

Администрирование ИС. Практикум 1. Тема – Диагностика сетей. Сетевые утилиты.

Введение

В практикуме рассматривается круг вопросов, связанных с основами сетевой диагностики. Целью практикума является развитие у студентов навыков использования сетевых утилит.

Постановка задачи

Используя стандартные сетевые утилиты, проанализировать конфигурацию сети на платформе ОС Windows, т.е. получить свой IP-адрес, узнать имя домена, имена компьютеров, входящих в домен, просмотреть и при необходимости подключить общие ресурсы, определить причину возможных неполадок, так же получить информацию об использовании портов.

Краткая теоретическая справка

Повседневная работа сетевого администратора сводится к мониторингу и анализу работы сети. Наличие простых и удобных инструментов позволяет быстро разобраться с неполадками и принять своевременные меры к их устранению.

Мониторинг и анализ сети представляют собой важные этапы контроля работы сети. Для решения этих задач регулярно производится сбор данных, который дает базу для изучения производительности сети. В сетевых операционных системах, и в частности, в Windows, существует множество мощных утилит для пересылки текстовых сообщений, управления общими ресурсами, диагностике сетевых подключений, поиска и обработки ошибок.

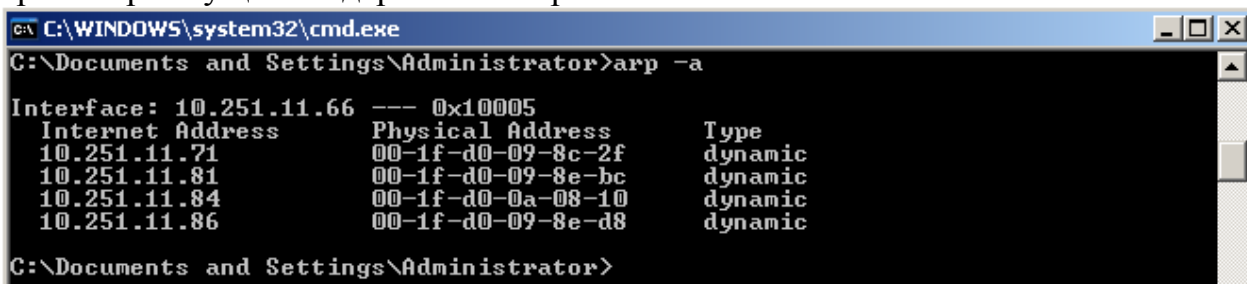
Сетевые утилиты

Утилита cmd

Командный интерпретатор операционных систем Windows. Используйте командный интерпретатор для запуска сетевых утилит.

Утилита arp.

Используется для просмотра arp - таблиц (arp - кэша) локального компьютера (хоста) а также внесения и удаления статических записей в arp кэш. Выполните просмотр текущего содержимого arp кэша.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>arp -a

Interface: 10.251.11.66 --- 0x10005
Internet Address      Physical Address      Type
10.251.11.71          00-1f-d0-09-8c-2f     dynamic
10.251.11.81          00-1f-d0-09-8e-bc     dynamic
10.251.11.84          00-1f-d0-0a-08-10     dynamic
10.251.11.86          00-1f-d0-09-8e-d8     dynamic
C:\Documents and Settings\Administrator>
```

Добавьте новую статическую запись в arp – кэш

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>arp -s 10.251.11.69 00-1f-d0-08-11-12
C:\Documents and Settings\Administrator>
```

Проверьте, что новая статическая запись добавлена в Arp – кэш.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>arp -s 10.251.11.69 00-1f-d0-08-11-12
C:\Documents and Settings\Administrator>arp -a

Interface: 10.251.11.66 --- 0x10005
Internet Address      Physical Address      Type
10.251.11.69          00-1f-d0-08-11-12    static
10.251.11.81          00-1f-d0-09-8e-bc    dynamic
10.251.11.84          00-1f-d0-0a-08-10    dynamic
10.251.11.86          00-1f-d0-09-8e-d8    dynamic
C:\Documents and Settings\Administrator>
```

Удалите статическую запись из Arp – кэша.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>arp -d 10.251.11.69
C:\Documents and Settings\Administrator>_
```

Убедитесь, что Arp – кэш не содержит статических записей.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>arp -d 10.251.11.69
C:\Documents and Settings\Administrator>arp -a

Interface: 10.251.11.66 --- 0x10005
Internet Address      Physical Address      Type
10.251.11.70          00-1f-d0-0c-cc-f9    dynamic
10.251.11.80          00-1f-d0-0c-cc-8a    dynamic
10.251.11.82          00-1f-d0-0a-00-5e    dynamic
10.251.11.84          00-1f-d0-0a-08-10    dynamic
10.251.11.86          00-1f-d0-09-8e-d8    dynamic
10.251.11.105         00-1f-d0-09-81-34    dynamic
C:\Documents and Settings\Administrator>_
```

Утилита hostname

Выводит сетевое имя локального компьютера (хоста). Она доступна только после установки поддержки протокола TCP/IP. Пример вызова команды.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>hostname
sserver
C:\Documents and Settings\Administrator>_
```

Утилита **ipconfig**

Выводит диагностическую информацию о конфигурации сети TCP/IP. Эта утилита позволяет просмотреть текущую сетевую конфигурацию узлов сети. Синтаксис утилиты **ipconfig**:

ipconfig [/all | /renew [адаптер] | /release [адаптер]] /displaydns /flushdns

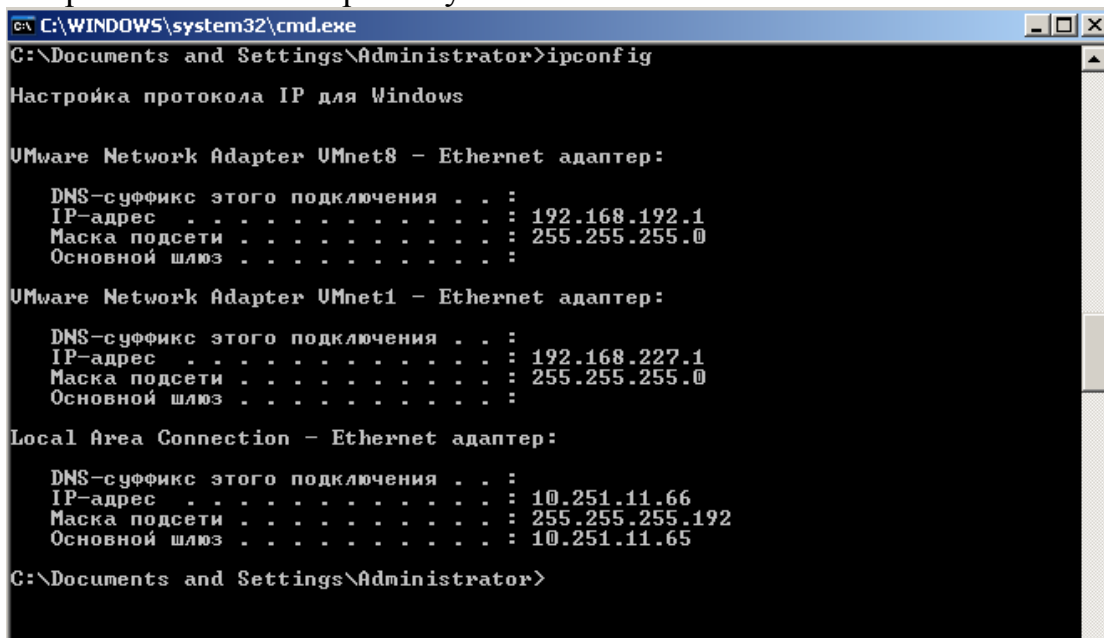
/all - выводит сведения о имени хоста, DNS (Domain Name Service), типе узла, IP-маршрутизации и др. Без этого параметра команда **ipconfig** выводит только IP-адреса, маску подсети и основной шлюз;

/renew [адаптер] - обновляет параметры конфигурации DHCP (Dynamic Host Configuration Protocol – автоматическая настройка IP-адресов). Эта возможность доступна только на компьютерах, где запущена служба клиента DHCP. Для задания адаптера используется имя, выводимое командой **ipconfig** без параметров;

/release [адаптер] - очищает текущую конфигурацию DHCP. Эта возможность отключает TCP/IP на локальных компьютерах и доступна только на клиентах DHCP. Для задания адаптера используется имя, выводимое командой **ipconfig** без параметров. Эта команда часто используется перед перемещением компьютера в другую сеть. После использования утилиты **ipconfig /release**, IP-адрес становится доступен для назначения другому компьютеру.

