Лабораторная работа № 1

Диагностические сетевые утилиты и их использование

1.1. Цель работы

Целью работы является изучение методов контроля и мониторинга сетей, построенных на базе стека протоколов TCP/IP с помощью диагностических утилит операционной системы Windows.

1.2. Теоретический материал

1.2.1. Адресация в IP-сетях

Сетевая операционная система Windows содержит набор утилит, полезных при диагностике сети, использующей протоколы TCP/IP. Основными задачами этих утилит являются:

- определение параметров и характеристик сети,
- определение работоспособности сети,
- в случае неправильного функционирования сети – локализация сегмента или сервиса, вызывающих неисправность.

Главными параметрами сетевых подключений являются их канальные и сетевые адреса и другие параметры, влияющие на работу сетевого уровня.

Каждый компьютер в сети Internet (их принято называть хостами) имеет адреса двух уровней: канального и сетевого.

Канальный адрес хоста определяется технологией, с помощью которой осуществляется его подключение к Internet. Для машин, объединенных в локальные сети по технологии Ethernet, это так называемый MAC-адрес (*Media Access Control* – управление доступом к среде) сетевого адаптера. MAC-адрес назначается производителем оборудования и является уникальным и имеет 48-разрядный формат (6 байтов):

- первый бит указывает: для одиночного (0) или группового (1) адресата предназначен кадр;
- следующий бит указывает, является ли MAC-адрес глобально (0) или локально (1) администрируемым;

• следующие 22 бита являются идентификатором фирмы производителя;

• младшие 3 байта назначаются уникальным образом самим производителем.

MAC-адреса обычно представляются в 16-разрядной системе, например, 00-E0-4C-78-23-FD. Адрес FF-FF-FF-FF-FF-FF является широковещательным.

В качестве сетевого адрес хоста Internet используется IP-адрес (*Internet Protocol Address*), который характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение. При связи через сеть Internet требуется глобальная уникальность адреса, что обеспечивается рекомендациями специального подразделения Internet InterNIC (*Network Information Center*). Провайдеры услуг Internet получают диапазоны адресов у представителей InterNIC, а затем распределяют их между своими абонентами. В случае изолированной от Internet уникальность сетевого адреса требуется лишь в ее пределах, при этом IP-адреса должны выбираться администратором из специально зарезервированных для таких сетей блоков «закрытых» адресов.

В наиболее распространенной четвертой версии протоколов Internet (IP.v4) IP-адрес представляет собой 32-битовое двоичное число, записываемое в виде четырех десятичных чисел (значения от 0 до 255), разделенных точками (например, 192.168.0.1). Адрес состоит из двух логических частей – номера сети и номера хоста в сети.

При классовой модели форматирования адресов, значения первых битов адреса определяют, какая его часть относится к номеру сети, а какая – к номеру хоста, как показано в табл. 1.1.

Таблица 1.1

Классовая модель форматирования адресов

<table>
<tr><th rowspan="2">Класс</th><th colspan="10">IP адрес</th><th rowspan="2">Диапазон адресов</th></tr>
<tr><th>31</th><th>30</th><th>29</th><th>28</th><th>27</th><th>25</th><th>24</th><th>23 16</th><th>15 8</th><th>7 0</th></tr>
<tr><td>A</td><td>0</td><td colspan="5">№ сети</td><td colspan="4">№ хоста</td><td>0.1.0.0–126.0.0.0</td></tr>
<tr><td>B</td><td>1</td><td>0</td><td colspan="4">№ сети</td><td colspan="3">№ хоста</td><td>128.0.0.0–191.255.0.0</td></tr>
<tr><td>C</td><td>1</td><td>1</td><td>0</td><td colspan="5">№ сети</td><td>№ хоста</td><td>192.0.1.0–223.255.255.0</td></tr>
<tr><td>D</td><td>1</td><td>1</td><td>1</td><td>0</td><td colspan="6">адрес группы multicast</td><td>224.0.0.0–
239.255.255.255</td></tr>
<tr><td>E</td><td>1</td><td>1</td><td>1</td><td>1</td><td>0</td><td colspan="5">зарезервировано</td><td>240.0.0.0–
247.255.255.255</td></tr>
</table>

Ряд адресов сетей и подсетей являются особыми:

- если весь IP-адрес состоит только из двоичных нулей, то он обозначает адрес того хоста, который сгенерировал этот пакет;
- если все двоичные разряды IP-адреса хоста равны 1, то пакет с таким адресом назначения является широковещательным, т.е. должен рассылаться всем хостам, находящимся в той же сети, что и источник этого пакета;
- если все двоичные разряды IP-адреса хоста равны 0, то этот адрес обозначает не отдельный хост, а всю сеть;
- адрес 127.0.0.1 означает пересылку в пределах одного и того же хоста (используется для автономной отладки сетевого программного обеспечения);
- адреса закрытых сетей (частная сеть, «серая сеть», сеть интранет) лежат в диапазонах 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 настоящее время классовая модель вытесняется бесклассовой, при которой выделение разрядов, отводимых для нумерации сети в IP-адресе, задается специальным четырехбайтовым кодом – маской подсети, что позволяет более экономно распределять IP-адреса между пользователями. Эти разряды маски имеют единичные значения. Например, маска 255.255.255.240 (код 11111111.11111111.11111111.11110000 в двоичной системе) указывает, что для нумерации сети используется 28 старших разрядов, а для нумерации хоста – только 4 младших разряда соответствующего IP-адреса. При бесклассовой модели часто применяется запись IP-адресов вида 192.96.10.0/28. Число после косой черты означает количество единичных разрядов в маске подсети.

IP-адреса для конкретных компьютеров могут устанавливаться администратором сети вручную (статическое распределение адресов), что весьма трудоемко. Для автоматизации процесса назначения IP-адресов хостам сети локальной сети применяется специальный протокол DHCP (*Dynamic Host Configuration Protocol*), который обеспечивает динамическое назначение IP-адресов. Назначаемые адреса формирует DHCP-сервер по запросам DHCP-клиентских программ, устанавливаемых на отдельных хостах.

При автоматическом статическом способе DHCP-сервер без вмешательства оператора присваивает IP-адрес и 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 по-прежнему, как и при ручном назначении, существует постоянное соответствие. Оно устанавливается в момент первичного назначения сервером DHCP IP-адреса клиенту. При всех последующих запросах сервер возвращает тот же самый IP-адрес.

При динамическом распределении адресов DHCP-сервер назначает адрес клиенту на ограниченное время, что дает возможность впоследствии повторно использовать IP-адреса другими компьютерами.

1.2.2. Отображение символьных адресов на IP-адреса: служба DNS

Компьютеры используют для взаимодействия числовые IP-адреса, тогда как людям удобнее работать со словесными именами. Чтобы в сетевых приложениях можно было применять словесные имена, требуется механизм преобразования имен в IP-адреса, реализуемый службой доменных имен DNS (*Domain Name System*) распределенной базой данных, поддерживающей иерархическую систему имен для идентификации хостов в сети Internet.

Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени хоста. DNS-серверы хранят часть базы данных о соответствии символьных имен и IP-адресов. Эта база данных распределена по административным доменам сети Internet. Клиенты сервера DNS знают IP-адрес сервера DNS своего административного домена и по протоколу IP передают запрос, в котором сообщают известное символьное имя и просят вернуть соответствующий ему IP-адрес.

Если данные о запрошенном соответствии хранятся в базе данного DNS-сервера, то он сразу посылает ответ клиенту, если же нет, то он посылает запрос DNS-серверу другого домена, который либо сам обрабатывает запрос, либо передает его другому DNS-серверу. Все DNS-серверы соединены иерархически, в соответствии с иерархией доменов сети Internet.

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, причем точки в имени отделяют части, соответствующие хостам домена.

Домены верхнего уровня назначаются для каждой страны, а также на организационной основе. Доменное имя строится из слов, разделенных точками и содержащих латинские буквы, цифры и значок дефис (-). Доменные имена могут содержать до 63 символов и нечувствительны к регистру букв, т.е. заглавные и строчные буквы считаются одинаковыми.

