Лабораторная работа №7

Определение параметров сетевого соединения компьютера и использование сетевых утилит ОС

1. Теоретическая часть

Сейчас любая локальная сеть, как правило, имеет подключение к глобальной сети Интернет. В Интернет передача данных осуществляется с помощью протоколов TCP/IP(Transmission Control Protocol/Internet Protocol) и в локальной сети эти протоколы оказываются также необходимы. Но использование протоколов стека TCP/IP позволяет решать и задачи обмена информацией между локальными компьютерами. Применение в локальных сетях протоколов TCP/IP сближает их с глобальными компьютерными сетями в смысле использования подобных способов адресации и методов администрирования.

1.1 IP-адресация

Передача сообщений в Интернет основана на том, что каждый компьютер сети имеет индивидуальный адрес – IP-адрес. Этот адрес выражается одним 32-разрядным числом, имеющим две смысловые части. Одна часть IP-адреса определяет номер сети, вторая – номер узла(компьютера) в сети. Так как оперировать длинными двоичными числами достаточно сложно, число, определяющее IP-адрес, разбивают на 4 октета – восьмиразрядных двоичных числа, а каждое из этих чисел представляют в десятичном виде. Октеты отделяют друг от друга точками. Таким образом, 32-разрядный IP-адрес представляется в виде: 255.255.255.255 (десятичное число может меняться от 0 до 255 – максимального значения восьмиразрядного двоичного числа). Например: 128.10.2.30 – десятичная форма представления IP-адреса, 10000000 00001010 00000010 00011110 – двоичная форма представления этого же адреса.

В сети Интернет различные глобальные сети, в зависимости от размера, делятся по классам:

- Сети класса A: большие сети общего пользования, первый октет определяет номер сети, три последующие октета – номер узла;
- Сети класса B: сети среднего размера. Два первых октета определяют номер сети, два оставшихся – номер узла;

- Сети класса С: сети малого размера. В этих сетях три первых октета определяют номер сети и последний октет – номер узла.

В таблице 1 представлена общая характеристика схемы Интернет-адресации.

Таблица 1

Класс	**Диапазон значений первого октета**	**Общее количество сетей**	**Максимальное количество узлов в каждой сети**
A	1 – 126	126	16 777 214
B	128 – 191	16 382	65 534
C	192 – 223	2 097 150	254

Некоторые IP-адреса имеют специальное назначение, например, адрес:

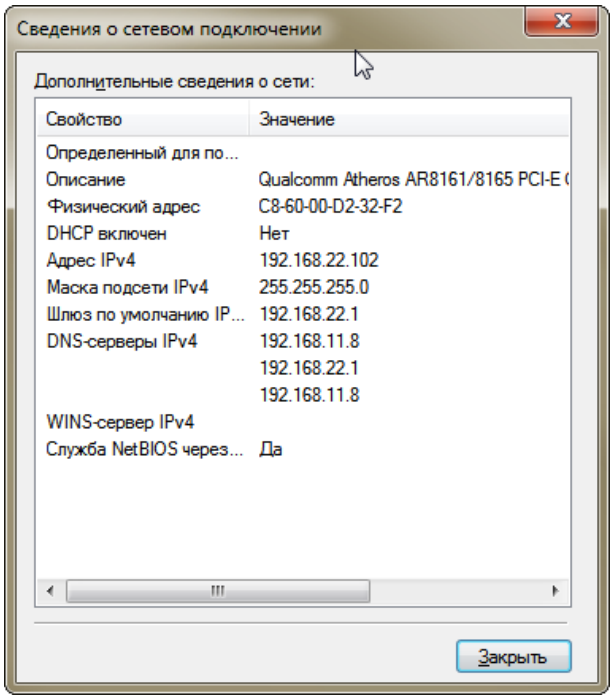
- 0.0.0.0 представляет адрес шлюза по умолчанию, т.е. адрес компьютера, которому следует направлять информационные пакеты, если они не нашли адресата в локальной сети;
- 127.любое число (часто 127.0.0.1) – адрес «петли». Данные, переданные по этому адресу, поступают на вход компьютера, как полученные по сети. Такой адрес необходим при отладке сетевых программ;
- 255.255.255.255 – широковещательный адрес. Сообщения, переданные поэтому адресу, получают все узлы локальной сети, содержащей компьютер-источник сообщения (в другие локальные сети оно не передается);
- Номер сети . все нули – адрес сети;
- Все нули . номер узла – узел в данной сети. Может использоваться для передачи сообщений конкретному узлу внутри локальной сети;
- Номер сети . все единицы (двоичные) – все узлы указанной сети, broadcast address.