/displaydns, **/flushdns** выводит/сбрасывает содержимое кэша локального распознавателя DNS (записи в кэше могут устаревать)

Просмотрите сетевые настройки узла.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig

Настройка протокола IP для Windows

VMware Network Adapter VMnet8 - Ethernet адаптер:
    DNS-суффикс этого подключения . . . :
    IP-адрес . . . . . : 192.168.192.1
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз . . . . . :

VMware Network Adapter VMnet1 - Ethernet адаптер:
    DNS-суффикс этого подключения . . . :
    IP-адрес . . . . . : 192.168.227.1
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз . . . . . :

Local Area Connection - Ethernet адаптер:
    DNS-суффикс этого подключения . . . :
    IP-адрес . . . . . : 10.251.11.66
    Маска подсети . . . . . : 255.255.255.192
    Основной шлюз . . . . . : 10.251.11.65

C:\Documents and Settings\Administrator>
```

Выведите полный перечень сетевых настроек узла.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig /all

Настройка протокола IP для Windows

Имя компьютера . . . . . : sserver
Основной DNS-суффикс . . . . . : class542.ru
Тип узла. . . . . : неизвестный
IP-маршрутизация включена . . . . . : нет
WINS-прокси включен . . . . . : нет
Порядок просмотра суффиксов DNS . . . . . : class542.ru

VMware Network Adapter VMnet8 - Ethernet адаптер:

DNS-суффикс этого подключения . . . :
Описание . . . . . : VMware Virtual Ethernet Adapter for VMnet
8
Физический адрес. . . . . : 00-50-56-C0-00-08
DHCP включен. . . . . : нет
IP-адрес . . . . . : 192.168.192.1
Маска подсети . . . . . : 255.255.255.0
Основной шлюз . . . . . :

VMware Network Adapter VMnet1 - Ethernet адаптер:

DNS-суффикс этого подключения . . . :
Описание . . . . . : VMware Virtual Ethernet Adapter for VMnet
1
Физический адрес. . . . . : 00-50-56-C0-00-01
DHCP включен. . . . . : нет
IP-адрес . . . . . : 192.168.227.1
Маска подсети . . . . . : 255.255.255.0
Основной шлюз . . . . . :

Local Area Connection - Ethernet адаптер:

DNS-суффикс этого подключения . . . :
```

Сделайте просмотр кэша DNS – распознавателя локального узла.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig /displaydns

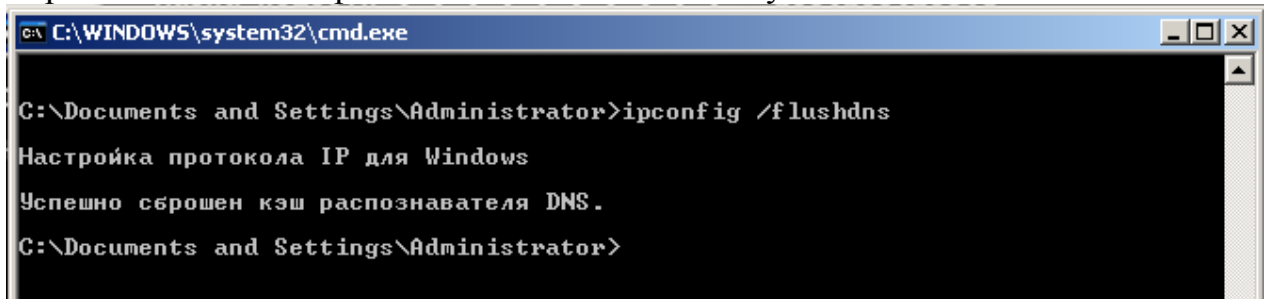
Настройка протокола IP для Windows

1.0.0.127.in-addr.arpa
-----
Имя записи . . . . . : 1.0.0.127.in-addr.arpa.
Тип записи . . . . . : 12
Срок жизни <TTL>. . . . . : 569946
Длина данных. . . . . : 4
Раздел . . . . . : Ответ
PTR-запись . . . . . : localhost

localhost
-----
Имя записи . . . . . : localhost
Тип записи . . . . . : 1
Срок жизни <TTL>. . . . . : 569946
Длина данных. . . . . : 4
Раздел . . . . . : Ответ
A-запись <узла> . . . . . : 127.0.0.1

C:\Documents and Settings\Administrator>
```

Сбросьте кэш DNS – распознавателя локального узла



```
C:\WINDOWS\system32\cmd.exe

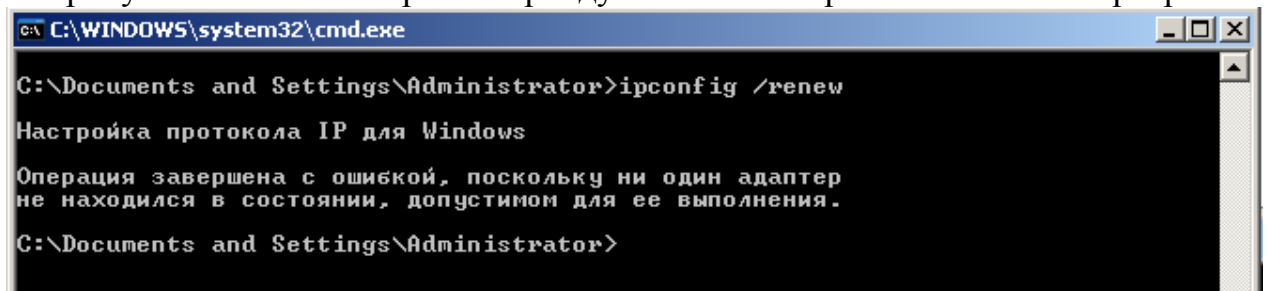
C:\Documents and Settings\Administrator>ipconfig /flushdns

Настройка протокола IP для Windows

Успешно сброшен кэш распознавателя DNS.

C:\Documents and Settings\Administrator>
```

Попробуйте обновить запрос на аренду сетевых настроек от DHCP – сервера.



```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator>ipconfig /renew

Настройка протокола IP для Windows

Операция завершена с ошибкой, поскольку ни один адаптер
не находился в состоянии, допустимом для ее выполнения.