Организация InterNIC, управляющая всем адресным пространством Internet, а также всем пространством имен, делегирует некоторым организациям право ведения доменов первого уровня, к которым относятся следующие «организационные» зоны (***com*** – коммерческие, ***edu*** – образовательные, ***gov*** – правительственные, ***int*** – международные, ***mil*** – военные, ***net*** – организации, обеспечивающие работу сети, ***org*** – некоммерческие организации, ***biz*** – то же самое, что и ***com***, ***info*** – информационные ресурсы), а также более двухсот «географических» доменов (***ru*** и ***su*** – Россия, ***uk*** – Великобритания, ***de*** – Германия, ***fr*** – Франция, ***ua*** – Украина и т.д.).

Владелец доменной зоны может организовывать в ней любые поддомены и делегировать функции администрирования этих поддоменов другим организациям. Поддомен создается путем дописывания к имени домена еще одного отделенного точкой слова слева. Каждый домен имеет уникальное имя, а каждый из поддоменов имеет уникальное имя внутри своего домена. Каждый хост в сети Internet однозначно определяется своим полным доменным именем, которое включает имена всех доменов по направлению от хоста к корню. Пример полного DNS-имени: ***vt.pnzgu.ru***.

Для ускорения процедуры разрешение имен на хосте размещается DNS-кэш (иногда называемый кэшем DNS-резольвера) — это временная база данных, поддерживаемая ОС компьютера, которая содержит записи обо всех последних посещениях и попытках посещений веб-сайтов и других интернет-ресурсах.

1.2.3. Системные утилиты сетевой диагностики

1.2.3.1. Утилита *ipconfig*

Утилита ***ipconfig*** предназначена для проверки правильности конфигурации TCP/IP для операционной системы Windows и для обновления некоторых параметров, задаваемых при автоматическом

конфигурировании сетевых интерфейсов при использовании протокола DHCP.

Утилита выводит значения для текущей конфигурации стека TCP/IP: MAC- и IP-адрес, маску подсети, адрес шлюза по умолчанию, адрес сервера DNS, использование DHCP. Кроме того утилита ***ipconfig*** выводит информацию о настройках NetBIOS (*Network Basic Input/Output System*), которая представляет собой интерфейс сеансового уровня, обеспечивающий взаимодействие приложений при сетевых операциях ввода-вывода и управления:

- регистрацию и проверку сетевых имен;
- установление и разрыв соединений;
- связь с подтверждением доставки информации;
- связь без подтверждения доставки информации;
- поддержку управления и мониторинга драйвера и сетевой карты.

NetBIOS работает поверх разных протоколов, самыми распространённым из которых являются NetBEUI, IPX и TCP.

NetBIOS взаимодействует со службой WINS (*Windows Internet Name Service*), которая выполняет задачи, аналогичные задачам службы DNS: динамическая регистрация имен компьютеров и других сетевых узлов и их IP-адресов на серверах WINS и разрешение имен компьютеров в IP-адреса. Главное отличие WINS в том, что эта служба функционирует в пространстве имен, которое не пересекается с пространством имен службы DNS.

На данный момент стандарт NetBIOS считается устаревшим и не рекомендуется к использованию. Однако поддержка NetBIOS сохранена и по сей день и код NetBIOS через TCP/IP всё еще присутствует в составе последних версий Windows, т.к. с его использованием было написано огромное количество разнообразного программного обеспечения.

При устранении неисправностей в сети TCP/IP следует сначала проверить правильность конфигурации с помощью утилиты ***ipconfig.***

Синтаксис утилиты: ***ipconfig*** **[*-option...*].** Параметры ***option*** (здесь и далее в квадратных скобках указаны необязательные параметры):

- ***?*** выводит справочное сообщение;
- ***all*** выдает весь список параметров, без этого ключа отображается только IP-адрес, маска и шлюз по умолчанию;

- ***displaydns*** выводит на экран содержимое кэш службы разрешения имен DNS хоста;
- ***flushdns*** очищает содержимое кэш службы разрешения имен DNS хоста;
- ***renew*** [***adapter***] на компьютерах, где запущена служба клиента DHCP, обновляет параметры конфигурации DHCP;
- ***release*** [***adapter***] освобождает выделенный DHCP IP-адрес после чего он становиться доступен для назначения другому компьютеру;
- ***registerdns*** выполняет обновление всех DHCP-аренд и перерегистрация DNS-имен;
- **showclassid** ***adapter*** отображает все допустимые для определенного адаптера идентификаторы классов DHCP;
- ***setclassid adapter*** **[***options class***]** для определенного адаптера устанавливает идентификатор класса DHCP ***options class***.

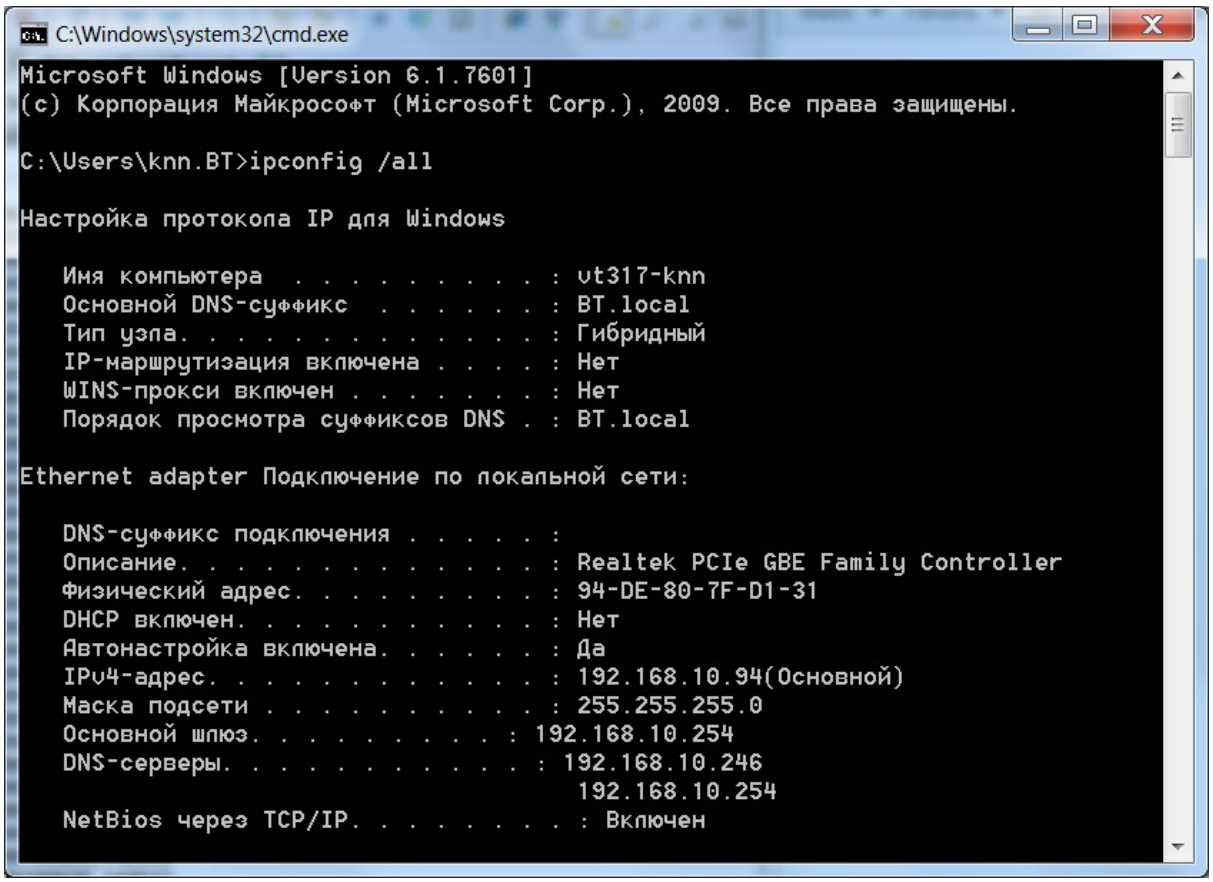
Указывать имени сетевого адаптера [***adapter***] необходимо, если действия задаваемые командой ***ipconfig*** должны относиться к определенному сетевому подключению из нескольких имеющихся в данной ЭВМ. Имена сетевых адаптеров выводится командой ***ipconfig*** без параметров.

