**Диагностические сетевые утилиты и их использование**

Целью работы является изучениеадресации в IP-сетях V.4. а также методов контроля и мониторинга сетей, построенных на базе стека протоколов TCP/IP с помощью диагностических утилит операционной системы Windows.

1. Адресация в IP-сетях V.4

Главными параметрами сетевых подключений (сетевых адаптеров компьютеров, принтеров и др.) являются их канальные и сетевые адреса.

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

**Канальный адрес**

Канальный адрес хоста определяется технологией, с помощью которой осуществляется его подключение к Internet. Для машин, входящих в локальные сети Ethernet, это так называемый МАС-адрес *(Media Access Control* - управление доступом к среде) сетевого адаптера, который назначается производителем оборудования и является уникальным. Для существующих технологий локальных сетей МАС-адрес 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.

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

**Сетевой адрес**

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 подразделений InterNIC, а затем распределяют их между своими абонентами. В случае изолированной от Internet локальной сети уникальность сетевого адреса требуется лишь в ее пределах, при этом IP-адреса должны выбираться администратором из специально зарезервированных для таких сетей блоков «закрытых или серых» адресов.

В наиболее (пока, т.к. на смену пришел протокол IP.v6) распространенной четвертой версии протоколов Internet (IP.v4) IP-адрес представляет собой 32-битовое двоичное число (4 байта).

Договорились записывать IP адрес не как единое десятичное число (эквивалент 32-разрядного двоичного), а в виде четырех десятичных чисел (значения от 0 до 255), разделенных точками (например, 192.168.0.1). Каждое такое число соответствует значению одного из четырех байтов (слева направо).

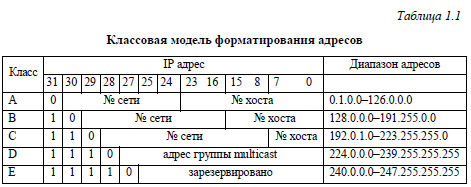
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 192 | | | | | | | | 168 | | | | | | | | 0 | | | | | | | | 1 | | | | | | | |
| адрес сети | | | | | | | | | | | | | | | | | | | | | | | | адрес хоста | | | | | | | |

Он состоит из двух частей - адреса сети и адреса хоста в сети.

Есть две модели формирования IP адреса:

* классовая;
* бесклассовая.

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



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 адрес, а всю сеть;

• адрес 127.0.0.1 означает пересылку в пределах одного и того же хоста (используется для автономной отладки сетевого ПО);

• адреса "серых" сетей (частная 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.

Пакеты не могут быть посланы по этим адресам в Интернет, т.к. не дойдут до своего адресата.

Сейчас в целях более экономного распределения IP-адресов между пользователями классовая модель вытеснена бесклассовой, при которой выделение разрядов в адресе, отводимых для адресации сети строго не регламентировано (как при классовой).

Как же в этом случае определяется какая часть из 32 битов относится к адресу сети, а какая к адресу узла.

Для этого задается специальный четырехбайтовый код - *маска сети*.

Маска сети используется для того чтобы определить какая часть из 32 битов относится к адресу сети, а какая к адресу узла. Эта маска накладывается на IP-адрес.

Те разряды маски, которые имеют единичные значения (они идут сплошняком), показывают биты, которые отводятся под адрес сети, а которые имеют нулевые значения – на адрес хоста.

Например, маска 255.255.255.240:

(двоичный код 11111111.11111111.11111111.11110000)

указывает, что для нумерации сети используется 28 старших разрядов, а для нумерации хоста - только 4 младших разряда соответствующего IP-адреса.

Часто применяется запись IP-адресов вида 192.96.10.0/28. Число после косой черты означает количество единичных разрядов в маске подсети.

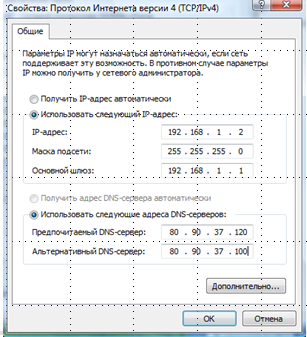
Назначение IP адреса

IP-адреса для конкретных компьютеров могут устанавливаться:

* статически;
* динамически.

При статическом способе адрес устанавливается администратором сети. Каждому компьютеру устанавливается:

* IP адрес;
* маска сети;
* адрес шлюза;
* адрес DNS.

****

При динамическом способе адрес устанавливается автоматически при загрузке операционной системы. Также каждому компьютеру устанавливается:

IP адрес;

маска сети;

адрес шлюза;

адрес DNS.

Для этого применяется специальный протокол DHCP *(Dynamic Host Configuration Protocol),* который обеспечивает динамическое назначение IP-адресов.

