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. Законспектуйте основні команди та утиліти.

3. Виконати дії з усіма розглянутими командами. Відобразити скріншоти вказаних дій у звіті.

4. Роботи надіслати на 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.

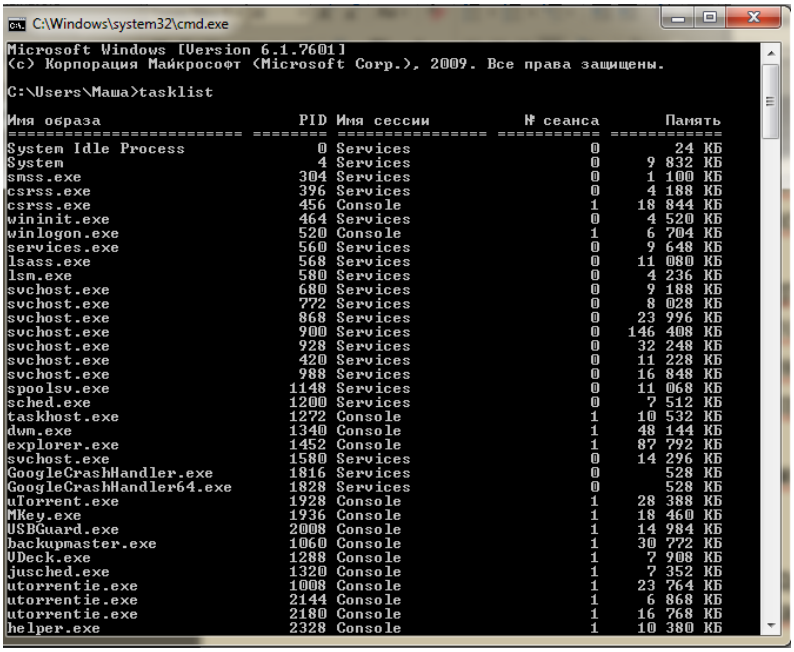

Рис. 1

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.