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 допускается применимо использование символа * в качестве шаблона, например ***Локальн**** – имя адаптера начинается с "Локальн".

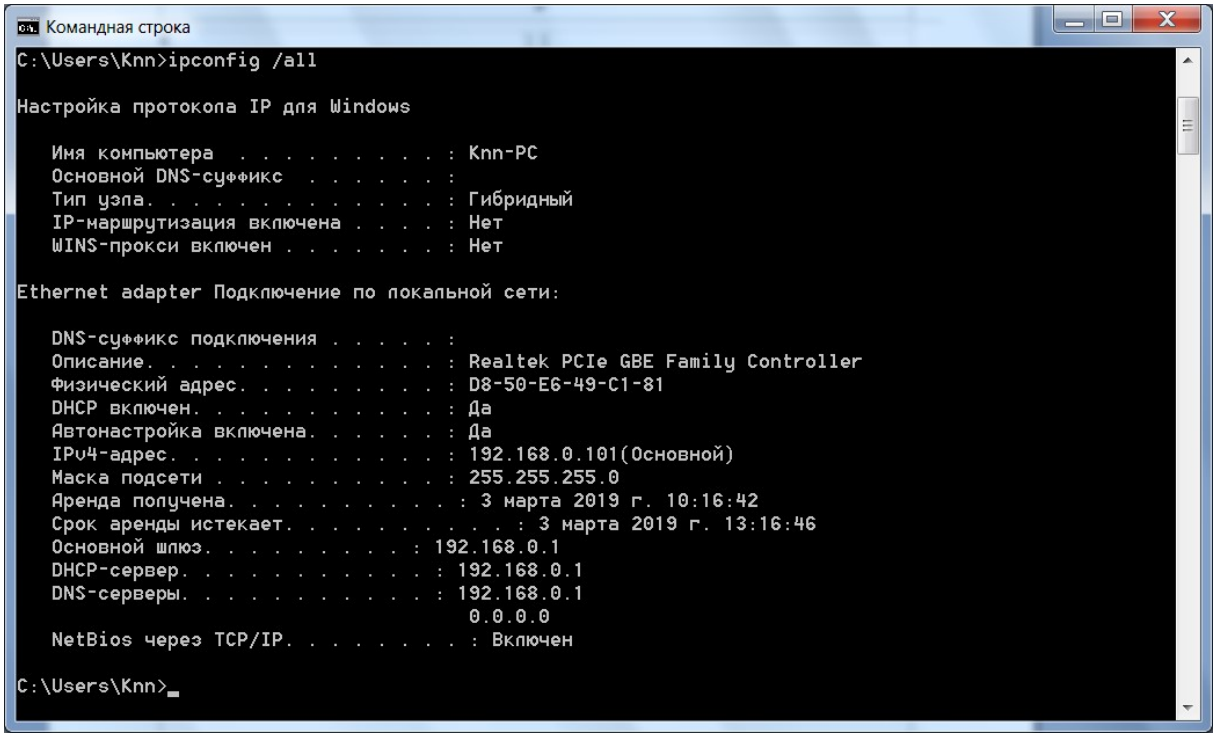
При вызове команды ***ipconfig*** без параметров выводятся IP-адрес, маска подсети и основной шлюз для каждого сетевого адаптера.

Наиболее часто для получения сведений о сетевых настройках хоста используется команда ***ipconfig /all.*** На рисунках 1.1а и 1.1б приведены примеры отображения этих настроек на экране.

Вывод команды ***ipconfig*** часто не помещается на экране, поэтому для постраничного отображения результатов можно использовать команду **more** в цепочке с командой ***ipconfig: ipconfig /all more..***



а)



б)

Рис. 1.1. Отображение утилитой ***ipconfig*** установленных на компьютере сетевых конфигураций при назначении IP-адреса: а) статически, б) с помощью протокола DHCP

Результаты работы утилиты ***ipconfig*** могут быть выведены также в стандартный буфер обмена Windows для последующего сохранения в текстовом файле, для чего нужно выполнить ее в цепочке с командой ***clip***: ***ipconfig /all | clip.*** Указанным образом можно сохранять в буфере обмена результаты и других сетевых утилит.

В разделе **«Настройка протокола IP для Windows»** выводятся:

- DNS-имя компьютера;
- значения основного DNS-суффикса, при этом имя хоста с DNS-суффиксом составляет так называемое полное имя компьютера (в настойках, отображенных на рисунке 1.1.а это ***vt317-knn.Bt.local***) ;
- параметра «**Тип узла», к**оторый определяет алгоритм определения и регистрации имен NETBIOS;
- указания на включения IP-маршрутизации и WINS-прокси;
- установленный порядок просмотра DNS-суффиксов при поиске.

В разделе отображения конфигураций сетевых адаптеров выводятся:

- имя сетевого подключения, присвоенное операционной системой имя сетевого адаптера;
- DNS-суффикс подключения Ethernet adapter Подключение по локальной сети :. . . . . : - DNS-суффикс из настроек сетевого подключения
- название сетевого адаптера;
- MAC- адрес данного адаптера;
- признаки признак использования DHCP для конфигурирования сетевого адаптера и включения автоматической настройки параметров адаптера с использованием функции автоматического назначения адресов (APIPA) при отсутствии сервера DHCP;
- используемый для данного адаптера IP – адрес;
- маска подсети;
- дата и время получения сетевой конфигурации от сервера DHCP ;
- срок истечения аренды сетевых настроек, определяемый сервером DHCP;
- IP-адрес основного шлюза - маршрутизатора, используемого в качестве шлюза по умолчанию, на который пакет отправляется в том случае, если маршрут к сети назначения пакета хосту не известен;

- IP – адрес адреса DNS - серверов, используемых для разрешения имен;
- указание на режим использования NETBIOS через протокол в IP-адреса.

1.2.3.2. Утилита ***nslookup***

Утилита **nslookup** предназначена для выполнения запросов к DNS-серверам на разрешение имен в IP-адреса и в простейшем случае имеет следующий синтаксис: **nslookup** [-***option***...] [***host*** [***server***]]. Параметры:

- ***host*** – доменное имя хоста, которое должно быть преобразовано в IP-адрес;
- ***server*** – адрес DNS-сервера, который будет использоваться для разрешения имени. Если этот параметр опущен, то будут использованы адреса DNS-серверов из параметров настройки протокола TCP/IP (отображаются утилитой ***ipconfig***).
- ***help или ?*** - печать сведений о стандартных командах;
- ***set OPTION*** - установить параметр;
- ***domain=NAME*** - установить имя домена по умолчанию NAME;
- ***root=NAME*** - установить корневой сервер NAME;
- ***retry=X*** - установить число повторов X;
- ***timeout=X -*** установить интервал времени ожидания в X секунд
- ***type=X*** - установить тип DNS записей, которые должна вернуть утилита ;
- ***class=X -*** установить класс запроса (***IN*** (Internet), ***ANY***);
- ***server NAME*** - установить сервер по умолчанию ***NAME,*** используя текущий сервер по умолчанию;
- ***lserver NAME*** - установить сервер по умолчанию ***NAME***, используя первоначальный сервер;
- ***root*** - сделать текущий сервер по умолчанию корневым сервером.

К основным типами ресурсных записей, возвращаемых утилитой относятся:

- ***A-***запись — задает преобразование имени хоста в IP-адрес.

• ***AAAA***-запись — задает преобразование имени хоста в IPV6-адрес.

• ***MX-***запись — определяет почтовый ретранслятор для доменного имени, т.е. узел, который обрабатывает или передает дальше почтовые сообщения, предназначенные адресату в указанном домене.

