ЛАБОРАТОРНАЯ РАБОТА №1

СИСТЕМНЫЕ УТИЛИТЫ СЕТЕВОЙ ДИАГНОСТИКИ

1 Утилита ipconfig

Утилита ipconfig (IP configuration) предназначена для настройки протокола IP для операционной системы Windows. В данной лабораторной работе эта утилита будет использоваться только для получения информации о соединении по локальной сети. Для получения этой информации выполните «Пуск» → «Выполнить» → cmd и в командной строке введите:

```
ipconfig /all
```

В разделе «Адаптер Ethernet Подключение по локальной сети» для данной лабораторной будут необходимы поля «DHCP», «IP-адрес» и «DNS-серверы».

2 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 задержка, 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).

Таблица 1

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	Максимальное количество переходов (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).

Пример:

```
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=734мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=719мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=688мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=704мс TTL=231
Превышен интервал ожидания для запроса.
Ответ от 207.227.119.2: число байт=32 время=719мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=1015мс TTL=231
Превышен интервал ожидания для запроса.
Ответ от 207.227.119.2: число байт=32 время=703мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=688мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=782мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=688мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=688мс TTL=231
```

```
Ответ от 207.227.119.2: число байт=32 время=688мс TTL=231
Превышен интервал ожидания для запроса.
Ответ от 207.227.119.2: число байт=32 время=687мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=735мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=672мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=704мс TTL=231

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

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: …
```

3 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 узлом назначения.

Пример:

```
tracert peak.mountin.net

Трассировка маршрута к peak.mountin.net [207.227.119.2] с максимальным
числом прыжков 30:
```

№	Пакет 1	Пакет 2	Пакет 3	DNS-имя узла и (или) его IP-адрес
1	<10 мс	<10 мс	<10 мс	SLAVE [192.168.0.1]
2	<10 мс	<10 мс	<10 мс	gw.b10.tpu.edu.ru [195.208.164.2]
3	<10 мс	<10 мс	<10 мс	195.208.177.62
4	<10 мс	<10 мс	<10 мс	news.runnet.tomsk.ru [195.208.160.4]
5	<10 мс	<10 мс	16 ms	ra.cctpu.tomsk.su [195.208.161.34]
6	781 ms	563 ms	562 ms	spb-2-gw.runnet.ru [194.85.33.9]
7	547 ms	594 ms	578 ms	spb-gw.runnet.ru [194.85.36.30]
8	937 ms	563 ms	562 ms	20.201.atm0-201.ru-gw.run.net [193.232.80.105]
9	1125 ms	563 ms	547 ms	fi-gw.nordu.net [193.10.252.41]

№	Пакет 1	Пакет 2	Пакет 3	DNS-имя узла и (или) его IP-адрес
10	906 ms	1016 ms	578 ms	s-gw.nordu.net [193.10.68.41]
11	844 ms	828 ms	610 ms	dk-gw2.nordu.net [193.10.68.38]
12	578 ms	610 ms	578 ms	sl-gw10-cop-9-0.sprintlink.net [80.77.65.25]
13	610 ms	968 ms	594 ms	sl-bb20-cop-8-0.sprintlink.net [80.77.64.37]
14	641 ms	672 ms	656 ms	sl-bb21-msq-10-0.sprintlink.net [144.232.19.29]
15	671 ms	704 ms	687 ms	sl-bb21-nyc-10-3.sprintlink.net [144.232.9.106]
16	985 ms	703 ms	765 ms	sl-bb22-nyc-14-0.sprintlink.net [144.232.7.102]
17	719 ms	734 ms	688 ms	144.232.18.206
18	891 ms	703 ms	734 ms	p1-0.nycmny1-nbr1.bbnplanet.net [4.24.8.161]
19	719 ms	985 ms	703 ms	so-6-0-0.chcgil2-br2.bbnplanet.net [4.24.4.17]
20	688 ms	687 ms	703 ms	so-7-0-0.chcgil2-br1.bbnplanet.net [4.24.5.217]
21	719 ms	703 ms	672 ms	p1-0.chcgil2-cr9.bbnplanet.net [4.24.8.110]
22	687 ms	719 ms	687 ms	p2-0.nchicago2-cr2.bbnplanet.net [4.0.5.242]
23	781 ms	703 ms	672 ms	p8-0-0.nchicago2-core0.bbnplanet.net [4.0.6.2]
24	672 ms	703 ms	687 ms	fa0.wcnet.bbnplanet.net [207.112.240.102]
25	734 ms	687 ms	688 ms	core0-s1.rac.cyberlynk.net [209.100.155.22]
26	1188 ms	*	890 ms	peak.mountin.net [207.227.119.2]

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.

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.

4 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 паспортные данные. Также обязательным является предоставление контактной информации. Часть этой информации становится свободно доступной для любого пользователя сети Интернет через сервис Whois. Получить интересующую информацию о владельце домена можно через Whois-клиент, например, в Unix это консольная команда whois, в ОС Windows – это приложение SmartWhois. Но проще всего отправить запрос можно через веб-форму on-line сервиса Whois, например через форму на странице http://www.nic.ru/whois/ или http://who.is

ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

Отчёт по лабораторной работе необходимо оформить в OpenOffice Word, либо в MS Word. В отчете должны быть включены следующие пункты:

1. титульный лист;
2. цель работы;
3. ход работы;
   3.1. использование утилиты ipconfig;
   3.2. проверка состояния связи до узлов;
   3.3. трассировка работоспособных узлов;
4. анализ результатов работы;
5. выводы.