В локальных сетях используются специальные, так называемые «серые» IP-адреса. Они определены документом RFC 1918 (RFC – Requests For Comments, предлагаемый проект стандарта, большинство документов, регламентирующих Интернет, описано в RFC) и приведены в табл. 2:

Таблица 2

Диапазоны IP-адресов, используемых в локальных сетях
10.0.0.0 − 10.255.255.255
172.16.0.0 − 172.31.255.255
192.168.0.0 − 192.168.255.255

В небольших по размеру локальных сетях обычно применяется последний диапазон адресов. Сетевые маршрутизаторы не передают информацию для узлов с этими адресами, поэтому она оказывается «запертой» внутри локальной сети. Такая схема позволяет в разных локальных сетях использовать одни и те же IP-адреса и не приводит к конфликтам.



Для повышения гибкости использования IP-адресов деление адреса на части с использованием классов дополняется технологией CIDR (Classless Inter Domain Routing) – бесклассовой междоменной маршрутизации. В этом случае адрес сети формируется с помощью двух чисел: адреса и маски. Маска это тоже 32-разрядное двоичное число, с помощью которого из IP-адреса выделяется адрес сети. Схема формирования адреса сети с использованием маски проста, ее можно пояснить на примере, допустим, адрес представлен двоичным числом 110101, маска числом 111100. Маска накладывается на адрес, как трафарет, в котором единицы соответствуют прорезям, в которых мы «увидим» адрес сети, в нашем примере адрес сети соответствует числу 110100. Маска всегда содержит такое двоичное число, старшие разряды которого подряд единицы, а младшие – нули, единицы представляют «прозрачную» часть трафарета, а нули – «непрозрачную». Маска так же, как и адрес, записывается в виде четырех десятичных чисел, разделенных точками и представляющих двоичные октеты.

Для компактной записи пары чисел: IP-адрес-маска, используется также другая форма, например: 10.0.0.8/30. Число до слеша представляет собой IP-адрес, а число после слеша – количество разрядов в IP-адресе, отводимых для адресации сети. Число 30 после слеша

соответствует маске 255.255.255.252. После определения адреса сети, оставшаяся часть IP-адреса используется для адресации узлов в сети.

1.2 Символьное представление имени компьютера в сети

Каждый компьютер в сети имеет уникальный адрес. При использовании IP-адресации это IP-адрес. Однако человеку достаточно трудно оперировать длинными наборами цифр, не несущих смысловой нагрузки, поэтому всегда применяются системы преобразования имен, ставящие в соответствие цифровому адресу компьютера его символьное имя. В глобальных сетях и сети Интернет это служба DNS (Domain Name System) − распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Интернет. Определенные части базы данных доменных имен хранятся на специальных серверах − DNS-серверах, обрабатывающих запросы любого компьютера и определяющие имя, соответствующее IP-адресу или наоборот. В каждой локальной сети, подключенной к Интернет, работает по крайней мере один DNS-сервер. База данных DNS имеет структуру дерева, называемого доменным пространством имен, в котором каждый домен (узел дерева) имеет имя и может содержать поддомены. Имя домена идентифицирует его положение в этой базе данных по отношению к родительскому домену, а точки в имени отделяют части, соответствующие узлам домена, например, www.miet.ru . Для именования компьютеров в локальных сетях используются плоские (не имеющие иерархии) символьные имена, так называемые NetBIOS-имена. Протокол NetBIOS (Network Basic Input/Output System), как расширение стандартных функций базовой системы ввода-вывода, был разработан в 1984г. компанией IBM и широко применяется в ее продуктах, а также продуктах компании Microsoft. В протоколе NetBIOS реализован механизм широковещательного разрешения имен, когда все компьютеры в локальной сети получают запрос на разрешение имени, соответствующего некоторому IP-адресу. Кроме того, компания Microsoft для своей сетевой операционной системы Windows NT разработала централизованную службу разрешения имен WINS(Windows Internet Name Service). WINS-сервер, работающий в локальной сети, централизованно обрабатывает все запросы, касающиеся разрешения имен в сетях Windows. При большом числе компьютеров в локальной сети WINS-сервер необходим. Однако в малых сетях, содержащих менее 10 компьютеров, часто используется широковещательный механизм разрешения имен протокола NetBIOS, упрощающий административное обслуживание таких сетей.

