

Задання для дистанційного навчання
група №39
предмет: “Комп’ютерні мережі”

тема: “ Виконання основних функцій з адміністрування та діагностування мереж”

Викладач: Миронова О.Ю.

Завдання

1. Ознайомтеся з теоретичними відомостями, що наведені нижче.
2. Законспекуйте основні команди та утиліти.
3. Виконати дії з усіма розглянутими командами. Відобразити скріншоти вказаних дій у звіті.
4. Роботи надіслати на електронну адресу olena_mironova@meta.ua

Діагностика роботи та адміністрування комп'ютерної мережі засобами мережевих команд (утиліт).

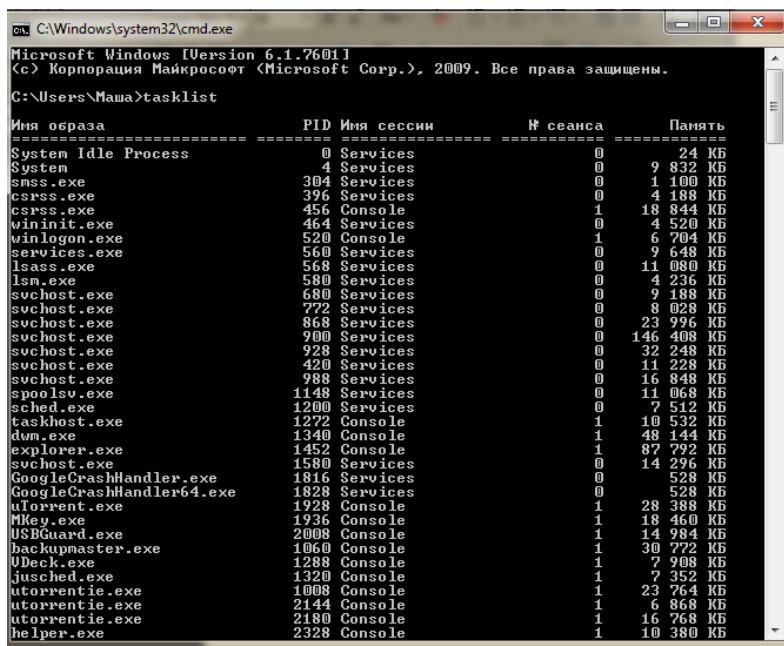
Основою роботи кожного системного адміністратора є моніторинг операційних систем і забезпечення нормальної роботи всіх процесів - принаймні такої, наскільки можна чекати. Уважне спостереження за журналами подій допомагає виявляти і відстежувати проблеми в додатках, безпеці та важливих службах. Виявивши або припускаючи проблему, адміністратор повинен докопатися до її причини і усунути її. Точне визначення причини проблеми може запобігти її повторній появі.

Кожен раз, коли операційна система або користувач запускає службу, додаток або команду, Microsoft Windows запускає один або більше процесів для керування відповідною програмою. Кілька утиліт командного рядка спростять вам моніторинг програм і керування ними.

Моніторинг і діагностика, робота з мережею через командний рядок Windows

За допомогою утиліти командного рядка Tasklist (Рис.1) можна перевірити процеси, що працюють в локальній або віддаленій системі. Tasklist дозволяє:

- отримати ідентифікатор процесу, його стан та інші важливі відомості про процеси в системі;
- побачити залежності між виконуваними процесами і службами, налаштованими в системі;
- переглянути список DLL, задіяних виконуваними в системі процесами;
- використовувати фільтри для включення або виключення процесів, які показуються Tasklist.



```
Microsoft Windows [Version 6.1.7601]
(C) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.
C:\Users\Маша>tasklist

Имя образа PID Имя сессии      № сеанса Память
-----
System Idle Process 0 Services 0 24 КБ
System 4 Services 0 9 832 КБ
smss.exe 304 Services 0 1 100 КБ
csrss.exe 396 Services 0 4 188 КБ
csrss.exe 456 Console 1 18 844 КБ
wininit.exe 464 Services 0 4 520 КБ
winlogon.exe 520 Console 1 6 704 КБ
services.exe 560 Services 0 9 648 КБ
lsass.exe 568 Services 0 11 080 КБ
lsass.exe 580 Services 0 4 236 КБ
svchost.exe 680 Services 0 9 188 КБ
svchost.exe 772 Services 0 8 028 КБ
svchost.exe 868 Services 0 23 996 КБ
svchost.exe 900 Services 0 146 408 КБ
svchost.exe 928 Services 0 32 248 КБ
svchost.exe 420 Services 0 11 228 КБ
svchost.exe 988 Services 0 16 848 КБ
spoolsv.exe 1148 Services 0 11 068 КБ
sched.exe 1200 Services 0 7 512 КБ
taskhost.exe 1272 Console 1 10 532 КБ
dwm.exe 1340 Console 1 48 144 КБ
explorer.exe 1452 Console 1 87 792 КБ
svchost.exe 1580 Services 0 14 296 КБ
GoogleCrashHandler.exe 1816 Services 0 528 КБ
GoogleCrashHandler64.exe 1828 Services 1 28 388 КБ
UFontent.exe 1928 Console 1 18 460 КБ
MKey.exe 1936 Console 1 14 984 КБ
USBGuard.exe 2008 Console 1 30 772 КБ
backupmaster.exe 1060 Console 1 7 908 КБ
UDeck.exe 1288 Console 1 7 352 КБ
jusched.exe 1008 Console 1 23 764 КБ
utorrentie.exe 2144 Console 1 6 868 КБ
utorrentie.exe 2180 Console 1 16 768 КБ
helper.exe 2328 Console 1 10 380 КБ
```