C:\Documents and Settings\Administrator>
```

Из – за назначения статических настроек эта команда должна выполняться с ошибкой.

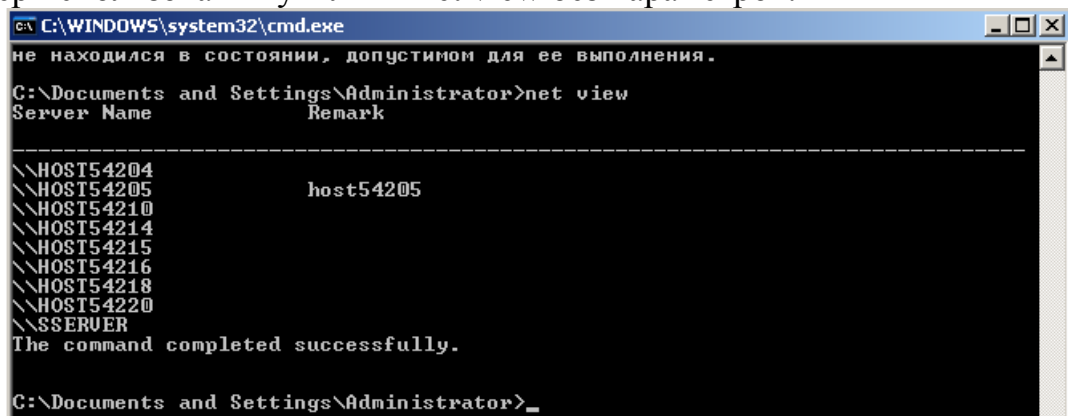
Утилита net view

Просматривает список доменов, компьютеров или общих ресурсов на данном компьютере. Синтаксис утилиты net view:

net view [/\\компьютер | /domain[:домен]];

net view /network:nw [/\\компьютер] – используется в сетях Novell NetWare, где \\компьютер - задает имя компьютера для просмотра общих ресурсов; /domain[:домен] - задает домен, для которого выводится список компьютеров. Если параметр не указан, выводятся сведения обо всех доменах в сети; Вызванная без параметров, утилита выводит список компьютеров в текущем домене.

Пример использования утилиты net view без параметров:



```
C:\WINDOWS\system32\cmd.exe

не находился в состоянии, допустимом для ее выполнения.

C:\Documents and Settings\Administrator>net view

Server Name          Remark
-----
\\HOST54204
\\HOST54205           host54205
\\HOST54210
\\HOST54214
\\HOST54215
\\HOST54216
\\HOST54218
\\HOST54220
\\SSERVER
The command completed successfully.

C:\Documents and Settings\Administrator>_
```

Просмотр открытых ресурсов локального узла.

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator>net view sserver
Shared resources at sserver

Share name      Type  Used as  Comment
-----
Distribs        Disk
for_students    Disk
NETLOGON        Disk      Общий сервер входа
nod             Disk
os              Disk
profile         Disk
public          Disk
SYSVOL          Disk      Общий сервер входа
The command completed successfully.

C:\Documents and Settings\Administrator>
```

Утилита pathping

Выполняет низкоуровневую диагностику сетевых соединений, отслеживая количество переданных, потерянных сетевых пакетов, статистику потерь в ходе передачи данных по сети.

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator>pathping sserver

Трассировка маршрута к sserver.class542.ru [10.251.11.66]
с максимальным числом прыжков 30:
 0 sserver.class542.ru [10.251.11.66]
 1 sserver.class542.ru [10.251.11.66]

Подсчет статистики за: 25 сек. ...
      Исходный узел      Маршрутный узел
Прыжок  RTT   Утер./Отпр.   %   Утер./Отпр.   %   Адрес
0
      0
      0/ 100 = 0%      0/ 100 = 0%   !   sserver.class542.ru [10.251.11.66]
1      0мс      0/ 100 = 0%      0/ 100 = 0%   sserver.class542.ru [10.251.11.66]

Трассировка завершена.

C:\Documents and Settings\Administrator>
```

1.3.4 Утилита ping

Проверяет сетевые соединения с удаленным компьютером или компьютерами. Эта команда доступна только после установки поддержки протокола TCP/IP. Синтаксис утилиты ping:

ping [-t] [-a] [-n счетчик] [-l длина] [-f] [-i ttl] [-v тун] [-r счетчик] [-s число] [[-j список_комп] | [-k список_комп]] [-w интервал] список_назначения;

где ***-t*** - повторяет запросы к удаленному компьютеру, пока программа не будет остановлена;

-a - разрешает имя компьютера в адрес;

-n счетчик - передается число пакетов ЕСНО, заданное параметром. По умолчанию – 4;

-l длина - отправляются пакеты типа ЕСНО, содержащие порцию данных заданной длины. По умолчанию - 32 байта, максимум – 65527;

-f - отправляет пакеты с флагом запрещения фрагментации (Do not Fragment). Пакеты не будут разрываться при прохождении шлюзов на своем маршруте;

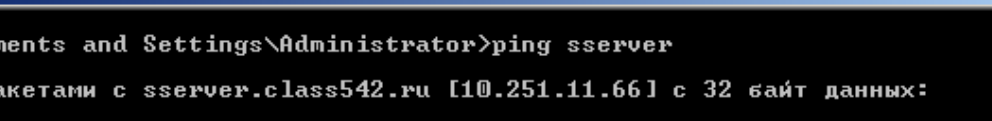
-i ttl - устанавливает время жизни пакетов TTL (Time To Live);

-v тип - устанавливает тип службы (Type Of Service) пакетов;

-r счетчик - записывает маршрут отправленных и возвращенных пакетов в поле записи маршрута Record Route. Параметр счетчик задает число компьютеров в интервале от 1 до 9;

-s число - задает число ретрансляций на маршруте, где делается отметка времени;

Выполните команду:



The screenshot shows a Windows command prompt window with the title bar "C:\WINDOWS\system32\cmd.exe". The command prompt shows the following text:

```
C:\Documents and Settings\Administrator>ping sserver

Обмен пакетами с sserver.class542.ru [10.251.11.66] с 32 байт данных:

Ответ от 10.251.11.66: число байт=32 время<1мс TTL=128
Ответ от 10.251.11.66: число байт=32 время<1мс TTL=128
Ответ от 10.251.11.66: число байт=32 время<1мс TTL=128
Ответ от 10.251.11.66: число байт=32 время<1мс TTL=128

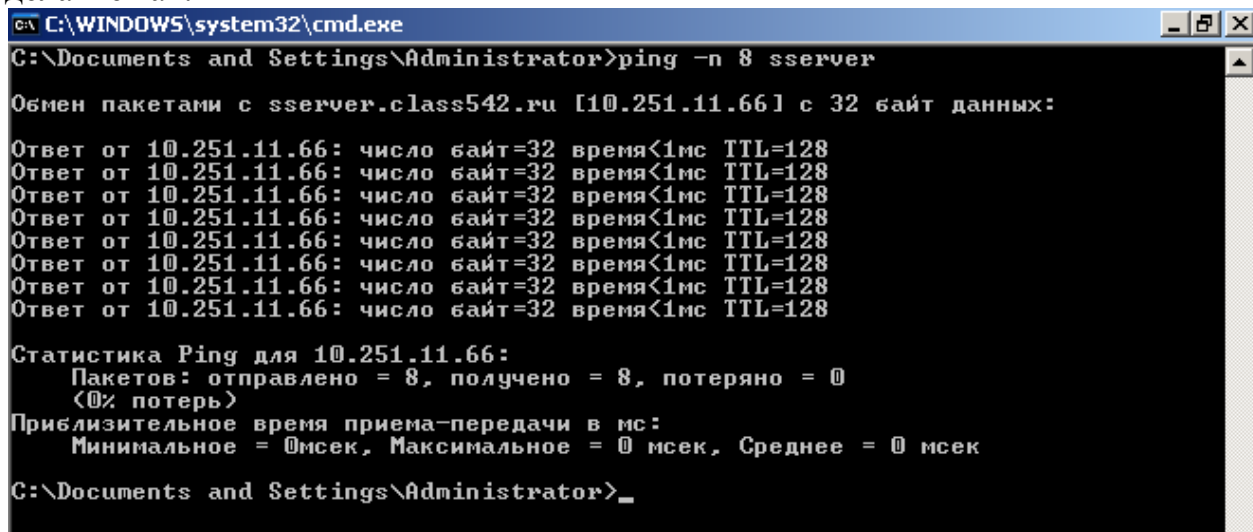
Статистика Ping для 10.251.11.66:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

