, как например, [Win32Whois](http://ab57.ru/soft/win32whois.zip). В поле ввода заносится доменное имя или IP - адрес и нажимается кнопка **Go** или клавиша **Enter** 



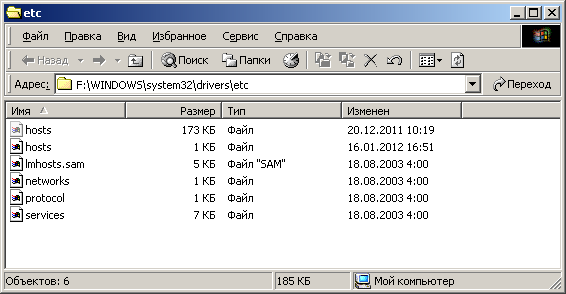
Как видим, IP-адрес **94.100.191.242** в самом деле принадлежит подсети **mail.ru**   
**inetnum: 94.100.184.0 - 94.100.191.255**Имя подсети:  
**netname: MAILRU-NET09**Описание:  
**descr: Mail.Ru**Если адрес сайта определяется верно, то проблема с созданием соединения по протоколу **HTTP** между вашим компьютером и сервером mail.ru. Локализация проблемы рассматривается во второй части статьи.  
  
Если же IP-адрес не определен или не имеет никакого отношения к подсети **mail.ru** то, очевидно, именно в этом кроется причина недоступности сайта. Здесь возможны различные варианты анализа ситуации и применяемых методик для ее исправления. 

**- IP адрес не может быть определен**

Если при выполнении **ping** получено сообщение, что не удалось обнаружить узел **mail.ru**, то это означает, что ни один из трех вышеперечисленных способов разрешения доменного имени не дал положительного результата. Поскольку в данном примере рассматривается случай недоступности только одного конкретного сайта, то причиной может быть лишь синтаксическая ошибка в имени или отсутствие записи в базе имен DNS-сервера. Если, например, в имени сервера букву **a**набрать в русской раскладке, то внешне, отображаемое на экране монитора имя сервера, останется прежним, но не будет соответствовать никакому IP-адресу. Второй вариант может быть вызван несколькими причинами:  
  
- повреждена или отсутствует запись в базе имен DNS-сервера, используемого в вашем сетевом подключении. Обычно - это DNS-сервер провайдера.   
  
- произошла подмена DNS-сервера вашего сетевого подключения сторонним (вредоносным) программным обеспечением. Этот вариант довольно экзотический, как и вариант с удалением записей из кэш службы разрешения имен. Особенно в среде Windows 7   
  
Для локализации проблемы можно воспользоваться классической утилитой **NSLOOKUP**. Данная утилита присутствует во всех версиях операционных систем семейства Windows и является основным средством диагностики сетевых проблем, связанных с разрешением доменных имен в IP-адреса. NSLOOKUP предоставляет пользователю возможность ручного просмотра базы данных DNS-сервера и построения определенные запросов для поиска нужных ресурсов. Практически, утилита выполняет функции службы DNS-клиент в командной строке Windows. В различных версиях операционных систем синтаксис командной строки может незначительно отличаться.  
  
После запуска, утилита переходит в режим ожидания ввода. Ввод символа **?** или команды **help** позволяет получить подсказку по использованию утилиты.  
  
Примеры использования:  
  
**nslookup** - запуск утилиты и ожидание ввода в команд.  
**mail.ru.**- отобразить IP-адрес (а) узла с именем mail.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 общедоступный DNS-сервер Google с IP-адресом 8.8.4.4 (также можно использовать адрес 8.8.8.8)  
**mail.ru.**- повторить запрос с использованием разрешения имени DNS-сервером Google.  
  
