

## Лабораторная работа № 9

### Анализ и исследование сетей с помощью служебных утилит и протокола управляющих сообщений ICMP

**Цель работы** Изучение протокола разрешения адресов ARP, протокола управляющих сообщений ICMP, выполнить анализ и TCP/IP соединений в локальной и глобальной сети с помощью служебных утилит и инструментального пакета IP tools

#### Теоретические сведения

##### Разрешение адресов канального и сетевого уровня.

Разрешение адресов выполняется при присоединении локальной сети типа Ethernet к глобальной сети Internet.

Протокол разрешения адреса ARP (Address Resolution Protocol) утилита с аналогичным названием используется для определения физического адреса узла по его IP-адресу. Протокол ARP работает различным образом в зависимости от того, какой протокол канального уровня работает в данной сети - протокол локальной сети (Ethernet, Token Ring, FDDI) с возможностью широковещательного доступа одновременно ко всем узлам сети, или же протокол глобальной сети (X.25, frame relay), не поддерживающий широковещательный доступ. Существует также протокол, решающий обратную задачу - нахождение IP-адреса по известному локальному адресу. Он называется реверсивный ARP - RARP (Reverse Address Resolution Protocol) и используется при старте бездисковых станций, не знающих в начальный момент своего IP-адреса, но знающих адрес своего сетевого адаптера.

В локальных сетях протокол ARP использует широковещательные кадры протокола канального уровня для поиска в сети узла с заданным IP-адресом. Когда сообщения ARP пересылаются от одной машины к другой, они должны передаваться в физических кадрах. Рисунок 2.1 показывает, что сообщение ARP передается как поле данных кадра.

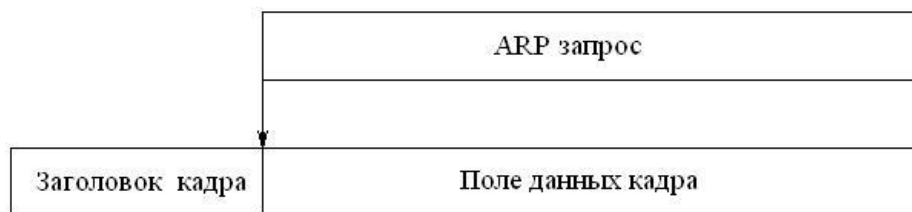


Рисунок 1. Сообщение ARP, заключенное в кадр физической сети

Чтобы идентифицировать, что кадр содержит запрос или ответ ARP, отправитель присваивает специальное значение полю типа в заголовке кадра и помещает сообщение ARP в поле данных кадра. Когда кадр прибывает на удаленный узел, система смотрит тип кадра, чтобы определить его содержимое. Например, в Ethernete, кадры, несущие сообщения ARP, имеют в поле типа значение 0806 в шестнадцатиричном формате. Это стандартное значение, назначенное ведомством, устанавливающим стандарты Ethernet.

В отличие от большинства протоколов, данные в пакетах ARP не имеют фиксированного формата заголовка. Вместо этого его сообщения были разработаны так, чтобы их можно было использовать для различных сетевых технологий. Поэтому, первые поля заголовка содержат счетчики, которые указывают длину следующих полей. Фактически, ARP можно использовать с произвольными физическими адресами и произвольными протокольными адресами.

Следующий рисунок показывает сообщение ARP по 4 байта в строке. В отличие от большинства протоколов, поля переменной длины в пакетах ARP не выровнены на границу 32 бит, что приводит к трудности восприятия диаграммы. Например, аппаратный адрес отправителя, помеченный как ОТПРАВИТЕЛЬ АА, занимает 6 непрерывных октетов, что приводит к появлению его на двух строках диаграммы.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
ТИП ОБОРУДОВАНИЯ																ТИП ПРОТОКОЛА															
HLEN								PLEN								ОПЕРАЦИЯ															
ОТПРАВИТЕЛЬ АА (октеты 0-3)																															
ОТПРАВИТЕЛЬ АА(октеты 4-5)																ОТПРАВИТЕЛЬ IP(октеты 0-1)															
ОТПРАВИТЕЛЬ IP(октеты 2-3)																ПОЛУЧАТЕЛЬ АА(октеты 0-1)															
ПОЛУЧАТЕЛЬ АА(октеты 0-1)																															
ПОЛУЧАТЕЛЬ IP(октеты 0-3)																															

Рисунок 2 Пример формата сообщения ARP/RARP для разрешения адресов IP-Ethernet.

Поле ТИП ОБОРУДОВАНИЯ определяет тип аппаратного интерфейса, для которого отправитель ищет ответ, оно содержит значение 1 для Ethernet. Аналогичным образом, поле ТИП ПРОТОКОЛА указывает тип адреса протокола более высокого уровня, который использует отправитель; оно содержит 0800 в шестнадцатичном формате для IP-адреса. Поле ОПЕРАЦИЯ указывает запрос ARP(1), ответ ARP(2), запрос RARP(3), или ответ RARP(4). Поля HLEN и PLEN позволяют использовать ARP в любых сетях, так как они указывают длину аппаратного адреса и адреса протокола верхнего уровня. Отправитель передает свой аппаратный адрес и IP-адрес, если они известны ему, в полях ОТПРАВИТЕЛЬ АА и ОТПРАВИТЕЛЬ IP.

При посылке запроса отправитель указывает IP-адреса назначения (ARP) или аппаратного адреса назначения(RARP), используя поля ПОЛУЧАТЕЛЬ АА и ПОЛУЧАТЕЛЬ IP. Отвечающая машина перед передачей ответа заполняет отсутствующие адреса, меняет местами пары отправителя и получателя и меняет код операции на ответ. Поэтому ответ содержит IP- и аппаратный адреса исходного отправителя, а также IP- и аппаратный адреса машины, которая разрешила эту связку. Пример работы утилиты ARP.

```
C:\users>arp -a
```

```
Интерфейс: 90.0.2.46 on Interface 0x1000002
Адрес IP          Физический адрес      Тип
90.0.2.21         00-07-e9-e7-3e-63     динамический
```

## Протокол ICMP

ICMP (Internet Control Message Protocol) - протокол управляющих сообщений Интернет, который управляет сетевыми сообщениями об ошибках и другими ситуациями, требующими вмешательства сетевых программ.

Протокол ICMP (Internet Control Message Protocol) служит для обмена сообщениями об ошибках и различных особых случаях, требующих обработки. ICMP-сообщения содержат управляющие данные, используемые либо на IP-уровне, либо на более высоком уровне (TCP или UDP). Некоторые ICMP-сообщения трансформируются в коды ошибок, возвращаемых пользовательским процессам. В иерархии протоколов ICMP часто относят к сетевому уровню, наряду с IP, но ICMP-сообщения инкапсулируются в IP-диаграммы.

Структура ICMP-сообщения включает:

Поле тип (type) (1 байт) идентифицирует разновидность ICMP-сообщения.

Поле код (code) (1 байт) для конкретизации тех или иных условий.

Поле контрольная сумма (checksum) относится ко всему ICMP-сообщению и является обязательным

В ICMP-сообщении об ошибке всегда возвращается IP-заголовок и первые 8 байтов IP-дейтаграммы, признанной ошибочной. Это позволяет ICMP-модулю сопоставить полученное им сообщение об ошибке с конкретным протоколом TCP или UDP (по значению поля протокол в возвращенном IP-заголовке) и с конкретным пользовательским процессом (по номеру порта, который находится в TCP или UDP-заголовке в возвращенных первых 8 байтах IP-дейтаграммы)

## Служебные утилиты для диагностики сети

Система Windows поставляется вместе с набором служебных программ, запускаемых преимущественно из командной строки и служащих для выявления проблем, которые могут возникнуть с TCP/IP-соединением. Большинство из них являются копиями популярных служебных программ операционной системы UNIX, для которой, собственно говоря, изначально и разрабатывается практически все программное обеспечение, так или иначе связанное с протоколом TCP/IP.

Большинство служебных утилит вызывается в режиме командной строки. Для ее запуска щелкните на кнопке Пуск (Start) и выберите команду Все программы – Стандартные – Командная строка.