C:\Documents and Settings\Administrator>
```

В определенных ситуациях (для диагностики) удобно посылать запросы в «бесконечном» режиме

[illegible]

Если вам необходимо послать строго фиксированное количество пакетов, делайте так.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ping -n 8 sserver

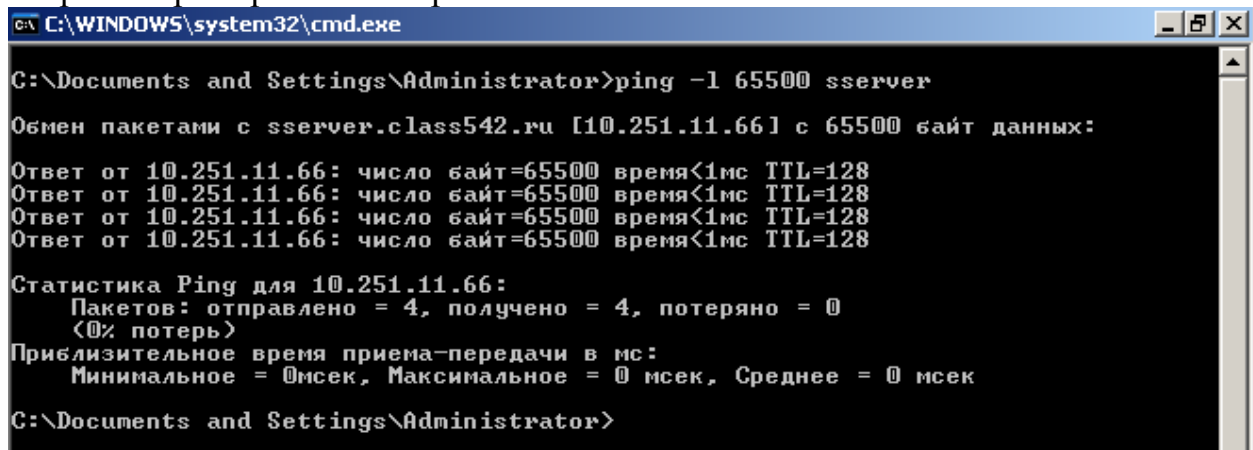
Обмен пакетами с sserver.class542.ru [10.251.11.66] с 32 байт данных:

Ответ от 10.251.11.66: число байт=32 время<1мс TTL=128
Ответ от 10.251.11.66: число байт=32 время<1мс TTL=128
Ответ от 10.251.11.66: число байт=32 время<1мс TTL=128
Ответ от 10.251.11.66: число байт=32 время<1мс TTL=128
Ответ от 10.251.11.66: число байт=32 время<1мс TTL=128
Ответ от 10.251.11.66: число байт=32 время<1мс TTL=128
Ответ от 10.251.11.66: число байт=32 время<1мс TTL=128
Ответ от 10.251.11.66: число байт=32 время<1мс TTL=128

Статистика Ping для 10.251.11.66:
    Пакетов: отправлено = 8, получено = 8, потеряно = 0
    (<0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

C:\Documents and Settings\Administrator>
```

Старые версии систем Linux можно было вывести из строя с помощью “пинга смерти”. Пример пинга смерти:



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ping -l 65500 sserver

Обмен пакетами с sserver.class542.ru [10.251.11.66] с 65500 байт данных:

Ответ от 10.251.11.66: число байт=65500 время<1мс TTL=128
Ответ от 10.251.11.66: число байт=65500 время<1мс TTL=128
Ответ от 10.251.11.66: число байт=65500 время<1мс TTL=128
Ответ от 10.251.11.66: число байт=65500 время<1мс TTL=128

Статистика Ping для 10.251.11.66:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (<0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

C:\Documents and Settings\Administrator>
```

Утилита netstat

Выводит статистику протокола и текущих подключений сети TCP/IP. Эта команда доступна только после установки поддержки протокола TCP/IP. Синтаксис утилиты netstat:

netstat [-a] [-e] [-n] [-s] [-p протокол] [-r] [интервал];

где -a - выводит все подключения и сетевые порты. Подключения сервера обычно не выводятся;

-e - выводит статистику Ethernet. Возможна комбинация с ключом -s;

-n - выводит адреса и номера портов в шестнадцатеричном формате (а не имена);

-s - выводит статистику для каждого протокола. По умолчанию выводится статистика для TCP, UDP, ICMP (Internet Control Message Protocol) и IP.

Ключ -р может быть использован для указания подмножества стандартных протоколов;

-р протокол - выводит соединения для протокола, заданного параметром. Параметр может иметь значения *tcp* или *udp*. Если используется с ключом -s для вывода статистики по отдельным протоколам, то параметр может принимать значения tcp, udp, icmp или ip;

-r - выводит таблицу маршрутизации;

Итак, используем утилиту netstat.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>netstat -e
Статистика интерфейса
```

	Получено	Отправлено
Байт	57002816	336204191
Одноадресные пакеты	381175	451965
Многоадресные пакеты	12888	5983
Отброшено	0	0
Ошибки	0	0
Неизвестный протокол	0	0

```
C:\Documents and Settings\Administrator>_
```

Детализация статистики по каждому протоколу

```
C:\WINDOWS\system32\cmd.exe
Неизвестный протокол 0
C:\Documents and Settings\Administrator>netstat -es
Статистика интерфейса
```

	Получено	Отправлено
Байт	57006866	336205355
Одноадресные пакеты	381207	451977
Многоадресные пакеты	12915	5995
Отброшено	0	0
Ошибки	0	0
Неизвестный протокол	0	0

```
Статистика IPv4
```

Получено пакетов	=	382915
Получено ошибок в заголовках	=	0
Получено ошибок в адресах	=	200
Направлено датаграмм	=	0
Получено неизвестных протоколов	=	0
Отброшено полученных пакетов	=	0
Доставлено полученных пакетов	=	381907
Запросов на вывод	=	462517
Отброшено маршрутов	=	0
Отброшено выходных пакетов	=	0
Выходных пакетов без маршрута	=	0
Требуется сборка	=	1032
Успешная сборка	=	24
Сбоев при сборке	=	0
Успешно фрагментировано датаграмм	=	24
Сбоев при фрагментации датаграмм	=	0
Создано фрагментов	=	1032

```
Статистика ICMPv4
```

	Получено	Отправлено
Сообщений	4785	4781
Ошибок	0	0
'Назначение недостижимо'	7	3
Превышений времени	0	0
Ошибок в параметрах	0	0
Просьба "снизить скорость"	0	0
Переадресовано	0	0
Эхо-сообщений	2848	1930
Ответных пакетов	1930	2848