Рис. 1

Зупинка процесів. Щоб зупинити процеси в локальній або віддаленій системі, застосовуйте утиліту командного рядка Taskkill (Рис.3). Параметр /IM використовується для вказівки імені образу процесу, який необхідно завершити.

```

C:\Windows\system32\cmd.exe
chrome.exe          5728 Console           1    31 604 KB
WINWORD.EXE        2200 Console           1    141 596 KB
cmd.exe             388 Console           1     2  28 KB
conhost.exe        5180 Console           1     5  700 KB
tasklist.exe       6444 Console           1     5  480 KB
MsiProbe.exe       6152 Services          0     6  160 KB

C:\Users\Маша>taskkill
Ошибка: Неправильный синтаксис. Не указаны параметры /FI, /PID или /IM.
Введите "TASKKILL /?" для получения справки по использованию.
C:\Users\Маша>taskkill/?
TASKKILL [/S <система> [/U <пользователь> [/P [<пароль>]]]
          < /FI <фильтр>] /PID <процесс> ; /IM <образ>] [/T] [/F]

Описание:
  Завершает процесс по его ID (PID) или имени образа.

Список параметров:
  /S <система>          Подключаемый удаленный компьютер.
  /U [<домен>\<пользователь>] Пользовательский контекст, в котором
                          должна выполняться эта команда.
  /P <пароль>          Пароль для этого пользовательского контекста.
                          Запрашивает пароль, если он не задан.
  /FI <фильтр>        Применение фильтра для выбора набора задач.
                          Разрешение использовать "ж". Пример,
                          !name eq аспе*
  /PID <процесс>      Идентификатор процесса, который требуется
                          завершить.
                          Используйте Tasklist, чтобы получить PID.
  /IM <образ>         Имя образа процесса, который требуется
                          завершить. Знак подстановки "*" может быть
                          использован для указания всех заданий или
                          имен образов.
  /T                  Завершение указанного процесса
                          и всех его дочерних процессов.
  /F                  Принудительное завершение процесса.
  /?                  Вывод справки по использованию.

Фильтры:
Имя фильтра  Допустимые операторы  Допустимые значения
STATUS      eq, ne                RUNNING ;
NOT RESPONDING ; UNKNOWN

```

Рис. 2 Виклик довідки для утиліти Taskkill

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\bishop>taskkill/im notepad.exe
Успешно: Процесс "notepad.exe", с идентификатором 1944, был завершен.

C:\Documents and Settings\bishop>

```

Рис. 3 Приклад виконання taskkill /IM notepad.exe - завершує роботу програми блокнот, яка була запущена

Мережеві утиліти командного рядка

Серед мережевих команд перш за все хотілося б виділити дві утиліти. Перша - це команда **ipconfig**, друга - **netstat**. Системні адміністратори використовують ці команди не тільки для моніторингу мережі, але і для захисту від небезпечних програм, які намагаються встановити контроль над системою.

За допомогою утиліти ipconfig користувач може дізнатися мережеву адресу свого комп'ютера, а викликавши цю команду з параметром / all, отримати повну інформацію про конфігурацію мережі на локальному комп'ютері.

За допомогою утиліти ipconfig користувач може дізнатися мережеву адресу свого комп'ютера, а викликавши цю команду з параметром / all, отримати повну інформацію про конфігурацію мережі на локальному комп'ютері.

```
C:\Windows\system32\cmd.exe
TASKKILL /F /FI "PID ge 1000" /FI "WINDOWTITLE ne untitled*"
TASKKILL /F /FI "USERNAME eq NT AUTHORITY\SYSTEM" /IM notepad.exe
TASKKILL /S <система> /U <домин><пользователь> /FI "USERNAME ne NT*" /IM *
TASKKILL /S <система> /U <пользователь> /P <пароль> /FI "IMAGENAME eq notepad*"

C:\Users\Маша>ipconfig/all

Настройка протокола IP для Windows
Имя компьютера . . . . . : Маша-ПК
Основной DNS-суффикс . . . . . :
Тип узла . . . . . : Гибридный
IP-маршрутизация включена . . . . . : Нет
WINS-прокси включен . . . . . : Нет
Порядок просмотра суффиксов DNS . . . . . : ASUS