### Утилита net

Определить имя компьютера и имя домена можно с помощью утилиты net. Пример:  
C:\users>net config [\S6](#).

```
Компьютер U6
Пользователь PRIM
Корневая папка C:\WINDOWS
Версия программы 4.10.1998
Версия программы переадресации 4.00
Команда выполнена успешно.
```

Она имеет множество ключей и развитую систему помощи. В качестве примера приведем протокол использования двух ее ключей:

- **view** для распечатки текущей конфигурации,

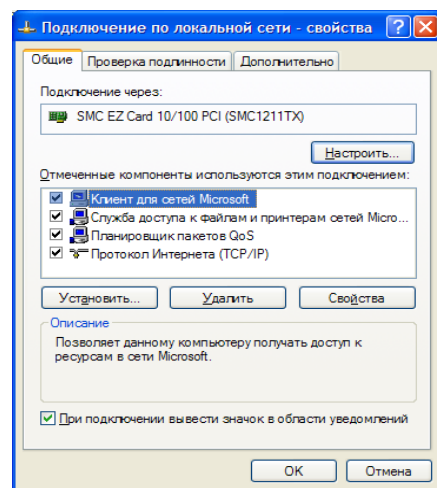
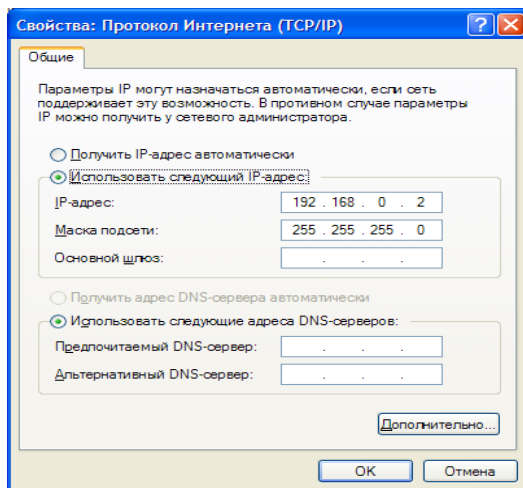
```
D:\Documents and Settings\andrey>net view
Имя сервера          Заметки
-----
\\ANDY
\\JORJXP
Команда выполнена успешно.
```

- **use** для управления сетевыми дисковыми ресурсами.

```
D:\Documents and Settings\andrey>net use
Новые подключения будут запомнены.
```

Состояние	Локальный	Удаленный	Сеть
ОК	Y:	\\JORJXP\Final	Microsoft Windows Network
Команда выполнена успешно.			

Если администратор сети разрешает, то текущие параметры и сетевые настройки можно изменить, используя значок Сети Windows в Панели управления. Также здесь можно посмотреть текущие настройки протокола TCP/IP.



## Утилита netstat

Для получения статистики работы сети по различным протоколам и списков активных подключений к ресурсам конкретного компьютера, используется утилита netstat. Пример работы утилиты.

```
D:\Documents and Settings\andrey>netstat -a
```

Активные подключения

Имя	Локальный адрес	Внешний адрес	Состояние
TCP	andy:epmap	0.0.0.0:0	LISTENING
TCP	andy:microsoft-ds	0.0.0.0:0	LISTENING
TCP	andy:1025	0.0.0.0:0	LISTENING
TCP	andy:1030	0.0.0.0:0	LISTENING
TCP	andy:2869	0.0.0.0:0	LISTENING
TCP	andy:3047	0.0.0.0:0	LISTENING
TCP	andy:3051	0.0.0.0:0	LISTENING
TCP	andy:5000	0.0.0.0:0	LISTENING
TCP	andy:3001	0.0.0.0:0	LISTENING
TCP	andy:3002	0.0.0.0:0	LISTENING
TCP	andy:3003	0.0.0.0:0	LISTENING
TCP	andy:3006	0.0.0.0:0	LISTENING
TCP	andy:netbios-ssn	0.0.0.0:0	LISTENING
TCP	andy:3047	jorjxp.mshome.net:5000	ESTABLISHED
TCP	andy:3051	jorjxp.mshome.net:5000	ESTABLISHED
TCP	andy:3053	0.0.0.0:0	LISTENING
TCP	andy:3053	jorjxp.mshome.net:netbios-ssn	ESTABLISHED
UDP	andy:epmap	*:*	
UDP	andy:microsoft-ds	*:*	
UDP	andy:isakm	*:*	

```
D:\Documents and Settings\andrey>netstat -s
```

#### Статистика IPv4

Получено пакетов	= 3516
Получено ошибок в заголовках	= 0
Получено ошибок в адресах	= 22
Направлено датаграмм	= 99
Получено неизвестных протоколов	= 0
Отброшено полученных пакетов	= 4
Доставлено полученных пакетов	= 3413
Запросов на вывод	= 3361
Отброшено маршрутов	= 0
Отброшено выходных пакетов	= 0
Выходных пакетов без маршрута	= 5
Требуется сборка	= 0
Успешная сборка	= 0
Сбоев при сборке	= 0
Успешно фрагментировано датаграмм	= 0
Сбоев при фрагментации датаграмм	= 0
Создано фрагментов	= 0

#### Статистика ICMPv4

	Получено	Отправлено
Сообщений	10	16
Ошибок	0	0
'Назначение недостижимо'	6	6
Превышений времени	0	0
Ошибок в параметрах	0	0
Просьба "снизить скорость"	0	0
Переадресовано	0	0
Эхо-сообщений	1	9
Ответных пакетов	3	1
Штатпов времени	0	0
Ответы на штампы времени	0	0
Масок адресов	0	0
Ответов на маски адресов	0	0

#### Статистика TCP для IPv4

Активных открыто	= 22
Пассивных открыто	= 49
Сбоев при подключении	= 1
Сброшено подключений	= 6
Текущих подключений	= 3
Получено сегментов	= 2494
Отправлено сегментов	= 2532
Повторно отправлено сегментов	= 2

#### Статистика UDP для IPv4

Получено датаграмм	= 627
Отсутствие портов	= 15
Ошибки при получении	= 0
Отправлено датаграмм	= 795

С помощью **netstat** можно ознакомиться с текущим состоянием специальной структуры данных, которая называется таблица маршрутизации. В ней отражены пути, которые использует для пересылки IP пакетов компонент ОС WINDOWS – программа **MPR** – многопротокольный маршрутизатор. Маршрутизация – это задача, решаемая в сложных многосегментных сетях для доставки пакетов информации по назначению. Для динамического изменения таблицы маршрутизации используется утилита **route**.

### Утилита ipconfig

Утилита позволяет просмотреть текущую конфигурацию адресов TCP/IP для всех установленных на данном компьютере сетевых адаптеров и коммутируемых соединений.

Утилита эффективна в системах, использующих протокол динамического распределения IP-адресов (Dynamic Host Configuration Protocol — DHCP), так как практически только с ее помощью можно определить IP-адрес компьютера. Запущенная без параметров, команда **ipconfig** выдает в качестве результата текущую конфигурацию адресов TCP/IP для всех установленных на данном компьютере сетевых адаптеров и коммутируемых соединений.

В результате выполнения программы можно получить примерно следующую таблицу (естественно, что для каждого компьютера его IP-адрес, адрес подсети и адрес шлюза будут другими):

Настройка протокола IP для Windows XP  
Адаптер Ethernet Подключение по локальной сети:  
DNS суффикс этого подключения . . : mycompany.com  
IP-адрес . . . . . : 202.201.200.166  
Маска подсети . . . . . : 255.255.255.224  
Основной шлюз . . . . . : 202.201.200.190

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

Запустив команду `ipconfig` с параметром `/all`, можно добавить к результату ее работы информацию об имени домена и о сервере имен доменов.

Например, результатом выполнения команды

**C:\>ipconfig/all**

будет отображение следующих сведений:

1. Имя компьютера (Host name) - Имя пользовательского компьютера.
2. Основной DNS суффикс (Primary DNS Suffix) - Основное имя домена, к которому принадлежит компьютер. (Во время использования коммутируемого соединения компьютер временно может принадлежать к нескольким доменам).
3. Тип узла (Node type) Метод, который использует компьютер с Windows для установки связи с другими компьютерами локальной сети при использовании технологии Windows Networking. Если на компьютере установлена операционная система Windows 2000 Server или же в локальной сети используется сервер WINS, тип узла должен быть *гибридным* (Hybrid); в противном случае — *широковещательным* (Broadcast).
4. Флаг включения IP-маршрутизации (IP routing enabled) - Определяет, перенаправляет ли пользовательский компьютер пакеты данных, полученные с других сетевых адаптеров, или посредством коммутируемого соединения (в таком случае данный компьютер называется шлюзом Internet).
5. Доверенный WINS-сервер (WINS proxy enabled) - Не существует для компьютеров с операционной системой Windows XP Professional.
6. Лист DNS суффиксов (DNS suffix search list) - Ограничивает разрешение использования неполных имен на данном компьютере. При введении неполного адреса он будет дополнен сначала основным суффиксом DNS, а затем, при неудачной попытке, дополнительными суффиксами DNS в определенном порядке.
7. DNS суффикс подключения (Connection-specific DNS suffix) - Имя домена текущего соединения. В основном необходимо для определения суффикса DNS текущего коммутируемого соединения.
8. Описание (Description) - Название производителя сетевого адаптера или тип коммутируемого соединения.
9. Физический адрес (Physical address) - Уровень управления доступом к среде (MAC-уровень) или физический адрес сетевого устройства.
10. Флаг включения DHCP - (DHCP enabled) - Определяет использование протокола динамической настройки узлов (DHCP). Значение Да (Yes) обозначает, что DHCP разрешен, и в этом случае присвоение адресов всем компьютерам сети будет выполняться автоматически. В противном случае IP-адреса необходимо задавать вручную.
11. IP-адрес (IP address) IP-адрес сетевого адаптера пользовательского компьютера
12. Маска подсети (Subnet mask) - Однозначно определяет локальную сеть, к которой подключен компьютер. Представляет собой 32-разрядное значение, записываемое

с помощью четырех чисел от 0 до 255. Вместе с IP-адресом маска подсети определяет, принадлежит данный адрес локальной сети или нет

13. Основной шлюз (Default gateway) - Адрес устройства, на которое передаются все пакеты, адресованные за пределы сети

14. DNS-серверы (DNS servers) - IP-адреса используемых серверов имен доменов

Команда `ipconfig` отображает большую часть информации, содержащейся в диалоговом окне свойств. Ее преимуществом является то, что она предоставляет реальные значения всех параметров.