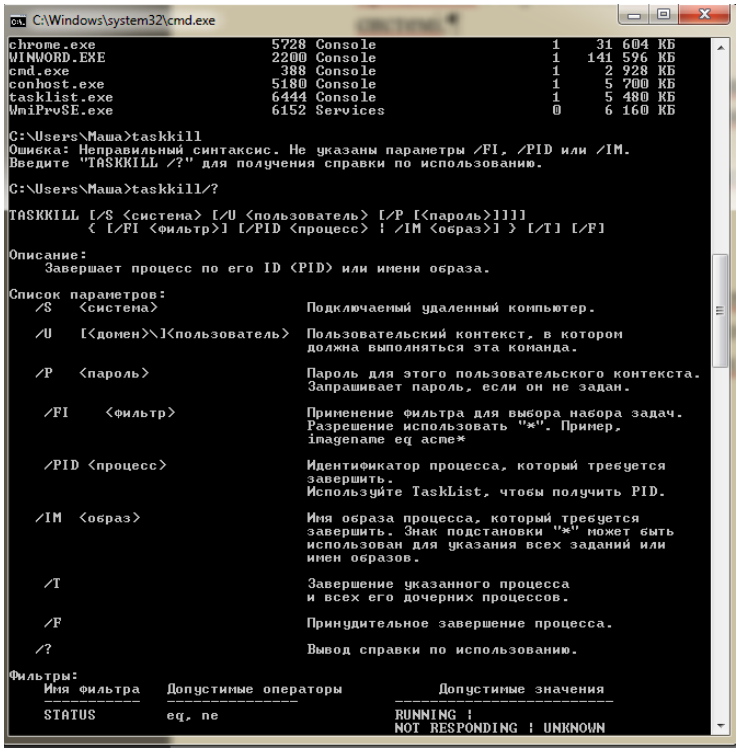

Рис. 2 Виклик довідки для утиліти Taskkill

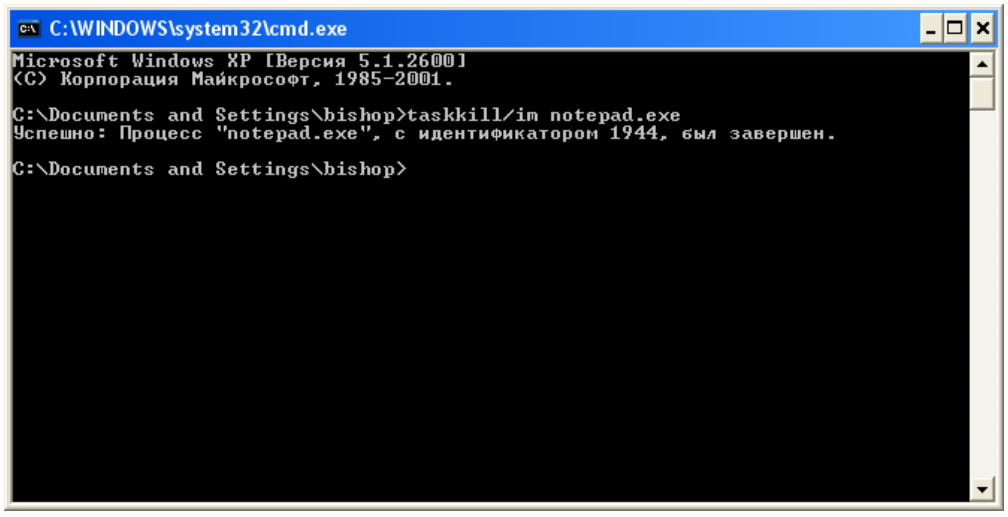

Рис. 3 Приклад виконання taskkill / IM notepad.exe - завершує роботу програми блокнот, яка була запущена

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.

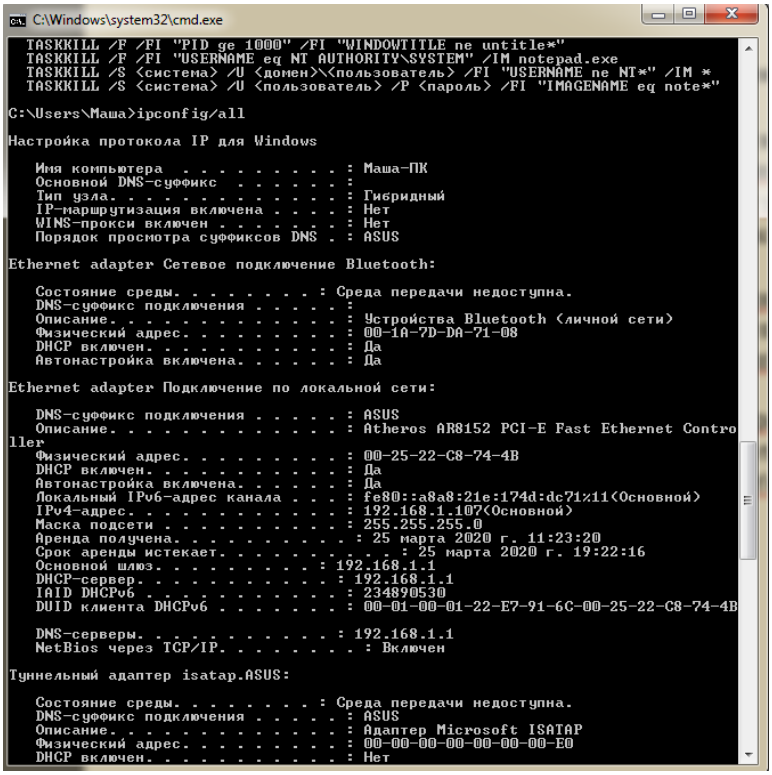

Рис. 4 Приклад виконання ipconfig / all

Команда IPCONFIG використовується для відображення поточних налаштувань 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..