Назначаемые адреса формирует DHCP-сервер (он должен быть установлен на одном из компьютеров сети) 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 (время аренды), что дает возможность впоследствии повторно использовать IP-адреса другими компьютерами.

Служба DNS

Компьютеры, при работе в сети, 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 адpeca, 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 (числового) 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: [alice.pnzgu.ru](http://alice.pnzgu.ru)*.*

2. Системные утилиты сетевой диагностики

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.

Утилита *ipconfig*

Утилита *ipconfig* предназначена для проверки правильности конфигурации TCP/IP для операционной системы Windows. Выводит значения для текущей конфигурации стека TCP/IP:

* МАС- и IP-адрес,
* маску подсети,
* адрес шлюза по умолчанию,
* адреса серверов WINS *(Windows Internet Naming Service)*
* DNS,
* использование DHCP.

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

Синтаксис утилиты:

*ipconfig [/all] [/renew[adapter]] [/release [adapter]].*

Параметры (здесь и далее в квадратных скобках указаны необязательные параметры):

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

• *renew [adapter]* обновляет параметры конфигурации DHCP для указанного сетевого адаптера именем *adapter* ;

• *release [adapter]* освобождает выделенный DHCP IP-адрес.

Таким образом, утилита *ipconfig* (рис. 1.1) позволяет выяснить, инициализирована ли конфигурация и не дублируются ли IP-адреса:

• если конфигурация инициализирована, то появляются IP-адрес, маска, шлюз;

• если IP-адреса дублируются, то маска сети будет 0.0.0.0;

• если при использовании DHCP компьютер не смог получить IP-адрес, то он будет равен 0.0.0.0 .

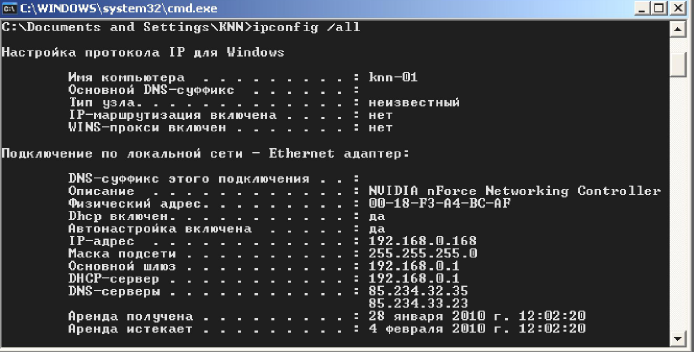
****

Рис. Отображение установленных на компьютере сетевых конфигураций утилитой *ipconfig*

Задание: с помощью утилиты *ipconfig* определить сетевые конфигурации компьютеров "ХР1"и "ХР2".

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 фрагменти-ровать 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 [-t] [-a] [-n count] [-l length] [-f [-i ttl] [-v tos] [-r count] [-s count]* [ *[-j host-list\ [-k host-list]* ] [-w *timeout] 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 фрагментиро-вать», запрещающим фрагментирование пакета на транзитных маршрутизаторах;

*• -i ttl* устанавливает время жизни пакета в величину *ttl* (каждый маршрутизатор уменьшает *ttl* на единицу, т.е. 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 из одной подсети в другую (хопов);

*• -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 рисунке.

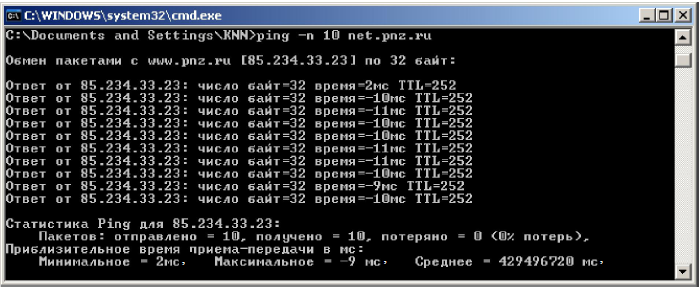
****

Рис. 1.2. Пример использования утилиты *ping*

Утилита *ping* может использоваться следующими способами:

1. Для проверки того, что TCP/IP установлен и правильно сконфигурирован на локальном компьютере, в команде ping задается адрес петли обратной связи : *ping 127.0.0.1*

Если тест успешно пройден, то вы получите следующий ответ:

*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*

2. Чтобы убедиться в том, что компьютер правильно добавлен в сеть и IP-адрес не дублируется, используется IP-адрес локального компьютера: *ping 1Р-адрес\_локального\_хоста.*

3. Чтобы проверить, что шлюз по умолчанию функционирует и можно установить соединение с любым хостом в локальной сети, задается IP-адрес шлюза по умолчанию: *ping 1Р-адрес\_шлюза.*

4. Для проверки возможности установления соединения через маршрутизатор в команде *ping* задается IP-адрес удаленного хоста: *ping 1Р-ад*рес\_удаленного хоста.