Выполнив эту команду, зачастую можно сразу же обнаружить какую-то сетевую ошибку. Если проблема заключается в оборудовании пользовательского компьютера (что обычно происходит при невозможности соединения с Internet), выполнение команды `ipconfig /all` поможет определить неисправный компонент.

## Утилита ping

Неудачная попытка соединения со службой Internet или получения доступа к файлам и папкам, находящимся на других компьютерах локальной сети, может быть вызвана тем, что другие компьютеры просто не получают отправленных им запросов на подключение или же не могут выполнить запрос из-за неисправностей на высших уровнях сетевого взаимодействия.

Утилита `ping` является средством для тестирования работоспособности соединения TCP/IP. Для того чтобы протестировать работоспособность пользовательского компьютера, сетевого аппаратного обеспечения, а также среды передачи данных, достаточно выполнить команду `ping x.x.x.x`, где `x.x.x.x` IP-адрес шлюза или любого компьютера сети. Если посланный пакет данных ECHO успешно возвратится на пользовательский компьютер, это значит, что с физической частью сети все в порядке. В противном случае необходимо выполнить команду `tracert` или воспользоваться другим средством для выяснения причины неполадок.

Совместное использование команд `ping` и `ipconfig` позволяет провести быстрое и надежное тестирование Internet-соединения.

Принцип работы команды `ping` состоит в следующем.

1. Команда отправляет запросы к удаленному компьютеру с использованием при этом специального протокола ECHO. Получив такой запрос, удаленный компьютер сразу же отправляет его обратно по тому адресу, откуда он пришел.

2. Команда `ping` позволяет узнать, пришли ли обратно посланные запросы. Таким образом, команда `ping` позволяет протестировать соединение между двумя компьютерами на очень низком (физическом) уровне. При успешном возвращении запросов можно быть уверенным в том, что среда передачи данных, программное обеспечение TCP/IP, а также все устройства (маршрутизаторы, повторители и др.), встретившиеся на пути между двумя компьютерами, работают нормально.

Команда `ping` имеет несколько параметров и варианты запуска. Вот два из них:

1. `C:\>ping имя_компьютера`
2. `C:\> ping nnn.nnn.nnn.nnn`

При выполнении обоих вариантов `ping` посылает четыре пакета типа ECHO на имя или IP-адрес компьютера, а затем ждет их возвращения и отображает соответствующий результат. Ниже приведен пример выполнения команды `ping`.

```
C:\>ping www.mycompany.com
```

```
Обмен пакетами с sumatra.mycompany.com [202.222.132.163] по 32 байт:
```

```
Ответ от 202.222.132.163: число байт=32 время<10мс TTL=32
```

```
Ответ от 202.222.132.163: число байт=32 время<10мс TTL=32
```

Ответ от 202.222.132.163: число байт=32 время<10мс TTL=32

Ответ от 202.222.132.163: число байт=32 время<10мс TTL=32

Фактически это означает, что пользовательский компьютер не испытывает проблем при соединении с узлом [www.mysompany.com](http://www.mysompany.com) и все физическое оборудование на пути между двумя компьютерами функционирует исправно.

Обратите внимание, что даже при отсутствии неисправностей на пути между двумя компьютерами, один или сразу несколько пакетов могут быть утеряны. Как правило, это связано с перегруженностью сети, а также с тем, что большинство маршрутизаторов отводит диагностирующим пакетам низкий приоритет. Если хотя бы один из посланных пакетов вернется, это уже будет означать исправность работы сети.

Еще одним из распространенных вариантов выполнения команды `ping` является использование параметра `-t`. Тогда утилита повторяет запросы к удаленному компьютеру, пока программа не будет остановлена с помощью комбинации клавиш `<Ctrl+C>`. Как правило, подобная практика бывает полезна при устранении неисправностей сети. Запущенный “бесконечный” тест команды `ping` наглядно поможет отслеживать результаты каких-либо внесенных изменений.

### **Утилита `tracert`**

Утилита подобна команде `ping`. Обе посылают в точку назначения эхо-пакеты и ожидают их возвращения. Главное отличие пакетов команды `tracert` заключается в том, что они имеют различный срок жизни. Первые пакеты помечаются специальной меткой, означающей, что они не могут быть пропущены маршрутизаторами. При достижении первого маршрутизатора на пути такие пакеты отсылаются обратно на тестирующий компьютер как пакеты, которые невозможно доставить по адресу. Возвращенные пакеты содержат адрес не пропустившего их маршрутизатора, определяя первое звено в тестируемом маршруте. Обычно им является либо сетевой шлюз (при подключении к Internet по локальной сети), либо устройство, принимающее модемные звонки в офисе провайдера услуг Internet (при коммутируемом подключении).

Затем `tracert` пересылает следующие пакеты, уже помечая их как пакеты, которые могут быть пропущены не более чем одним маршрутизатором. Таким образом, будет определено второе звено в тестируемом маршруте.

Количество маршрутизаторов, через которые может пройти пакет, будет каждый раз увеличиваться на единицу до тех пор, пока пакет не достигнет точки назначения. Таким образом, с помощью команды `tracert` можно получить подробный маршрут прохождения пакетов данных между компьютером, на котором была запущена `tracert`, и любым удаленным компьютером сети.

Утилита `tracert` - средство обнаружения неисправностей в сетевом соединении: в случае возникновения проблемы с подключением к Web-узлу или к какой-нибудь другой службе Internet так как она может определить участок, на котором возникла проблема. Важнее всего определить зону возникновения неисправностей. Если неисправности связаны с локальной сетью, их можно и нужно устранить.

Пример работы утилиты.



```
D:\Documents and Settings\andrey>tracert www.microsoft.com
```

Трассировка маршрута к a562.cd.akamai.net [211.196.154.230]  
с максимальным числом прыжков 30:

1	*	*	*	Превышен интервал ожидания для запроса.
2	110 ms	110 ms	109 ns	inet-core.lanck.net [62.152.64.25]
3	108 ms	110 ms	109 ns	EPB11-P200.101.transitcom.net [217.150.38.166]
4	170 ms	170 ms	170 ns	ge-4-0.2-cr02.ldn01.pccwbt.net [63.218.13.41]
5	166 ms	169 ms	170 ns	kt-london.router.fei [195.66.224.147]
6	322 ms	320 ms	325 ns	211.48.63.101
7	461 ms	461 ms	461 ns	211.48.63.229
8	457 ms	461 ms	461 ns	211.216.216.81
9	668 ms	466 ms	486 ns	220.73.168.154
10	2820 ms	566 ms	476 ns	218.145.44.74
11	462 ms	461 ms	461 ns	210.222.17.195
12	1571 ms	837 ms	506 ns	211.196.154.230

Трассировка завершена.

Из приведенной выше информации можно сделать вывод о том, что на пути от пользовательского компьютера до Web-узла [www.ricochet.net](http://www.ricochet.net) пакеты данных проходят через 13 промежуточных маршрутизаторов, которые принадлежат, по всей видимости, двум компаниям — поставщикам услуг Internet.

Команда `tracert` имеет некоторые особенности. Например, в приведенном примере в качестве параметра команде `tracert` было передано имя узла [www.ricochet.net](http://www.ricochet.net), однако при отображении результатов обнаружилось, что фактически маршрут определялся для узла [www.metricom.com](http://www.metricom.com). Дело вот в чем. Очень часто Web-узлы имеют сразу несколько имен доменов. Команда `tracert` же выбирает из всех имен данного узла каноническое (первоначальное) имя, соответствующее его IP-адресу.

Также брандмауэры многих организаций блокируют тестовые пакеты `tracert` при попытке их проникновения в локальную сеть. Таким образом, получается, что эхо-пакету вообще не удастся попасть в точку назначения. В таком случае после достижения брандмауэра команда `tracert` начинает отображать следующие повторяющиеся строки:

```
14 * * * Превышен интервал ожидания для запроса.
15 * * * Превышен интервал ожидания для запроса.
16 * * * Превышен интервал ожидания для запроса.
```

Так будет продолжаться до исчерпания лимита отправки пакетов (30 попыток). Чтобы прервать выполнение `tracert`, надо нажать комбинацию клавиш <Ctrl+C>.

