Лабораторная работа № 5

Изучение сетевых утилит командной строки Windows

**Цель работы:** изучить утилиты командной строки Windows, предназначенные для контроля и мониторинга сетей, построенных на базе стека протоколов TCP/IP.

**Оборудование:** персональный компьютер, Windows с установленной сетью IP

Сетевая операционная система Windows содержит набор утилит, полезных при диагностике сети. Основными задачами этих программ является:

1. Определение работоспособности сети
2. Определение параметров и характеристик сети
3. В случае неправильного функционирования сети – локализация службы или сервиса, вызывающих неисправность.

Главными параметрами сетевых подключений являются их канальные и сетевые адреса и параметры, влияющие на работу сетевого уровня.

Единственным параметром канального уровня, который может быть просмотрен, являются МАС адреса сетевых адаптеров. Для их просмотра можно воспользоваться утилитой IPCONFIG, которая покажет МАС адреса для каждого адаптера, или, для последних версий Windows, с помощью [ROUTE PRINT](file:///%5C%5CAsubru%5CWebAsu%5C%D0%A3%D1%87%D0%B5%D0%B1%D0%BD%D0%BE-%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5%20%D0%BC%D0%B0%D1%82%D0%B5%D1%80%D0%B8%D0%B0%D0%BB%D1%8B%5C%D0%94%D0%B8%D1%81%D1%86%D0%B8%D0%BF%D0%BB%D0%B8%D0%BD%D1%8B%20%D0%BA%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D1%8B%5C%D0%A3%D0%9C%D0%9A_2018_%D0%A0%D0%91%5C_%D0%A1%D0%B5%D1%82%D0%B8%20%D0%AD%D0%92%D0%9C%20%D0%B8%20%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D0%BD%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%B9%5CAPOS-2006-11-%D0%9B%D0%B0%D0%B1%D0%A0%D0%B0%D0%B1%5Ccontent%5Clab4.htm#z05). Для изменения МАС адресов следует воспользоваться драйверами соответствующих сетевых адаптеров, если, конечно, они допускают подобную операцию.

# IPCONFIG

Параметры IP просматривают с помощью утилиты IPCONFIG.

Использование:

ipconfig [/? | /all | /release [адаптер] | /renew [адаптер] |

 /flushdns | /displaydns /registerdns |

 /showclassid адаптер |

 /setclassid адаптер [устанавливаемый\_код\_класса\_dhcp] ]

Параметры:

адаптер – полное имя или имя, содержащие подстановочные знаки "\*" и "?" (\* – любое количество знаков, ? – один любой знак). См. примеры

ключи:

/? – отобразить это справочное сообщение.

/all – отобразить полную информацию о настройке параметров.

/release – освободить IP–адрес для указанного адаптера.

/renew – обновить IP–адрес для указанного адаптера.

/flushdns– очистить кэш разрешений DNS.

/registerdns – обновить все DHCP–аренды и перерегистрировать DNS–имена

/displaydns – отобразить содержимое кэша разрешений DNS.

/showclassid – отобразить все допустимые для этого адаптера коды (IDs)
DHCP–классов.

/setclassid – изменить код (ID) DHCP–класса.

По умолчанию отображается только IP–адрес, маска подсети и стандартный шлюз для каждого подключенного адаптера, для которого выполнена привязка с TCP/IP.

Для ключей /release и /renew, если не указано имя адаптера, то будет освобожден или обновлен IP–адрес, выданный для всех адаптеров, для которых существуют привязки с TCP/IP.

Для ключа /setclassid, если не указан код класса (ID), то существующий код класса будет удален.

Примеры:

ipconfig – отображает краткую информацию.

Настройка протокола IP для Windows

Подключение по локальной сети 2 – Ethernet адаптер:

DNS–суффикс этого подключения . . :

IP–адрес автонастройки. . . . . . : 169.254.236.138

Маска подсети . . . . . . . . . . : 255.255.0.0

Основной шлюз . . . . . . . . . . :

Main – PPP адаптер:

DNS–суффикс этого подключения . . :

IP–адрес. . . . . . . . . . . . : 82.209.222.238

Маска подсети . . . . . . . . . . : 255.255.255.255

Основной шлюз . . . . . . . . . . : 82.209.222.238

ipconfig /all – отображает полную информацию.