Список открытых сокетов

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>netstat -a

Активные подключения

Имя      Локальный адрес      Внешний адрес      Состояние
TCP      sserver:ftp          sserver.class542.ru:0 LISTENING
TCP      sserver:domain       sserver.class542.ru:0 LISTENING
TCP      sserver:http          sserver.class542.ru:0 LISTENING
TCP      sserver:kerberos     sserver.class542.ru:0 LISTENING
TCP      sserver:epmap        sserver.class542.ru:0 LISTENING
TCP      sserver:ldap         sserver.class542.ru:0 LISTENING
TCP      sserver:microsoft-ds sserver.class542.ru:0 LISTENING
TCP      sserver:kpaswd       sserver.class542.ru:0 LISTENING
TCP      sserver:http-rpc-epmap sserver.class542.ru:0 LISTENING
TCP      sserver:ldaps        sserver.class542.ru:0 LISTENING
TCP      sserver:912          sserver.class542.ru:0 LISTENING
TCP      sserver:1026         sserver.class542.ru:0 LISTENING
TCP      sserver:1027         sserver.class542.ru:0 LISTENING
TCP      sserver:1044         sserver.class542.ru:0 LISTENING
TCP      sserver:1171         sserver.class542.ru:0 LISTENING
TCP      sserver:1188         sserver.class542.ru:0 LISTENING
TCP      sserver:2221         sserver.class542.ru:0 LISTENING
TCP      sserver:msft-gc      sserver.class542.ru:0 LISTENING
TCP      sserver:msft-gc-ssl  sserver.class542.ru:0 LISTENING
TCP      sserver:3306         sserver.class542.ru:0 LISTENING
TCP      sserver:5750         sserver.class542.ru:0 LISTENING
TCP      sserver:epmap        sserver.class542.ru:3731 ESTABLISHED
TCP      sserver:netbios-ssn  sserver.class542.ru:0 LISTENING
TCP      sserver:ldap         sserver.class542.ru:3681 ESTABLISHED
TCP      sserver:1026         sserver.class542.ru:1175 ESTABLISHED
TCP      sserver:1026         sserver.class542.ru:1329 ESTABLISHED
TCP      sserver:1026         sserver.class542.ru:3732 ESTABLISHED
TCP      sserver:1175         sserver.class542.ru:1026 ESTABLISHED
TCP      sserver:1329         sserver.class542.ru:1026 ESTABLISHED
TCP      sserver:3681         sserver.class542.ru:ldap ESTABLISHED
TCP      sserver:3731         sserver.class542.ru:epmap ESTABLISHED
TCP      sserver:3732         sserver.class542.ru:1026 ESTABLISHED
TCP      sserver:ldap         sserver.class542.ru:1046 ESTABLISHED
TCP      sserver:ldap         sserver.class542.ru:1047 ESTABLISHED
TCP      sserver:ldap         sserver.class542.ru:1048 ESTABLISHED
TCP      sserver:ldap         sserver.class542.ru:3668 ESTABLISHED
```

Таблица маршрутизации.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>netstat -rn

IPv4 таблица маршрута
=====
Список интерфейсов
0x1 ..... MS TCP Loopback interface
0x2 ...00 50 56 c0 00 08 ..... VMware Virtual Ethernet Adapter for VMnet8
0x3 ...00 50 56 c0 00 01 ..... VMware Virtual Ethernet Adapter for VMnet1
0x10005 ...00 16 17 91 d5 10 ..... Realtek RTL8139 Family PCI Fast Ethernet NIC
=====
Активные маршруты:
Сетевой адрес      Маска сети      Адрес шлюза      Интерфейс      Метрика
0.0.0.0            0.0.0.0         10.251.11.65     10.251.11.66   20
10.251.11.64       255.255.255.192 10.251.11.66     10.251.11.66   20
10.251.11.66       255.255.255.255 127.0.0.1        127.0.0.1      20
10.255.255.255     255.255.255.255 10.251.11.66     10.251.11.66   20
127.0.0.0          255.0.0.0       127.0.0.1        127.0.0.1      1
169.254.0.0        255.255.0.0     10.251.11.66     10.251.11.66   30
192.168.192.0      255.255.255.0   192.168.192.1    192.168.192.1  20
192.168.192.1      255.255.255.255 127.0.0.1        127.0.0.1      20
192.168.192.255    255.255.255.255 192.168.192.1    192.168.192.1  20
192.168.227.0      255.255.255.0   192.168.227.1    192.168.227.1  20
192.168.227.1      255.255.255.255 127.0.0.1        127.0.0.1      20
192.168.227.255    255.255.255.255 192.168.227.1    192.168.227.1  20
224.0.0.0          240.0.0.0       10.251.11.66     10.251.11.66   20
224.0.0.0          240.0.0.0       192.168.192.1    192.168.192.1  20
224.0.0.0          240.0.0.0       192.168.227.1    192.168.227.1  20
255.255.255.255    255.255.255.255 10.251.11.66     10.251.11.66   1
255.255.255.255    255.255.255.255 192.168.192.1    192.168.192.1  1
255.255.255.255    255.255.255.255 192.168.227.1    192.168.227.1  1
Основной шлюз:      10.251.11.65
=====
Постоянные маршруты:
Отсутствует
C:\Documents and Settings\Administrator>
```

Можно еще так сделать.

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator>route print

IPv4 таблица маршрута
=====
Список интерфейсов
0x1 ..... MS TCP Loopback interface
0x2 ...00 50 56 c0 00 08 ..... VMware Virtual Ethernet Adapter for VMnet8
0x3 ...00 50 56 c0 00 01 ..... VMware Virtual Ethernet Adapter for VMnet1
0x10005 ...00 16 17 91 d5 10 ..... Realtek RTL8139 Family PCI Fast Ethernet NIC
=====

Активные маршруты:
Сетевой адрес      Маска сети      Адрес шлюза      Интерфейс      Метрика
0.0.0.0            0.0.0.0         10.251.11.65     10.251.11.66   20
10.251.11.64       255.255.255.192 10.251.11.66     10.251.11.66   20
10.251.11.66       255.255.255.255 127.0.0.1        127.0.0.1      20
10.255.255.255     255.255.255.255 10.251.11.66     10.251.11.66   20
127.0.0.0          255.0.0.0       127.0.0.1        127.0.0.1      1
169.254.0.0        255.255.0.0     10.251.11.66     10.251.11.66   30
192.168.192.0      255.255.255.0   192.168.192.1    192.168.192.1  20
192.168.192.1      255.255.255.255 127.0.0.1        127.0.0.1      20
192.168.192.255    255.255.255.255 192.168.192.1    192.168.192.1  20
192.168.227.0      255.255.255.0   192.168.227.1    192.168.227.1  20
192.168.227.1      255.255.255.255 127.0.0.1        127.0.0.1      20
192.168.227.255    255.255.255.255 192.168.227.1    192.168.227.1  20
224.0.0.0          240.0.0.0       10.251.11.66     10.251.11.66   20
224.0.0.0          240.0.0.0       192.168.192.1    192.168.192.1  20
224.0.0.0          240.0.0.0       192.168.227.1    192.168.227.1  20
255.255.255.255    255.255.255.255 10.251.11.66     10.251.11.66   1
255.255.255.255    255.255.255.255 192.168.192.1    192.168.192.1  1
255.255.255.255    255.255.255.255 192.168.227.1    192.168.227.1  1
Основной шлюз:      10.251.11.65
=====
Постоянные маршруты:
Отсутствует

C:\Documents and Settings\Administrator>
```

Утилита tracert

Диагностическая утилита, предназначенная для определения маршрута до точки назначения с помощью послышки эхо-пакетов протокола ICMP с различными значениями срока жизни (TTL, Time-To-Live). При этом требуется, чтобы каждый маршрутизатор на пути следования пакетов уменьшал эту величину по крайней мере на 1 перед дальнейшей пересылкой пакета. Это делает параметр TTL эффективным счетчиком числа ретрансляций. Предполагается, что когда параметр TTL становится равен 0, маршрутизатор посылает системе-источнику сообщение ICMP «Time Exceeded». Утилита tracert определяет маршрут путем послышки первого эхо-пакета с параметром TTL, равным 1, и с последующим увеличением этого параметра на единицу до тех пор, пока не будет получен ответ из точки назначения или не будет достигнуто максимальное допустимое значение TTL. Маршрут определяется проверкой сообщений ICMP «Time Exceeded», полученных от промежуточных

маршрутизаторов. Однако некоторые маршрутизаторы сбрасывают пакеты с истекшим временем жизни без отправки соответствующего сообщения. Эти маршрутизаторы невидимы для утилиты `tracert`. Синтаксис утилиты `tracert`:

tracert [-d] [-h макс_узел] [-j список_компьютеров] [-w интервал] точка_назн;

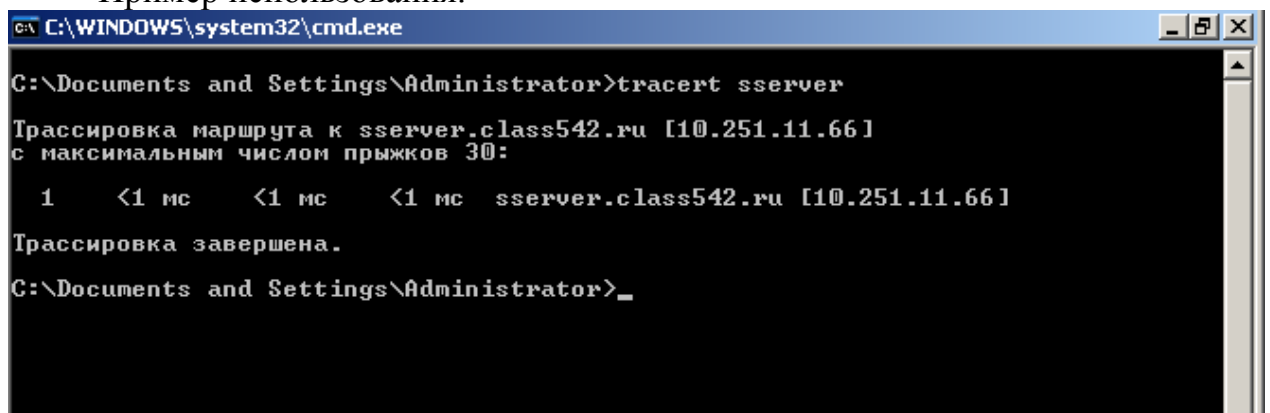
где `-d` - отменяет разрешение имен компьютеров в их адреса;

`-h макс_узел` - задает максимальное количество ретрансляций, используемых при поиске точки назначения;

`-j список_компьютеров` - задает список компьютеров для свободной маршрутизации;

`-w интервал` - задает интервал в миллисекундах, в течение которого будет ожидаться ответ;

Пример использования.