**exit**- команда завершения работы nslookup  
  
Возможно использование утилиты NSLOOKUP не в интерактивном режиме:  
  
**nslookup mail.ru**- определить IP-адрес узла mail.ru с использованием сервера DNS, заданного настройками сетевого подключения.  
**nslookup mail.ru 8.8.8.8** - определить IP-адрес узла mail.ru с использованием DNS-сервера 8.8.8.8 (публичный DNS-сервер Google)   
  
В рассматриваемом примере доменному имени **mail.ru** соответствует группа IP-адресов - это обычная ситуация для крупных доменов. Если доменное имя разрешается с использованием стороннего DNS - сервера, то проблема - в используемом по умолчанию сервере (обычно - DNS сервере вашего провайдера). Для смены используемого DNS сервера можно воспользоваться командой **netsh** (синтаксис для Windows 7):  
  
**netsh interface ipv4 set dnsservers name="Подключение по локальной сети 2" static 8.8.8.8 primary**  
  
Имя сетевого подключения ( **Подключение по локальной сети 2**) содержащее пробелы заключается в двойные кавычки. Изменения в настройках сетевого подключения можно также выполнить через панель управления, отменив в свойствах сетевого подключения автоматическое назначение DNS-серверов и заполнив поля адресов первичного и вторичного серверов DNS.   
  
В качестве публичных DNS-серверов, также, можно использовать:  
  
208.67.222.222  
208.67.220.220  
67.138.54.100  
207.225.209.66  
156.154.70.1  
156.154.71.1  
4.2.2.1 - 4.2.2.6

**- IP адрес сайта определяется неверно**

Здесь, как и в предыдущем случае, возможны варианты:  
  
- изменились сетевые настройки узла сайта и обновление зон DNS не вступили в силу. Система разрешения доменных имен довольно инерционна и, например, изменение IP-адреса сайта может отразиться на используемом DNS-сервере через несколько часов или даже больше.   
- технические неполадки на используемом DNS-сервере.   
- влияние вредоносного программного обеспечения.  
  
Первые 2 варианта можно разрешить таким же способом, как и рассмотренный выше. Желательно также в подобных случаях обратиться в службу технической поддержки серверов (обычно - к вашему провайдеру), поскольку они могут даже не знать о наличии данной проблемы.  
  
Третий вариант возникает тогда, когда произошло заражение компьютера вирусом, использующим блокировки определенных доменных имен, связанных с антивирусными средствами, поисковыми системами, сайтами социальных сетей и т.п. Нередко, даже после удаления вируса, проблема доступа к некоторым сайтам может оставаться и для ее решения одного антивирусного ПО окажется недостаточно.   
  
Самый простой способ блокировки сайтов - подмена содержимого специального файла **hosts**, используемого для определения IP-адресов для заданных имен . Как уже упоминалось выше, приоритет записи в **hosts** выше, чем данные, получаемые от DNS-сервера. Поэтому, если адрес узла определен в файле **hosts**, то будет использоваться именно он, а обращение к серверу имен выполняться не будет.   
  
Стандартно, в операционных системах семейства Windows, файл **hosts** находится в папке **\windows\system32\drivers\etc\** и представляет собой обычный текстовый файл с комментариями (строки, начинающиеся с символа **#**) и одной записью в виде:  
  
**127.0.0.1 localhost**  
  
Запись означает, что для имени **localhost** используется IP-адрес равный 127.0.0.1 Это, так называемый, **петлевой интерфейс ( или внутренняя петля (loopback)**, при сетевом обмене через который, реальная передача данных не выполняется. Обычно данный интерфейс используется для межпрограммной передачи данных по IP-протоколу внутри системы, когда и клиент, и сервер находятся на одном компьютере. Если в файл hosts, например, добавить строку: **127.0.0.1 mail.ru**  
  
то доменному имени mail.ru будет сопоставлен IP-адрес внутренней петли и сайт станет недоступным. Если же вместо адреса 127.0.0.1 указать, например, IP-адрес поддельного сервера, то посетитель попадет совсем не туда, куда он предполагал попасть. Данный прием нередко используется вредоносными программами для воровства паролей с применением метода подмены страниц регистрации пользователей популярных социальных сетей (vk.com, odnoklassniki.ru, mail.ru... и т.п.)   
  
