МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«_24_» _____ 2017 г.

СЕТЕВЫЕ УТИЛИТЫ И ИХ ИСПОЛЬЗОВАНИЕ

Методические указания к лабораторной работе
для студентов укрупненной группы специальностей и
направлений подготовки 10.00.00 «Информационная безопасность»

Курск 2017

УДК 621.(076.1)

Составитель: М.О. Таныгин

Рецензент

Кандидат технических наук, доцент кафедры
«Информационная безопасность» И.В. Калуцкий

Сетевые утилиты и их использование [Текст] : методические указания к лабораторной работе/ Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. – Курск, 2017. – 11 с.: ил. 4. – Библиогр.: с. 11.

Содержат сведения по вопросам лабораторной работы по основам мониторинга безопасности инфокоммуникационных систем и сетей. Указывается порядок выполнения лабораторной работы, правила оформления отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность».

Текст печатается в авторской редакции

Подписано в печать 24.11.17. Формат 60x84 1/16.
Усл.печ. л. 0,64. Уч.-изд. л. 0,58. Тираж 100 экз. Заказ. Бесплатно. 2143
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Цель работы: определение настроек для подключения к локальной сети и к сети Internet с использованием утилиты ipconfig. Исследование вероятностно-временных характеристик фрагментов сети Internet с использованием утилиты ping. Исследование топологии фрагментов сети Internet с использованием утилиты tracert[1].

Методические указания к выполнению лабораторной работы

Адресация в IP-сетях, типы адресов

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

1. 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.

2. 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.

3. Символьный идентификатор (такой адрес, называемый также DNS-именем) - имя, например, SERV1.IBM.COM. Этот адрес назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени

[1] Вычислительные системы, сети и телекоммуникации: учебник / А.П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. - 3-е изд., доп. и перераб. – М.: Финансы и статистика, 2006.

домена, 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 - 128.10.2.30 - традиционная десятичная форма представления адреса, 10000000 00001010 00000010 00011110 - двоичная форма представления этого же адреса.

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. В сетях класса A количество узлов должно быть больше 216, но не превышать 224);
- если первые два бита адреса равны 10, то сеть относится к классу B и является сетью средних размеров с числом узлов 28 – 216 (в сетях класса B под адрес сети и под адрес узла отводится по 16 бит - 2 байта);
- если адрес начинается с последовательности 110 - сеть класса C с числом узлов не больше 28 (адрес сети - 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.

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.

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 посылает ответ клиенту, если нет - то он посылает запрос DNS-серверу другого домена, который может сам обработать запрос, либо передать его другому DNS-серверу. 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 (записывают во внутреннюю память) информацию, предоставляемую по запросам.

База данных DNS имеет структуру дерева, называемого доменным пространством имен, в котором каждый домен (узел дерева) имеет имя и может содержать поддомены. Корень базы данных DNS управляется центром Internet Network Information Center. Домены верхнего уровня назначаются для каждой страны, а также на организационной основе:

- .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 узел в сети Internet однозначно определяется своим полным доменным именем (fully qualified domain name, FQDN), которое включает имена всех доменов по направлению от этого узла к корню. Например - server.aics.acs.cctpu.edu.ru.

Далее в описании команд используется:

- < текст > - текст в угловых скобках - обязательный параметр;
- [текст] - текст в квадратных скобках - необязательный параметр;
- (текст) - текст в круглых скобках - выбрать один из параметров;
- вертикальная черта «|» - разделитель для взаимоисключающих параметров - нужно выбрать один из них;
- многоточие «...» - возможно повторение указанных параметров.

Утилита ipconfig

Утилита ipconfig (IP configuration) предназначена для настройки протокола IP для операционной системы Windows (рис. 1). Для получения этой информации запустите интерпретатор команд cmd.exe «Пуск» → «Найти программы и файлы» → cmd и в командной строке введите: ipconfig (используя команды cd/ и cls можно перейти в корневой каталог и очистить экран, соответственно, для удобства работы).