1.3 Автоматизация процесса назначения IP-адресов узлам сети

IP-адреса могут назначаться администратором сети вручную. Это представляет для администратора достаточно сложную и длительную процедуру, если количество компьютеров в локальной сети достаточно велико. Если происходят изменения в сети, например, появляются новые компьютеры, процедуру необходимо выполнить и для них, а в некоторых случаях и выполнить коррекцию предыдущих настроек на уже работающих компьютерах. Протокол DHCP (Dynamic Host Configuration Protocol) был разработан для того, чтобы освободить администратора от этих проблем. Основным назначением DHCP является динамическое назначение IP-адресов. В локальной сети, содержащей DHCPсервер, каждый компьютер при включении посылает запрос этому серверу на получение IP-адреса. Способы выдачи адресов могут быть различными. При автоматическом статическом способе выделения адреса DHCP-сервер присваивает IP-адрес (и, возможно, другие параметры конфигурации клиента) из пула (набора) наличных IP-адресов. Границы пула назначаемых адресов задает администратор при конфигурировании DHCP-сервера. Между идентификатором клиента и его IP-адресом в этом случае, как и при ручном назначении, существует постоянное соответствие. При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время (время подключения к сети), что дает возможность впоследствии повторно использовать этот же IP-адрес другими компьютерами (пользователями).

1.4 Адресация компьютеров на канальном уровне

Каждый компьютер, подключенный к сети, имеет сетевой адаптер (сетевую карту) с присвоенным ему адресом. Этот адрес носит название MAC-адреса, он задается при изготовлении сетевого адаптера и впоследствии не изменяется. Длина и другие особенности MAC-адреса зависят от используемой в локальной сети технологии. В сетях Ethernet MAC-адрес имеет длину 6 байт, записанных в шестнадцатеричном формате и разделенных дефисами (например, 00-AA-00-4F-2A-9C). Для определения локального адреса по IP-адресу используется протокол разрешения адреса ARP (Address Resolution Protocol). Существует также протокол, решающий обратную задачу − нахождение IP-адреса по известному локальному адресу. Он называется RARP − реверсивный ARP, и используется при старте бездисковых станций, не знающих в начальный момент своего IP-адреса, но знающих адрес своего сетевого адаптера. Необходимость в обращении к протоколу ARP возникает каждый раз, когда модуль IP передает пакет на уровень сетевых

интерфейсов, например драйверу Ethernet. IP-адрес узла назначения известен модулю IP. Требуется на его основе найти MAC-адрес узла назначения. Работа протокола ARP начинается с просмотра так называемой ARP-таблицы.

```
Интерфейс: 192.168.22.102 --- 0xb
  адрес в Интернете      Физический адрес      Тип
  169.254.75.86         38-ea-a7-08-a3-ff     динамический
  192.168.22.1          00-22-4d-7f-c8-fb     динамический
  192.168.22.5          00-24-01-e9-97-29     динамический
  192.168.22.49         50-46-5d-90-22-56     динамический
  192.168.22.100        c8-60-00-d2-33-4c     динамический
  192.168.22.101        c8-60-00-d2-32-7b     динамический
  192.168.22.103        c8-60-00-d2-32-87     динамический
  192.168.22.104        c8-60-00-d2-33-44     динамический
  192.168.22.106        c8-60-00-97-aa-df     динамический
```