Нередко встречаются случаи изменения не содержимого файла hosts, а его местонахождения. Стандартный файл в этом случае остается без изменения, но для разрешения имен в IP-адреса, будет использоваться не он, а совсем другой файл **hosts**, размещенный в любом подкаталоге файловой системы. Расположение файла **hosts** определяется содержимым парметра реестра  
  
**HKLM\System\CurrentControlSet\services\Tcpip\Parameters\DataBasePath**  
  
Стандартное значение - строка типа REG\_EXPAND\_SZ **%SystemRoot%\System32\drivers\etc**т.е. указывает на каталог, где должен находиться файл **hosts**. Если запись изменить, например, на %TEMP% то для определения IP-адресов узлов будет использоваться файл hosts из каталога, заданного значением переменной TEMP (каталог временных файлов). Значение переменной TEMP можно посмотреть с использованием команд:  
  
**echo %temp%**или  
**set temp**  
  
Вполне понятно, что в большинстве случаев, пользователи проверяют содержимое стандартно размещенного файла **hosts**, не предполагая того, что в разрешении имен используется совсем другой файл.  
  
Довольно необычный подход к подмене содержимого файла hosts появился в некоторых вредоносных программах, в частности, семейства Win32/Vundo. Троянец переименовывает "настоящий" файл hosts в файл hоsts, где латинская буква "o" заменена на точно такую же по отображаемому виду, кириллическую "o" и создает поддельный **скрытый** файл hosts, с правильным именем и поддельным содержанием. Естественно, файл, имя которого содержит русскую букву "о", в разрешении доменных имен не принимает никакого участия и предназначен для введения в заблуждение пользователя, который попытается проверить его содержимое. При ручном просмотре каталога **%SystemRoot%\System32\drivers\etc**( стандартно C:\windows\system32\drivers\etc) пользователь либо видит единственный файл hоsts (c измененной буквой в имени) , либо, если включен режим отображения скрытых файлов, - два, одинаковых по написанию имени, файла hosts. 



Файловая система Windows не позволяет создать 2 файла с одним и тем же именем. Просто один из них, размером 173 кб и имеющий атрибут "скрытый" - это измененный вирусом файл с правильным именем, а второй - файл, в имени которого изменена латинская буква "o" на русскую букву "о". В файле с неверным именем, который не будет использоваться для разрешения имен в IP-адреса, вирус оставил его исходное содержание, а в файл с правильным - занес нужные для перенаправления записи вроде:   
  
31.214.145.172 mail.ru - для подмены адреса сайта mail.ru  
127.0.0.1 avast.com - для блокировки доступа к сайту антивируса Avast!  
  
Сайты - подделки , как правило, через короткое время удаляются или блокируются и вместо поддельного сайта посетитель получает недоступный.   
  
В дополнение.   
  
*Для выяснения причин недоступности сайта удобно использовать общедоступные прокси- серверы.*[*Здесь подробности и свежие списки прокси.*](http://ab57.ru/proxylist.html)*Дело в том, что при заходе на сайт через прокси сервер, разрешении имен в адреса выполняется программными средствами прокси, а не с использованием службы разрешения имен вашего компьютера. Если через прокси сайт доступен, то проблему нужно искать на вашем компьютере. Если же сайт не доступен и через прокси - возможны варианты, как, например, реконструкция или технические работы, DDoS - атака на сайт, блокировка сайта прокси-сервером в соответствии с его политикой доступа, блокировка по финансовым причинам и т.п. Удобнее всего использовать анонимайзеры (eevropa.ru, http://2ip.ru/anonim/ , http://www.kalarupa.com/ и др.)*

**Что делать, если причиной недоступности сайта является невозможность соединения по протоколу HTTP**

    Для того, чтобы сразу исключить браузер из списка возможных причин невозможности открытия страниц сайта, можно выполнить ручное TCP-подключение на порт 80 проблемного сервера с помощью утилиты **telnet**.   
  
