Лабораторная работа № 6
Адресация и маршрутизация в сетях TCP/IP

Цель работы: практически освоить работу с утилитами TCP/IP, определить настройки для подключения к локальной сети и к сети Internet с использованием утилиты ipconfig , исследовать вероятностно-временных характеристики фрагментов сети Internet с использованием утилиты ping, исследовать топологии фрагментов сети Internet с использованием утилиты tracert.

Задания

1. Изучите приложение.
2. Выведите на экран справочную информацию по утилитам ipconfig, ping, tracert, hostname. Для этого в командной строке введите имя утилиты без параметров или с /?.

Изучите ключи, используемые при запуске утилит.

3. Выведите на экран имя локального хоста с помощью команды hostname.
4. Проверьте конфигурацию TCP/IP с помощью утилиты ipconfig. Заполните таблицу:

Имя хоста	Ws21
IP-адрес	192.168.12.21
Маска подсети	255.255.255.0
Основной шлюз	192.168.12.1
Используется ли DHCP (адрес DHCP-сервера)	no
Описание адаптера	PCI FAST ETHERNET realtek rtl8139
Физический адрес сетевого адаптера	00-c0-26-2b-66-fe
Адрес DNS-сервера	no
Адрес WINS-сервера	no

5. С помощью команды ping проверьте перечисленные ниже адреса и для каждого из них отметьте время отклика. Попробуйте увеличить время отклика.
   a) www.arcotel.ru
   b) www.google.com

Задайте различную длину посылаемых пакетов. Запишите времена прохождения пакетов для всех случаев.

10. С помощью команды tracert проверьте для перечисленных ниже адресов, через какие промежуточные узлы идет сигнал. Отметьте их:

a) www.arcotel.ru

b) www.google.com

11. С помощью утилиты arp просмотрите ARP-таблицу локального компьютера.

12. Выполните команду tracert www.google.com. Запишите адреса и имена промежуточных узлов, через которые осуществляется трассировка маршрута.

13. Выполните команду tracert www.arcotel.ru>c:\temp\mytrace.txt

14. Проанализируйте полученный файл mytrace.txt. Оцените времена задержек пакетов трассировки в пути.

15. Выполните команду tracert и ping до Мельбурнского(www.mbs.unimelb.edu.au), Токийского (www.tufs.ac.jp) и Владивостокского (www.vvsu.ru) университетов. Сравните времена доступа.

16. Выполните команду route для определения маршрутов, по которым пакеты от вашего компьютера доставляются на следующие узлы сети. Например при выполнении команды route print мы можем получить следующие результаты.

>route print

```
===========================================================================
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0     10.18.5.161     10.18.5.161       1
          0.0.0.0          0.0.0.0     172.16.1.1      172.16.0.105     21
         10.18.0.7  255.255.255.255     172.16.1.1      172.16.0.105     20
      10.18.5.161  255.255.255.255      127.0.0.1       127.0.0.1       50
   10.255.255.255  255.255.255.255     10.18.5.161     10.18.5.161      50
        127.0.0.0        255.0.0.0      127.0.0.1       127.0.0.1       1
      172.16.0.0    255.255.254.0     172.16.0.105    172.16.0.105      20
    172.16.0.105  255.255.255.255      127.0.0.1       127.0.0.1       20
  172.16.255.255  255.255.255.255     172.16.0.105    172.16.0.105      20
        224.0.0.0        240.0.0.0     172.16.0.105    172.16.0.105      20
        224.0.0.0        240.0.0.0     10.18.5.161     10.18.5.161       1
  255.255.255.255  255.255.255.255     172.16.0.105    172.16.0.105      1
Основной шлюз:        10.18.5.161
===========================================================================
Постоянные маршруты:
  Отсутствует
```

17. С помощью утилиты netstat выведите перечень сетевых соединений и статистическую информацию для протоколов UDP, TCP, ICMP, IP.

Контрольные вопросы

1.Прочитайте справочный материал о протоколе DHCP (Dynamic Host Configuration
Protocol)

2. Прочитайте справочный материал о серверах службы имен Microsoft WINS
(Windows Internet Naming Service).

3. Изучите ключи утилит ping и tracert вашей операционной системы

4. Проанализируйте другие возможности серверов NOC.CARAVAN.RU и WWW.SIRENA.NET

5. Прочтите материал о всемирной службе доменных имен и возможностях утилиты nslookup.

