ЛАБОРАТОРНАЯ РАБОТА № 6 (1)

"Сетевые утилиты ipconfig, arp, ping, tracert, nslookup”

1. ЦЕЛЬ РАБОТЫ

Ознакомление с сетевыми утилитами ipconfig, arp, ping, tracert, nslookup.

2. ВВОДНЫЕ ПОЛОЖЕНИЯ.

Для работы компьютера в сети TCP/IP он должен быть надлежащим образом сконфигурирован. На его сетевых интерфейсах должны быть прописаны IP-адреса и маски, должны быть заданы адреса шлюза, серверов DNS и другие параметры. Для задания и просмотра этих параметров, а также для определения некоторых параметров других компьютеров в сети используются утилиты, рассматриваемые в данной работе.

2.1 Типы адресов в сетях TCP/IP : физический (MAC-адрес), сетевой (IP-адрес) и символьный (DNS-имя).

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

- Физический адрес - 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.
- Сетевой адрес - 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 IP-адресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.
- Символьный идентификатор-имя, например, spbstu.ru. Символьное имя более понятно для человека, более легко запоминается. Символьное имя назначается администратором сети и состоит из нескольких частей, разделяемых точкой, например, имени машины, имени организации, имени домена. Соответствие символьных имен и IP-адресов поддерживается службой доменных имен (DNS).

Если не вдаваться в подробности, то существует сеть DNS серверов, на которых хранится вся необходимая информация об IP-адресах и соответствующих им доменах. Время от времени они обмениваются между собой информацией, чтобы база данных была полной и актуальной. Когда компьютеру нужно обратиться к какому-либо сайту по символьному имени, он запрашивает его IP-адрес у DNS-сервера, а затем сохраняет его в локальном кэше. DNS-

запросы могут отсылаться не только автоматически, их может формировать и отправлять утилита nslookup.

2.2 Команда ipconfig

Данная команда предназначена для настройки IP-протокола и вывода информации об установленных параметрах. В лабораторной работе команда используется только для вывода информации о настройке IP протокола. При вызове команды **ipconfig** без дополнительных ключей выводится только IP-адрес, маска подсети и основной шлюз для каждого сетевого адаптера.

Для ознакомления с синтаксисом и возможностями команды следует набрать
ipconfig /? или ipconfig -? .
Синтаксис:
ipconfig /? Отображает справочное сообщение
ipconfig /all Вывод полной конфигурации TCP/IP для всех адаптеров.
ipconfig Выводит только IP-адреса, маску подсети и основной шлюз для каждого адаптера.

Команда **ipconfig** отображает параметры только подключенных к сети сетевых адаптеров. Для проводных сетей соответствующие разъемы компьютера должны быть подключены кабелем к работающим сетевым устройствам.

2.3. Команда ping

ping (расшифровывается как **p**acket **in**ternet **g**roper – *отправитель пакетов интернет*) – это служебная компьютерная программа, предназначенная для проверки соединений в сетях на основе TCP/IP. Она отправляет запросы Echo-Request протокола ICMP указанному узлу сети и фиксирует поступающие ответы (ICMP Echo-Reply). Время между отправкой запроса и получением ответа (RTT, от англ. Round Trip Time) позволяет определять двусторонние задержки по маршруту и частоту потери пакетов, то есть косвенно определять загруженность каналов передачи данных и промежуточных устройств.
Иногда пингом называют время, затраченное на передачу пакета информации в компьютерных сетях от клиента к серверу и обратно от сервера к клиенту, оно измеряется в миллисекундах.
Время пинга связано со скоростью соединения и загруженностью каналов на всём протяжении от клиента к серверу. Полное отсутствие ICMP-ответов может также означать, что удалённый узел (или какой-либо из промежуточных маршрутизаторов) блокирует ICMP Echo-Reply или игнорирует ICMP Echo-Request.
Программа ping является одним из основных диагностических средств в сетях TCP/IP и входит в поставку всех современных сетевых операционных систем.
Синтаксис:
ping –t Повторяет запросы к удаленному компьютеру, пока программа не будет остановлена. Для вывода статистики и продолжения – Ctrl+Break. Прекращение команды – Ctrl+C
ping –a Определение адресов по именам узлов
ping -n число Число отправляемых запросов (по умолчанию – 4)
ping -l длина Задает размер буфера отправки. По умолчанию - 32 байта, максимум - 65527.
ping –f Отправляет пакеты с флагом запрета фрагментации (Do not Fragment). Пакеты не будут разрываться при прохождении шлюзов на своем маршруте.
ping -i ttl Устанавливает поле времени жизни пакетов TTL (Time To Live).
ping -v тип Устанавливает поле типа службы (Type Of Service) пакетов.
ping -r счетчик Запись маршрута для указанного числа переходов
ping -s число Задает число ретрансляций на маршруте, где будет делаться отметка времени.