**telnet mail.ru 80**- подключиться на порт 80 сервера mail.ru.   
  
В случае удачного подключения вы увидите пустой черный экран. Если подключения невозможно выполнить - программа выдаст сообщение об ошибке (сбой подключения). Для выхода из **telnet.exe** нужно нажать комбинацию клавиш **Ctrl+]** и ввести команду **exit**. В Windows 7, при стандартной установке системы, утилита **telnet.exe** отсутствует, что создает некоторые неудобства в работе системного администратора, поскольку она часто используется для конфигурирования сетевых устройств и является быстрым и удобным средством проверки доступности TCP-порта. Для установки **telnet.exe** нужно перейти в **Панель управления - Программы и компоненты.** В левой части окна выбрать пункт **Включение или отключение компонентов Windows** и в списке компонентов установит флажок для "Клиент Telnet" .  
  
Если подключение на порт TCP 80 проблемного сайта выполняется с помощью **telnet** без ошибок, то причиной недоступности сайта с большой долей вероятности, можно считать используемый браузер (настройки безопасности, подключаемые модули антивирусов и блокировщиков рекламы, модули контроля и т.п.).   
  
Вредоносные программы довольно часто для блокировки определенных сайтов, используют создание ложных статических маршрутов в таблице маршрутизации. При этом, некоторые IP-адреса (группы адресов) становятся также недостижимыми.  
  
    Если, в рассматриваемом выше примере, подмены адреса сайта ложным содержимым файла hosts не произошло, то при разрешении доменного имени будет получен правильный IP - адрес сервера, который, естественно, не принадлежит диапазону адресов локальной сети, т.е не достижим локально и программные средства IP-протокола на вашем компьютере должны будут установить соединение с сайтом через **маршрутизатор (шлюз)**Обычно это выполняется через **шлюз по умолчанию** (default gateway), задаваемый в настройках сетевого подключения. Все соединения на серверы, адреса которых не принадлежат диапазону вашей сети, выполняются через него. Но таблица маршрутов может содержать и специально заданные маршруты для обмена с другими сетями, недоступными через шлюз по умолчанию. Приоритет таких маршрутов выше приоритета шлюза по умолчанию. Если в таблицу маршрутизации добавить статический маршрут, задающий путь для конкретного IP-адреса (или подсети), то подключение будет выполняться через указанный в этом маршруте, шлюз (маршрутизатор). И если такого маршрутизатора не существует или он неработоспособен, - подключение к серверу сайта не выполнится. Именно такой прием и используется вредоносными программами для блокировки отдельных узлов или подсетей.   
  
    Статические маршруты задают путь для достижения конкретного узла и сохраняются в разделе реестра**HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PersistentRoutes**  
Для добавления постоянного маршрута обычно используется команда **route add** с параметром /P или прямая запись в данный раздел реестра, что обычно и делается вредоносными программами. При отсутствии статических маршрутов данный раздел не содержит никаких записей.  
Посмотреть таблицу маршрутизации можно с использованием команды :   
  
**route print**  
  
В ответ вы получите данные о сетевых интерфейсах и таблицу маршрутизации:  
  
**===========================  
Список интерфейсов  
0x1 ...................... MS TCP Loopback interface  
0x10003 00 1a 92 b3 a8 0d Network adapter Broadcom 802.11g  
===========================  
===========================  
Активные маршруты:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Сетевой адрес  0.0.0.0  127.0.0.0  192.168.1.0  192.168.1.3  192.168.1.255  224.0.0.0  255.255.255.255** |  | **Маска сети  0.0.0.0  255.0.0.0  255.255.255.0  255.255.255.255  255.255.255.255  240.0.0.0  255.255.255.255** |  | **Адрес шлюза  192.168.1.1  127.0.0.1  192.168.1.3  127.0.0.1  192.168.1.3  192.168.1.3  192.168.1.3** |  | **Интерфейс  192.168.1.3  127.0.0.1  192.168.1.3  127.0.0.1  192.168.1.3  192.168.1.3  192.168.1.3** |  | **Метрика  1  1  1  1  1  1  1** |  |  |