Каждая строка таблицы устанавливает соответствие между IP-адресом и MAC-адресом. Поле «Тип записи» может содержать одно из двух значений − «динамический» или «статический». Статические записи создаются вручную с помощью утилиты arp и не имеют срока устаревания, точнее, они существуют до тех пор, пока компьютер или маршрутизатор не будут выключены. Динамические же записи создаются модулем протокола ARP, использующим широковещательные возможности локальных сетевых технологий. Динамические записи должны периодически обновляться. Если запись не обновлялась в течение определенного времени (порядка нескольких минут), то она исключается из таблицы. Таким образом, в ARP-таблице содержатся записи не обо всех узлах сети, а только о тех, которые активно участвуют в сетевых операциях. Поскольку такой способ хранения информации называют кэшированием, ARP-таблицы иногда называют ARP-кэш. после того как модуль IP обратился к модулю ARP с запросом на разрешение адреса, происходит поиск в ARP-таблице указанного в запросе IP-адреса. Если таковой адрес в ARP-таблице отсутствует, то исходящий IP-пакет, для которого нужно было определить локальный адрес, ставится в очередь. Далее протокол ARP формирует свой запрос (ARP-запрос), вкладывает его в кадр протокола канального уровня и рассылает запрос широковещательно. Все узлы локальной сети получают ARP-запрос и сравнивают указанный там IP-адрес с собственным. В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес, а затем отправляет его уже по адресу компьютера, сформировавшего запрос, так как в адрес отправителя указан в самом запросе.

1.5 Сетевые утилиты

В операционной системе Windows существует большое число утилит (специальных программ), предназначенных для управления и анализа сетевых соединений, рассмотрим

некоторые из них: HOSTNAME, IPCONFIG, ARP, NETSTAT, PING, TRACERT, NSLOOKUP.

1.5.1 Утилита HOSTNAME

Позволяет узнать назначенное DNS имя текущего компьютера. Для этого нужно просто вызвать ее без параметров в командной строке:

```
 Lab #7 >hostname
ZELENOGRAD-102
```

1.5.2 Утилита IPCONFIG

Позволяет просмотреть текущую конфигурацию адресов TCP/IP для всех установленных на данном компьютере сетевых адаптеров и коммутируемых соединений, с ее помощью можно определить IP-адрес данного компьютера. Запущенная без параметров, команда ipconfig выдает в качестве результата текущую конфигурацию адресов TCP/IP для всех установленных на данном компьютере сетевых адаптеров и коммутируемых соединений:

```
Настройка протокола IP для Windows


Ethernet adapter Подключение по локальной сети 4:

   DNS-суффикс подключения . . . . . :
   Локальный IPv6-адрес канала . . . : fe80::15c4:d46:3444:6f34%18
   IPv4-адрес. . . . . . . . . . . . : 10.254.253.94
   Маска подсети . . . . . . . . . . : 255.255.255.0
   Основной шлюз. . . . . . . . . :

Ethernet adapter Подключение по локальной сети 2:

   DNS-суффикс подключения . . . . . :
   Локальный IPv6-адрес канала . . . : fe80::e90f:86cd:88cb:8eb6%15
   Автонастройка IPv4-адреса . . . . : 169.254.142.182
   Маска подсети . . . . . . . . . . : 255.255.0.0
   Основной шлюз. . . . . . . . . :

Ethernet adapter Подключение по локальной сети:

   DNS-суффикс подключения . . . . . :
   IPv4-адрес. . . . . . . . . . . . : 192.168.22.102
   Маска подсети . . . . . . . . . . : 255.255.255.0
   Основной шлюз. . . . . . . . . : 192.168.22.1
```

Команду ipconfig следует первой использовать для диагностирования возможных проблем с соединением TCP/IP. С ее помощью можно определить, был ли вообще назначен IP-адрес сетевому адаптеру, а также узнать адрес шлюза.