Настройка протокола IP для Windows

Имя компьютера. . . . . . . . . : home

Основной DNS–суффикс. . . . . . :

Тип узла. . . . . . . . . . . . . : неизвестный

IP–маршрутизация включена . . . . : нет

WINS–прокси включен . . . . . . . : нет

Подключение по локальной сети 2 – Ethernet адаптер:

DNS–суффикс этого подключения . . :

Описание. . . . . . . . . . . . : Realtek RTL8029(AS)–based

Ethernet адаптер (Универсальный) #2

Физический адрес. . . . . . . . . : 52–54–05–E2–77–88

Dhcp включен. . . . . . . . . . . : да

Автонастройка включена. . . . . : да

IP–адрес автонастройки. . . . . . : 169.254.236.138

Маска подсети . . . . . . . . . . : 255.255.0.0

Основной шлюз . . . . . . . . . . :

Main – PPP адаптер:

DNS–суффикс этого подключения . . :

Описание. . . . . . . . . . . . : WAN (PPP/SLIP) Interface

Физический адрес. . . . . . . . . : 00–53–45–00–00–00

Dhcp включен. . . . . . . . . . . : нет

IP–адрес. . . . . . . . . . . . : 82.209.222.238

Маска подсети . . . . . . . . . . : 255.255.255.255

Основной шлюз . . . . . . . . . . : 82.209.222.238

DNS–серверы . . . . . . . . . . . : 194.158.206.206

193.232.248.2

NetBIOS через TCP/IP. . . . . . . : отключен

ipconfig /renew– обновляет сведения для всех адаптеров.

ipconfig /renew EL\* – обновляет сведения для адаптеров, начинающихся с EL

ipconfig /release \*ELINK?21\* – освобождает IP–адреса для всех адаптеров, имена которых удовлетворяют запросу: ELINK–21 или myELELINKi21adapter и т.п.

# ARP

Соответствие МАС и IP адресов производится службой ARP. Для работы с этой службой имеется утилита ARP.

Служба ARP работает с таблицей ARP, состоящей из двух колонок: IP адрес и MAC адрес (физический адрес). При необходимости отправить пакет по какому–то IP адресу в таблице ARP находят соответствующий ему MAC адрес и на канальном уровне передают информацию. Если передача производится через шлюз, то в таблице ищут MAC адрес шлюза и передают пакет с IP адресом получателя и MAC адресом шлюза.

Если в таблице ARP нет нужного IP адреса, то посылается запрос – специальный пакет ARP по IP адресу получателя с широковещательным MAC адресом. Получатель, получив такой пакет, посылает ответ от своего IP адреса и своего MAC адреса. Отправитель, получив этот ответ, добавляет запись в ARP таблицу.

Таблица ARP динамическая, поэтому запись в ней «живет» некоторое время, после которого удаляется, но имеется возможность создавать в таблице и постоянные (статические) записи.

Отображение и изменение таблиц преобразования IP–адресов в физические, используемые протоколом разрешения адресов (ARP).

Использование:

ARP –s inet\_addr eth\_addr [if\_addr]

ARP –d inet\_addr [if\_addr]

ARP –a [inet\_addr] [–N if\_addr]

Параметры:

–a – отображает текущие ARP–записи, опрашивая текущие данные протокола. Если задан inet\_addr, то будут отображены IP и и физический адреса только для заданного компьютера. Если более одного сетевого интерфейса используют ARP, то будут отображаться записи для каждой таблицы.

–g – то же, что и ключ –a.

inet\_addr – определяет IP–адрес.

–N if\_addr – отображает ARP–записи для заданного в if\_addr сетевого интерфейса.

–d – удаляет узел, задаваемый inet\_addr. inet\_addr может содержать символ шаблона \* для удаления всех узлов.

–s – добавляет узел и связывает internet адрес inet\_addr с физическим адресом eth\_addr. Физический адрес задается 6 байтами (в шестнадцатеричном виде), разделенных дефисом. Эта связь является постоянной.

eth\_addr – определяет физический адрес.

if\_addr – если параметр задан – он определяет интернет адрес интерфейса, чья таблица преобразования адресов должна измениться. Eсли не задан – будет использован первый доступный интерфейс.