Ethernet adapter Сетевое подключение Bluetooth:
Состояние среды . . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание . . . . . : Устройства Bluetooth (личной сети)
Физический адрес . . . . . : 00-1A-7D-DA-71-08
DHCP включен . . . . . : Да
Автонастройка включена . . . . . : Да

Ethernet adapter Подключение по локальной сети:
DNS-суффикс подключения . . . . . : ASUS
Описание . . . . . : Atheros AR8152 PCI-E Fast Ethernet Controlle
Физический адрес . . . . . : 00-25-22-C8-74-4B
DHCP включен . . . . . : Да
Автонастройка включена . . . . . : Да
Локальный IPv6-адрес канала . . . . . : fe80::a8a8:21e:174d:dc71%11<Основной>
IPv4-адрес . . . . . : 192.168.1.107<Основной>
Маска подсети . . . . . : 255.255.255.0
Аренда получена . . . . . : 25 марта 2020 г. 11:23:20
Срок аренды истекает . . . . . : 25 марта 2020 г. 19:22:16
Основной шлюз . . . . . : 192.168.1.1
DHCP-сервер . . . . . : 192.168.1.1
IAD DHCPv6 . . . . . : 234890530
DUID клиента DHCPv6 . . . . . : 00-01-00-01-22-E7-91-6C-00-25-22-C8-74-4B

DNS-серверы . . . . . : 192.168.1.1
NetBios через TCP/IP . . . . . : Включен

Туннельный адаптер isatap.ASUS:
Состояние среды . . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . : ASUS
Описание . . . . . : Адаптер Microsoft ISATAP
Физический адрес . . . . . : 00-00-00-00-00-00-E0
DHCP включен . . . . . : Нет
```

Рис. 4 Пример выполнения ipconfig / all

Команда IPCONFIG используется для отображения поточных наладувань протоколу TCP / IP і для поновлення деяких параметрів, що задаються при автоматичному конфігуруванні мережевих інтерфейсів при використанні протоколу Dynamic Host Configuration Protocol (DHCP).

Синтаксис:

```
ipconfig [/ allcompartments] [/ all] [/ renew [Adapter]] [/ release [Adapter]] [/ renew6 [Adapter]] [/ release6 [Adapter]] [/ flushdns] [/ displaydns] [/ registerdns] [/ showclassidAdapter] [/ setclassidAdapter [ClassID]]
```

ipconfig / all - відобразити всі мережеві настройки для всіх мережевих адаптерів (Рис.4).

Ці параметри прописані в налаштуваннях мережі вашого комп'ютера. Треба лише натиснути правою клавішею миші на значок на панелі задач (Рис.5) , і натиснути Центр керування мережами та загальним доступом..

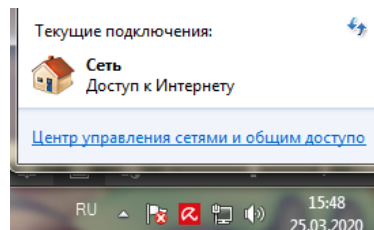


Рис. 5

Ви побачити стан підключення по локальній мережі та зможете отримати відомості про мережеве підключення (Рис.6).

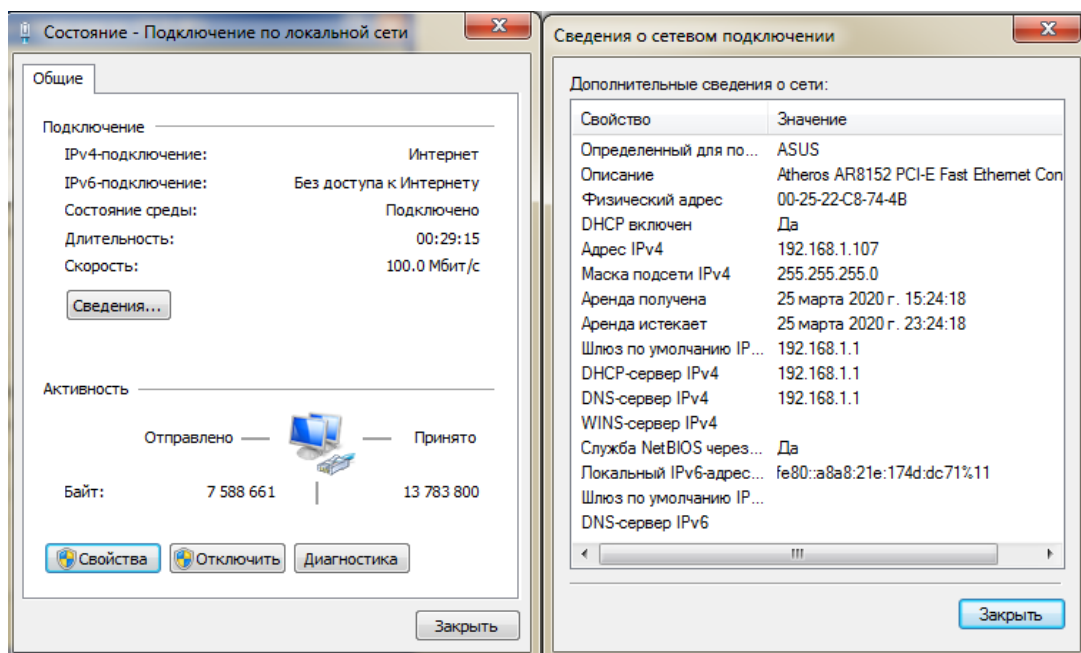


Рис. 6

Тип адреси DHCP (англ. Dynamic Host Configuration Protocol — протокол динамічної конфігурації вузла) — це мережний протокол, що дозволяє комп'ютерам автоматично одержувати IP-адресу й інші параметри, необхідні для роботи в мережі TCP/IP. Для цього комп'ютер звертається до спеціального серверу, під назвою сервер DHCP. Мережевий адміністратор може задати діапазон адрес, що розподіляють серед комп'ютерів. Це дозволяє уникнути ручного налаштування комп'ютерів мережі й зменшує кількість помилок. Протокол DHCP використовується в більшості великих мереж TCP/IP.

IP-адреса (Internet Protocol address) — це ідентифікатор (унікальний числовий номер) мережевого рівня, що використовується для адресації комп'ютерів чи пристроїв у мережах, що побудовані з використанням протоколу TCP/IP (наприклад Інтернет). IP-адреса складається з чотирьох 8-бітних чисел, які називають октетами. Прикладом IP-адреси може бути адреса 192.168.0.31. Процес перетворення доменного імені у IP-адресі виконується DNS-сервером.

У термінології мереж TCP / IP **маскою підмережі** або маскою мережі називається бітова маска, яка визначає, яка частина IP-адреси вузла мережі відноситься до адреси

мережі, а яка - до адреси самого вузла в цій мережі. Наприклад, вузол з IP-адресою 12.34.56.78 і маскою підмережі 255.255.255.0 знаходиться в мережі 12.34.56.0/24 з довжиною префікса 24 біта. У разі адресації IPv6 адреса 2001:0 DB8: 1:0:6 C1F: A78A: 3CB5: 1ADD з довжиною префікса 32 біта (/ 32) знаходиться в мережі 2001:0 DB8 :: / 32. Інший варіант визначення - це визначення підмережі IP-адрес. Наприклад, за допомогою маски підмережі можна сказати, що один діапазон IP-адрес буде в одній підмережі, а інший діапазон відповідно в іншій підмережі.

Мережевий шлюз (англ. gateway) - апаратний маршрутизатор або програмне забезпечення для сполучення комп'ютерних мереж, що використовують різні протоколи (наприклад, локальної та глобальної). Мережевий шлюз конвертує протоколи одного типу фізичного середовища в протоколи інший фізичного середовища (мережі). Наприклад, при з'єднанні локального комп'ютера з мережею Інтернет зазвичай використовується мережевий шлюз. Роутери (маршрутизатори) є одним із прикладів апаратних мережевих шлюзів.

DNS-сервер — програма, призначена для відповідей на DNS-запити за відповідним протоколом. Також DNS-сервером можуть називати хост, на якому запущено відповідну програму. **Доменна система імен** (англ. Domain Name System, DNS) — розподілена система перетворення імені хоста (комп'ютера або іншого мережевого пристрою) в IP-адресу. Кожен комп'ютер в Інтернеті має свою власну унікальну адресу — число, яке складається з чотирьох байтів. Оскільки запам'ятовування десятків чи навіть сотень — не досить приємна процедура, то всі (чи майже всі) машини мають імена, запам'ятати які (особливо якщо знати правила утворення імен) значно легше. Уся система імен в Інтернеті — ієрархічна. Це зроблено для того, щоб не підтримувати одне централізоване джерело, а роздати владу на місця.

Windows Internet Name Service (укр. Служба інтернет імен Windows, WINS: інша назва — NetBIOS Name Server, NBNS) — служба зіставлення NetBIOS-імен комп'ютерів з IP-адресами вузлів. Сервер WINS здійснює реєстрацію імен, виконання запитів і звільнення імен. При використанні NetBIOS поверх TCP/IP необхідний WINS сервер для визначення коректних IP-адрес. Використовує 137 порт по TCP і UDP.

MAC-адреса (від англ. Media Access Control — управління доступом до носія) — це унікальний ідентифікатор, що зіставляється з різними типами устаткування для комп'ютерних мереж. Більшість мережевих протоколів каналного рівня використовують один з трьох просторів MAC-адрес, керованих IEEE: **MAC-48**, **EUI-48** і **EUI-64**. Адреси в кожному з просторів теоретично мають бути глобально унікальними. Не всі протоколи використовують MAC-адреси, і не всі протоколи, що використовують MAC-адреси, потребують подібної унікальності цих адрес. У ширококомовних мережах (таких, як мережі на основі Ethernet) MAC-адреса дозволяє унікально ідентифікувати кожен вузол мережі і доставляти дані тільки цьому вузлу. Таким чином, MAC-адреси формують основу мереж на каналному рівні, яку використовують протоколи вищого рівня. Для перетворення MAC-адрес в адреси мережевого рівня і назад застосовуються спеціальні протоколи (наприклад, ARP і RARP в мережах TCP/IP).

Якщо ви помітили, що з вашим комп'ютером відбувається щось недобре, то в цьому випадку допоможе команда **netstat**, яка не тільки вкаже на відкриті мережеві порти, за якими зловмисники могли під'єднатися до вашої системи, але й ідентифікує процеси, запущені на сервері без вашого відома. Так, ключ / **o** виводить інформацію про

ідентифікатори процесу (PID), що використовує те або інше мережеве з'єднання. Існує можливість подивитися, які комп'ютери в мережі взаємодіють з вашою локальною операційною системою (Рис.7).