```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator>tracert sserver

Трассировка маршрута к sserver.class542.ru [10.251.11.66]
с максимальным числом прыжков 30:

  1    <1 мс    <1 мс    <1 мс  sserver.class542.ru [10.251.11.66]

Трассировка завершена.
C:\Documents and Settings\Administrator>_
```

Утилита `net use`

Подключает общие сетевые ресурсы или выводит информацию о подключениях компьютера. Команда также управляет постоянными сетевыми соединениями. Синтаксис утилиты `net use`:

net use [устройство | *] [\\компьютер\ресурс[том]] [пароль | *] [/user:[домен\]имя_пользователя] [/delete] [/persistent:{yes | no}]

net use устройство [/home[пароль | *]] [/delete:{yes | no}]

net use [/persistent:{yes | no}],

где устройство - задает имя ресурса при подключении/отключении. Существует два типа имен устройств: дисководы (от D: до Z:) и принтеры (от LPT1: до LPT3:). Ввод символа звездочки обеспечит подключение к следующему доступному имени устройства;

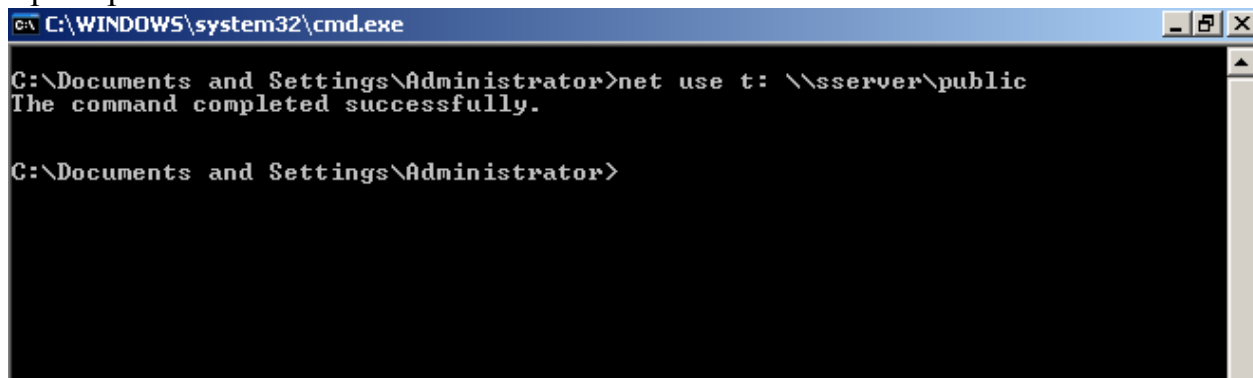
\\компьютер\ресурс - указывает имя сервера и общего ресурса. Если параметр компьютер содержит пробелы, все имя компьютера от двойной обратной черты (\\) до конца должно быть заключено в кавычки (" "). Имя компьютера может иметь длину от 1 до 15 символов;

том - задает имя тома системы Novell NetWare. Для подключения к серверам Novell NetWare должна быть запущена служба клиента сети Novell NetWare

(для Windows 2000 Professional) или служба шлюза сети Novell NetWare (для Windows 2000 Server);

пароль - задает пароль, необходимый для подключения к общему ресурсу;

Пример использования net use.

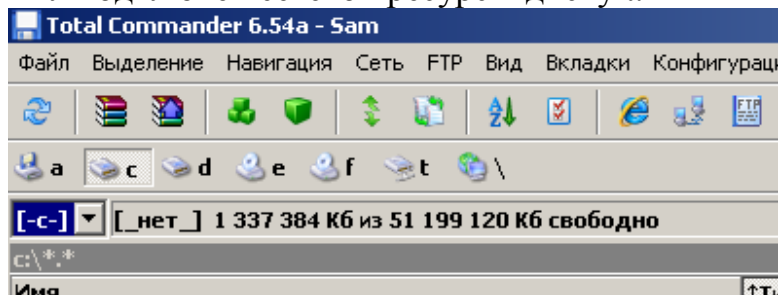


```
C:\WINDOWS\system32\cmd.exe

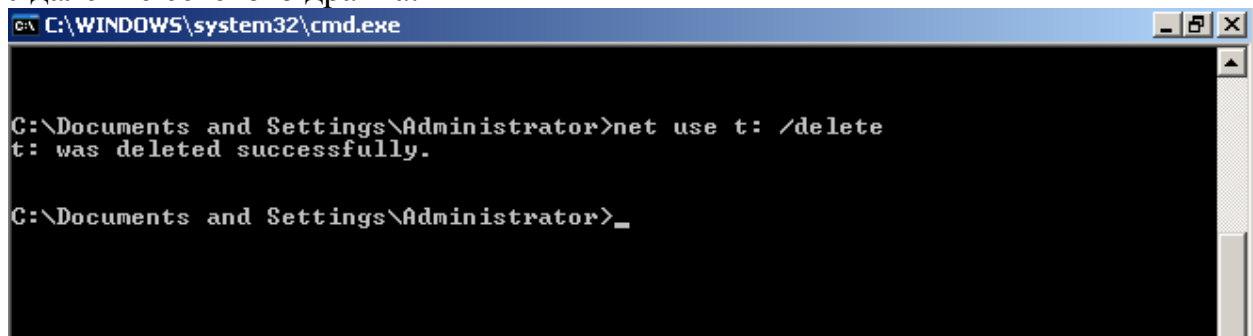
C:\Documents and Settings\Administrator>net use t: \\sserver\public
The command completed successfully.

C:\Documents and Settings\Administrator>
```

Был подключен сетевой ресурс к диску t.



Удаление сетевого драйва.



```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator>net use t: /delete
t: was deleted successfully.