1.5.3 Утилита NETSTAT

Команда позволяет получить подробную информацию о соединениях, активных в настоящее время. Дополнительные ключи позволяют также получить информацию о сетевых портах, об IP-адресах компьютеров, участвующих в подключении, а также о других сетевых параметрах.

Так же с помощью этой утилиты можно узнать, какие программы передают данные по сети.

Параметр	Описание
-a	Вывод всех активных подключений TCP и прослушиваемых компьютером портов TCP и UDP
-e	Вывод статистики Ethernet, например количества отправленных и принятых байтов и пакетов.
-n	Вывод активных подключений TCP с отображением адресов и номеров портов в числовом формате без попыток определения имен
-b	Отображение исполняемого файла, участвующего в создании каждого подключения, или ожидающего порта.

```
Активные подключения

  Имя    Локальный адрес        Внешний адрес          Состояние
  TCP    0.0.0.0:135            0:0                    LISTENING
  TCP    0.0.0.0:445            0:0                    LISTENING
  TCP    0.0.0.0:3389           0:0                    LISTENING
  TCP    0.0.0.0:5357           0:0                    LISTENING
  TCP    0.0.0.0:14017          0:0                    LISTENING
  TCP    0.0.0.0:14027          0:0                    LISTENING
  TCP    0.0.0.0:49152          0:0                    LISTENING
  TCP    0.0.0.0:49153          0:0                    LISTENING
  TCP    0.0.0.0:49154          0:0                    LISTENING
  TCP    0.0.0.0:49188          0:0                    LISTENING
  TCP    0.0.0.0:49194          0:0                    LISTENING
  TCP    0.0.0.0:49195          0:0                    LISTENING
  TCP    0.0.0.0:57667          0:0                    LISTENING
  TCP    0.0.0.0:64026          0:0                    LISTENING
  TCP    10.254.253.94:139      0:0                    LISTENING
  TCP    10.254.253.94:59938    82.179.184.70:ms-wbt-server  ESTABLISHED
  TCP    127.0.0.1:5939         0:0                    LISTENING
  TCP    127.0.0.1:5939         lmlicenses:49237       ESTABLISHED
  TCP    127.0.0.1:23401        0:0                    LISTENING
  TCP    127.0.0.1:49237        lmlicenses:5939        ESTABLISHED
  TCP    169.254.142.182:139    0:0                    LISTENING
  TCP    192.168.22.102:139     0:0                    LISTENING
  TCP    192.168.22.102:49197   server10003:5938       ESTABLISHED
  TCP    192.168.22.102:49238   185.31.17.133:https    CLOSE_WAIT
  TCP    192.168.22.102:49250   149.154.167.51:https   ESTABLISHED
  TCP    192.168.22.102:49265   ivan:microsoft-ds      ESTABLISHED
  TCP    192.168.22.102:52262   lh-in-f108:imaps       ESTABLISHED
  TCP    192.168.22.102:53420   209-20-75-76:https     CLOSE_WAIT
  TCP    192.168.22.102:53645   push:5222              ESTABLISHED
  TCP    192.168.22.102:53646   lj-in-f109:imaps       ESTABLISHED
  TCP    192.168.22.102:54450   ivan:http              CLOSE_WAIT
  TCP    192.168.22.102:55921   149.154.167.51:https   ESTABLISHED
```

1.5.4 Утилита ARP

Служит для вывода и изменения записей кэша протокола ARP, который содержит одну или несколько таблиц, использующихся для хранения IP-адресов и соответствующих им физических адресов Ethernet или Token Ring. Для каждого сетевого адаптера Ethernet или Token Ring, установленного в компьютере, используется отдельная таблица. Запущенная без параметров, команда arp выводит справку.

Параметры

-a Вывод таблиц текущего протокола ARP для всех интерфейсов

Чтобы вывести записи ARP для определенного IP-адреса, следует указать его после ключа через пробел:

Arp -a IP-адрес

Чтобы вывести таблицы кэша ARP для определенного интерфейса, следует указать параметр –N

Arp -a -N ip_адрес

где ip_адрес − это IP-адрес, назначенный интерфейсу. Параметр –N вводится с учетом регистра.