## Утилита `pathping`

Это средство трассировки маршрутизации, объединяющее возможности команд `ping` и `tracert`, с дополнительными сведениями, которые не предоставляет ни одна из этих команд.

Утилита `pathping` выполняет трассировку маршрутизации несколько быстрее, так как отводит всего лишь по одному пакету данных на каждый транзитный участок, в отличие от трех пакетов данных команды `tracert`.

После определения маршрута `pathping` проводит тест сетевого трафика каждого маршрутизатора, встретившегося на пути от пользовательского до тестируемого компьютера, посылая ему 100 пакетов данных, аналогичных пакетам команды `ping`. Затем подсчитывает коэффициент потери пакетов и среднее время ожидания ответа для каждого маршрутизатора, выводя результаты своей работы в таблице.

На выполнение диагностирующего теста команды `pathping` может уйти довольно много времени. По умолчанию тестирующие пакеты посылаются с задержкой в 250 мс (одна четвертая часть секунды), так что, к примеру, на стандартный тест в 100 пакетов для 12 маршрутизаторов уйдет около 5 минут. При потере же некоторых пакетов время может

значительно увеличиться, так как pathping проводит в ожидании возвращения посланного пакета до трех секунд.

Для того чтобы прервать тест pathping, достаточно нажать комбинацию клавиш <Ctrl+C>.

Это ускорит процесс завершения работы, однако при этом не будут получены необходимые результаты. Выход из данной ситуации можно найти, воспользовавшись несколькими замечательными параметрами команды pathping, список которых можно получить, введя команду

pathping /?

## Утилита route

Хотя подавляющее большинство пользователей имеют только один модем или только одну сетевую плату для подключения к Internet или локальной сети, операционная система Windows XP способна поддерживать сразу несколько сетевых плат или адаптеров удаленного доступа, установленных в одном компьютере. В случае установки сразу нескольких соединений Windows должно быть известно, какое из них использовать при обращении к другому удаленному компьютеру. Для соединения TCP/IP подобная информация представляется в виде таблицы маршрутов (routing table). Эта таблица содержит список IP-адресов и подсетей (блоков IP-адресов), а также включает информацию об адаптере (интерфейсе), который необходимо использовать Windows при обращении к каждому из них. Правда, информация о таблице маршрутов и маршрутизации может существовать для большинства пользователей лишь теоретически, за исключением следующих случаев:

- одновременное использование коммутируемого соединения и сетевого адаптера;
- использование нескольких сетевых адаптеров;
- использование соединений виртуальной частной сети (Virtual Private Networking).

При выполнении какого-либо из этих условий и при наличии проблем с подключением к Internet выполняется команда route. Ее результат выводится в виде такой таблицы:

=====

Список интерфейсов

0x1 ..... MS TCP Loopback interface

0x2 ...0e c3 24 1f 09 3f ..... NDIS 5.0 driver

=====

Активные маршруты:

Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика
0.0.0.0	0.0.0.0	202.201.200.190	202.201.200.166	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
202.201.200.160	255.255.255.224	202.201.200.166	202.201.200.166	1
202.201.200.166	255.255.255.255	127.0.0.1	127.0.0.1	1
202.201.200.255	255.255.255.255	202.201.200.166	202.201.200.166	1
224.0.0.0	224.0.0.0	202.201.200.166	202.201.200.166	1
255.255.255.255	255.255.255.255	202.201.200.166	202.201.200.166	1

Default Gateway: 202.201.200.190

=====

Постоянные маршруты: Отсутствует

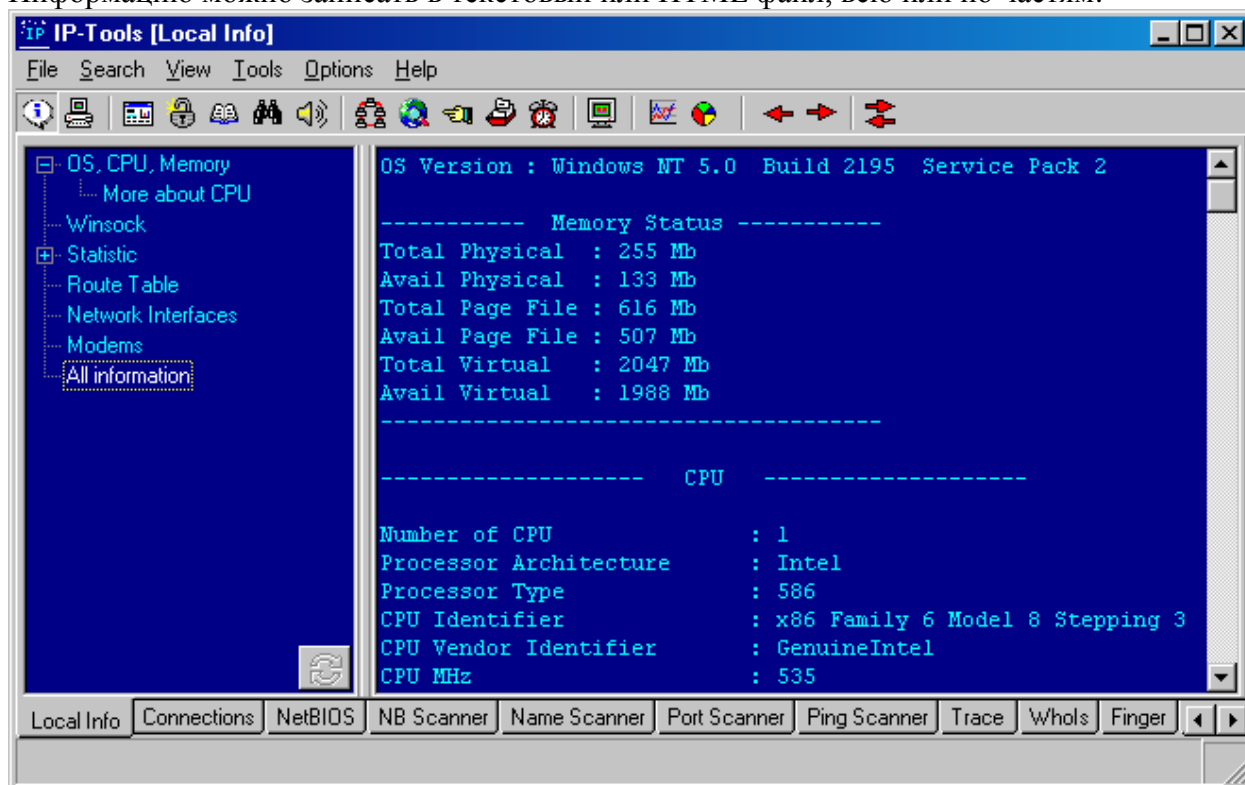
Здесь приведено много информации, но самой важной при возникновении проблемы с подключением к Internet является строка, содержащая адрес 0.0.0.0 — эффективный адрес шлюза для выхода в Internet. Естественно, на каждом конкретном

компьютере данный адрес может отличаться, особенно во время активного коммутируемого подключения или подключения виртуальной частной сети. В свою очередь, это может означать временную невозможность выхода в Internet.

## Другие сетевые утилиты в программе IP Tools

Пакет IP-Tools включает в себя ряд других утилит для работы с TCP/IP сетями.

1. Local Info. Данная утилита отображает информацию о Вашем компьютере: процессор, память, WinSock, модемы, сетевые интерфейсы, таблица маршрутизации и т.д. Информацию можно записать в текстовый или HTML файл, всю или по частям.



2. Connections. Эта утилита выдает информацию о том, какие порты слушает ваша машина и с кем она соединена. Обновление делается каждый раз при переключении на эту страницу или при выборе пункта "Refresh" локального меню (вызывается правой кнопкой мыши). Есть и автообновление (AutoRefresh). IP-Tools может записывать в Log File все изменения в статусах портов. Кроме того, Вы можете выставить фильтр по типу портов, по статусу портов, по IP адресам. Настройки утилиты находятся в диалоге "Options" на странице "Connections". Может помочь для обнаружения троянов типа backdoor.