```

C:\Windows\system32\cmd.exe - netstat /o
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.
C:\Users\Маша>netstat /o
Активные подключения
Имя      Локальный адрес      Внешний адрес      Состояние      PID
TCP      127.0.0.1:37167      *:*:49489          ESTABLISHED    1888
TCP      127.0.0.1:49161      *:*:49162          ESTABLISHED    1032
TCP      127.0.0.1:49162      *:*:49161          ESTABLISHED    1032
TCP      127.0.0.1:49163      *:*:49164          ESTABLISHED    1032
TCP      127.0.0.1:49164      *:*:49163          ESTABLISHED    1032
TCP      127.0.0.1:49165      *:*:49166          ESTABLISHED    1032
TCP      127.0.0.1:49166      *:*:49165          ESTABLISHED    1032
TCP      127.0.0.1:49167      *:*:49168          ESTABLISHED    1032
TCP      127.0.0.1:49168      *:*:49167          ESTABLISHED    1032
TCP      127.0.0.1:49169      *:*:49170          ESTABLISHED    1032
TCP      127.0.0.1:49170      *:*:49169          ESTABLISHED    1032
TCP      127.0.0.1:49173      *:*:49174          ESTABLISHED    1032
TCP      127.0.0.1:49174      *:*:49173          ESTABLISHED    1032
TCP      127.0.0.1:49175      *:*:49176          ESTABLISHED    1032
TCP      127.0.0.1:49176      *:*:49175          ESTABLISHED    1032
TCP      127.0.0.1:49177      *:*:49178          ESTABLISHED    1032
TCP      127.0.0.1:49178      *:*:49177          ESTABLISHED    1032
  
```

Рис. 7 Приклад виконання netstat /o

Утиліта **ROUTE.EXE** використовується для перегляду і модифікації таблиці маршрутів на локальному комп'ютері. При запуску без параметрів, на екран виводиться підказка по використанню route:

route [-f] [-p] [команда [кінцева_точка] [mask маска_мережі] [шлюз] [metric метрика]] [if інтерфейс]]

route print - відображає поточну таблицю маршрутів (Рис.8).

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.
C:\Users\Маша>route print
=====
Список интерфейсов
13...00 1a 7a da 71 08 .....Устройства Bluetooth (личной сети)
11...00 25 22 e8 74 4b .....Atheros AR8152 PCI-E Fast Ethernet Controller
1 .....Software Loopback Interface 1
12...00 00 00 00 00 00 e0 Адаптер Microsoft ISATAP
14...00 00 00 00 00 00 e0 Адаптер Microsoft ISATAP #2
=====
IPv4 таблица маршрута
=====
Активные маршруты:
Сетевой адрес      Маска сети      Адрес шлюза      Интерфейс      Метрика
0.0.0.0            0.0.0.0        192.168.1.1      192.168.1.107  20
127.0.0.0          255.0.0.0      On-link          127.0.0.1      306
127.0.0.1          255.255.255.255 On-link          127.0.0.1      306
127.255.255.255    255.255.255.255 On-link          127.0.0.1      306
192.168.1.0        255.255.255.0  On-link          192.168.1.107  276
192.168.1.107     255.255.255.255 On-link          192.168.1.107  276
192.168.1.255     255.255.255.255 On-link          192.168.1.107  276
224.0.0.0          240.0.0.0      On-link          127.0.0.1      306
255.255.255.255    255.255.255.255 On-link          192.168.1.107  276
255.255.255.255    255.255.255.255 On-link          127.0.0.1      306
255.255.255.255    255.255.255.255 On-link          192.168.1.107  276
=====
Постоянные маршруты:
Отсутствует
=====
IPv6 таблица маршрута
=====
Активные маршруты:
Метрика  Сетевой адрес      Шлюз
1        306  ::1/128            On-link
11       276  fe80::/64          On-link
11       276  fe80::a8a8:21e:174d:dc71/128
On-link
1        306  ff00::/8           On-link
11       276  ff00::/8           On-link
=====
Постоянные маршруты:
Отсутствует
C:\Users\Маша>
  