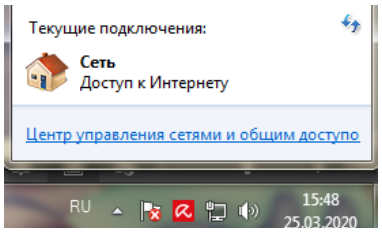

Рис. 5

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

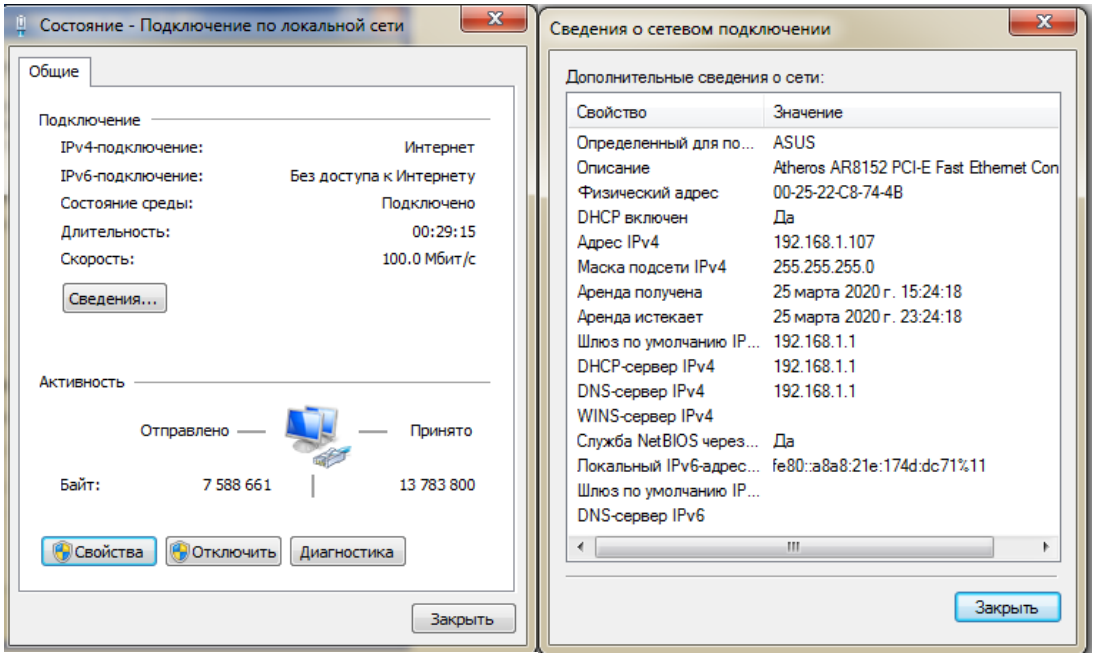

Рис. 6

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 використаннямпротоколу 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 інший 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 канального 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 широкомовних 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 канальному 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 системі, 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 локальної операційною системою (Рис.7).

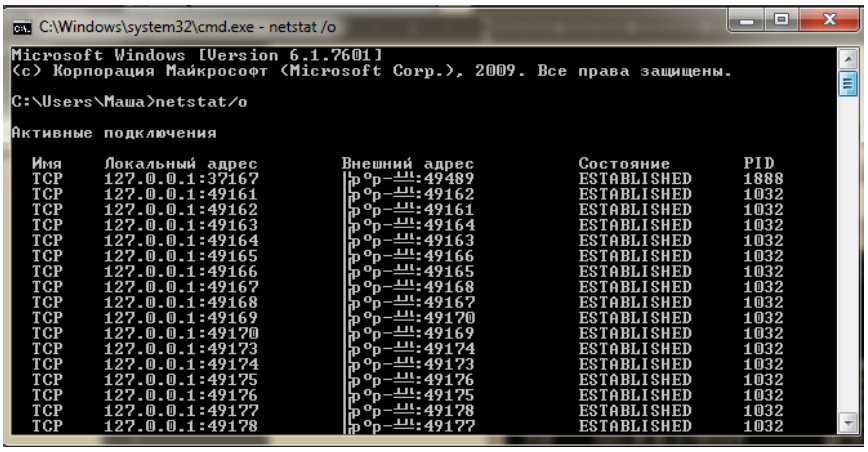

Рис. 7 Приклад виконання netstat / o

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).