• ***NS***-записи — определяют DNS-серверы, которые являются авторитативными для данной зоны.

• ***CNAME***-запись — определяет отображение псевдонима в каноническое имя узла.

• ***SRV***-запись — позволяет получить имя для искомой службы, а также протокол, по которому эта служба работает.

• ***TXT***-запись — содержит общую текстовую информацию, например, для указаниеместорасположения хоста.

При запуске ***nslookup*** без параметров, утилита переходит в интерактивный режим, позволяющий выполнять различные внутренние команды, полный список доступных команд утилиты можно вывести, набрав знак вопроса, выйти из утилиты можно введя команду ***exit.***

Результаты выполнения команды ***nslookup*** для разрешения имени ***pnzgu.ru***, приведены на рис. 1.2, приэтом запрашиватся DNS-сервер, заданный по умолчанию,. Для разных версий ***nslookup*** и разных DNS-серверов, обслуживающих запрос, отображаемая информация может незначительно отличаться.

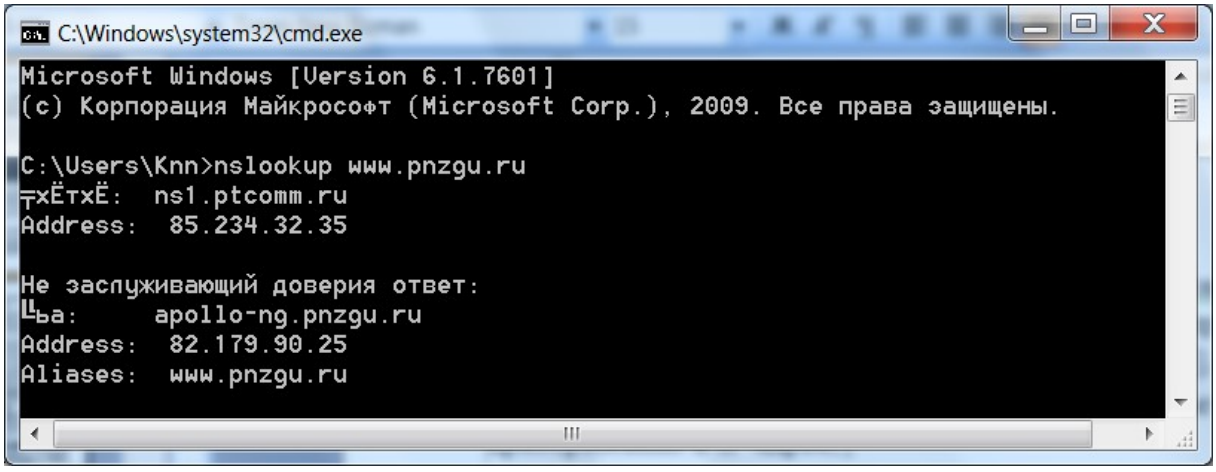


Рис. 1.2. Пример отображения утилитой **nslookup** запроса к DNS

Первые две строки ответа содержат имя и IP-адрес DNS-сервера, который был использован для разрешения имени. Следующие строки содержат реальное доменное имя хоста и его IP-адрес и указание «**Не**

заслуживающий доверия ответ» означающее, что ответ получен не с DNS-сервера, ответственного за зону ***pnzgu.ru*** и для разрешения имени использовался рекурсивный запрос к другому DNS-серверу. Строка ***Aliase*** содержит альтернативное имя искомого сервера.

Чтобы получит авторитетный ответ (authoritative answer) необходимо узнать IP-адреса DNS-серверов, обслуживающих домен ***pnzgu.ru***, для чего повторим запрос к DNS-серверу ***ns1.ptcomm.ru***, установив ключ ***type=any*** на отображение любых типов записей. Сервер ***ns1.ptcomm.ru*** ответит на запрос утилиты ***nslookup*** перечислением искомых DNS серверов (см. рисунок 1.3).

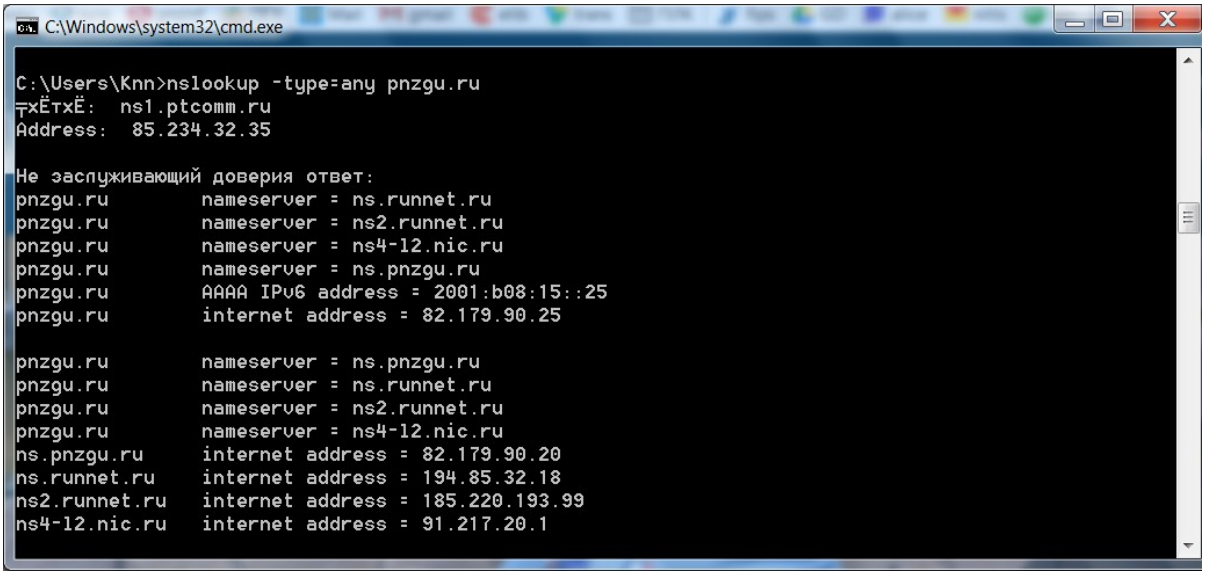


Рис. 1.3. Ответ с перечислением DNS серверов, обслуживающих домен ***pnzgu.ru***

Если теперь отправить запрос к DNS-серверу с адресом 82.179.90.20, то будет получен авторитетный ответ, представленный на рисунке 1.4 .

Рис. 1.4. Авторитетный ответ на запрос утилиты ***nslookup***

1.2.3.3. Утилита ***ping***

Утилита ***ping*** (*Packet Internet Grouper*) используется для проверки конфигурирования TCP/IP и диагностики ошибок соединения. Она определяет доступность и функционирование конкретного хоста – любого сетевого устройства, обменивающегося информацией с другими сетевыми устройствами по TCP/IP. Использование ***ping*** есть лучший способ проверки существования маршрута между локальным компьютером и сетевым хостом.

Команда ***ping*** проверяет соединение с удаленным хостом путем посылки к нему эхо-пакетов протокола ICMP (*Internet Control Message Protocol*) и прослушивания эхо-ответов. ***Ping*** выводит количество переданных и принятых пакетов. Каждый принятый пакет проверяется в соответствии с переданным сообщением. Если связь между хостами плохая, из сообщений ***ping*** станет ясно, сколько пакетов потеряно.

По умолчанию передаются четыре эхо-пакета длиной 32 байта, представляющих собой последовательность символов алфавита в верхнем регистре. ***Ping*** позволяет изменить размер и количество пакетов, указать, следует ли записывать маршрут, который она использует, какую величину времени жизни устанавливать, можно ли фрагментировать пакет и т.д. При получении ответа в поле определяется, за какое время (в миллисекундах) посланный пакет доходит до удаленного хоста и возвращается назад. Так как значение по умолчанию для ожидания отклика равно 1 с, то все значения данного поля будут меньше 1000 мс. Если получается сообщение «Превышен интервал ожидания», то, возможно, увеличение времени ожидания отклика позволит пакету дойди до удаленного хоста.