```

Рис. 8 Приклад виконання route print

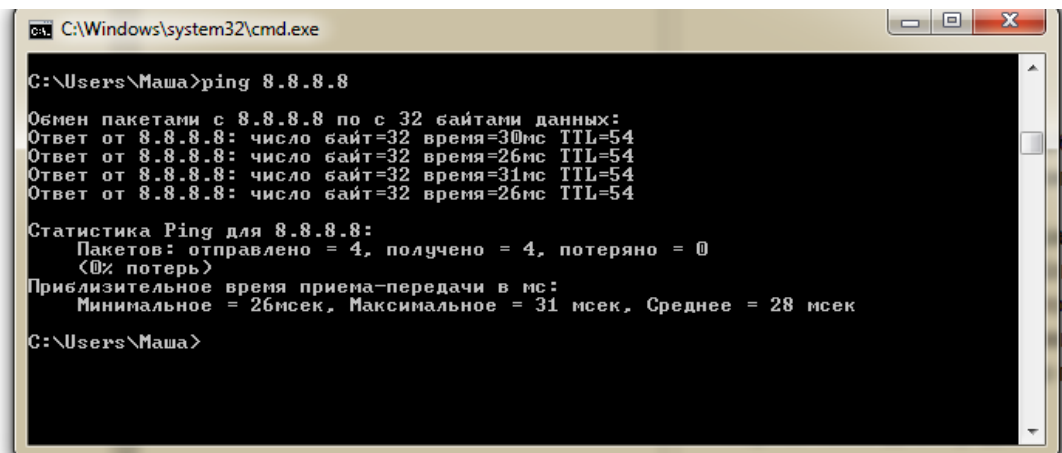
PING.EXE - це, напевно, найбільш часто використовувана мережева утиліта командного рядка. Існує у всіх версіях всіх операційних систем з підтримкою мережі і є простим і зручним засобом опитування вузла по імені або його IP-адресою.

Для обміну службовою та діагностичною інформацією в мережі використовується спеціальний протокол керуючих повідомлень ICMP (Internet Control Message Protocol). Команда ping дозволяє виконати відправку керуючого повідомлення типу Echo Request (тип дорівнює 8 і вказується в заголовку повідомлення) потрібному вузлу і інтерпретувати отриману від нього відповідь в зручному для аналізу вигляді. У відповідь на такий запит, опитуваний вузол повинен відправити ісмп-пакет з тими ж даними, які були прийняті, і типом повідомлення Echo Reply (код типу в заголовку дорівнює 0). Якщо при обміні ісмп-повідомленнями виникає якась проблема, то утиліта ping виведе інформацію для її діагностики.

Формат командного рядка:

ping [-t] [-a] [-n число] [-l розмір] [-f] [-i TTL] [-v TOS] [-r число] [-s число] [[-] списокВузлів] | [-k списокВузлів]] [-w таймаут] кінцевеІм'я

ping 8.8.8.8 - виконати опитування вузла з IP-адресою 8.8.8.8 з параметрами за замовчуванням (Рис.9).



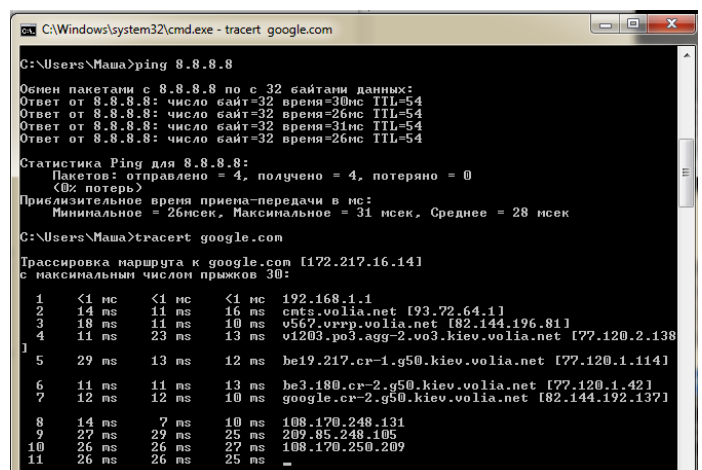
```
C:\Windows\system32\cmd.exe
C:\Users\Маша>ping 8.8.8.8
Обмен пакетами с 8.8.8.8 по 32 байтами данных:
Ответ от 8.8.8.8: число байт=32 время=30мс TTL=54
Ответ от 8.8.8.8: число байт=32 время=26мс TTL=54
Ответ от 8.8.8.8: число байт=32 время=31мс TTL=54
Ответ от 8.8.8.8: число байт=32 время=26мс TTL=54

Статистика Ping для 8.8.8.8:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  (0% потерь)
Приблизительное время приема-передачи в мс:
  Минимальное = 26мсек, Максимальное = 31 мсек, Среднее = 28 мсек

C:\Users\Маша>
```