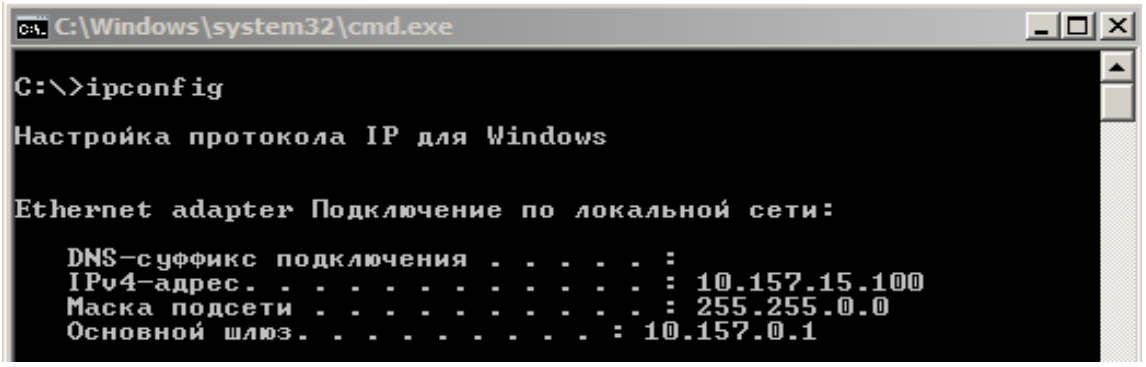

Рис. 1. Настройки протокола IP для операционной системы Windows

Утилита ping

Утилита ping (Packet Internet Groper) является одним из главных средств, используемых для отладки сетей, и служит для принудительного вызова ответа конкретного узла (отправляет пакеты на указанный адрес и анализирует параметры вернувшихся пакетов). 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. В Windows утилита ping имеется в комплекте поставки и представляет собой программу, запускаемую из командной строки (рис. 2).

Обратите внимание: некоторые серверы в целях безопасности могут не посылать эхо-ответы (например, www.microsoft.com).

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

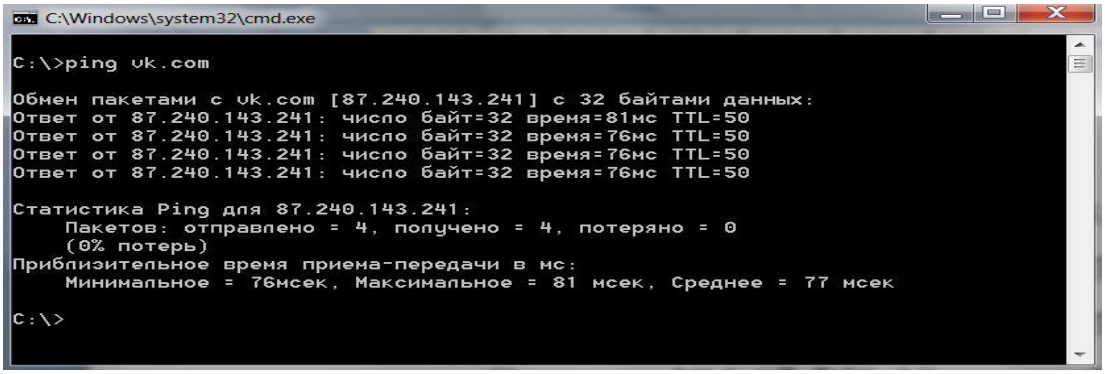

Рис. 2. Утилита ping - программа, запускаемая из командной строки

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). По умолчанию передается четыре запроса по 32 байта в каждом, после чего выводятся статистические данные по полученным пакетам.

Утилита tracert

Утилита tracert позволяет выявлять последовательность маршрутизаторов, через которые проходит IP-пакет на пути к пункту своего назначения и время задержки на каждом из них.

Формат команды: tracert имя_машины (имя_машины - может быть именем узла, DNS или IP-адресом компьютера). Выходная информация представляет собой список машин, начиная с первого шлюза и заканчивая пунктом назначения. Пакеты посылаются по три на каждый узел (рис. 3).

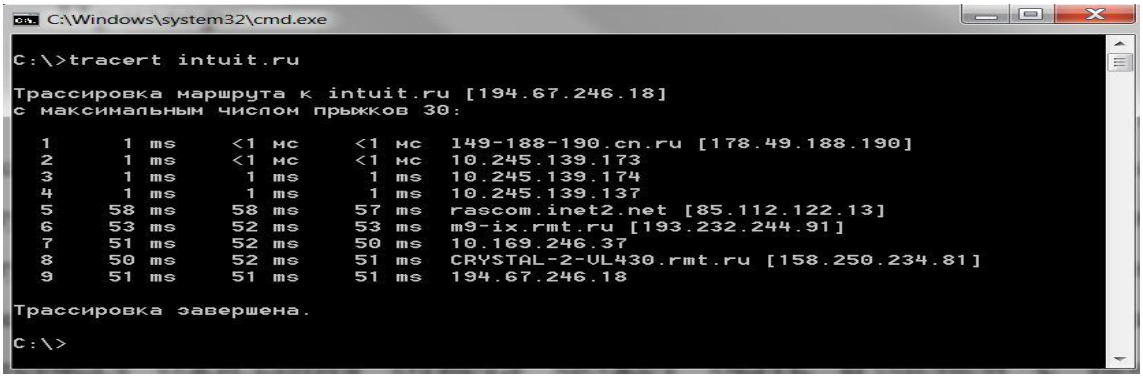

Рис. 3. Утилита tracert

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.