При пользовании утилитой ***ping*** следует помнить:

- задержка, определенная утилитой, вызвана не только пропускной способностью канала передачи данных до проверяемой машины, но и загруженностью этой машины;
- некоторые серверы в целях безопасности могут не посылать эхо-ответы, так как с утилиты ***ping*** может начинаться хакерская атака.

Ping можно использовать для тестирования как с доменным именем хоста, так и с его IP-адресом. Если ***ping*** с IP-адресом выполнилась успешно, а с именем – неудачно, это значит, что проблема заключается в распознавании соответствия адреса и имени, а не в сетевом соединении.

Синтаксис: ***ping*** [**-**option...] ***destination-list.*** Параметры**:**

- ***-t*** выполняет команду ***ping*** до прерывания (***Ctrl-Break*** – посмотреть статистику и продолжить, ***Ctrl-C*** – прервать выполнение команды);
- ***-a*** позволяет определить доменное имя удаленного компьютера по его IP-адресу;
- ***-n count*** посылает количество пакетов *Echo*, указанное параметром ***count*** (по умолчанию передается четыре запроса);
- ***-l length*** посылает пакеты длиной ***length*** байт (максимальная длина 8192 байта);
- ***-f*** посылает пакет с установленным флагом «не фрагментировать», запрещающим фрагментирование пакета на транзитных маршрутизаторах;
- ***-i ttl*** устанавливает время жизни пакета в величину ***ttl*** (каждый маршрутизатор уменьшает ***ttl*** на единицу, т.к. время жизни является счетчиком пройденных маршрутизаторов (хопов));
- ***-v tos*** устанавливает значение поля «сервис», задающее приоритет обработки пакета;
- ***-r count*** записывает путь выходящего пакета и возвращающегося пакета в поле записи пути, ***count*** – от 1 до 9 хостов;
- ***-s count*** задает максимально возможное количество переходов (хопов) из одной подсети в другую;
- ***-j host-list*** направляет пакеты с помощью списка хостов, определенного параметром ***host-list.***), максимальное количество хостов равно 9;
- ***-k host-list*** направляет пакеты через список хостов, определенный в ***host-list***, причем указанные хосты не могут быть разделены промежуточными маршрутизаторами (жесткая статическая маршрутизация);
- ***-w timeout*** указывает время ожидания ***timeout*** ответа от удаленного хоста в миллисекундах (по умолчанию – 1с);
- ***-destination-list*** указывает удаленный узел, к которому надо направить пакеты ***ping,*** может быть именем хоста или IP-адресом машины.

На практике в формате команды чаще всего используются опции ***-t*** и ***-n.***

Пример работы утилиты ***ping*** приведен на рис. 1.5.

Утилита ***ping*** может использоваться вледующих целях:

• для проверки того, что протоколы TCP/IP установлены и правильно сконфигурированы на локальном компьютере, в команде ***ping*** задается адрес петли обратной связи: ***ping 127.0.0.1***;

• чтобы убедиться в том, что компьютер правильно добавлен в сеть и IP-адрес не дублируется, используется IP-адрес локального компьютера: ***ping IP-адрес_локального_хоста;***

• чтобы проверить, что шлюз по умолчанию функционирует и можно установить соединение с любым хостом в локальной сети, задается IP-адрес шлюза по умолчанию: ***ping IP-адрес_шлюза;***

• для проверки возможности установления соединения через маршрутизатор в команде ***ping*** задается IP-адрес удаленного хоста: ***ping IP-адрес_удаленного хоста.***

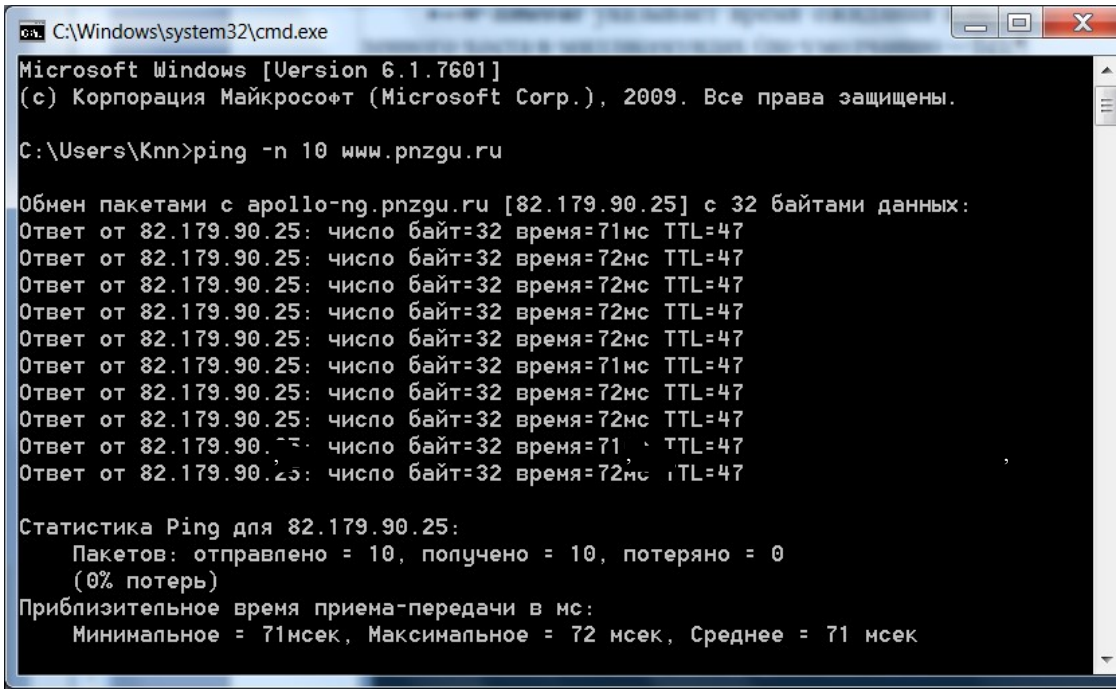


Рис. 1.5. Пример использования утилиты ***ping***

Следует помнить, если на ***ping*** -запросы не получено ответов, это не означает, что узел недоступен — просто сервер или промежуточные устройства для безопасности могут быть настроены не отвечать на ping-запросы.

1.2.3.4. Утилита ***tracert***

Утилита ***tracert*** (*trace route*) позволяет выявлять последовательность маршрутизаторов, через которые проходит IP-пакет на пути к

пункту своего назначения путем изучения сообщений ICMP, которые присылаются обратно промежуточными маршрутизаторами.

Утилита ***tracert*** работает следующим образом:

Посылается по три пробных эхо-пакета протокола ICMP с параметром «Время жизни» TTL=1 на узел назначения. Время жизни пакета измеряется в хопах - участках между двумя узлами сети, по которому передаются сетевые пакеты. Значение хоп обычно характеризует «расстояние» между узлами.

Первый маршрутизатор пошлет в хост-источник сообщение ICMP «**Время истекло**».

Затем TTL увеличивается на 1 в каждой последующей посылке до тех пор, пока пакет не достигнет хоста назначения либо не будет достигнута максимально возможная величина TTL (по умолчанию 30).

Имя машины может быть именем хоста или IP-адресом машины. Выходная информация представляет собой список хостов, начиная с первого шлюза и заканчивая пунктом назначения. На экран при этом выводится время ожидания ответа на каждый пакет.

В тех случаях, когда удаленный узел не достижим, применение утилиты ***tracert*** более удобно, чем ***ping,*** так как с ее помощью можно локализовать район сети, в которой имеются проблемы со связью. Если возникли проблемы, то утилита выводит на экран звездочки (*****) либо сообщения типа «**Заданная сеть недоступна**», «**Время истекло**». Следует помнить, что некоторые маршрутизаторы просто уничтожают пакеты с истекшим TTL и поэтому не будут видны утилите ***tracert***.