ping -j список_комп Направляет пакеты по маршруту, задаваемому параметром список_комп. Компьютеры в списке могут быть разделены промежуточными шлюзами (свободная маршрутизация). Максимальное количество, разрешаемое протоколом IP, равно 9.
ping -k список_комп Направляет пакеты по маршруту, задаваемому параметром список_комп. Компьютеры в списке не могут быть разделены промежуточными шлюзами (ограниченная маршрутизация) Максимальное количество, разрешаемое протоколом IP, равно 9.
ping -w интервал Указывает промежуток времени ожидания (в миллисекундах).

2.4. Утилита arp

Команда arp позволяет редактировать и просматривать arp-таблицы компьютера, отражающие соответствие IP-адресов и MAC-адресов узлов локальной сети. Таблицы заполняются либо администратором вручную (статическая запись), либо автоматически с помощью протокола ARP -Address Resolution Protocol (динамическая запись).

arp –a [inet_addr] Отображает текущие ARP-записи, опрашивая текущие данные протокола. Если задан inet_addr, то будут отображены IP и физический адреса только для заданного компьютера. Если более одного сетевого интерфейса используют ARP, то будут отображаться записи для каждой таблицы.
arp –N if_addr Отображает ARP-записи для заданного в if_addr сетевого интерфейса.
arp –s inet_addr eth_addr [if_addr] Добавляет узел и связывает IP адрес inet_addr с физическим адресом eth_addr. Физический адрес задается 6 байтами (в шестнадцатеричном виде), разделенных дефисом. Эта связь является постоянной (статической). Если параметр if_addr задан - он определяет IP-адрес интерфейса, чья таблица преобразования адресов должна измениться. Если не задан, - будет использован первый доступный интерфейс.

Для того, чтобы в таблице появилась запись с адресами узла N, необходимо послать IP-пакет этому узлу (например, ping). Динамическая запись в таблице исчезает через 3-4 минуты после окончания сеанса связи с данным узлом. В последних версиях ОС Windows, время жизни ARP-записи может быть изменено.

Команда tracert

Программа Tracert позволяет посмотреть маршрут, по которому двигаются IP-дейтаграммы от одного хоста к другому. В ее работе используются стандартные функции протоколов ICMP и IP. Для понимания работы программы следует вспомнить порядок обработки поля TTL (время жизни пакета) в заголовке IP-дейтаграммы.
Каждый маршрутизатор, обрабатывающий дейтаграмму, уменьшает значение поля TTL в ее заголовке на единицу. При получении дейтаграммы с TTL равным 1, маршрутизатор уничтожает ее и посылает хосту, который ее отправил, ICMP-сообщение "время истекло" (time exceeded). При этом дейтаграмма, содержащая это ICMP-сообщение, имеет в качестве адреса источника IP-адрес маршрутизатора, удалившего дейтаграмму.
Это и используется в программе Tracert. На хост назначения отправляется IP-дейтаграмма (ping-запрос), в которой поле TTL, установлено в единицу. Первый маршрутизатор на пути дейтаграммы, уничтожает ее (так как TTL равно 1) и отправляет ICMP-сообщение об истечении времени (time exceeded). Таким образом, определяется первый маршрутизатор в маршруте. Затем Tracert отправляет дейтаграмму с полем TTL равным 2, что позволяет получить IP-адрес второго маршрутизатора. Аналогичные действия продолжаются до тех пор, пока дейтаграмма не достигнет хоста назначения. Если дейтаграмма прибыла именно на хост назначения, он не уничтожит ее и не сгенерирует ICMP-сообщение об истечении времени, так как дейтаграмма достигла своего конечного назначения. Поскольку дейтаграмма несет в себе эхо-запрос, узел назначения отвечает обычным эхо-ответом. Это свидетельствует о доставке