Arp -d IP-адрес [ip_адрес]

Выполняет удаление записи с определенным IP-адресом. Чтобы удалить запись таблицы для определенного интерфейса, следует указать этот интерфейс после IP-адреса. Чтобы удалить все записи, нужно ввести звездочку (*) вместо параметра IP-адрес.

-s IP-адрес Ethernet_адрес [ip_адрес]

Добавление статической записи, которая сопоставляет IP-адрес с физическим адресом в кэш ARP. Чтобы добавить статическую запись кэша ARP в таблицу для определенного интерфейса, следует указать параметр ip_адрес, где ip_адрес − это IP-адрес, назначенный интерфейсу.

1.5.5 Команда PING

Команда PING является едва ли не самой используемой в локальных сетях командой. Она позволяет тестировать сетевое соединение, получая иформацию о различных его аспектах. Неудачная попытка соединения с каким-либо компьютером, или ошибка получения доступа к общим файлам и папкам, находящимся на других компьютерах локальной сети, может быть вызвана тем, что другие компьютеры просто не получают отправленных им по сети запросов. После введения в командной строке имени команды, в качестве параметра для нее, указывается адрес по которому будут направляться специальные эхо-пакеты, это может быть IP-адрес, или символьное имя компьютера. Получив эхо-запрос, удаленный компьютер сразу же отправляет его обратно по тому адресу, откуда он пришел, команда ping позволяет узнать, пришли ли обратно посланные запросы, проверяя таким образом не только целостность физической среды передачи данных, но и корректную обработку информации на всех остальных семи уровнях модели OSI.

```
 Lab #7 >ping 127.0.0.1

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

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

 Lab #7 >ping miet.ru

Обмен пакетами с miet.ru [82.179.190.60] с 32 байтами данных:
Ответ от 82.179.190.60: число байт=32 время=196мс TTL=63
Ответ от 82.179.190.60: число байт=32 время=192мс TTL=63
Ответ от 82.179.190.60: число байт=32 время=192мс TTL=63
Ответ от 82.179.190.60: число байт=32 время=25мс TTL=63

Статистика Ping для 82.179.190.60:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 25мсек, Максимальное = 196 мсек, Среднее = 151 мсек
```

При успешном возвращении запросов можно быть уверенным в том, что среда передачи данных, программное обеспечение TCP/IP, а также все устройства (маршрутизаторы, повторители и др.), встретившиеся на пути между двумя компьютерами, работают нормально. Необходимо отметить, что даже при отсутствии каких-либо неисправностей на пути между двумя компьютерами, один или сразу несколько пакетов могут быть утеряны, как правило, это бывает в случае перегруженности сети, а также с тем, что диагностирующие пакеты имеют очень низкий приоритет и могут быть отброшены в процессе передачи. Если хотя бы один из посланных пакетов вернется, это уже будет означать исправность работы сети. По умолчанию размер эхо-пакета составляет 32 байта, по указанному адресу направляются эхо-пакеты и после выполнения команды выводится статистика прохождения эхо-пакетов по сети.

1.5.6 Команда TRACERT

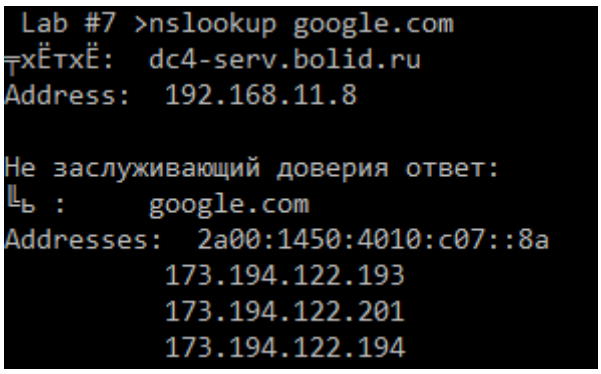
Эта команда подобна команде PING, обе посылают в точку назначения эхо-пакеты и затем ожидают их возвращения. Отличие пакетов команды **TRACERT** от пакетов PING заключается в том, что они имеют различный срок жизни (Time to Live, TTL). Каждый