Синтаксис утилиты: ***tracert*** [***--option...***] ***destination-list***. Параметры:

- ***-d*** указывает, что не нужно распознавать адреса для имен хостов;
- ***-h maximum_hops*** указывает максимальное число хопов (по умолчанию – 30);
- ***-j host-list*** указывает нежесткую статическую маршрутизацию в соответствии с ***host-list***;
- ***-w timeout*** указывает, что нужно ожидать ответ на каждый эхо-пакет заданное число мс;
- ***-destination-list*** указывает удаленный узел, к которому надо направить пакеты ***ping***.

Пример работы утилиты ***tracert*** приведен на рис. 1.6.

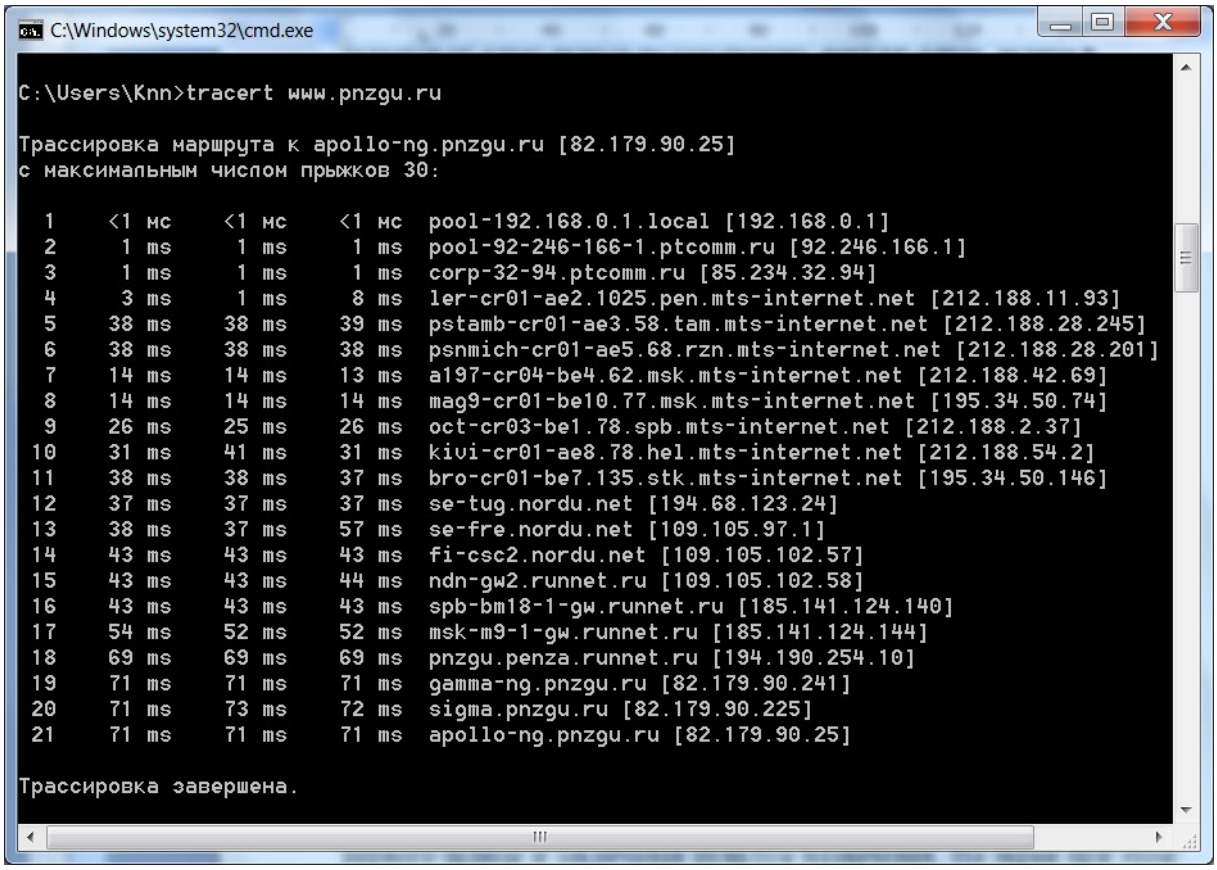


Рис. 1.6. Пример использования утилиты ***tracert***

1.2.3.5. Утилита ***arp***

Утилита ***arp*** (*Address Resolution Protocol* – протокол разрешения адресов) позволяет управлять так называемым ARP-кэшем – таблицей, используемой для трансляции IP-адресов в соответствующие локальные адреса. Записи в ARP-кэше формирует протокол ARP. Если необходимая запись в таблице не найдена, то протокол ARP отправляет широковещательный запрос ко всем компьютерам локальной подсети, пытаясь найти владельца данного IP-адреса.

В кэше могут содержаться два типа записей: статические и динамические. Статические записи вводятся вручную и хранятся в кэше постоянно. Динамические записи помещаются в кэш в результате выполнения широковещательных запросов. Для них существует понятие времени жизни. Если в течение определенного времени (по умолчанию 2 мин) запись не была востребована, то она удаляется из ARP-кэша.

Синтаксис утилиты: ***arp*** [***-option...***]**.** Параметры:

- ***-s inet_addr eth_addr*** заносит в кэш статическую запись с указанными IP-адресом и MAC-адресом;
- ***-d inet_addr*** удаляет из кэша запись для определенного IP-адреса;
- ***-a*** просматривает содержимое кэша для всех сетевых адаптеров локального компьютера, как показано на рис. 1.7.

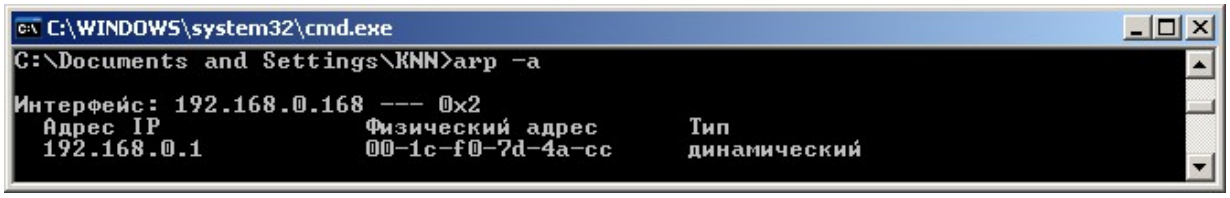


Рис. 1.7. Пример использования утилиты ***arp***

Следует помнить, что использование параметров –***s*** и –***d*** требует административных прав для пользователя утилиты.

1.2.3.6. Утилита ***netstat***

Утилита ***netstat*** выводит статистику протоколов и текущих TCP/IP соединений и имеет следующий синтаксис: ***netstat*** [***--a***][***-e***][***-n***] [***-s***][***-p name***][***-r***][***interval***]. Параметры:

- ***-a*** отображает полную информацию по всем соединениям и портам, на которых компьютер ожидает соединения;
- ***-e*** отображает статистику Ethernet (этот ключ может применяться вместе с ключом – ***s***);
- ***-n*** отображает адреса и номера портов в числовом формате, без их преобразования в символьные имена DNS и в название сетевых служб, что делается по умолчанию ***t***;
- ***-p name*** задает отображение информации для протокола ***name*** (допустимые значения ***name***: ***tcp***, ***udp*** или ***ip***) и используется вместе с ключом ***s***;
- ***-r*** отображает содержимое таблицы таблица маршрутизации;
- ***-s*** отображает подробную статистику по протоколам. По умолчанию выводятся данные для TCP, UDP и IP.
- ***-p*** позволяет задать вывод данных по определенному протоколу,

- ***-interval*** инициирует повторный вывод статистических данных через указанный в секундах интервал (в этом случае для прекращения вывода данных надо нажать клавиши ***Ctrl+C***).

Результатом выполнения команды можут являться статистические данные об обработанном трафике определенного протокола, например IP (см. рисунок 1.8).