6. Определите адрес и доменное имя маршрутизатора, через который совершается ваш выход в Интернет и протрассируйте маршрут к нему командой tracert <маршрутизатор>

Приложение

Типы адресов**:** физический **(MAC**-адрес**),** сетевой **(IP-**адрес**)** и символьный **(DNS**-имя**)**

Каждый компьютер в сети TCP/IP имеет адреса трех уровней:

- Локальный адрес узла, определяемый технологией, с помощью которой построена отдельная сеть, в которую входит данный узел. Для узлов, входящих в локальные сети, это MAC-адрес сетевого адаптера или порта маршрутизатора, например, 11-A0-17-3D-BC-01. Эти адреса назначаются производителями оборудования и являются уникальными адресами, так как управляются централизовано. Для всех существующих технологий локальных сетей MAC-адрес имеет формат 6 байтов: старшие 3 байта - идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем.
- IP-адрес, состоящий из 4 байт, например, 109.26.17.100. Этот адрес используется на сетевом уровне. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения Internet (Network Information Center, NIC), если сеть должна работать как составная часть Internet. Обычно провайдеры услуг Internet получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами. Номер узла в протоколе IP назначается независимо от локального адреса узла. Деление IP-адреса на поле номера сети и номера узла - гибкое, и граница между этими полями может устанавливаться весьма произвольно. Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IPадресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.
- Символьный идентификатор-имя, например, SERV1.IBM.COM. Этот адрес назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена. Такой адрес, называемый также DNS-именем, используется на прикладном уровне, например, в протоколах FTP или telnet.

Три основных класса **IP**-адресов

IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме, и разделенных точками, например:

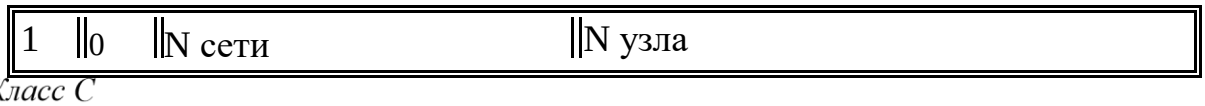
128.10.2.30 - традиционная десятичная форма представления адреса,

10000000 00001010 00000010 00011110 - двоичная форма представления этого же адреса.

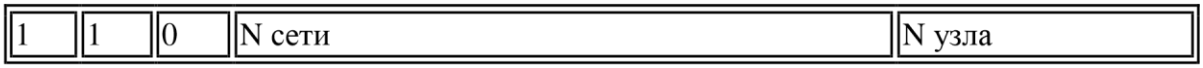
Далее показана структура IP-адреса в зависимости от класса сети.

Класс A

Класс B

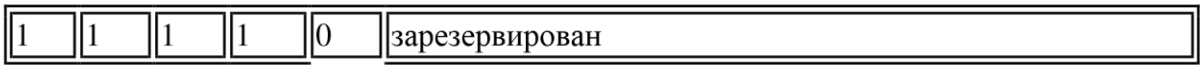


Класс C



Класс D

Класс E



Адрес состоит из двух логических частей - номера сети и номера узла в сети. Какая часть адреса относится к номеру сети, а какая к номеру узла, определяется значениями первых битов адреса:

- Если адрес начинается с 0, то сеть относят к классу A, и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса A имеют номера в диапазоне от 1 до 126. (Номер 0 не используется, а номер 127 зарезервирован для специальных целей, о чем будет сказано ниже.) В сетях класса A количество узлов должно быть больше 2^{16} , но не превышать 2^{24}.
- Если первые два бита адреса равны 10, то сеть относится к классу B и является сетью средних размеров с числом узлов 2^8 - 2^{16}. В сетях класса B под адрес сети и под адрес узла отводится по 16 бит, то есть по 2 байта.
- Если адрес начинается с последовательности 110, то это сеть класса C с числом узлов не больше 2^8. Под адрес сети отводится 24 бита, а под адрес узла - 8 бит.
- Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес - multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес.
- Если адрес начинается с последовательности 11110, то это адрес класса E, он зарезервирован для будущих применений.

В таблице приведены диапазоны номеров сетей, соответствующих каждому классу сетей.