**Основной шлюз: 192.168.1.1  
======================  
Постоянные маршруты:   
Отсутствует**Это нормальная таблица для компьютера с одной сетевой картой и настройкой сетевого подключения:   
**IP-адрес 192.168.1.3   
маска 255.255.255.0   
шлюз по умолчанию 192.168.1.1**Эти настройки соответствуют одному из наиболее распространенных вариантов локальной сети с IP-адресацией -   
**192.168.1.0 / 255.255.255.0**  
Данная запись означает адрес сети - 192.168.1.0 и маска 255.255.255.0 - сеть может включать в свой состав узлы, старшая часть адреса которых одинакова (первые 3 байта маски принимают значение 1 во всех разрядах или 0xFF в шестнадцатеричной системе счисления или 255 в десятичной) а младшая принимать значения 1-254. Самый младший адрес 192.168.1.0 называется адресом сети, а самый старший - 192.168.1.255 - широковещательным адресом. Первый адрес не может использоваться для обмена данными и пакет, отправленный на этот адрес не будет принят никем, а пакет, отправленный на широковещательный адрес - будет принят всеми. Обмен данными между "своими" узлами определяется маршрутом   
  
**Сетевой адрес - 192.168.1.0 Маска сети - 255.255.255.0 Адрес шлюза - 192.168.1.3 Интерфейс - 192.168.1.3 Метрика - 1**   
  
Что означает, что для обмена с адресами 192.168.1.0 - 192.168.1.255 в качестве адреса шлюза используется адрес своей сетевой карты (192.168.1.3) и ее же сетевой интерфейс, т.е. пакет отправляется напрямую адресату   
Если же адрес не принадлежит диапазону 192.168.1.0-192.168.1.255, то программные средства протокола отправят такой пакет данных маршрутизатору для передачи в другую сеть. При отсутствии статических маршрутов, адрес маршрутизатора будет равен адресу шлюза по умолчанию (default gateway) - в данном случае - 192.168.1.1 . Пакет будет отправлен ему и от него дальше - маршрутизатору в сети интернет-провайдера и далее в соответствии с его таблицей маршрутов, пока не будет доставлен адресату.  
  
Это несколько упрощенное представление, но для понимания принципа блокировки некоторых сайтов вредоносными программами, вполне достаточное. Мне приходилось сталкиваться с такой ситуацией, когда таблица маршрутизации обычного домашнего компьютера с одной сетевой картой содержала не несколько строк, а несколько сотен строк вида:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Сетевой адрес  74.55.40.0  74.55.74.0  74.55.143.0  74.86.125.0  74.86.232.0** |  | **Маска сети  255.255.255.0  255.255.255.0  255.255.255.0  255.255.255.0  255.255.255.0** |  | **Адрес шлюза  192.168.1.0  192.168.1.0  192.168.1.0  192.168.1.0  192.168.1.0** |  | **Интерфейс  192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2** |  | **Метрика  1  1  1  1  1** |  |  |

...   
  