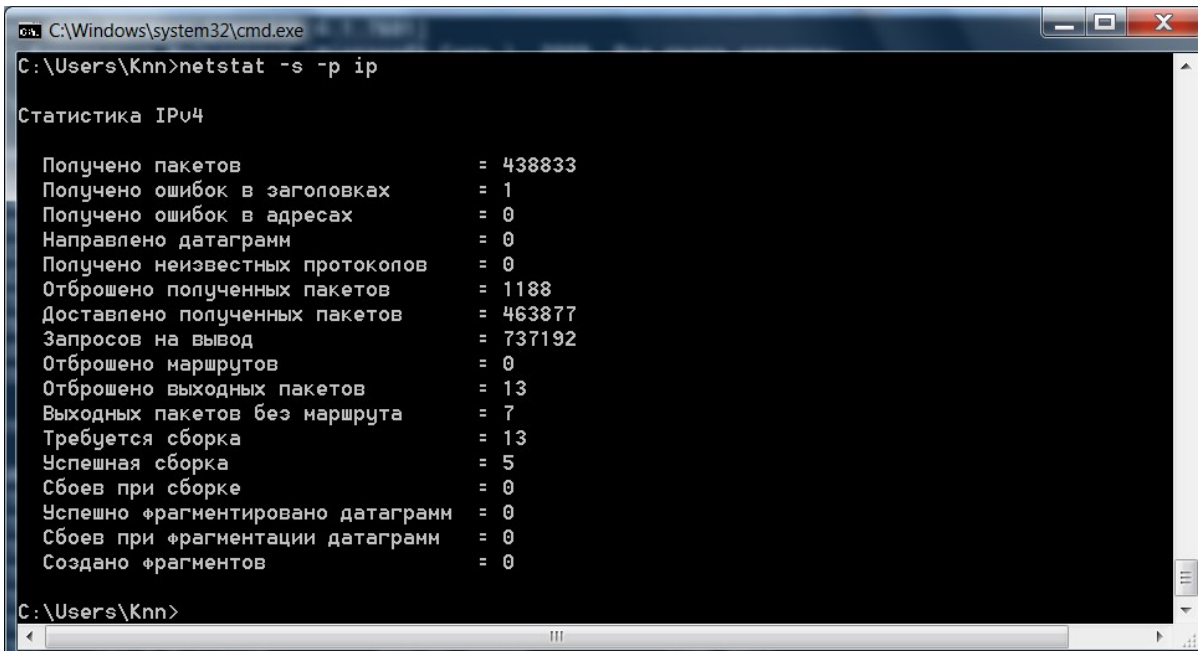


Рис. 1.8. Пример отображения утилитой ***netstat*** статистики протокола IP

При использовании ключей ***–a, -s –p tcp*** открытые TCP-порты обозначаются в колонке «Состояние» строкой ***LISTENING*** – пассивно открытые соединения («слушающие» сокеты) или ***ESTABLISHED*** – установленные соединения, т.е. уже используемые сетевыми сервисами (см. рисунок 1.9). Содержание состояний протокола TCP (всего имеется 11 состояний) раскрыто в лабораторной работе № 2 настоящего практикума.

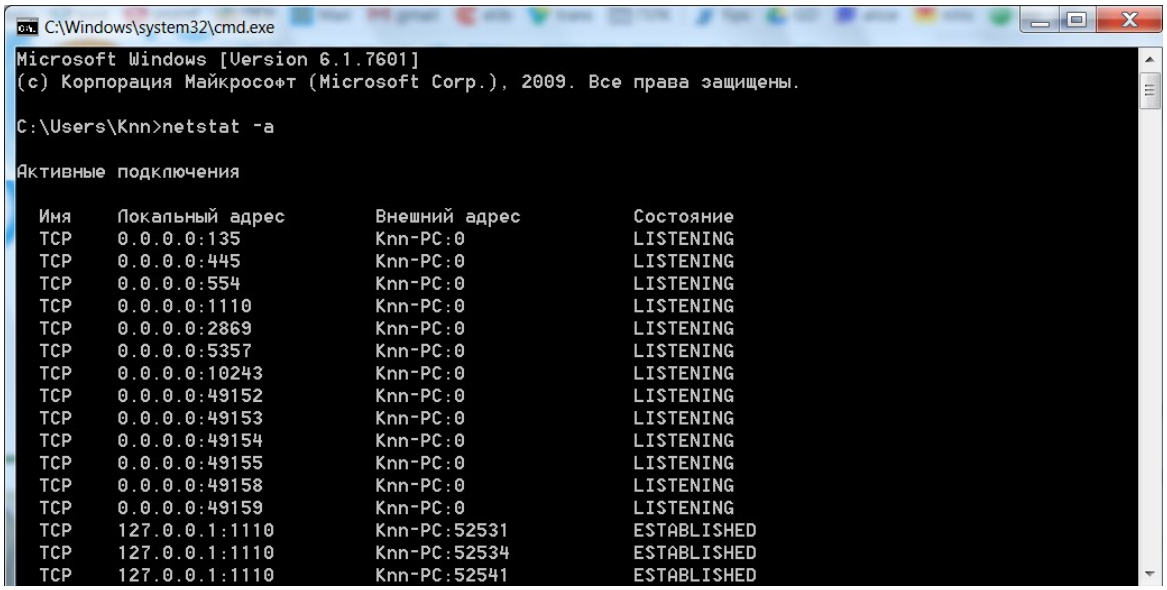


Рис. 1.9. Пример отображения утилитой ***netstat*** всех подключений и открытых портов.

Часть портов, связанных с системными службами Windows и отображаются не по номеру, а по названию – ***epmap, microsoft-ds***, ***netbios-ss*** и др. Порты, не относящиеся к стандартным службам, отображаются по номерам. UDP-порты не могут находиться в разных состояниях, поэтому специальная пометка ***LISTENING*** в их отношении не используется. Как и TCP-порты, они могут отображаться по именам или по номерам.

На практике, в виду большого объема выводимой информации утилиту ***netstat*** удобно использовать в цепочке с командами постраничного вывода (***more***), перенаправления стандартного вывода в файл (>) и поиска текста в результатах вывода (***find***).

1.2.3.7. Сервис ***Whois***

При трассировке маршрутов или проверке доступности хоста в *Internet* часто возникает необходимость определить по IP-адресу хоста его юридического владельца и контактные данные его администратора.

В отношении доменов второго уровня эта информация становится свободно доступной для любого пользователя сети Internet через сервис ***Whois***, предоставляемый многими сайтами, например, on-line сервис ***Whois*** можно получить через форму на странице сайта http://www.nic.ru/whois. Подробная официальная информация содержится в базах данных пяти региональных интернет-регистраторов выполняющих распределение *Internet* -ресурсов, а также связанную с этим регистрацию и координацию деятельности,

направленную на глобальную поддержку функционирования *Internet.* Для Европы, Ближнего Востока и Центральной Азии региональным интернет-регистратором является организация RIPE NCC, доступ к базе данных *RIPE Database* которой можно получить на сайте http://www.ripe.net.

Пример ответа на запрос о данных на домен, содержащий IP-адрес 82.179.90.25 представлен на рисунке 1.10.

База данных представляет следующую информацию:

- диапазон IP-адресов, закрепленных за доменом,
- сетевое имя домена,
- организация-владелец домена и ее почтовый адрес;
- данные о представителе организации для административного контакта;
- данные и техническом специалисте - администратора домена;
- данные службы технической поддержки (службы авторизации), отвечающей за корректность информации о домене в базе данных;
- данные о авремени создания и последней модификации информации в базе.