Класс	Наименьший адрес	Наибольший адрес
A	01.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.1.0.	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Отображение символьных адресов на **IP**-адреса**:** служба **DNS**

DNS (Domain Name System) - это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Internet. Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени узла. Спецификация DNS определяется стандартами RFC 1034 и 1035. DNS требует статической конфигурации своих таблиц, отображающих имена компьютеров в IP-адрес.

Протокол DNS является служебным протоколом прикладного уровня. Этот протокол несимметричен - в нем определены DNS-серверы и DNS-клиенты. DNS-серверы хранят часть распределенной 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 может сам обработать запрос, либо передать его другому DNScерверу. Все DNS-серверы соединены иерархически, в соответствии с иерархией доменов сети Internet. Клиент опрашивает эти серверы имен, пока не найдет нужные отображения. Этот процесс ускоряется из-за того, что серверы имен постоянно кэшируют информацию, предоставляемую по запросам. Клиентские компьютеры могут использовать в своей работе IP-адреса нескольких DNS-серверов, для повышения надежности своей работы.

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 узлам домена.

Корень базы данных DNS управляется центром Internet Network Information Center. Домены верхнего уровня назначаются для каждой страны,

а также на организационной основе. Имена этих доменов должны следовать международному стандарту ISO 3166. Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, а для различных типов организаций используются следующие аббревиатуры:

- com - коммерческие организации (например, microsoft.com);
- edu - образовательные (например, mit.edu);
- gov - правительственные организации (например, nsf.gov); • org - некоммерческие организации (например, fidonet.org); • net - организации, поддерживающие сети (например, nsf.net).

Каждый домен DNS администрируется отдельной организацией, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям. Каждый домен имеет уникальное имя, а каждый из поддоменов имеет уникальное имя внутри своего домена. Имя домена может содержать до 63 символов. Каждый хост в сети Internet однозначно определяется своим полным доменным именем *(fully qualified domain name, FQDN),* которое включает имена всех доменов по направлению от хоста к корню. Пример полного DNS-имени: server.aics.acs.cctpu.edu.ru

Автоматизация процесса назначения **IP**-адресов узлам сети - протокол **DHCP**

IP-адреса могут назначаться администратором сети вручную. Это представляет для администратора утомительную процедуру. Ситуация усложняется еще тем, что многие пользователи не обладают достаточными знаниями для того, чтобы конфигурировать свои компьютеры для работы в интерсети и должны поэтому полагаться на администраторов. Протокол *Dynamic Host Configuration Protocol (DHCP)* был разработан для того, чтобы освободить администратора от этих проблем. Основным назначением DHCP является динамическое назначение IP-адресов. Однако, кроме динамического, DHCP может поддерживать и более простые способы ручного и автоматического статического назначения адресов.

В ручной процедуре назначения адресов активное участие принимает администратор, который предоставляет DHCP-серверу информацию о соответствии IPадресов физическим адресам или другим идентификаторам клиентов. Эти адреса сообщаются клиентам в ответ на их запросы к DHCP-серверу.

При автоматическом статическом способе DHCP-сервер присваивает IP-адрес (и, возможно, другие параметры конфигурации клиента) из пула (набора) наличных IPадресов без вмешательства оператора. 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 IPадреса клиенту. При всех последующих запросах сервер возвращает тот же самый IPадрес.

При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, что дает возможность впоследствии повторно использовать IP-адреса другими компьютерами. Динамическое разделение адресов позволяет строить IP-сеть, количество узлов в которой намного превышает количество имеющихся в распоряжении администратора IP-адресов.

Системные утилиты сетевой диагностики

В состав TCP/IP входят диагностические утилиты, предназначенные для проверки конфигурации стека и тестирования сетевого соединения.