Рис. 9 Приклад виконання ping 8.8.8.8

Не дивлячись на появу утиліти **PATHPING**, класична утиліта трасування маршруту до заданого вузла **TRACERT**, як і раніше залишається найбільш часто використовуваним інструментом мережевої діагностики. Утиліта дозволяє отримати ланцюжок вузлів, через які проходить IP-пакет, адресований кінцевому вузлу. В основі трасування закладено метод аналізу відповідей при послідовній відправці ICMP-пакетів на вказану адресу із збільшуваним на 1 полем TTL. ("Час життя" - Time To Live) (Рис.10).



```
C:\Windows\system32\cmd.exe - tracert google.com
C:\Users\Маша>ping 8.8.8.8
Обмен пакетами с 8.8.8.8 по 32 байтами данных:
Ответ от 8.8.8.8: число байт=32 время=30мс TTL=54
Ответ от 8.8.8.8: число байт=32 время=26мс TTL=54
Ответ от 8.8.8.8: число байт=32 время=31мс TTL=54
Ответ от 8.8.8.8: число байт=32 время=26мс TTL=54

Статистика Ping для 8.8.8.8:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  (0% потерь)
Приблизительное время приема-передачи в мс:
  Минимальное = 26мсек, Максимальное = 31 мсек, Среднее = 28 мсек

C:\Users\Маша>tracert google.com
Трасировка маршрута к google.com [172.217.16.14]
с максимальным числом прыжков 30:
 0  <1 мс <1 мс <1 мс 192.168.1.1
 1  14 мс 11 мс 16 мс cmts.volia.net [93.72.64.1]
 2  18 мс 11 мс 10 мс v567.vrrp.volia.net [82.144.196.84]
 3  11 мс 23 мс 13 мс v1203.po3.aggr-2.vo3.kiev.volia.net [77.120.2.138]
 4
 5  29 мс 13 мс 12 мс be19.217.cr-1.g50.kiev.volia.net [77.120.1.114]
 6  11 мс 11 мс 13 мс be3.180.cr-2.g50.kiev.volia.net [77.120.1.42]
 7  12 мс 12 мс 10 мс google.cr-2.g50.kiev.volia.net [82.144.192.137]
 8  14 мс 7 мс 10 мс 108.170.248.131
 9  27 мс 29 мс 25 мс 209.85.248.105
10  26 мс 26 мс 27 мс 108.170.250.209
11  26 мс 26 мс 25 мс -
```

Рис. 10 Приклад виконання tracert google.com

Команда PATHPING виконує трасування маршруту до кінцевого вузла аналогічно команді TRACERT, але додатково, виконує відправку ICMP-ехо запитів на проміжні вузли маршруту для збору інформації про затримки і втрати пакетів на кожному з них (Рис.11).

При запуску PATHPING без параметрів, відображається коротка довідка:

pathping [-g Список] [-h Число_стрибків] [-i Адреса] [-n] [-p Пауза] [-q Число_запитів] [-w Таймаут] [-P] [-R] [-T] [-4] [-6] вузол

```

C:\Windows\system32\cmd.exe
с максимальным числом прыжков 30:
0 Мама-ПК.ASUS [192.168.1.107]
1 192.168.1.1
2 cnts.volvia.net [93.72.64.1]
3 v567.vrrp.volvia.net [82.144.196.81]
4 v1203.po3.agg-2.vo3.kiev.volvia.net [77.120.2.138]
5 be19.217.cr-1.g50.kiev.volvia.net [77.120.1.114]
6 be3.180.cr-2.g50.kiev.volvia.net [77.120.1.42]
7 mirohost-1-ix.giganet.ua [185.1.62.13]
8 vps1.ho.ua [91.228.147.0]
9 035.vps.ho.ua [91.228.147.35]

Подсчет статистики за: 225 сек. ...
Прыжок RTT Исходный узел Маршрутный узел % Адрес
0 0мс 0/100 = 0% 0/100 = 0% Мама-ПК.ASUS [192.168.1.107]
1 0мс 0/100 = 0% 0/100 = 0% 192.168.1.1
2 13мс 0/100 = 0% 0/100 = 0% cnts.volvia.net [93.72.64.1]
3 12мс 0/100 = 0% 0/100 = 0% v567.vrrp.volvia.net [82.144.196.81]
4 12мс 0/100 = 0% 0/100 = 0% v1203.po3.agg-2.vo3.kiev.volvia.net [77.120.2.138]
5 12мс 0/100 = 0% 0/100 = 0% be19.217.cr-1.g50.kiev.volvia.net [77.120.1.114]
6 12мс 0/100 = 0% 0/100 = 0% be3.180.cr-2.g50.kiev.volvia.net [77.120.1.42]
7 12мс 0/100 = 0% 0/100 = 0% mirohost-1-ix.giganet.ua [185.1.62.13]
8 12мс 0/100 = 0% 0/100 = 0% vps1.ho.ua [91.228.147.0]
9 12мс 0/100 = 0% 0/100 = 0% 035.vps.ho.ua [91.228.147.35]

Трассировка завершена.
C:\Users\Мама>
  
```

Рис. 11 Приклад виконання pathping http://do.cpoitpd.kiev.ua/

Утиліта NSLOOKUP присутня у всіх версіях операційних систем Windows і є класичним засобом діагностики мережеских проблем, пов'язаних з вирішенням доменних імен в IP-адреси. NSLOOKUP надає користувачеві можливість перегляду бази даних DNS-сервера і побудови певних запитів для пошуку потрібних ресурсів DNS. Практично, утиліта виконує функції служби DNS-клієнт у командному рядку Windows.