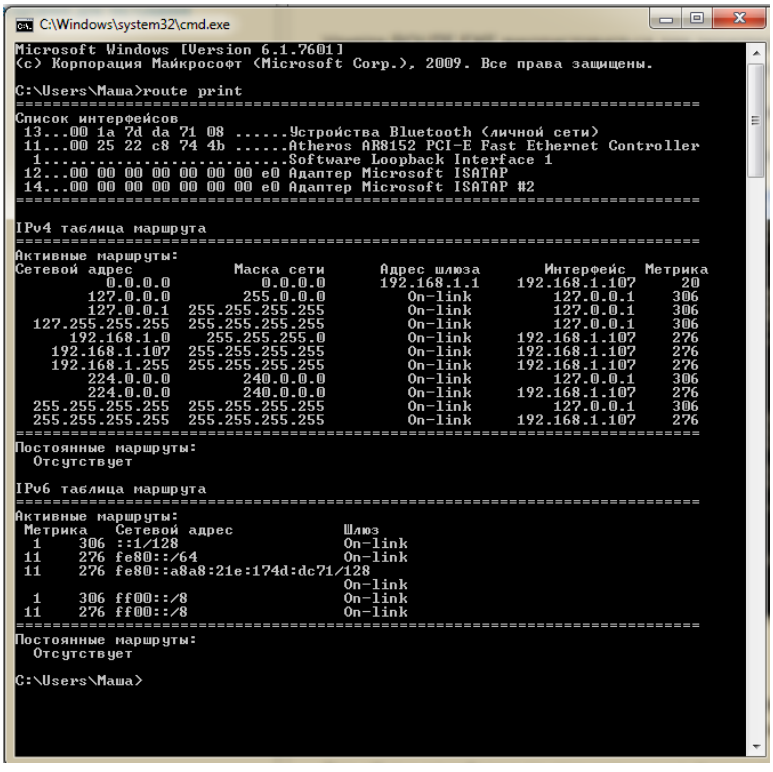

Рис. 8 Приклад виконання route print

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 icmp-пакет з тими ж даними, які були прийняті, і типом повідомлення Echo Reply (код типу в заголовку дорівнює 0). Якщо при обміні icmp-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] [[-j 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).

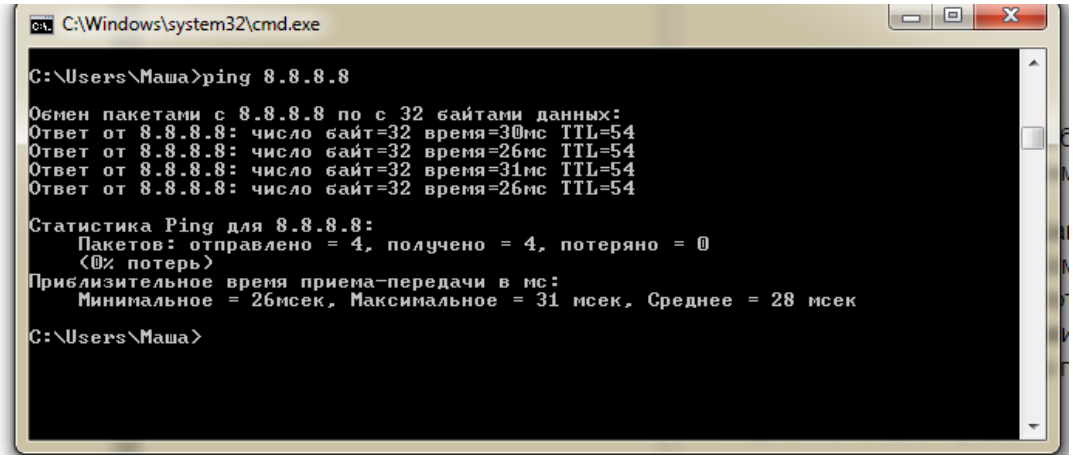

Рис. 9 Приклад виконання ping 8.8.8.8

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).

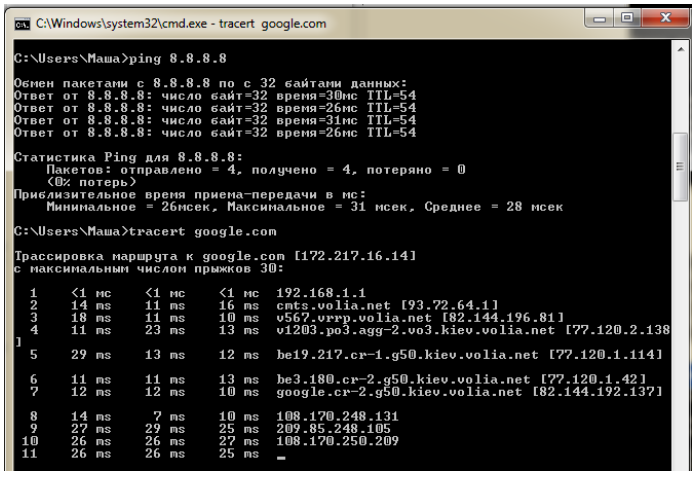

Рис. 10 Приклад виконання tracert google.com

Команда PATHPING виконує трасування маршруту до кінцевого вузла аналогічно команді TRACERT, але додатково, виконує відправку ICMP-exo 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