Возможные значения статусов TCP портов :

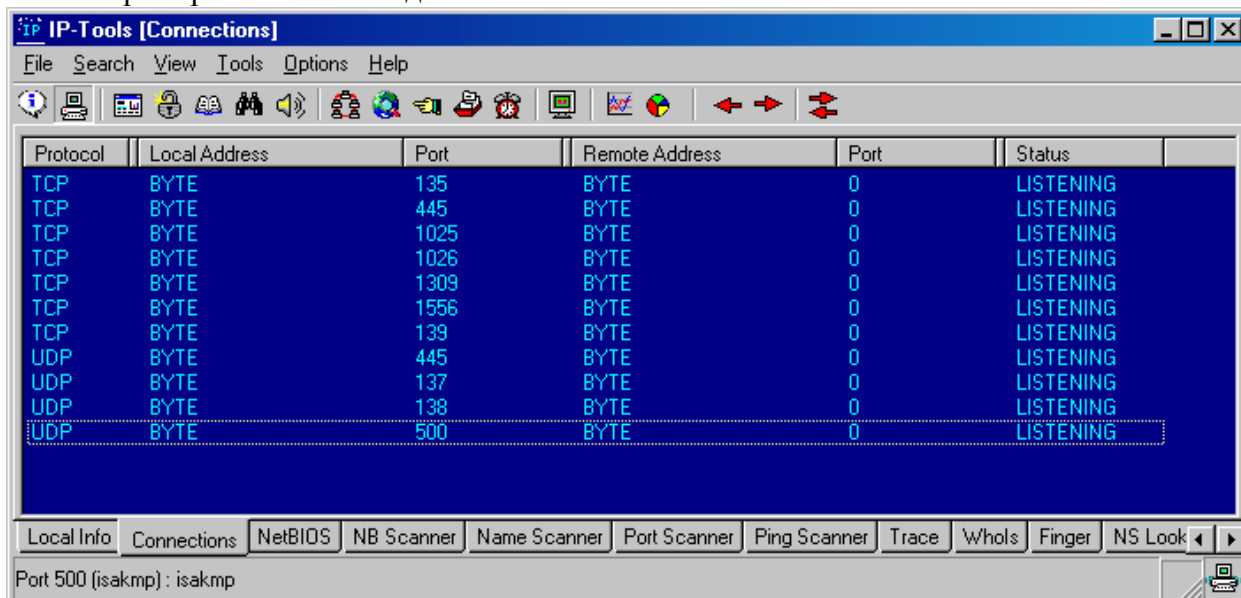
- CLOSED - порт закрыт и никак не используется.
- LISTENING - порт открыт и ждет входящие соединения.
- SYN\_SENT - послали запрос на установление соединения, ожидание парного запроса.
- SYN\_RECEIVED - ожидание подтверждения после того, как запрос соединения уже принят и отправлен.
- ESTABLISHED - соединение установлено.
- CLOSE\_WAIT - ожидание запроса на закрытие соединения со стороны своего клиента.
- FIN\_WAIT\_1 - ожидание запроса от чужой программы TCP или подтверждения ранее отправленного запроса на закрытие соединения.
- CLOSING - ожидание подтверждения со стороны чужой программы TCP запроса о закрытии соединения.

- LAST\_ACK - ожидание запроса на закрытие соединения, ранее отправленного чужой программе TCP (запрос включал также подтверждение получения чужого запроса на закрытие соединения).

- FIN\_WAIT\_2 - ожидание запроса на закрытие соединения со стороны чужой программы TCP.

- TIME\_WAIT - ожидание, когда истечет достаточное количество времени и можно быть уверенным, что чужая программа TCP получила подтверждение своего запроса на закрытие соединения.

Пример состояния соединений:

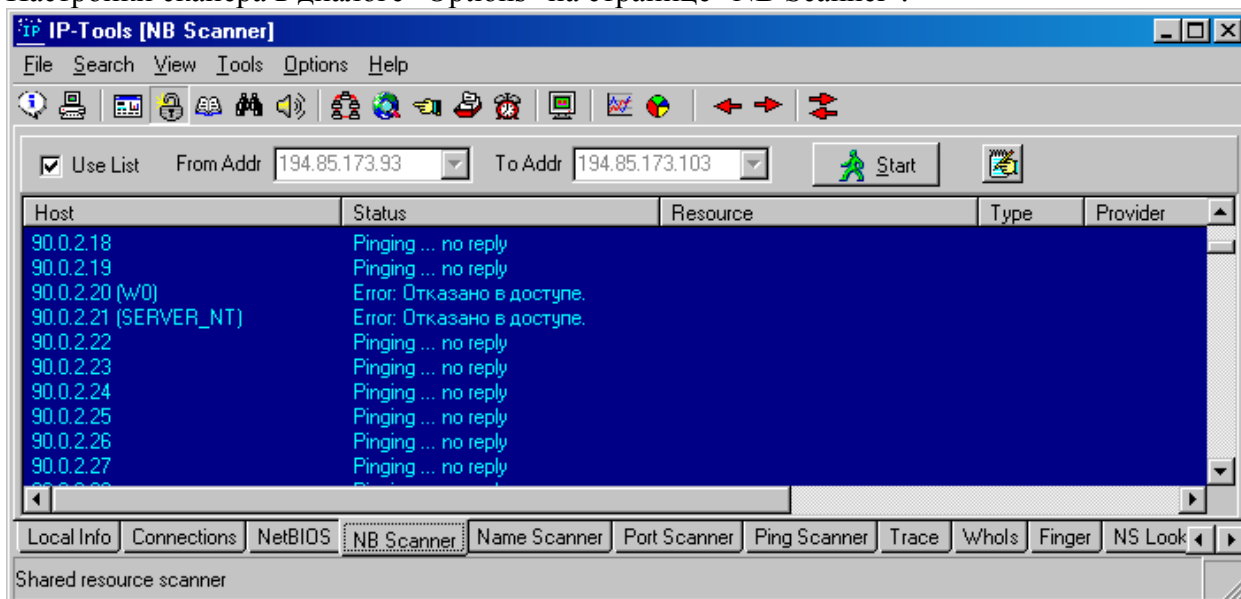


The screenshot shows the 'IP-Tools [Connections]' window. It has a menu bar (File, Search, View, Tools, Options, Help) and a toolbar with various icons. Below is a table with columns: Protocol, Local Address, Port, Remote Address, Port, and Status. The table lists several listening ports for both TCP and UDP protocols, all with 'Local Address' as 'BYTE' and 'Remote Address' as 'BYTE'. The status for all is 'LISTENING'. At the bottom, there are tabs for 'Local Info', 'Connections', 'NetBIOS', 'NB Scanner', 'Name Scanner', 'Port Scanner', 'Ping Scanner', 'Trace', 'Whois', 'Finger', and 'NS Look'. The 'Connections' tab is selected. Below the tabs, it says 'Port 500 (isakmp) : isakmp'.

Protocol	Local Address	Port	Remote Address	Port	Status
TCP	BYTE	135	BYTE	0	LISTENING
TCP	BYTE	445	BYTE	0	LISTENING
TCP	BYTE	1025	BYTE	0	LISTENING
TCP	BYTE	1026	BYTE	0	LISTENING
TCP	BYTE	1309	BYTE	0	LISTENING
TCP	BYTE	1556	BYTE	0	LISTENING
TCP	BYTE	139	BYTE	0	LISTENING
UDP	BYTE	445	BYTE	0	LISTENING
UDP	BYTE	137	BYTE	0	LISTENING
UDP	BYTE	138	BYTE	0	LISTENING
UDP	BYTE	500	BYTE	0	LISTENING

3. NetBIOS. С ее помощью можно увидеть информацию о своих сетевых интерфейсах, а задав имя машины ("123.23.21.12" или "www.us.ru" или, если это машина в локальной сети, "nova\_computer" или "\*" для своей машины) и диапазон номеров интерфейсов можно получить информацию сетевых интерфейсах удаленной машины: MAC адрес, таблицу имен и т.д.

4. Nb Scanner. Существует возможность сканирования выделенных сетевых ресурсов машин из заданного диапазона или по заданному списку адресов. Результат сканирования можно записать в таблицу (пункт "Save as HTML.." локального меню). Настройки сканера в диалоге "Options" на странице "NB Scanner".