C:\Documents and Settings\Administrator>_
```

Утилита net send

Отправка сообщения другому пользователю, компьютеру или псевдониму в сети. Служба сообщений должна быть запущена на компьютере для получения сообщений. Синтаксис утилиты net send:

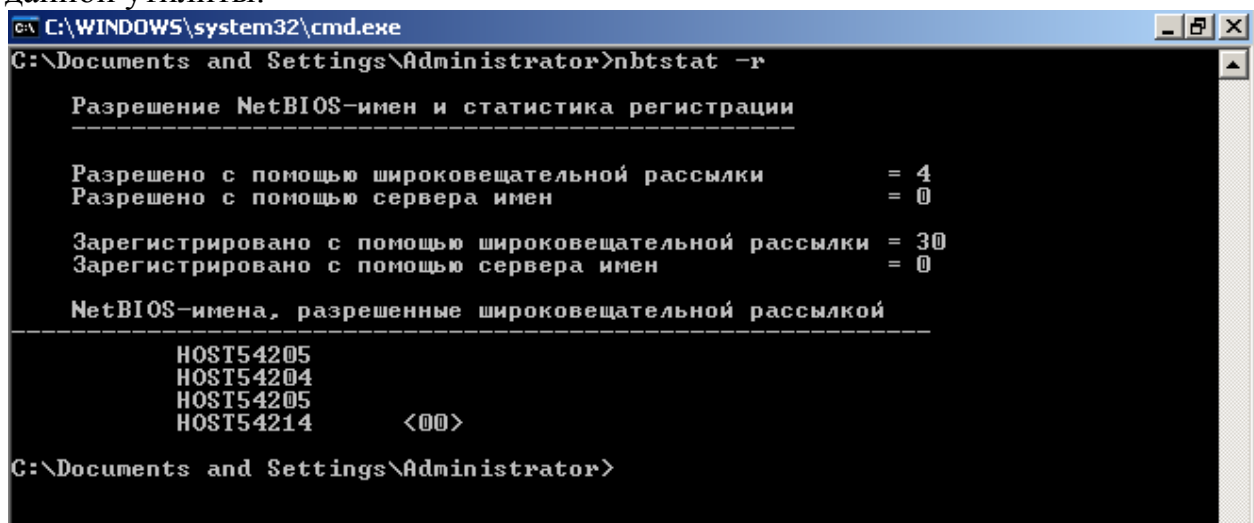
net send {имя | * | /domain[:имя] | /users} сообщение,

где имя - указывает имя пользователя, имя компьютера или псевдоним, которому будет отправлено сообщение. Если имя компьютера содержит пробелы, оно должно быть заключено в кавычки (" "). Длинные имена пользователей, введенные в формате NetBIOS, могут привести к возник-

новению исключительных ситуаций. Имена NetBIOS ограничены 16 символами, но Windows 2000 резервирует 16-ый символ; сообщение - указывает текст сообщения.

Утилита nbtstat.

Статистика и подключения протокола NetBIOS over TCP/IP. С использованием данной утилиты можно определить, есть ли в сети сервер Wins, сколько запросов на разрешение netbios имен было выполнено с использованием широковещательной рассылки, какие имена зарегистрированы в сети, где находится главный обозреватель сети и т.д. Пример использования данной утилиты.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>nbtstat -r

Разрешение NetBIOS-имен и статистика регистрации
-----

Разрешено с помощью широковещательной рассылки      = 4
Разрешено с помощью сервера имен                    = 0

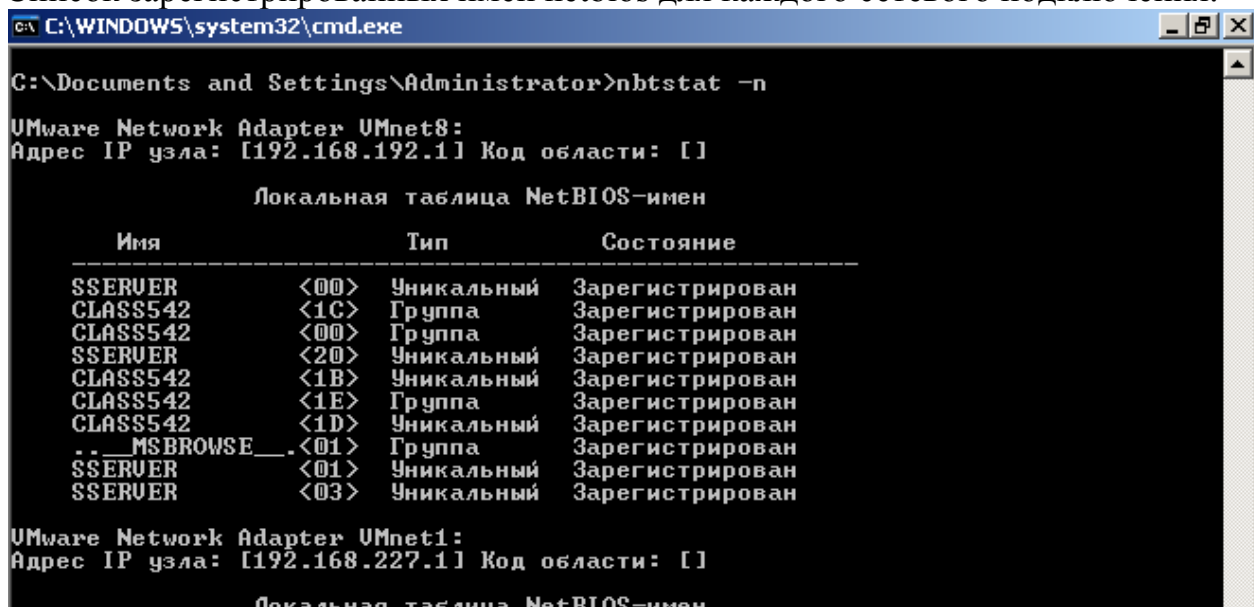
Зарегистрировано с помощью широковещательной рассылки = 30
Зарегистрировано с помощью сервера имен              = 0

NetBIOS-имена, разрешенные широковещательной рассылкой
-----
HOST54205
HOST54204
HOST54205
HOST54214      <00>

C:\Documents and Settings\Administrator>
```

В сети нету сервера Wins, что наглядно показывает скриншот выше.

Список зарегистрированных имен netbios для каждого сетевого подключения.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>nbtstat -n

VMware Network Adapter VMnet8:
Адрес IP узла: [192.168.192.1] Код области: []

      Локальная таблица NetBIOS-имен

      Имя                Тип                Состояние
      -----
SSERVER                  <00>              Уникальный   Зарегистрирован
CLASS542                 <1C>              Группа       Зарегистрирован
CLASS542                 <00>              Группа       Зарегистрирован
SSERVER                  <20>              Уникальный   Зарегистрирован
CLASS542                 <1B>              Уникальный   Зарегистрирован
CLASS542                 <1E>              Группа       Зарегистрирован
CLASS542                 <1D>              Уникальный   Зарегистрирован
.._MSBROWSE_             <01>              Группа       Зарегистрирован
SSERVER                  <01>              Уникальный   Зарегистрирован
SSERVER                  <03>              Уникальный   Зарегистрирован

VMware Network Adapter VMnet1:
Адрес IP узла: [192.168.227.1] Код области: []