Пример:

 arp –s 157.55.85.212 00–aa–00–62–c6–09 – добавляет статическую запись.

 arp –a – выводит ARP–таблицу.

# Протокол ICMP

Для мониторинга и управления сетями передачи данных разработан и используется протокол ICMP. На его базе можно:

1. Проверить доступность адресов сети
2. Определить маршрут
3. Определить время достижения пакетами узлов сети.

Решается это посылкой специальных пакетов.

Опции маршрутизации и временных меток являются весьма интересными, так как они обеспечивают способ наблюдения или управления тем, как межсетевые шлюзы маршрутизируют дейтаграммы.

Опция запись маршрута позволяет источнику создать пустой список IP–адресов и заставить каждый шлюз, обрабатывающий дейтаграмму, добавлять свой IP–адрес к этому списку. Всякий раз, когда машина обрабатывает дейтаграмму, имеющую опцию записи маршрута, она добавляет свой адрес к списку записи маршрута (в опции должно быть выделено достаточно места исходным отправителем для того, чтобы поместились все нужные элементы).

При прибытии дейтаграммы машина–получатель должна выделить и обработать список IP–адресов.

Если получатель обрабатывает дейтаграмму обычным образом, он будет игнорировать записанный путь.

Отметим, что отправитель должен разрешить наличие опции записи маршрута, а получатель должен быть согласен обработать полученный список; сама по себе машина не получит автоматически информацию о пройденном пути автоматически, если она включит опцию записи маршрута.

Опция временных меток работает аналогично опции записи маршрута в том отношении, что опция временных меток содержит вначале пустой список, а каждый шлюз на всем протяжении пути от источника к назначению заполняет элемент в этом списке.

Каждый элемент в списке состоит из двух 32–битных частей: IP–адреса шлюза, заполнившего этот элемент, и 32–битового целого числа – временной метки.

Временные метки определяют время и дату, когда шлюз обрабатывал дейтаграмму, и выражаются в миллисекундах после полуночи по Гринвичу. Если стандартное представление времени невозможно, шлюз может использовать любое представление локального времени.

# PING

Для определения достижимости заданного адреса используется утилита PING

Принцип работы: посылает адресату пакет заданного размера, который при приеме получателем посылается обратно. Программа проверяет и показывает время между отправкой и приемом пакета. Это позволяет оценить возможность доставки пакета на заданный адрес и, оценив скорость передачи, определить среднюю пропускную способность сети по следующей формуле:



Использование:

ping [–t] [–a] [–n число] [–l размер] [–f] [–i TTL] [–v TOS] [–r число] [–s число] [[–j список Узлов] | [–k список Узлов]] [–w таймаут] конечноеИмя

Параметры:

–t – отправка пакетов на указанный узел до команды прерывания. Для вывода статистики и продолжения нажмите <Ctrl>+<Break>, для прекращения – <Ctrl>+<C>.

–a – определение адресов по именам узлов.

–n число – число отправляемых запросов.

–l размер – размер буфера отправки.

–f – установка флага, запрещающего фрагментацию пакета.

–i TTL – задание срока жизни пакета (поле "Time To Live").

–v TOS – задание типа службы (поле "Type Of Service").

–r число – запись маршрута для указанного числа переходов.

–s число – штамп времени для указанного числа переходов.

–j список Узлов – свободный выбор маршрута по списку узлов.

–k список Узлов – жесткий выбор маршрута по списку узлов.

–w таймаут – таймаут каждого ответа в миллисекундах.

Примеры:

#### ping mogilev.by

Обмен пакетами с mogilev.by [194.158.206.206] по 32 байт:

Ответ от 194.158.206.206: число байт=32 время=173мс TTL=62

Ответ от 194.158.206.206: число байт=32 время=173мс TTL=62

Ответ от 194.158.206.206: число байт=32 время=172мс TTL=62

Ответ от 194.158.206.206: число байт=32 время=160мс TTL=62

Статистика Ping для 194.158.206.206:

Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),

Приблизительное время приема–передачи в мс:

Минимальное = 160мсек, Максимальное = 173 мсек, Среднее = 169 мсек

#### ping 194.158.206.206

Обмен пакетами с 194.158.206.206 по 32 байт:

Ответ от 194.158.206.206: число байт=32 время=141мс TTL=62

Ответ от 194.158.206.206: число байт=32 время=134мс TTL=62

Ответ от 194.158.206.206: число байт=32 время=133мс TTL=62

Ответ от 194.158.206.206: число байт=32 время=132мс TTL=62

Статистика Ping для 194.158.206.206:

Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),

Приблизительное время приема–передачи в мс:

Минимальное = 132мсек, Максимальное = 141 мсек, Среднее = 135 мсек

Следует отметить, что, изменив размер посылаемых пакетов, можно оценить пропускную способность сети.

# TRACERT

Для оценки маршрута прохождения пакетов используют утилиту TRACERT (trace route)

В отличие от PING на пробные пакеты постоянного размера отвечает каждый узел, через который этот пакет проходит. Программа измеряет и показывает время между отправкой пакета и получением ответа.

Использование:

tracert [–d] [–h максЧисло] [–j списокУзлов] [–w интервал] имя

Параметры:

–d – без разрешения в имена узлов.

–h максЧисло – максимальное число прыжков при поиске узла.

–j списокУзлов – свободный выбор маршрута по списку узлов.

–w интервал – интервал ожидания каждого ответа в миллисекундах.

Примеры:

#### tracert www.lycos.com

Трассировка маршрута к mia–search.mia.lycos.com [209.202.248.101]

с максимальным числом прыжков 30:

1 136 ms 149 ms 149 ms194.158.206.83

2 136 ms 209 ms 139 ms194.158.206.197

3 164 ms 149 ms 149 ms193.232.249.18

4 132 ms 149 ms 219 ms193.232.248.128

5 160 ms 149 ms 169 ms80.77.105.197

6 158 ms 149 ms 149 mssl–bb21–sto–8–0.sprintlink.net [80.77.96.41]

7 185 ms 159 ms 189 mssl–bb21–cop–12–0.sprintlink.net

[213.206.129.33]

8 163 ms 159 ms 189 mssl–bb20–cop–15–0.sprintlink.net [80.77.64.33]

9 270 ms 269 ms 229 mssl–bb21–msq–10–0.sprintlink.net

[144.232.19.29]

 10 257 ms 249 ms 259 mssl–bb20–msq–15–0.sprintlink.net

[144.232.9.109]

 11 235 ms 249 ms 249 mssl–bb25–nyc–6–0.sprintlink.net

[144.232.20.75]

 12 232 ms 239 ms 252 mssl–bb21–nyc–15–0.sprintlink.net

[144.232.13.2]

 13 239 ms 239 ms 299 mssl–bb23–nyc–3–0.sprintlink.net

[144.232.7.109]

 14 246 ms 239 ms 339 mssl–gw31–nyc–0–0.sprintlink.net

 [144.232.13.32]

 15 244 ms 249 ms 259 mssl–tiws–2–0.sprintlink.net [144.232.230.2]

 16 296 ms 319 ms 279 msSo7–2–0–0–grtmiabr4.red.telefonica–

wholesale.net[213.140.38.254]

 17 296 ms 289 ms 299 msSo2–0–0–0–grtmiana2.red.telefonica–

wholesale.net[213.140.36.89]

 18 274 ms 289 ms 299 msteusa–7–3–0–0–grtmiana2.red.telefonica–

wholesale.net[213.140.39.50]

 19 271 ms 298 ms 299 ms66.119.71.166

 20 283 ms 319 ms 279 msmia–search.mia.lycos.com [209.202.248.101]

Трассировка завершена.

TRACERT позволяет обнаружить некоторые ошибки маршрутизации в сети. Такими ошибками являются отсутствие правила маршрутизации в каком либо шлюзе, или петля маршрутов по умолчанию.

Пример отсутствия правила на узле:

#### tracert 10.249.0.100

Трассировка маршрута к 10.249.0.100

с максимальным числом прыжков 30:

1 13 ms 14 ms 14 ms10.7.11.11

2 \* \* \*Сеть недоступна [10.7.11.11]

Трассировка завершена.