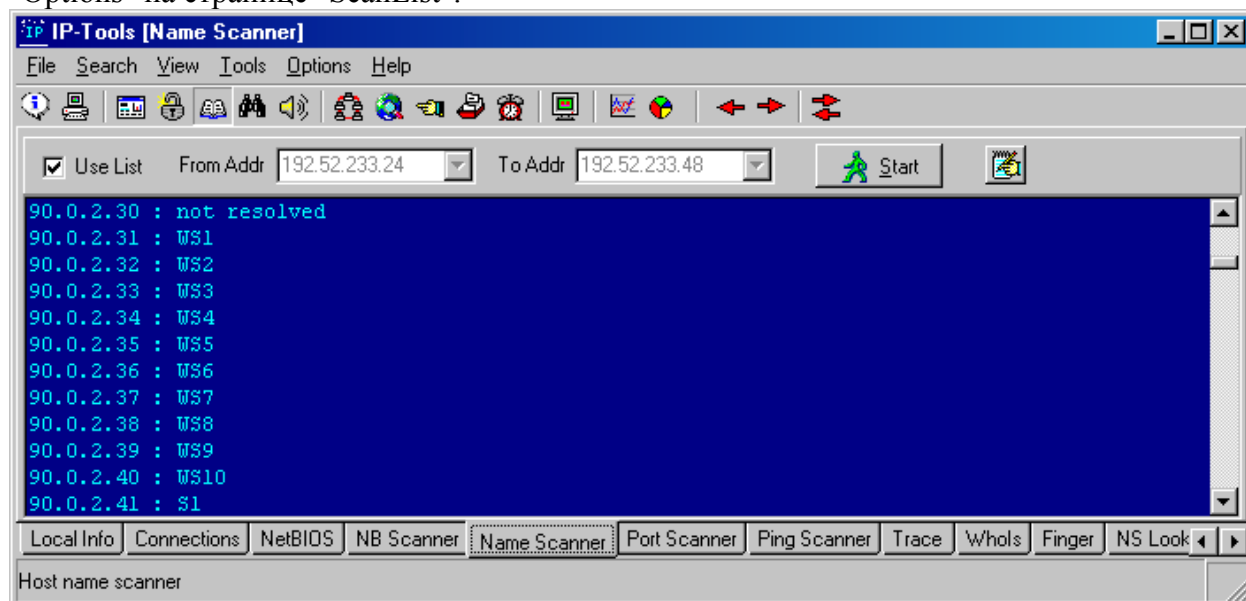


The screenshot shows the 'IP-Tools [NB Scanner]' window. It has a menu bar (File, Search, View, Tools, Options, Help) and a toolbar. Below the toolbar, there are input fields for 'From Addr' (194.85.173.93) and 'To Addr' (194.85.173.103), a 'Start' button, and a 'Use List' checkbox. Below this is a table with columns: Host, Status, Resource, Type, and Provider. The table shows results for a range of IP addresses from 90.0.2.18 to 90.0.2.27. The status for most is 'Pinging ... no reply', while for 90.0.2.20 and 90.0.2.21, it says 'Error: Отказано в доступе.'. At the bottom, there are tabs for 'Local Info', 'Connections', 'NetBIOS', 'NB Scanner', 'Name Scanner', 'Port Scanner', 'Ping Scanner', 'Trace', 'Whois', 'Finger', and 'NS Look'. The 'NB Scanner' tab is selected. Below the tabs, it says 'Shared resource scanner'.

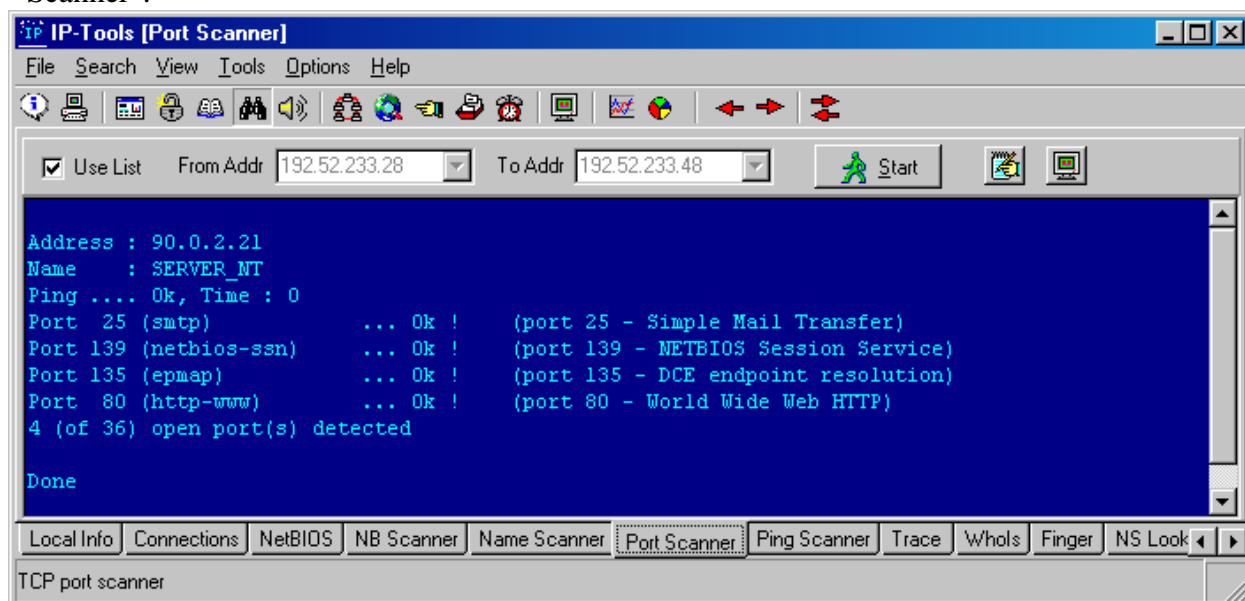
Host	Status	Resource	Type	Provider
90.0.2.18	Pinging ... no reply			
90.0.2.19	Pinging ... no reply			
90.0.2.20 (W0)	Error: Отказано в доступе.			
90.0.2.21 (SERVER_NT)	Error: Отказано в доступе.			
90.0.2.22	Pinging ... no reply			
90.0.2.23	Pinging ... no reply			
90.0.2.24	Pinging ... no reply			
90.0.2.25	Pinging ... no reply			
90.0.2.26	Pinging ... no reply			
90.0.2.27	Pinging ... no reply			

5. Name Scanner. Утилита осуществляет сканирование хоть всего Интернета за раз используя GetHostByName (выдает имя машин из DNS) по диапазону адресов (например

1.1.1.1 - 255.255.255.255) или по списку адресов. Список адресов определяется в диалоге "Options" на странице "ScanList".



6. Port Scanner. Утилита предназначена для сканирования TCP портов по диапазону адресов (например, 1.1.1.1 - 255.255.255.255) или по списку адресов. Прежде чем сканировать порты, программа может попытаться узнать имя машины и пропинговать ее, кроме того, при сканировании портов IP-Tools может посылать заданную строку на сканируемый порт и показывать ответ от сервера. Список портов задается в диалоговом окне "Options" на странице "Ports", а параметры самого сканирования на странице "Port Scanner".

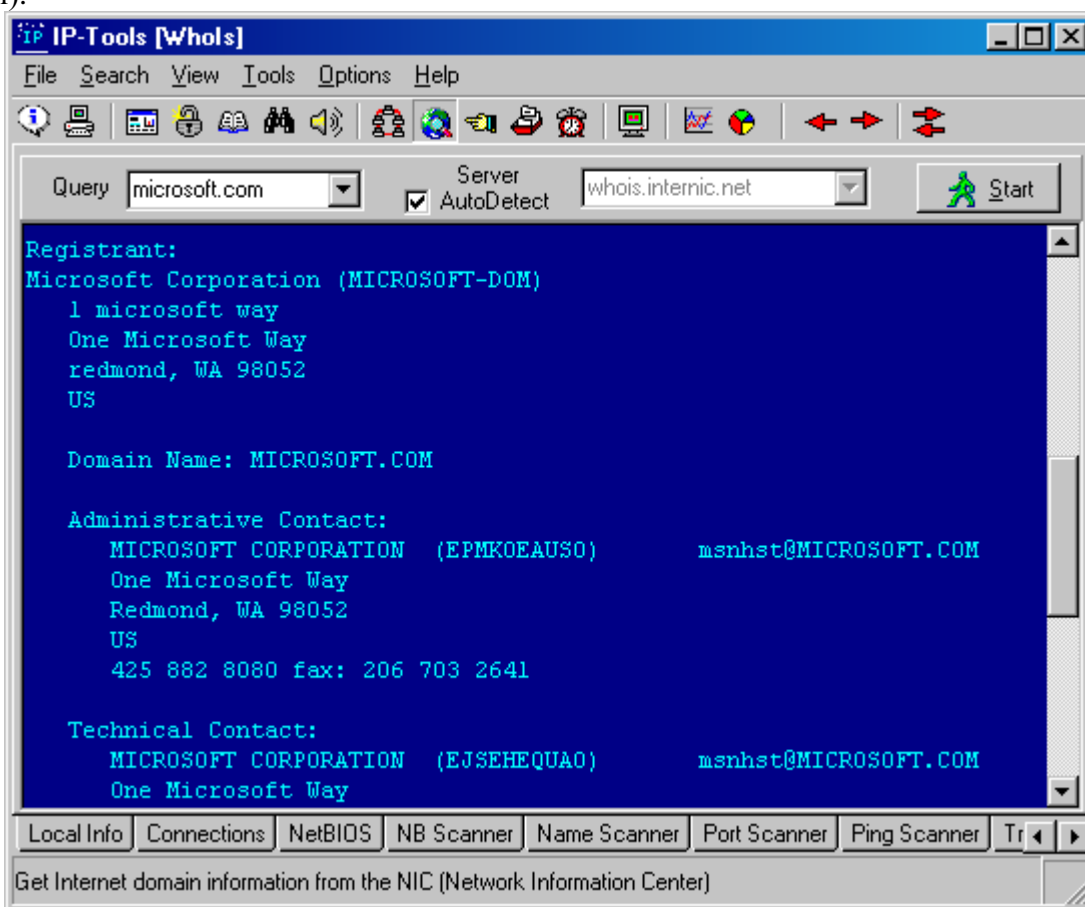


7. Ping Scanner. Данная утилита проверяет подключения к удаленному компьютеру (компьютерам), проверку можно выполнять по диапазону или по списку адресов. Настройки находятся в диалоговом окне "Options" на странице "Ping/Trace".