В соответствии с первой строкой при соединении с адресами 74.55.40.0 - 74.55.40.255 будет использоваться адрес маршрутизатора 192.168.1.0, т.е. адрес, который является номером сети и никак не может быть использован при обмене данными. Программные средства IP-протокола, определив, что IP-адрес из этого диапазона, например, 74.55.40.226, принадлежащий серверу антивирусного продукта Avast!, не входит в диапазон адресов собственной локальной сети и проверят наличие статического маршрута для нее. Если бы этой записи не было в таблице маршрутизации, то обмен пошел бы через шлюз по умолчанию, но статический маршрут имеет более высокий приоритет и как раз для того и предназначен, чтобы использовать конкретный шлюз, а не общий, принятый для всех внешних (по отношению к своей сети ) адресатов. А поскольку такого шлюза не существует, сервер avast.com с IP=74.55.40.226 станет недоступным для данного компьютера. Если быть точным, то у avast несколько десятков серверов, и конкретно этот адрес принадлежит узлу a529sm.avast.com. При чем в соответствии с маской 255.255.255.0 станут недоступными все адреса в диапазоне 74.55.40.0 - 74.55.40.255, куда попадают не только адреса серверов антивирусной компании, но и адреса других узлов, не имеющих к ней никакого отношения.   
Последующие строки в таблице маршрутизации заблокируют новый диапазон IP-адресов   
74.55.143.0 - 74.55.143.255  
74.86.125.0 - 74.86.125.255  
И т.д.   
При чем, в одном конкретном случае, таблица маршрутизации содержала более 400 записей подобного вида, что позволило заблокировать более 100000 адресов узлов. Естественно, авторы вируса не особо заботились тем фактом, что кроме антивирусных серверов блокируется и доступ к сайтам, не имеющим к ним никакого отношения. В их числе оказались довольно популярные ресурсы. Мне приходилось сталкиваться с такими случаями, когда "под раздачу" попадали mail.ru, odnoklassniki.ru, vk.com, интернет-поисковики и торрент-трекеры, т.е. популярные ресурсы, регулярно посещаемые пользователями. В какой-то степени, это даже можно считать удачей, поскольку, недоступность случайно посещаемых сайтов, вряд ли была бы логически связана с последствиями вирусного заражения.   
  
    Для исправления ситуации нужно просто удалить неверные маршруты из таблицы маршрутизации. Для этого используется та же команда **route** выполняемая с ключом **delete** и привилегиями администратора. Кстати, если бы пользователь работал под обычной пользовательской учетной записью, заражения могло бы и не произойти, а таблица маршрутизации почти наверняка, осталась бы нетронутой. В подавляющем большинстве случаев, главной причиной успешного внедрения вируса в систему является работа пользователя под учетной записью с правами администратора.   
  
**route delete 74.55.40.0**- удалит первый маршрут в примере.   
**route delete 74.55.74.0** - удалит второй   
и т.д.   
  
Процесс можно упростить, выдав таблицу маршрутизации в файл с использованием перенаправления вывода:  
  
**route print > C:\routes.txt**   
  
После выполнения команды на диске C: будет создан текстовый файл routes.txt с таблицей маршрутизации. Не обращайте внимания на нечитаемые символы в DOS-кодировке - они вам не нужны. Остается удалить лишнее и перед каждым маршрутом добавить route delete. После чего остается переименовать расширение файла в .bat или .cmd и запустить его на выполнение двойным щелчком. Для тех кто пользуется файловым менеджером **FAR** задача значительно упрощается. Встроенный редактор FAR, вызываемый по F4 позволяет выделять прямоугольник текста и вырезать его, что позволит быстро отсечь правую часть после адреса. Затем можно выполнить замену всех пробелов на пустой символ (комбинация CTRL-F7), и занести пробел в первую позицию каждой строки. После чего с помощью CTRL-F7 заменить его на route delete (с пробелом после delete). В результате у вас должен получиться командный файл со строками :   
  
**route delete 74.50.0.0  
route delete 74.52.233.0  
route delete 74.53.70.0  
route delete 74.53.201.0  
route delete 74.54.46.0  
...**  
    При большом количестве поддельных записей в таблице маршрутизации, удалять статические маршруты вручную долго и трудно, поэтому, есть смысл воспользоваться командой **route** с ключом **-f**.   
  
**route -f**  
  
Параметр **-f** используется для удаления из таблицы маршрутизации всех записей, которые не являются узловыми маршрутами (маршруты с маской подсети 255.255.255.255), сетевым маршрутом петлевого интерфейса (маршруты с конечной точкой 127.0.0.0 и маской подсети 255.0.0.0) и маршрутами для широковещательной рассылки (с сетевым адресом 255.255.255.255).   
Таким образом, маршруты, добавленные вирусом, будут удалены. Естественно, будут удалены и вручную прописанные статические маршруты (если они у вас были) и шлюз по умолчанию (основной шлюз), что приведет к временной недоступности сети. Для пересоздания таблицы маршрутизации на данной конфигурации сетевых интерфейсов, можно просто остановить и снова запустить сетевые адаптеры или перезагрузить систему. После перезагрузки, нормальный доступ в сеть должен быть восстановлен.  
  