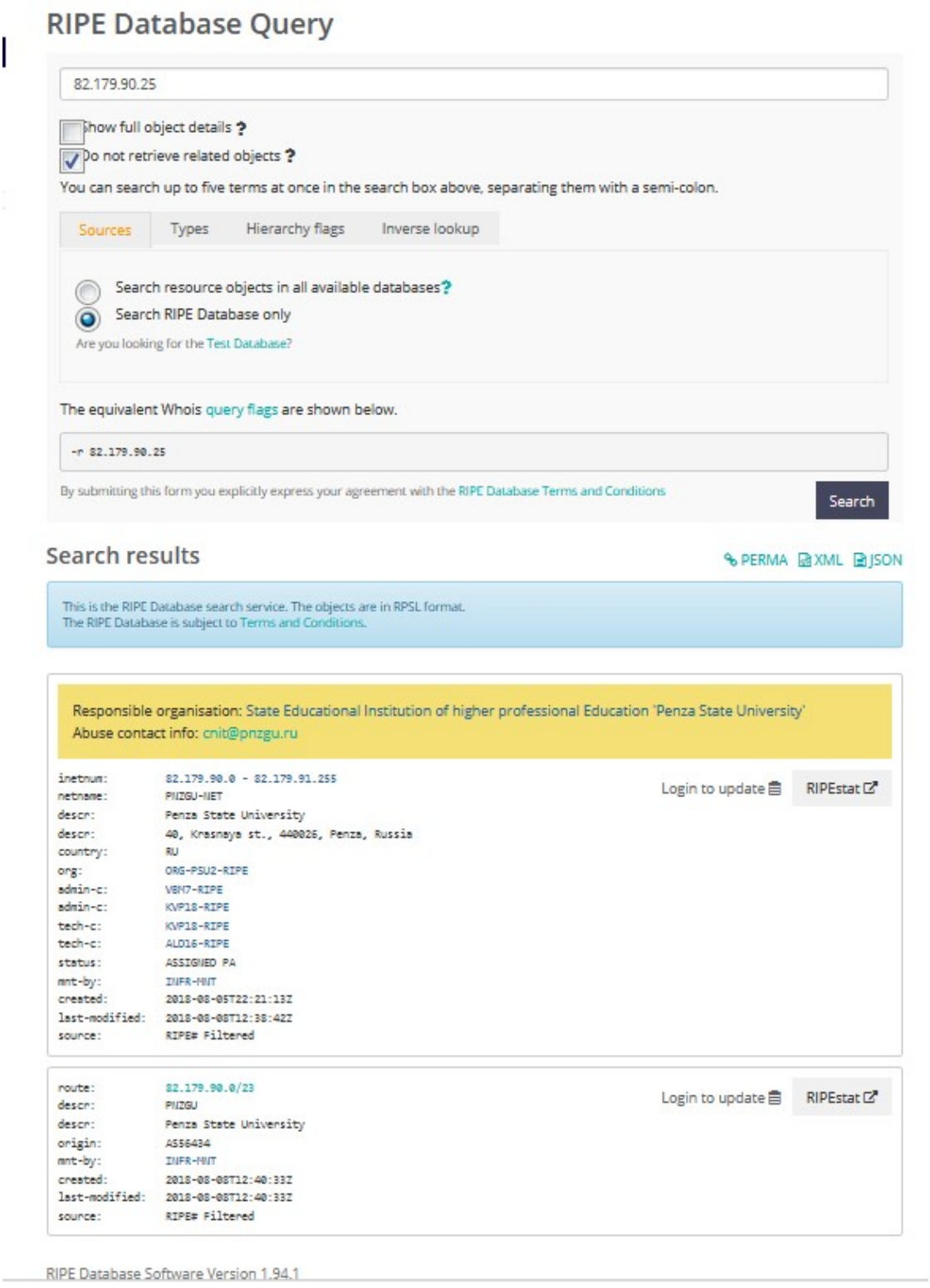


Рис. 1.10. Пример ответа на запрос данных о домене

1.3. Задание на лабораторную работу

1.3.1. С помощью утилиты ***ipconfig,*** запущенной из командной строки, определить имя, IP-адрес и физический адрес основного

сетевого интерфейса компьютера, IP-адрес шлюза, IP-адреса DNS-серверов и использование DHCP. Результаты представить в виде таблицы.

1.3.2. С помощью утилиты ***nslookup*** определить IP-адрес одного из удаленных серверов, доменные имена которых указаны в табл. 1.2, используя при этом DNS-сервер установленный по умолчанию и авторитетный DNS-сервер.

1.3.3. С помощью утилиты ***ping*** проверить состояние связи с любыми компьютером и шлюзом локальной сети, а также с одним из удаленных серверов, доменные имена которых указаны в табл. 1.2.

Таблица 1.2

Доменные имена удаленных серверов

№	Адрес	№	Адрес
1	*penza.myttk.ru*	7	*penza.b2b.domru.ru*
2	*progorod58.ru*	8	*mypenza.ru*
3	*www.penzainform.ru*	9	*penza.com.ru*
4	*penzartc.ru*	10	*penza.domru.ru*
5	*www.penza.ru*	11	*www.zato.ru*
6	*penza.rt.ru*	12	*www.pradas.ru*

Число отправляемых запросов должно составлять не менее 10. Для каждого из исследуемых хостов отразить в виде таблицы IP-адрес хоста назначения, среднее время приема-передачи, процент потерянных пакетов.

1.3.4. С помощью утилиты ***arp*** проверить состояние ARP-кэша. Провести пингование какого либо хоста локальной сети, адрес которого не был отражен в кэше. Повторно открыть ARP-кэш и проконтролировать модификацию его содержимого. Представить полученные значения ARP-кэша в отчете.

1.3.5. С помощью утилиты ***tracert*** провести трассировку одного из удаленных хостов в соответствии с вариантом, выбранным в п. 1.3.2. Если есть потери пакетов, то для соответствующих хостов среднее время прохождения необходимо определять с помощью утилиты ***ping*** по 10 пакетам. В отчете привести копию окна с результатами работы утилиты ***tracert***.

1.3.6. Определить участок сети между двумя соседними маршрутизаторами, который характеризуется наибольшей задержкой

при пересылке пакетов. Для найденных маршрутизаторов с помощью сервиса ***Whois*** определить название организаций и контактные данные администратора (тел., e-mail). Полученную информацию привести в отчете.

1.3.7. С помощью утилиты ***netstat*** посмотреть активные текущие сетевые соединения и их состояние на вашем компьютере, для чего:

- запустить веб-браузера, загрузив из его различные страницы с разных веб-сайтов (по указанию преподавателя);
- закрыть браузеры и с помощью ***netstat*** проверить изменение списка сетевых подключений.

Проконтролировать сетевые соединения в реальном масштабе времени, для чего:

- закрыть ранее открытые сетевые приложения;
- запустить из командной строки утилиту ***netstat***, задав числовой формат отображения адресов и номеров портов и повторный вывод с периодом 20–30 с;
- в отдельном окне командной строки запустить утилиту ***ping*** в режиме «до прерывания»;
- наблюдать отображение ***netstat***, текущей статистики сетевых приложений;
- с помощью клавиш ***Ctrl+C*** последовательно закрыть утилиты ***ping*** и ***netstat***.

В отчете привести копии окон с результатами работы утилиты ***netstat*** с пояснением отображаемой информации.

1.4. Вопросы для самопроверки

1. Каковы назначение и форматы MAC- и IP-адресов? С какой целью применяется «маска подсети»?
2. Как по IP-адресу и маске одной из рабочих станций определить адрес, принадлежащий всей локальной сети?
3. Как определить MAC-адрес сетевого адаптера, установленного в компьютере?
4. Что такое «основной шлюз»?
5. Каким образом утилита ***ping*** проверяет соединение с удаленным хостом?
6. Сколько промежуточных маршрутизаторов сможет пройти IP-пакет, если его время жизни равно 30?

7. Как работает утилита ***tracert***?

8. Что изменится в работе ***tracert,*** если убрать ключ ***-d***? Какой дополнительный трафик при этом будет генерироваться?

9. Каково назначение утилиты ***arp***?

10. С помощью каких утилит можно определить по доменному имени хоста его IP-адрес?

11. Как утилита ***ping*** разрешает имена хостов в IP-адреса?

12. Какие могут быть причины неудачного завершения ***ping*** и ***tracert***?

13. Какая служба позволяет узнать символьное имя хоста по его IP-адресу?

14. Какие операции можно выполнить с помощью утилиты ***netstat***?

15. Какой DNS-сервер называется авторитетным.