8. Trace. Показывает маршрут, по которому проходят IP пакеты до заданного узла. Настройки находятся в диалоговом окне "Options" на странице "Ping/Trace".

9. WhoIs. Утилита получает регистрационную информацию о доменах с официальных WhoIs серверов. Например, если Вы хотите получить информацию о том, кому принадлежит сервер "www.brainriver.com" введите имя домена "brainriver.com" и узнаете имена, телефоны, почтовые адреса владельцев и/или администраторов. IP-Tools содержит встроенный список WhoIs серверов для всех доменов верхнего уровня. Но Вы можете создать ваш собственный список (диалог Options, страница WhoIs), причем

информация из Вашего списка имеет более высокий приоритет, чем из внутреннего списка (то есть IP-Tools будет искать сервер во внутреннем списке только если не найдет в Вашем).



10. Finger. Эта утилита выдает информацию о пользователе (пользователях) заданного хоста (если, конечно, на нем запущен Finger сервис). Показывает имя пользователя, его домашний каталог, время подключения, время последнего получения почты и время последнего чтения почты, и т.д. Синтаксис запроса :

user@host.domain для получения информации о конкретном пользователе или host.domain для получения информации о всех пользователях.

11. LookUp. Выдает информацию о имени хоста, его IP адресе и алиасах (если они есть) из DNS. Вы можете задать либо имя хоста (например, www.chat.ru) либо его IP адрес (212.24.32.192). Также эта утилита может работать со списком адресов.

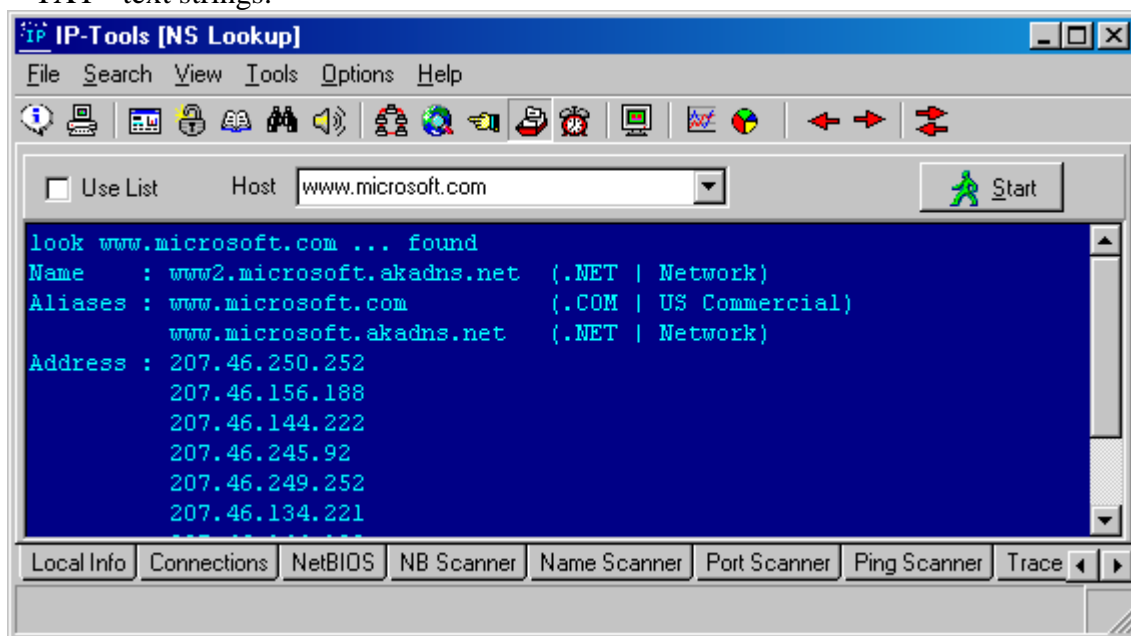
Кроме того, Вы можете переключить эту утилиту в режим "Advanced Name Server Lookup". В этом случае Вы сможете изменить:

- DNS сервер;
- порт и протокол (TCP, UDP);
- таймаут и количество попыток получить ответ от сервера;
- тип запроса: A, ANY, CNAME, HINFO, MX, NS, PTR, SOA, или TXT;
- включить или отключить рекурсию;
- режим вывода информации: Full, Medium, или Compact.

IP-Tools поддерживает следующие типы записей:

- A - a host address
- NS - an authoritative name server
- MD - a mail destination
- MF - a mail forwarder
- CNAME - the canonical name for an alias
- SOA - marks the start of a zone of authority
- MB - a mailbox domain name

- MG - a mail group member
- MR - a mail rename domain name
- WKS - a well known service description
- PTR - a domain name pointer
- HINFO - host information
- MINFO - mailbox or mail list information
- MX - mail exchange
- TXT - text strings.



12. Get Time. Данная утилита получает время с TimeServers (с серверов точного времени). Причем программа может синхронизировать время в автоматическом режиме, например, каждый раз при загрузке машины. Для этого нужно запустить программу с параметрами:

> ip\_tools.exe /SetTime TryCount Host1 [Host2 [Host3 [...]]], где :

TryCount - число попыток соединения с указанными серверами (0..255)

Host1 .. HostN - адреса серверов точного времени

Программа по очереди пытается соединиться с серверами; если ей это удалось, она получает время, устанавливает его на локальной машине и завершает работу. Если же программа не может соединиться с сервером, она берет следующий адрес из списка, если список пройден до конца, программа начинает с начала списка, и так TryCount раз.

Example :> ip\_tools.exe /SetTime 2 ха.ха.net 192.43.244.18

13. Telnet client. Telnet client - программа эмулирующая терминал в TCP/IP сетях, ее назначение позволять пользователю соединиться с удаленным компьютером и водить команды которые будут выполняться так как если бы пользователь вводил эти команды непосредственно на удаленной машине. На этой странице два окошка :

- нижнее почти не умеет обрабатывать ESC-последовательности, зато запоминает все, что в него попадает, работает как лог.

- верхнее окно это и есть telnet клиент, виртуальный терминал, который обрабатывает ESC-последовательности, но помнит только то, что поместилось на его консоль.

14. Ip Monitor. IP-Monitor показывает в реальном масштабе времени графики количества входящих, исходящих, ошибочных пакетов для протоколов TCP,UDP,ICMP.

TCP In - общее количество полученных TCP пакетов;

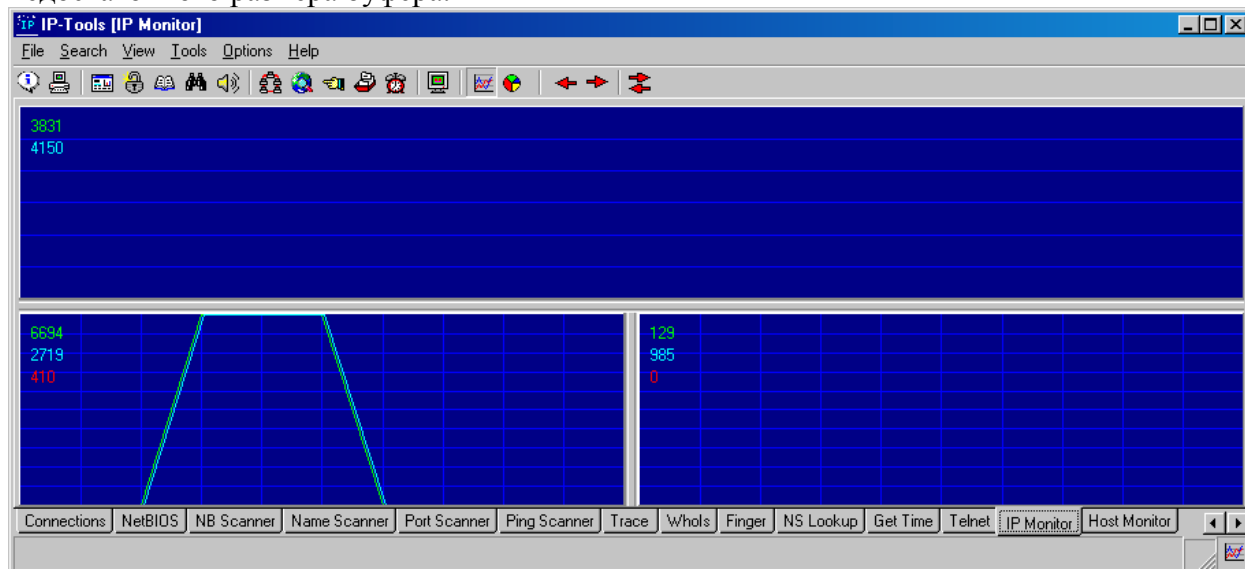
TCP Out - общее количество отправленных TCP пакетов;

UDP In - общее количество полученных UDP датаграмм;

UDP Out - общее количество отправленных UDP датаграмм;



UDP Error - количество полученных ошибочных UDP пакетов;  
 ICMP In - общее количество полученных ICMP пакетов (включая ошибочные);  
 ICMP Out - общее количество отправленных ICMP пакетов (включая ошибочные);  
 ICMP Error - количество ICMP пакетов которые были получены но определены как содержащие ошибки (плохая контрольная сумма, неверная длина, и т.д.) + количество ICMP пакетов которые не получилось отправить из-за разных проблем, например недостаточного размера буфера.