Утилита	Применение
arp	Выводит для просмотра и изменения таблицу трансляции адресов, используемую протоколом разрешения адресов ARP (Address Resolution Protocol - определяет локальный адрес по IP-адресу)
hostname	Выводит имя локального хоста. Используется без параметров.
ipconfig	Выводит значения для текущей конфигурации стека TCP/IP: IPадрес, маску подсети, адрес шлюза по умолчанию, адреса WINS (Windows Internet Naming Service) и DNS (Domain Name System)
nbtstat	Выводит статистику и текущую информацию по NetBIOS, установленному поверх TCP/IP. Используется для проверки состояния текущих соединений NetBIOS.
netstat	Выводит статистику и текущую информацию по соединению TCP/IP.
nslookup	Осуществляет проверку записей и доменных псевдонимов хостов, доменных сервисов хостов, а также информации операционной системы, путем запросов к серверам DNS.
ping	Осуществляет проверку правильности конфигурирования TCP/IP и проверку связи с удаленным хостом.
route	Модифицирует таблицы маршрутизации IP. Отображает содержимое таблицы, добавляет и удаляет маршруты IP.

tracert	Осуществляет проверку маршрута к удаленному компьютеру путем отправки эхо-пакетов протокола ICMP (Internet Control Message Protocol). Выводит маршрут прохождения пакетов на удаленный компьютер.

Утилита **ipconfig**

При устранении неисправностей и проблем в сети TCP/IP следует сначала проверить правильность конфигурации TCP/IP. Для этого используется утилита ipconfig.

Эта команда полезна на компьютерах, работающих с DHCP (Dynamic Host Configuration Protocol), так как дает пользователям возможность определить, какая конфигурация сети TCP/IP и какие величины были установлены с помощью DHCP. Синтаксис:

ipconfig [/all | /renew[adapter] | /release]

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;

release[adapter] освобождает выделенный DHCP IP-адрес; adapter – имя сетевого адаптера;

displaydns выводит информацию о содержимом локального кэша клиента DNS, используемого для разрешения доменных имен.

Таким образом, утилита ipconfig позволяет выяснить, инициализирована ли конфигурация и не дублируются ли IP-адреса:

- если конфигурация инициализирована, то появляется 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 .

Например при выполнении команды ipconfig мы можем получить следующие результаты.

>ipconfig

Настройка протокола *IP* для *Windows*

Подключение по локальной сети *2 - Ethernet* адаптер*:*

DNS-суффикс этого подключения . . *: voliacable.com*
IP-адрес . . . . . *: 82.144.223.226*
Маска подсети . . . . . *: 255.255.252.0*
Основной шлюз . . . . . *: 82.144.220.1*

Утилита **ping**

Утилита ping (Packet Internet Groper) является одним из главных средств, используемых для отладки сетей, и служит для принудительного вызова ответа конкретной машины. Она позволяет проверять работу программ TCP/IP на удаленных машинах, адреса устройств в локальной сети, адрес и маршрут для удаленного сетевого устройства. В выполнении команды ping участвуют система маршрутизации, схемы разрешения адресов и сетевые шлюзы. Это утилита низкого уровня, которая не требует наличия серверных процессов на проверяемой машине, поэтому успешный результат при прохождении запроса вовсе не означает, что выполняются какие-либо сервисные программы высокого уровня, а говорит о том, что сеть находится в рабочем состоянии, питание проверяемой машины включено, и машина не отказала ("не висит").

В Windows утилита ping имеется в комплекте поставки и представляет собой программу, запускаемую из командной строки.

Запросы утилиты ping передаются по протоколу ICMP (Internet Control Message Protocol). Получив такой запрос, программное обеспечение, реализующее протокол IP у адресата, посылает эхо-ответ. Если проверяемая машина в момент получения запроса была загружена более приоритетной работой (например, обработкой и перенаправлением большого объема трафика), то ответ будет отправлен не сразу, а как только закончится выполнение более приоритетной задачи. Поэтому следует учесть, что задержа, рассчитанная утилитой ping, вызвана не только пропускной способностью канала передачи данных до проверяемой машины, но и загруженностью этой машины. Эхо-запросы посылаются заданное количество раз (ключ -n). По умолчанию передается четыре запроса, после чего выводятся статистические данные.