маршрутизатор при прохождении через него пакета уменьшает значение поля TTL в нем на единицу. Первые пакеты, отправляемые командой **TRACERT** имеют TTL=1, поэтому первый маршрутизатор, получив такой пакет и уменьшив на единицу поле TTL, обнаруживает, что пакет не может быть доставлен по адресу (пакет с TTL=0 не передается маршрутизатором) и возвращает сообщение об ошибке, содержащее IP-адрес маршрутизатора. Получив это сообщение, команда выводит на экран информацию об IP-адресе маршрутизатора и отправляет по прежнему адресу эхо-пакет с TTL=2. Количество маршрутизаторов, через которые может пройти пакет, будет каждый раз увеличиваться на единицу до тех пор, пока пакет не достигнет точки назначения. Таким образом, с помощью команды **TRACERT** можно получить подробный маршрут прохождения пакетов данных между компьютером, на котором была запущена **TRACERT**, и любым удаленным компьютером сети. Это делает **TRACERT** весьма ценным средством обнаружения неисправностей в сетевом соединении: в случае возникновения проблемы с подключением к Web-узлу или к какой-нибудь другой службе Internet можно определить участок, на котором она возникла.

```
 Lab #7 >tracert yandex.ru

Трассировка маршрута к yandex.ru [77.88.55.66]
с максимальным числом прыжков 30:

  1    <1 мс    <1 мс    <1 мс  prog-11-32.bolid.ru [192.168.22.1]
  2    <1 мс    <1 мс    <1 мс  ixgbe-151-gw-access-city.dapl.ru [93.188.46.1]
  3    <1 мс    <1 мс    <1 мс  ae0-50-atlas.dapl.ru [93.188.40.229]
  4     2 ms     2 ms     2 ms  msk-ix-std.yandex.net [195.208.208.116]
  5     3 ms     3 ms     3 ms  std-p2-be1.yndx.net [87.250.239.133]
  6     2 ms     2 ms     2 ms  iva-b-c2-ae7.yndx.net [87.250.239.14]
  7     2 ms     2 ms     2 ms  yandex.ru [77.88.55.66]

Трассировка завершена.
```

1.5.7 Утилита NSLOOKUP

Утилита nslookup (англ. name server lookup поиск на сервере имён) — утилита, предоставляющая пользователю интерфейс командной строки для обращения к системе DNS (проще говоря, DNS-клиент). Позволяет задавать различные типы запросов и запрашивать произвольно указываемые сервера.



2. Практическая часть

Используя описанные утилиты произвести исследование и анализ параметров и настроек локальной сети, протестировать соединение с серверами находящимися на разном расстоянии от вас. Подготовить отчет.

2.1 Определить параметры сетевого подключения

Используя утилиты hostname, ipconfig, netstat, arp заполнить следующие таблицы:

Параметры сетевого подключения

Символьное имя ПК	Адрес локальной сети	IP-Адрес ПК	MAC-Адрес ПК	Адрес DNS-сервера	IP-Адрес файл-сервера	MAC-Адрес файл-сервера

Таблица маршрутизации. Выпишите только маршруты протокола IPv4

Таблица маршрутизации. Активные маршруты:				
Сетевой адрес	Маска подсети	Адрес шлюза	Интерфейс	Метрика

Таблица ARP-кэша. Выпишите первые 5 записей. Если при запросе у вас отображается менее 5 записей, выясните, как это изменить.

IP-адрес	MAC-адрес	Тип

2.2 Получение информации об удаленных серверах

Используя утилиты PING, TRACERT, NSLOOKUP получить информацию о нескольких произвольно выбранных серверах в сети интернет. Сервер необходимо выбрать самостоятельно:

1. Местный, зеленоградский сервер
2. Удаленный российский сервер
3. Удаленный зарубежный сервер

Время прохождения пакета:

Имя сервера	IP-Адрес сервера	Минимальное время	Максимальное время

Количество промежуточных узлов между вами и сервером

Имя сервера	Количество прыжков