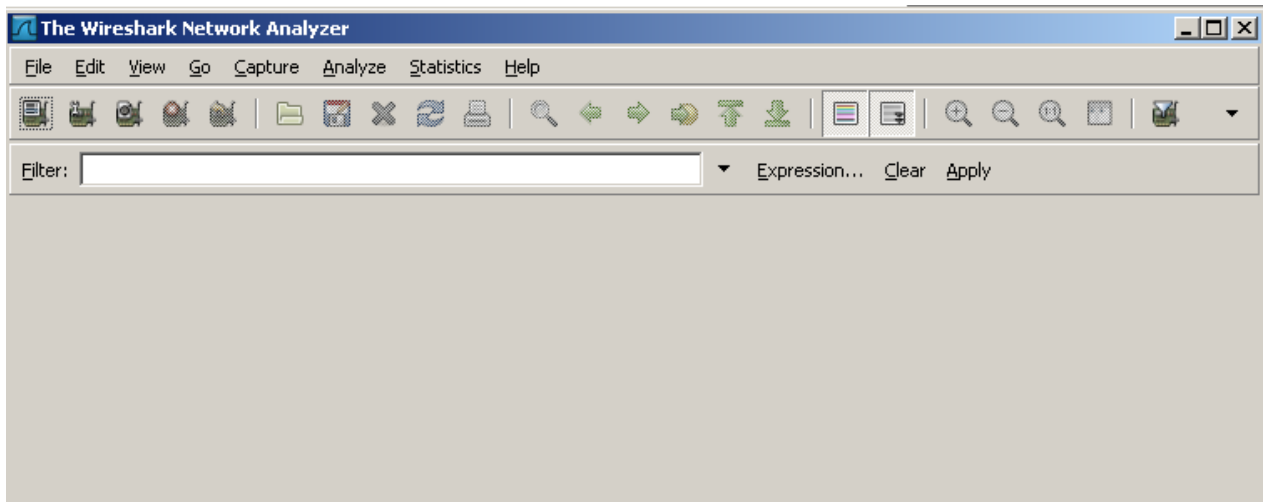
      Локальная таблица NetBIOS-имен
```


Рекомендации и замечания

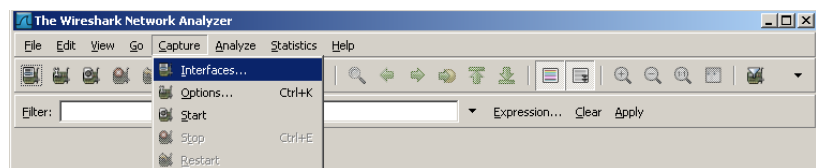
На основе рассмотренных сетевых утилит ОС Windows разрабатываются пользовательские приложения, реализующие мониторинг и диагностику локальных сетей. Они позволяют минимизировать усилия по поиску и исправлению ошибок в конфигурации сети и помогают системному администратору контролировать трафик. В настоящее время создано большое количество программ этого направления: Monitor It, Nautilus NetRanger, CiscoWorks 2000, ServiceSentinel и д.р. Они распространяются через Internet на условиях freeware. Windows NT Server обладает встроенными инструментами мониторинга: Event Viewer, Performance Monitor, Network Monitor.

Диагностика сетевого трафика

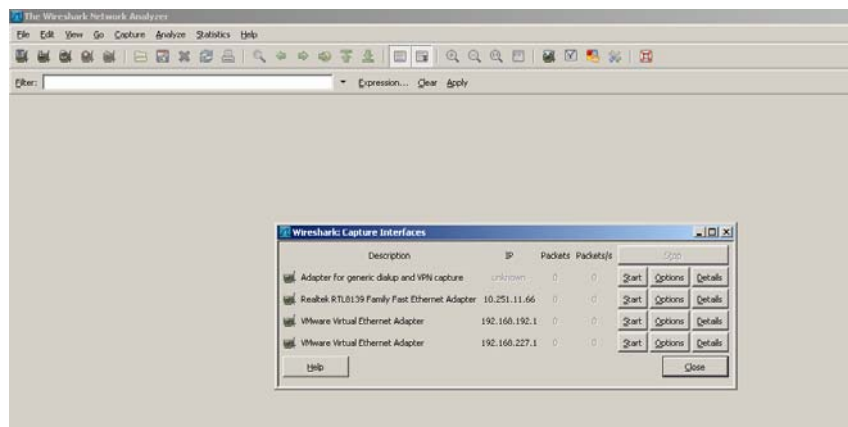
В определенных ситуациях требуется детальная диагностика передаваемых по сети данных и их анализ. Тестирование работоспособности сетевых служб и протоколов на низком уровне может быть выполнено с использованием специализированного программного обеспечения – **сетевых снифферов**, которые позволяют детально диагностировать сетевую активность, тестировать протоколы и т.д. Существует много программ для решения подобных задач (tcpdump – Unix, Network Monitor – Windows и т.д.). Рекомендуется для работы использовать **wireshark** (широко используется сетевыми профессионалами по всему миру). Внешний вид программы показан на рисунке ниже.



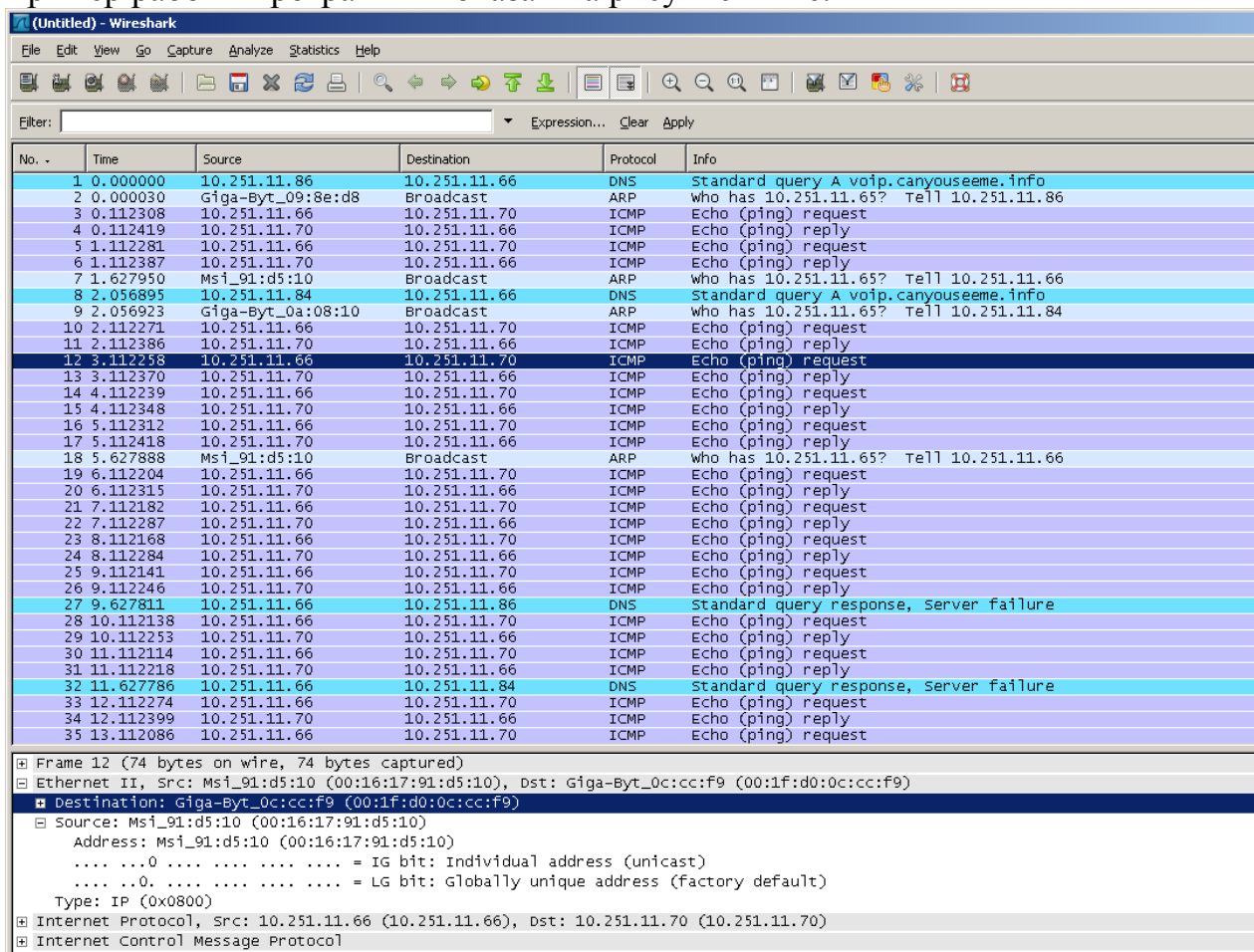
С использованием данного инструмента можно решать комплекс задач сетевой диагностики любой сложности, начиная от сбоев сетевых подключений, заканчивая детальным анализом данных, передаваемых по сетевым протоколам. Список подключенных сетевых интерфейсов можно просмотреть на вкладке **interfaces**



Кнопка **Start** позволяет перевести сетевую плату в режим захвата сетевых пакетов, которые впоследствии можно детально проанализировать в ходе работы.



Пример работы программы показан на рисунке ниже.



Вопросы на практикум.

- 1. Установите Wireshark;**
- 2. Определите, какие данные передаются эхо – запросом утилиты ping.**
- 3. Какой номер порта используют DNS запрос?**
- 4. Какова структура пакета, при передаче http – запроса?**
- 5. Какие данные передаются клиентом при подключении к http – серверу?**