15. Host Monitor. Host Monitor умеет пинговать заданные хосты и показывать их статус (Up/Down). Интервалы через которые нужно проверять хосты и параметры пингования задаются отдельно для каждого хоста. Программа также может проигрывать wav-файлы при изменении состояния хоста и записывать изменения статуса хостов в Log file. Для каждого хоста можно задать команды для запуска внешних программ, которые будут выполняться если хост меняет статус dead -> alive или наоборот. В команде можно задавать макроподстановки :

%DateTime% - IP-Tools подставит дату и время

%HostName% - IP-Tools подставит имя хоста

В каталоге "SAMPLES\" есть примеры :

- "message.exe" - программа message, которая просто выводит диалоговое окно с текстом, который передается через командную строку

- "sendmail.exe" – программа, которая может отсылать письма без участия человека; при этом все нужные параметры можно передать через командную строку

Например, можно задать такую команду "samples\sendmail.exe To=admin@firm.com "Subject=%datetime% host %hostname% is Dead" StartAfterLoad"

А поскольку по e-mail можно отправлять сообщения даже на пейджер, то IP-Tools может сообщить админу о падении сервера даже на пляже (чему он, несомненно, обрадуется).

В любой утилите можно нажать правую кнопку мыши для вызова контекстного меню.

Все настройки программы находятся в диалоге Options.

Preferences

Здесь Вы можете изменить параметры интерфейса программы :

- Colors palette - палитра цветов (стандартная для ОС WINDOWS: зеленое на черном, желтое на синем, голубое на синем)

- Fonts- шрифт текста в окнах с информацией и шрифт для telnet клиента

- Help language - язык помощи (help language) (Русский, Английский, Испанский)

- Tab position можно выбрать, где будут размещаться закладки страниц: сверху (Top) или внизу (Bottom) окна.



- Auto save options of main window pages: если включена эта опция то при нажатии кнопки [Start] утилита запоминает свои параметры, например имя хоста. IP-Monitor запоминает размеры своих подокон. И при следующем запуске программа восстанавливает запомненные значения.

- Auto save current page: если включить эту опцию, то программа будет запоминать (и при следующем запуске выбирать) активную утилиту.

- Kept in lists recent addresses: если включить эту опцию, то программа будет запоминать введенные вами адреса в списках.

- Clear old info: если включить эту опцию то, при нажатии на кнопку Start старое содержимое окна будет удаляться.

- Scroll down: по завершении работы утилиты перемещается в низ окна

- Minimize to tray отвечает за минимизацию IP-Tools в tray.

- Always top: если включить данную опцию, то IP-Tools будет всегда поверх других окон, даже если активна другая программа.

Interface:

- Toolbar position: показать панель инструментов (toolbar) сверху/снизу или совсем ее не показывать.

- Tabs position: тоже самое для закладок страниц (утилит).

- Allow page multiline: если включить эту опцию, то закладки страниц (утилит) программы при необходимости будут размещаться в несколько строчек. А если не включать, то закладки будут в одну строчку, но с кнопочками для скроллинга.

- Status bar: показать/спрятать строку состояния (status bar).

- Show ScanList dialog when user marks "Use list" option

Некоторые утилиты (NetBIOS, Lookup, все сканеры) могут работать со списками адресов. Если Вы включите эту опцию, IP-Tools будет показывать диалог с этим списком адресов каждый раз когда Вы будете включать опцию "Use list".

## **Порядок выполнения работы**

### **Задание 1. Анализ и исследование протокола разрешения адресов**

1. Изучить теоретическую часть.
2. Установить программу CommView, обеспечивающую перехват и последующий анализ сетевых пакетов.
3. Изучить возможности программы CommView.
4. Начать захват пакетов в программе CommView.
5. С помощью программы ping послать запрос к соседнему компьютеру сети.
6. Исследовать структуру пакетов с запросом и ответом, выяснить значение всех полей перехваченных пакетов.
7. Просмотрите таблицу преобразования IP адресов в физические с помощью команды ARP. Проверьте, как меняется таблица после выполнения команды ping.
8. В случае отсутствия пакетов ARP (MAC-адрес назначения уже известен), удалить соответствующие записи из таблицы адресов с помощью программы arp.
9. С помощью программы ping послать запрос к недоступному компьютеру.
10. Проанализировать передаваемые пакеты.

### **Задание 2. Анализ и исследование сетей с помощью служебных утилит**

1. С помощью утилиты Ipconfig получите и проанализируйте информацию о локальном компьютере в сети, и кафедральной сети:

- a. определите настройки сетевых подключений и запишите их;
  - b. определите имя компьютера и имя домена;
  - c. определите тип сетевой карты и ее драйвера;
  - d. идентифицируйте, какие протоколы привязаны к сетевой карте;
  - e. определите IP адрес машины;
  - f. определите маску подсети и IP адрес заданного по умолчанию шлюза (маршрутизатора);
  - g. определите, используется ли DNS, DHCP и WINS; определите IP адреса серверов, обеспечивающих эти услуги;
  - h. определите MAC адрес сетевой платы;
  - i. Результаты сохраните в отчете.
2. С помощью команды ping в различных вариантах проверьте доступность серверов и других компьютеров кафедральной сети. Результаты сохраните в отчете.
  3. С помощью команды tracert определите и проанализируйте маршрут в локальной сети до университетского сайта [www.pnzgu.ru](http://www.pnzgu.ru).
  4. С помощью команды tracert определите и проанализируйте маршрут в глобальной сети, по которому передаются пакеты от пользовательского компьютера до узла согласно варианту задания. Результаты сохраните в отчете.
  5. Выполните пункты 3,4 с помощью другой команды pathping. Результаты сохраните в отчете.
  6. С помощью команды route получите и проанализируйте информацию о таблице маршрутов и маршрутизации. Результаты сохраните в отчете.
  7. Используя утилиту netstat, получите:
    - a. список подключений;
    - b. статистику сети для разных протоколов;
    - c. таблицы маршрутизации.
    - d. Проанализируйте полученные результаты.
  8. Используйте утилиту NET для управления ресурсами ЛВС по протоколу NetBIOS:
    - a. получите сетевые сведения
    - b. подключите и отключите любой сетевой ресурс
    - c. для получения справки об утилите наберите net help
    - d. Результаты сохраните в отчете.

#### **Задание 4. Анализ и исследование сетей с помощью утилит пакета IP Tools**

1. Запустите программу IP-Tools и изучите приемы работы с ее сетевыми утилитами.
2. Получите информацию о локальной машине: конфигурация, сетевые интерфейсы, таблицу маршрутизации. Сохраните скриншоты результатов для отчета.
3. Получите список текущих подключений с номерами и именами портов; протокол изменения подключений при доступе к общим ресурсам со стороны других пользователей (для этого доступ надо, естественно, разрешить). Собирайте информацию о всех пользователях, подключенных к серверу кафедры в данный момент. Сохраните скриншоты результатов для отчета.
4. Соберите информацию о сетевых интерфейсах на машине соседа. Сохраните скриншоты результатов для отчета.
5. Определите список выделенных ресурсов в локальной сети кафедры. Подключитесь к найденным ресурсам. Сохраните скриншоты результатов для отчета.
6. Получите список имен машин в локальной сети кафедры с IP адресами. Сохраните скриншоты результатов для отчета.

7. Получите список открытых портов на машине соседа и на сервере с описанием портов. Сохраните скриншоты результатов для отчета.

8. Составьте список маршрутизаторов с их адресами между своим узлом и узлом согласно варианту задания. Используя утилиту WhoIs получите сведения об удаленном узле. Сохраните скриншоты результатов для отчета.

9. Получите информацию об имени хоста, его IP адресе и алиасах согласно варианту из предыдущей работы. Сохраните скриншоты результатов для отчета.

## **Защита работа**

Для защиты данной работы, необходимо:

- Предоставить отчет с результатами исследования процедур разрешения адресов.
- Предоставить отчет с результатами исследования сетей сужеными диагностическими утилитами.
- Уметь ответить на контрольные вопросы.