Файл с отчетом необходимо назвать в следующем формате: "НОМЕР_ЛАБОРАТОРНОЙ ГРУППА ФИО", например: "1 8820 Иванов А.С.". Файл с отчетом необходимо, необходимо загрузить в систему Moodle и скопировать в папку:

```
\\112b-vs\public\igsavenko\[номер группы]\completed
```

Поместить изображение текущего окна в отчёт можно следующим способом: нажмите ALT+PrintScreen, перейдите в редактор и нажмите CTRL+V. Скопировать текст из окна командной строки можно следующим образом: выделите необходимый текст с помощью мыши и нажмите на выделенном участке правой кнопкой мыши, затем перейдите в текстовый редактор и нажмите Ctrl+V. Список адресов узлов для всех вариантов приведён ниже.

Задание 1

С помощью утилиты ipconfig определить IP адрес и физический адрес основного сетевого интерфейса компьютера, IP адрес шлюза, IP адреса DNS-серверов и используется ли DHCP. Результаты представить **в виде таблицы** и разместить после таблицы изображение окна.

Таблица 2

Результат выполнения задания 1

IP-адрес (десятичный вид)	
IP-адрес (двоичный вид)	
Адрес сети (десятичный вид)	
Длина маски подсети (количество битов)	

Физический адрес	
IP-адрес шлюза (десятичный вид)	
IP-адреса DNS-серверов (десятичный вид)	
Используется ли DHCP (да или нет)	

Задание 2

Проверить состояние связи с любыми двумя узлами (работоспособными) в соответствии с вариантом задания. Число отправляемых запросов должно составлять не менее 20. В качестве результата отразить для каждого из исследуемых узлов в виде таблицы и разместить после таблицы изображение окна:

Таблица 3

Результат выполнения задания 2

Имя узла	
IP адрес узла	
Имя узла, полученное по IP-адресу узла	
Класс сети, к которой принадлежит данный узел	
Процент потерянных пакетов	
Среднее время приема-передачи	
Количество маршрутизаторов (с учетом шлюза) до опрашиваемого узла	

В отчёте необходимо пояснить, как были определены значения.

Задание 3

Произвести трассировку двух работоспособных узлов в соответствии с вариантом задания. Результаты запротоколировать в таблице.

Таблица 4

Результат выполнения задания 3.1

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

Если значения времени прохождения трёх пакетов отличаются более, чем на 10 мс, либо если есть потери пакетов, то для соответствующих узлов среднее время прохождения необходимо определять с помо-

щью утилиты ping по 20 пакетам. По результатам таблицы в отчете привести график изменения среднего времени прохождения пакета. В отчёте привести одну копию окна с результатами команды tracert. Для каждого опрашиваемого узла определить участок сети между двумя соседними маршрутизаторами, который характеризуется наибольшей задержкой при пересылке пакетов. По DNS-именам маршрутизаторов попробуйте определить их географическое расположение и сделайте выводы о причинах задержек. Для найденных маршрутизаторов с помощью сервиса Whois определить название организации и контактные данные (тел., email) и представить в виде таблицы.

Таблица 5

Результат выполнения задания 3.2

	DNS-имя узла	DNS-имя узла	DNS-имя узла	DNS-имя узла
Название организации				
Контактный телефон				
Контактный email				
Имя администратора				

Полученную информацию необходимо указать в отчёте.

ВАРИАТЫ ЗАДАНИЙ

1	www.alibaba.com	**2**	www.ecplaza.net	**3**	www.ecvv.com
	www.tradekey.com		www.dhgate.com		www.diytrade.com
	www.made-in-china.com		www.ec21.com		www.importers.com
4	www.busytrade.com	**5**	www.dealextreme.com	**6**	www.modashop.net
	www.helpmart.ru		www.chinawebshop.ru		www.made-in-china.com
	www.chinavasion.com		www.lightinthebox.com		www.webstorelist.com
7	www.imobile.com.cn	**8**	www.vtcom.lv	**9**	www.taobao.com
	www.vancl.com		www.happigo.com		www.shop.com
	www.paipai.com		www.buynow.com.cn		www.hktdc.com
10	www.aliexpress.com	**11**	www.tias.com	**12**	www.tradekey.com
	www.china-direct-buy.com		www.chinatronic.com		www.ecvv.com
	www.chinabuye.com		www.amazon.cn		www.importers.com
13	www.ecplaza.net	14	www.made-in-china.com	**15**	www.ec21.com
	www.dealextreme.com		www.imobile.com.cn		www.dhgate.com
	www.made-in-china.com		www.helpmart.ru		www.chinawebshop.ru
16	www.diytrade.com	**17**	www.lightinthebox.com	**18**	www.alibaba.com
	www.modashop.net		www.vancl.com		www.made-in-china.com
	www.busytrade.com		www.webstorelist.com		www.ecvv.com
19	www.tradekey.com	**20**	www.importers.com		
	www.diytrade.com		www.helpmart.ru		
	www.chinavasion.com		www.chinawebshop.ru		