Після запуску, утиліта переходить в режим очікування введення. Введення символу ? або команди help дозволяє отримати підказку по використанню утиліти (Рис.12).

```

C:\Windows\system32\cmd.exe
C:\Users\Мама>nslookup
?хЕтхЕ яю съмьурш1: UnKnown
Address: 192.168.1.1


?
Команды: <идентификаторы отображаются в верхнем регистре, квадратные скобки "[ ]" обозначают необязательные параметры>
NAME - печать сведений об узле или домене NAME с помощью сервера по умолчанию
NAME1 NAME2 - та же операция, но в качестве сервера используется NAME2
help or ? - печать сведений о стандартных командах
set OPTION - установить параметр
all - печать параметров, текущего сервера и узла
no debug - печать отладочных сведений
no id2 - печать полных отладочных сведений
no defname - добавить имя домена ко всем запросам
no recursive - запрос рекурсивного ответа на запрос
no search - использовать список поиска доменов
no lvs - всегда использовать виртуальную схему
domain=NAME - установить имя домена по умолчанию NAME
schlist=N1|N2/.../N6] - установить домен N1 и список поиска N1,N2 и т.д.
root=NAME - установить корневой сервер NAME
retry=X - установить число повторов X
timeout=X - установить интервал времени ожидания в X секунд
type=X - установить тип запроса <пр. A,AAAA,ANY,CNAME,MX,NS, PTR,SOA,SRU>
NS, PTR, SOA, SRU>
querytype=X - то же, что и type
class=X - установить класс запроса <пр. IN (Internet), ANY>
no nsxfr - использовать быструю зону MS для передачи
ixfrver=X - текущая версия, использующаяся в передаче запросов IXFR

R
server NAME - установить сервер по умолчанию NAME, используя текущий сервер по умолчанию
lserver NAME - установить сервер по умолчанию NAME, используя первоначальный сервер
root - сделать текущий сервер по умолчанию корневым сервером
ls [opt] DOMAIN [D] FILE - перечисление адресов в домене DOMAIN (необязательно: вывод в файл FILE)
-d - перечисление канонических имен и псевдонимов
-d - перечисление всех записей
-t TYPE - перечисление записей указанного типа RFC <пр. A,CNAME,MX,NS,PTR etc.>
view FILE - сортировка файла "ls" и его просмотр с помощью pg
exit - выход из программы

C:\Users\Мама>
  
```

Рис. 12 Приклад виконання nslookup, набравши ?, а потім exit.

Для перегляду всіх параметрів тієї чи іншої команди необхідно ввести в командний рядок команду, що вас цікавить та дописати /? або /help до неї (Рис.13).



```
CA\Windows\system32\cmd.exe
-t TYPE - перечисление записей указанного типа RFC (пр. A,CNAME,MX,NS,P
IR etc.)
view FILE - сортировка файла "ls" и его просмотр с помощью rd
exit - выход из программы
> exit
C:\Users\Маша>ping/help
Неверный параметр /help.

Использование:
ping [-t] [-a] [-n <число>] [-l <размер>] [-f] [-i <TTL>] [-v <TOS>]
[-r <число>] [-s <число>] [-j <список_узлов>] [-k <список_узлов>]
[-w <тайм-аут>] [-R] [-S <адрес_источника>] [-4] [-6] конечный_узел

Параметры
-t Проверка связи с указанным узлом до прекращения.
Для отображения статистики и продолжения проверки
нажмите сочетание клавиш CTRL+BREAK;
для прекращения нажмите CTRL+C.
-a Определение имен узлов по адресам.
-n <число> Число отправляемых запросов эха.
-l <размер> Размер буфера отправки.
-f Установка в пакете флага, запрещающего
фрагментацию (только IPv4).
-i <TTL> Задание срока жизни пакетов.
-v <TOS> Задание типа службы (только IPv4). Этот параметр
недоступен и не влияет на поле TOS в заголовке IP.
-r <число> Запись маршрута для указанного числа прыжков
(только IPv4).
-s <число> Отметка времени для указанного числа прыжков
(только IPv4).
-j <список_узлов> Свободный выбор маршрута по списку узлов
(только IPv4).
-k <список_узлов> Жесткий выбор маршрута по списку узлов
(только IPv4).
-w <тайм-аут> Тайм-аут для каждого ответа (в миллисекундах).
Использование заголовка для проверки также и
обратного маршрута (только IPv6).
-S <адрес_источника> Используемый адрес источника.
-4 Принудительное использование протокола IPv4.
-6 Принудительное использование протокола IPv6.

C:\Users\Маша>
```

Рис. 13. Пример выполнения ping/help