Восстановление настроек TCP/IP можно выполнить с помощью антивирусной утилиты AVZ (Пункт 20 меню восстановления системы "Настройки TCP/IP. Удалить статические маршруты").  
  
    Кроме подмены содержимого файла hosts и внедрения ложных статических маршрутов, для блокировки доступа к определенным IP может использоваться подмена адреса используемого DNS-сервера на адрес поддельного, или изменение настроек браузера таким образом, чтобы подключение выполнялось через вредоносный прокси-сервер, что, впрочем, чисто теоретически возможно, но на практике не встречается. 

    Статистика Ping дает полную картину обмена между вашим компьютером и пингуемым узлом. Поле TTL в эхо-ответе зависит от реализации IP-протокола отвечающего узла (упрощенно, можно считать, что от типа и версии операционной системы). Необходимо учитывать, что некоторые узлы настроены таким образом, что на ping не отвечают (microsoft.com, например)   
  
Еще примеры использования ping.exe:  
  
**ping -t yandex.ru** - выполнять ping до нажатия комбинации CTRL-C или CTRL-Break  
**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 yandex.ru** - выполнить ping 1 раз (ключ -n 1), определять адрес по имени (ключ -a), выдавать маршрут для первых 9 переходов (-r 9)  
  
    Использование ключа **-r**, в какой-то степени, позволяет получить трассировку маршрута, аналогичную получаемой с помощью команды tracert.exe, но максимальное число переходов может быть равно 9, чего, обычно, бывает недостаточно. Поэтому желательно использовать tracert.exe.   
  
**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.  
  
  
    Напомню, как это работает. При разработке IP-протокола, для достижения узлов, адреса которых не принадлежат текущей сети, была предусмотрена маршрутизация, предназначенная для передачи IP-пакетов между разными сетями. Когда вы выполняете команду "tracert google.com", сначала определяется IP-адрес google.com (74.125.45.100), который не принадлежит диапазону адресов вашей локальной сети, задаваемого значением IP-адреса сетевой карты и маской подсети (192.168.1.0-192.168.1.255). Такой пакет будет отправлен маршрутизатору, адрес которого, задан в качестве шлюза по умолчанию. В результатах трассировки вы видите его первым (192.168.1.1). Затем (упрощенно конечно) работает тот же алгоритм - если узел google.com не достижим локально, определяется, через какой маршрутизатор должен быть отправлен пакет, и выполняется его отправка.   
    В результатах трассировки, приведенных выше для достижения узла google.com понадобилось 18 переходов. А теперь представьте, что на узле номер 10 (209.85.255.178) для достижения узла google.com ошибочно прописан маршрут не к узлу номер 11, а например, к узлу номер 5. Результатом такой ошибки стало бы зацикливание и вечное циркулирование пакета между узлами 5 и 10. Для того, чтобы подобная ситуация не возникала, разработчики IP-протокола предусмотрительно ввели в заголовок IP-пакетов поле TTL ("Время жизни" - Time To Live) длиной в 1 байт, принимающее значения от 0 до 255. 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).   
    При выполнении команды tracert.exe сначала выполняется отправка ICMP пакета с полем TTL равным **1** и первый в цепочке маршрутизатор (ваш модем) обнуляет TTL 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, т.е. ваш модем)  
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** - ваш маршрутизатор его уменьшит до 1 и отправит следующему в цепочке - т.е. маршрутизатору провайдера. Тот после вычитания 1 обнулит TTL и сообщит о превышении времени жизни. И так далее, пока не будет достигнут заданный узел (google.com) или не будет обнаружена неисправность, не позволяющая доставить пакет получателю.  
    В результатах трассировки могут присутствовать записи об узлах в виде звездочек (узел номер 3 в примере) - это не является признаком неисправности и скорее всего, говорит о том, что настройки данного узла запрещают ICMP-протокол из соображений безопасности (борьба с DDoS - атаками)