Обратите внимание*:* поскольку с утилиты *ping* начинается хакерская атака, некоторые серверы в целях безопасности могут не посылать эхо-ответы *(*например, *www.microsoft.com).* Не ждите напрасно, введите команду прерывания *(CTRL+C).*

Формат команды*:* ping [-t][-a][-n][-l][-f][-i TTL][-v TOS]
[-r][][имя машины][[-j списокУзлов]|[-k списокУзлов]][-w]

Параметры утилиты ping

Ключи	Функции
-t	Отправка пакетов на указанный узел до команды прерывания
-a	Определение имени узла по IP-адресу
-n	Число отправляемых запросов
-l	Размер буфера отправки
-f	Установка флага, запрещающего фрагментацию пакета
-i TTL	Задание времени жизни пакета (поле "Time To Live")

На практике большинство опций в формате команды можно опустить, тогда в командной строке может быть*: ping* имя узла *(*для зацикливания вывода информации о соединении используется опция *–t;* для вывода информации *n*-раз используется опция *–n* количество раз*).*

Например при выполнении команды ping www.google.com.ua мы получим следующие результаты *ping google.com.ua*

Обмен пакетами с *google.com.ua [216.239.39.99]* по *32* байт*:*

Ответ от *216.239.39.99:* число байт*=32* время*=154*мс *TTL=236*
Ответ от *216.239.39.99:* число байт*=32* время*=156*мс *TTL=236*
Ответ от *216.239.39.99:* число байт*=32* время*=156*мс *TTL=236*
Ответ от *216.239.39.99:* число байт*=32* время*=171*мс *TTL=236*

Статистика *Ping* для *216.239.39.99:*
Пакетов*:* отправлено *= 4,* получено *= 4,* потеряно *= 0 (0%* потерь*),* Приблизительное время приема-передачи в мс*:*
Минимальное *= 154*мсек, Максимальное *= 171* мсек, Среднее *= 159* мсек

ping –n 20 peak.mountin.net

Обмен пакетами с *peak.mountin.net [207.227.119.2]* по *32* байт*:*
Превышен интервал ожидания для запроса.
Ответ от *207.227.119.2:* число байт*=32* время*=734*мс *TTL=231*
Ответ от *207.227.119.2:* число байт*=32* время*=719*мс *TTL=231*
Ответ от *207.227.119.2:* число байт*=32* время*=688*мс *TTL=231*
Ответ от *207.227.119.2:* число байт*=32* время*=704*мс *TTL=231*
Превышен интервал ожидания для запроса.
Ответ от *207.227.119.2:* число байт*=32* время*=719*мс *TTL=231*
Ответ от *207.227.119.2:* число байт*=32* время*=1015*мс *TTL=231* Превышен интервал ожидания для запроса.
Ответ от *207.227.119.2:* число байт*=32* время*=703*мс *TTL=231*
Ответ от *207.227.119.2:* число байт*=32* время*=688*мс *TTL=231*
Ответ от *207.227.119.2:* число байт*=32* время*=782*мс *TTL=231*
Ответ от *207.227.119.2:* число байт*=32* время*=688*мс *TTL=231*
Ответ от *207.227.119.2:* число байт*=32* время*=688*мс *TTL=231*
Ответ от *207.227.119.2:* число байт*=32* время*=688*мс *TTL=231*
Превышен интервал ожидания для запроса.
Ответ от *207.227.119.2:* число байт*=32* время*=687*мс *TTL=231*
Ответ от *207.227.119.2:* число байт*=32* время*=735*мс *TTL=231*

Ответ от *207.227.119.2:* число байт=*32* время=*672*мс *TTL=231*
Ответ от *207.227.119.2:* число байт=*32* время=*704*мс *TTL=231*

Статистика *Ping* для *207.227.119.2:*
Пакетов*:* отправлено = *20*, получено = *16*, потеряно = *4 (20%* потерь*)*, Приблизительное время передачи и приема*:* наименьшее = *672*мс, наибольшее = *1015*мс, среднее = *580*мс

Пример определения имени узла по *IP*-адресу
ping –a 194.67.57.26
Обмен пакетами с *mail.ru [194.67.57.26]* по *32* байт*: …*

Утилита **tracert**

Утилита tracert позволяет выявлять последовательность маршрутизаторов, через которые проходит IP-пакет на пути к пункту своего назначения.