Пример петли маршрутизации:

#### tracert 10.250.0.100

Трассировка маршрута к 10.250.0.100

с максимальным числом прыжков 30:

1 13 ms 14 ms 14 ms10.7.11.11

2 18 ms 17 ms 17 ms10.7.10.11

3 19 ms 18 ms 24 ms10.7.11.11

4 28 ms 14 ms 19 ms10.7.10.11

5 23 ms 14 ms 22 ms10.7.11.11

6 19 ms 16 ms 33 ms10.7.10.11

…

Хорошо видно, что шлюз 10.7.11.11 посылает пакет на 10.7.10.11, а 10.7.11.11 на 10.7.10.11. Это возможно, если либо для сети, к которой принадлежит адрес 10.250.0.100 неправильно прописаны правила маршрутизации, либо неправильно прописана маршрутизация по умолчанию на одном или обоих узлах.

# NSLOOKUP

Имеется специальная служба, сопоставляющая доменные адреса Интернет с IP адресами – DNS (domain name service). Для проверки ее работоспособности используют утилиту NSLOOKUP. Для работы этой утилиты должен быть определен сервер DNS в параметрах IP компьютера. С его помощью и будет производиться распознавание имен.

Использование:

nslookup [–подкоманда ...] [{искомый\_компьютер| [–сервер]}]

Параметры:

–подкоманда ... – задает одну или несколько подкоманд nslookup как параметры командной строки.

искомый\_компьютер – ищет данные для параметра искомый\_компьютер, используя текущий, заданный по умолчанию сервер имен DNS, если никакого другого сервера не указано

–сервер – указывает, что данный сервер следует использовать в качестве сервера имен DNS. Если параметр –сервер не указан, используется сервер DNS, заданный по умолчанию.

–help|? – Выводит краткое описание подкоманд nslookup.

Пример:

#### nslookup

Default Server:mail.mogilev.by

Address:194.158.206.206

> lycos.com

Server:mail.mogilev.by

Address:194.158.206.206

Non–authoritative answer:

Name:lycos.com

Address:209.202.248.101

> hp.com

Server:mail.mogilev.by

Address:194.158.206.206

DNS request timed out.

timeout was 2 seconds.

Non–authoritative answer:

Name:hp.com

Addresses:192.6.234.8, 192.6.234.9, 192.6.234.10, 192.151.52.187

161.114.22.105

> bru.mogilev.by

Server:mail.mogilev.by

Address:194.158.206.206

Name:bru.mogilev.by

Address:82.209.221.110

> exit

# Задания для выполнения

1. Используя утилиту PING определить пропускную способность сети до адресов 10.7.0.120, 10.219.0.1, 10.239.1.1 и 10.7.15.15. Объясните разницу в результатах.
2. Используя утилиту TRACERT и таблицу маршрутизации шлюза (используйте файл «APOS–LR#04–router2», а точнее адреса шлюзов), постройте схему сети университета.
3. Передайте пакеты участникам сети напрямую и через шлюз. Объясните полученные записи в таблице ARP.
4. Определите IP адреса [www.microsoft.com](file:///%5C%5CAsubru%5CWebAsu%5C%D0%A3%D1%87%D0%B5%D0%B1%D0%BD%D0%BE-%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5%20%D0%BC%D0%B0%D1%82%D0%B5%D1%80%D0%B8%D0%B0%D0%BB%D1%8B%5C%D0%94%D0%B8%D1%81%D1%86%D0%B8%D0%BF%D0%BB%D0%B8%D0%BD%D1%8B%20%D0%BA%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D1%8B%5C%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D1%8B%20%D0%B8%20%D0%BC%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D1%87%D0%BA%D0%B8%5C%D0%A1%D0%B5%D1%82%D0%B8%5Cwww.microsoft.com), [www.hp.com](http://www.hp.com/), [www.tut.by](http://www.tut.by/), ftp.cdrom.ru при помощи утилиты NSLOOKUP.

# Контрольные вопросы

1. Для чего используется утилита PING?
2. Как с помощью утилиты PING оценить пропускную способность сети? Объясните формулу.
3. Что такое петля маршрутизации?
4. Как выглядят правила маршрутизации, образующие петлю?
5. Зачем нужна таблица ARP?
6. Объясните разницу во времени между обращениями к одному и тому же хосту по имени и IP адресу.