Утилита *tracert*

Утилита ***tracert*** *(trace route)* позволяет выявлять последовательность промежуточных маршрутизаторов (шлюзов), через которые проходит IP-пакет на пути к пункту своего назначения путем изучения сообщений ICMP, которые присылаются обратно маршрутизаторами.

Утилита ***tracert*** работает следующим образом: посылается по три пробных эхо-пакета протокола ICMP с TTL=1 на узел назначения.

Первый на пути маршрутизатор пошлет в компьютер-источник сообщение ICMP «Время истекло». Затем TTL увеличивается на "1" и пакет отсылается к следующему маршрутизатору.

Так делается и 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 числовым IP-адресом машины.

Результат работы утилиты − список хостов (маршрутизаторов), начиная с первого шлюза и заканчивая пунктом назначения. При этом на экран выводится еще и время ожидания ответа на каждый пакет.

В тех случаях, когда удаленный узел не достижим (***ping*** не проходит), применение утилиты ***tracert*** позволяет локализовать место 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 не будут видны утилите tracert.

Синтаксис утилиты: tracert [-d] [-h maximumhops ] [-j host-list] [-w timeout] 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 рисунке.

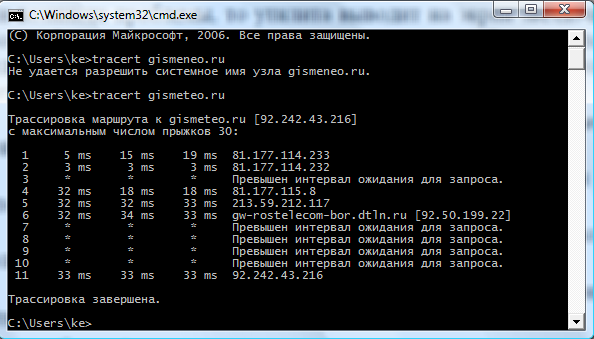


Рис. Пример использования утилиты ***tracert***

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.

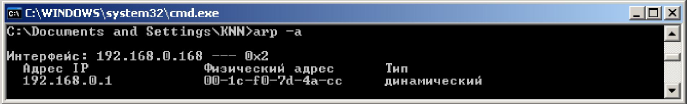
Синтаксис утилиты: arp [-s inetaddr ethaddr] [-d inetaddr] [-a].

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 рисунке.



Пример использования утилиты arp

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 маршрутов (таблица маршрутизации);

• -s отображает подробную статистику по протоколам. По умолчанию выводятся данные для TCP, UDP и IP. Ключ p позволяет задать вывод данных по определенному протоколу, ключ 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 является список активных подключений, в который входят установленные соединения и открытые порты (см. рисунок).

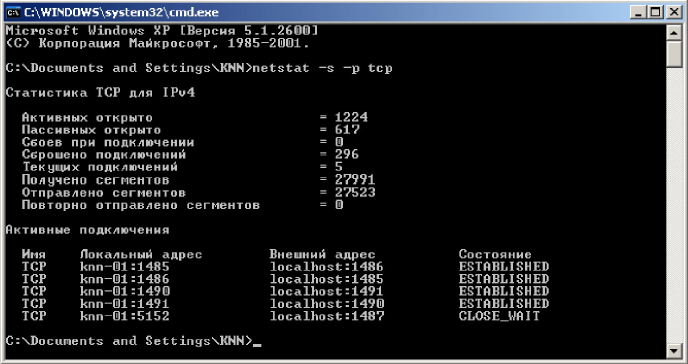


Рис. Пример отображения утилитой netstat установленных на компьютере TCP-соединений

Открытые TCP-порты обозначаются в колонке «Состояние» строкой LISTENING - пассивно открытые соединения («слушающие» сокеты) или ESTABLISHED - установленные соединения, т.е. уже используемые сетевыми сервисами.

Часть портов связана с системными службами Windows и отображается 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.

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 [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).

Результаты выполнения команды nslookup приведены на рисунке.

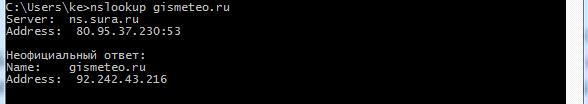


Рис. Пример отображения утилитой nslookup запроса к DNS

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 **Non-authoritative answer (Неофициальный ответ)**, означающее, что ответ получен не с DNS-сервера, ответственного за зону [sura.ru](http://penza.ru). Также может присутствовать строка Aliase, которая содержит альтернативные имена искомого сервера.arp