Формат команды*:* tracert имя_машины

имя_машины может быть именем узла или IP-адресом машины. Выходная информация представляет собой список машин, начиная с первого шлюза и заканчивая пунктом назначения. Например при выполнении команды tracert www.google.com.ua мы получим следующие результаты

>tracert www.google.com.ua

Трассировка маршрута к *www.l.google.com [66.249.93.104]* с максимальным числом прыжков *30:*

1 45 ms 31 ms 31 ms c7-2.sub-5.volia.net [82.144.220.1]
2 15 ms 15 ms 31 ms gig0-1-5.diamond.volia.net [82.144.192.225]
3 187 ms 46 ms 31 ms datagroup-gw.volia.net [80.91.180.69]
4 77 ms 93 ms 93 ms peer-sprint-r.newline.net.ua [80.91.180.6]
5 106 ms 77 ms 61 ms sl-bb20-fra-6-1.sprintlink.net [217.147.96.68]
6 77 ms 77 ms 62 ms sl-bb21-par-4-0.sprintlink.net [213.206.129.149]
7 187 ms 77 ms 62 ms sle-franc1-3-0.sprintlink.net [213.206.131.42]
8 77 ms 77 ms 93 ms 193.251.128.117
9 124 ms 93 ms 93 ms 193.251.132.73
10 93 ms 93 ms 109 ms 193.251.249.62
11 93 ms 108 ms 77 ms 216.239.46.48
12 93 ms 124 ms 109 ms 64.233.175.248
13 124 ms 93 ms 93 ms 216.239.43.89
14 109 ms 109 ms 109 ms 66.249.94.54
15 109 ms 93 ms 109 ms 66.249.94.50

16 187 ms 109 ms 93 ms 66.249.93.104

Трассировка завершена.

Пакеты посылаются по три на каждый узел. Для каждого пакета на экране отображается величина интервала времени между отправкой пакета и получением ответа. Символ * означает, что ответ на данный пакет не был получен. Если узел не отвечает, то при превышении интервала ожидания ответа выдается сообщение «Превышен интервал ожидания для запроса». Интервал ожидания ответа может быть изменен с помощью опции –w команды tracert.

Примечание*:*

Некоторые маршрутизаторы просто молча уничтожают пакеты с истекшим временем ожидания и не будут видны утилите *tracert.* Синтаксис:

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] имя_целевого_хоста Параметры:

-d указывает, что не нужно распознавать адреса для имен хостов;

-h maximum_hops указывает максимальное число хопов для того, чтобы искать цель;

-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 мсек.

Команда tracert работает путем установки поля времени жизни (числа переходов) исходящего пакета таким образом, чтобы это время истекало до достижения пакетом пункта назначения. Когда время жизни истечет, текущий шлюз отправит сообщение об ошибке на машину-источник. Каждое приращение поля времени жизни позволяет пакету пройти на один маршрутизатор дальше.

Примечание*:*

Для вывода информации в файл используйте символ перенаправления потока вывода *«>».* Данный символ справедлив и для утилит *ping* и *tracert*.

Пример*:*

tracert 195.208.164.1 > tracert.txt

Отчет о трассировке маршрута до указанного узла будет помещен в файл tracert.txt.

Утилита **ARP.**

Основная задача протокола ARP – трансляция IP-адресов в соответствующие локальные адреса. Для этого ARP-протокол использует информацию из ARP-таблицы (ARP-кэша). 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 кэша. Синтаксис:

arp [-s inet_addr eth_addr] | [-d inet_addr] | [-a]

Параметры:

-s занесение в кэш статических записей;

-d удаление из кэша записи для определенного IP-адреса;

-a просмотр содержимого кэша для всех сетевых адаптеров локального компьютера;

inet_addr - IP-адрес;

eth_addr - MAC-адрес.

Утилита **netstat.**

Утилита netstat позволяет получить статическую информацию по некоторым из протоколов стека (TCP, UDP, IP, ICMP), а также выводит сведения о текущих сетевых соединениях. Особенно она полезна на брандмауэрах, с ее помощью можно обнаружить нарушения безопасности периметра сети. Синтаксис:

netstat [-a] [-e] [-n] [-s] [-p protocol] [-r]

Параметры:

-a выводит перечень всех сетевых соединений и прослушивающихся портов локального компьютера;

-e выводит статистику для Ethernet-интерфейсов (например, количество полученных и отправленных байт);

-n выводит информацию по всем текущим соединениям (например, TCP) для всех сетевых интерфейсов локального компьютера. Для каждого соединения выводится информация об IP-адресах локального и удаленного интерфейсов вместе с номерами используемых портов; -s выводит статистическую информацию для протоколов UDP, TCP, ICMP, IP.

Ключ «/more» позволяет просмотреть информацию постранично; -r выводит содержимое таблицы маршрутизации.