Сервис Whois

При регистрации доменных имен второго уровня обязательным условием является предоставление верных сведений о владельце этого домена: для юридических лиц - название организации, для физических лиц - ФИО и паспортных данных. Также обязательным является предоставление контактной информации. Часть этой информации становится свободно доступной для любого пользователя сети Интернет через сервис Whois (англ. who is - «кто такой?»). Основное его назначение - получение регистрационных данных о владельцах доменных имён и IP-адресов. Получить интересующую информацию о владельце домена можно через Whois-клиент ОС Windows, но проще всего отправить запрос можно через веб-форму on-line сервиса Whois, например – nic.ru/whois, whois-service.ru, sbup.com/whois.php (рис. 4).

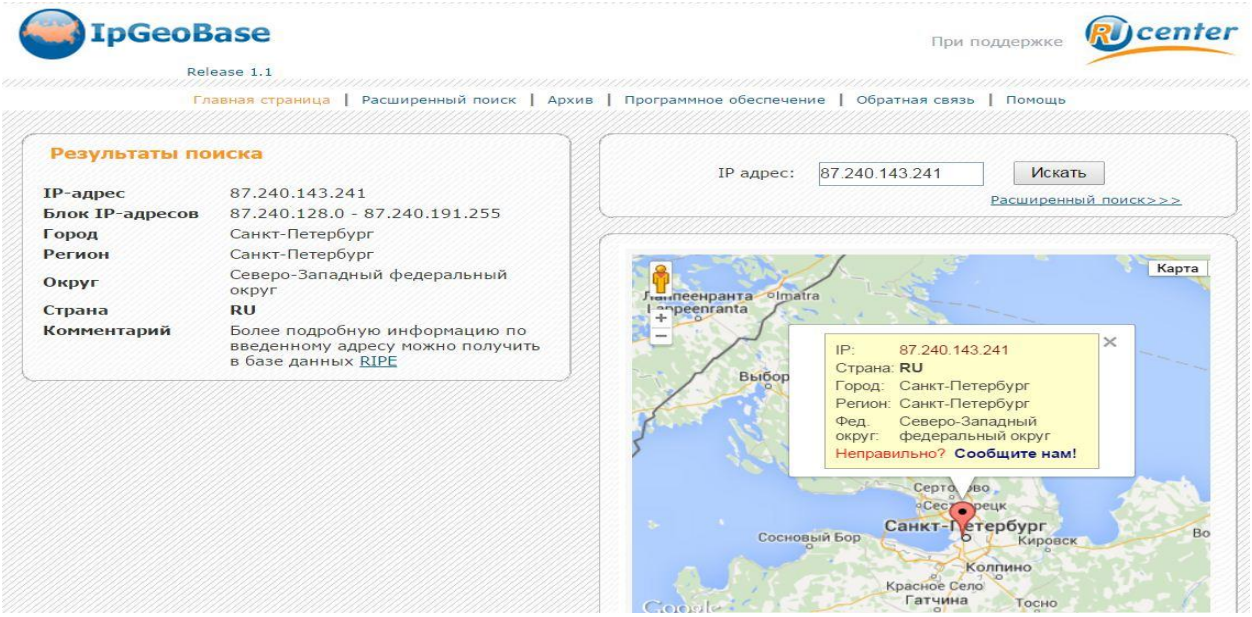

Рис. 4. Сервис Whois

(Информация о сервисах - http://yandex.ru/yandsearch?text=%D1%81%D0%B5%D1%80%D0%B2%D0%B8%D1%81%20whois&lr=65)

Задание на лабораторную работу

Оформите отчет по работе, опишите выполнение упражнений.

Упражнение 1. С помощью утилиты ipconfig определить IP адрес ПК.

Упражнение 2. С помощью утилиты ping проверить состояние связи с двумя любыми работоспособными узлами. Результат отразить для каждого из исследуемых узлов в виде таблицы:

a. IP адрес узла;

в. процент потерянных пакетов;

с. среднее время приема-передачи.

Упражнение 3. Произвести трассировку двух работоспособных узлов. Результаты отразить в таблице.

№ узла	время прохождения пакета №1	время прохождения пакета №2	время прохождения пакета №3	среднее время прохождения	IP-адрес маршрутизатора

Определить участок сети, который характеризуется наибольшей задержкой при пересылке пакетов. Для найденных маршрутизаторов с помощью сервиса Whois определить название организации, контактные данные (тел., e-mail) и др. (Выполнить на разных сервисах Whois) Полученную информацию указать в отчёте.