дейтаграммы в пункт назначения и генерация эхо запросов прекращается. Пример вывода программы показан на рис 1.

```
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\я>tracert yundex.ru

Трассировка маршрута к yundex.ru [109.206.181.75]
с максимальным числом прыжков 30:

  1    <1 мс    <1 мс    <1 мс  rtc-sw1.neva.ru [195.208.112.30]
  2    <1 мс    <1 мс    <1 мс  rtc-gw.neva.ru [194.85.4.13]
  3    <1 мс    <1 мс    <1 мс  odu-gw3.neva.ru [194.85.4.26]
  4    <1 мс    <1 мс    <1 мс  kt12-1-gw.spb.runnet.ru [194.190.255.229]
  5     7 ms     7 ms     7 ms  tv11-2-gw.msk.runnet.ru [194.85.40.137]
  6     *        *        *     Превышен интервал ожидания для запроса.
  7     8 ms     8 ms     8 ms  ae0-929.msk-m9-1-gw.runnet.ru [194.85.40.111]
  8    20 ms    20 ms    20 ms  tun4.sth-tug-1-gw.runnet.ru [194.85.40.131]
  9    20 ms    20 ms    44 ms  se-tug.nordu.net [109.105.102.45]
 10    34 ms    37 ms    34 ms  dk-uni.nordu.net [109.105.97.10]
 11    54 ms    53 ms    54 ms  uk-hex.nordu.net [109.105.97.127]
 12     *        *        *     Превышен интервал ожидания для запроса.
 13    64 ms    79 ms    67 ms  109.206.160.255.serverel.net [109.206.160.255]
 14    51 ms    51 ms    51 ms  75.181.serverel.net [109.206.181.75]

Трассировка завершена.
```

Рис. 1. Вывод программы TRACERT

Первая строка, без номера содержит имя и IP адрес пункта назначения и указывает на то, что величина TTL не может быть больше 30.

Следующие строки вывода начинаются с распечатки значения TTL (1, 2, 3 и т.д.) и содержат имя (IP-адрес) хоста или маршрутизатора и время возврата ICMP-сообщения.

Для каждого значения TTL отправляется 3 дейтаграммы. Для каждого возвращенного ICMP-сообщения рассчитывается и печатается время возврата.

Если ответ на дейтаграмму не получен в течение пяти секунд, печатается звездочка, после чего отправляется следующая дейтаграмма.

Команда nslookup

Утилита nslookup формирует запросы к DNS-серверу и позволяет ознакомиться с функционированием службы доменных имен. Утилита, имеет несколько подкоманд и параметров, позволяющих просматривать различные записи на DNS серверах. На начальной стадии ознакомимся с простейшими запросами.

Для определения IP-адреса узла по его имени (например, www.rtc.ru) необходимо выполнить команду nslookup www.rtc.ru .

Для определения имени компьютера по его IP-адресу, в качестве параметра следует набрать IP-адрес: nslookup 195.208.112.25.

Для определения почтового сервера домена (например, domain.ru) следует использовать команду nslookup -type=mx domain.ru

Программа работы

1. Убедиться, что компьютер подключен к проводной сети. (Кабель подключен).

2. Включить компьютер.

3. Перейти в командный режим (в строке поиска набрать команду cmd). Дальнейшие действия выполнять в появившемся окне терминала. Для получения справки по команде следует набрать команду с ключом -?, например, ipconfig -? или ping -?.

4. **Команда ipconfig**. Выполнить команду ipconfig -?. Ознакомиться с синтаксисом и возможностями команды ipconfig.

5. С помощью команды ipconfig определить установленные в компьютере значения параметров IP-протокола и занести их в отчет.

6. Выполнить команду ipconfig при отключенном сетевом кабеле. Занести результат в отчете.

7. **Утилита ping**. Ознакомиться с синтаксисом и возможностями утилиты ping.

8. Выполнить команду ping к узлу spbstu.ru.

9. Выполнить команду ping, указав число запросов, длину пакета и адрес узла в соответствии с вариантом. Занести результат в отчет и пояснить.

10. **Команда arp**. Ознакомиться с синтаксисом и возможностями команды arp.

11. Выполнить команду **arp –a.** Записать результат в отчет. Пояснить результат.

12. Выполнить команду **ping** *адрес шлюза,* затем сразу команду **arp –a.** Записать результат в отчет.

13. Подождать 5 минут и повторить команду **arp –a.** Пояснить результат.

14. С помощью команд ping и arp определить MAC- и IP-адреса двух компьютеров из локальной сети в соответствии с вариантом. Записать используемые команды и результаты в отчет.

15. **Утилита tracert**. Ознакомиться с синтаксисом и возможностями утилиты tracert.

16. С помощью утилиты tracert определить маршрут прохождения пакетов к WEB-серверу в соответствии с вариантом. Пояснить результат.

17. Повторить п.16, используя утилиту tracert с опцией -d. Пояснить результат.

18. **Команда nslookup**. Ознакомиться с назначением, синтаксисом и возможностями команды.

19. С помощью команды nslookup определить:

a) IP-адрес компьютера в учебном классе в соответствии с заданием.

b) IP-адрес WEB-сервера в сети Интернет в соответствии с заданием.

c) Имя компьютера в сети Интернет с IP = 94.100.180.n, где n - номер варианта.

В отчете указать: - Номер рабочего места
- Номер варианта
Для каждой команды привести:
- Назначение команды
- Распечатку выполнения команды по своему варианту.
Выводы.