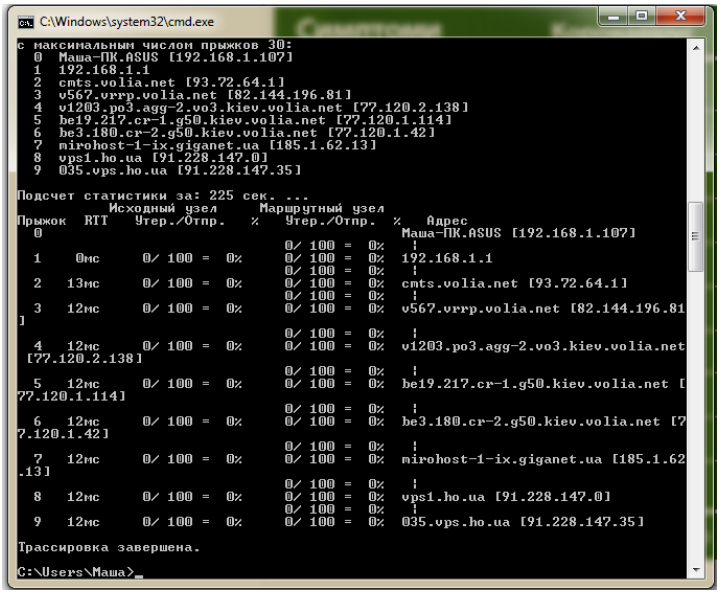

Рис. 11 Приклад виконання pathping http://do.cpoitpd.kiev.ua/

Утиліта NSLOOKUP присутня у всіх версіях операційних систем Windows і є класичним засобом діагностики мережевих 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).

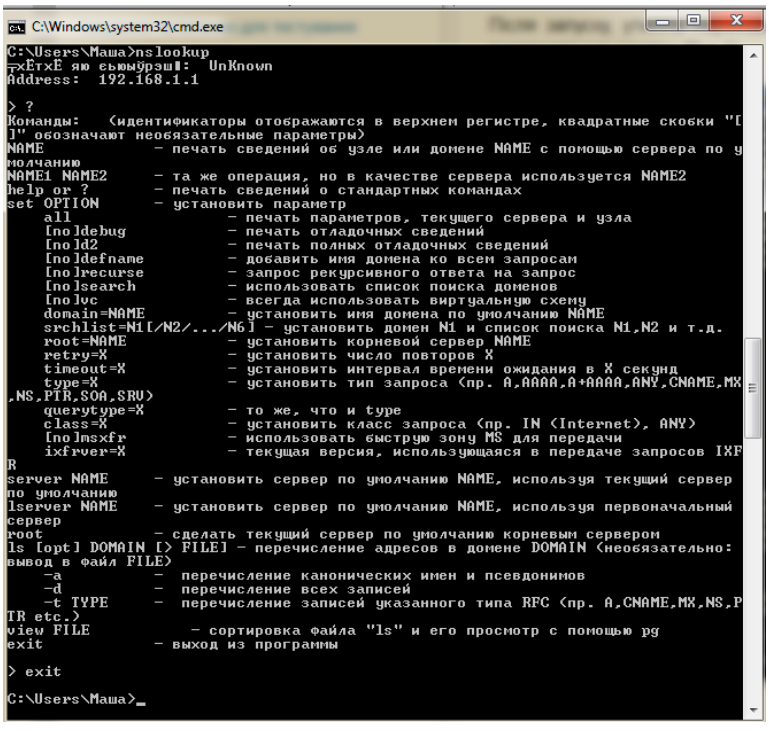

Рис. 12 Приклад виконання nslookup, набравши ?, а потім exit.

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).

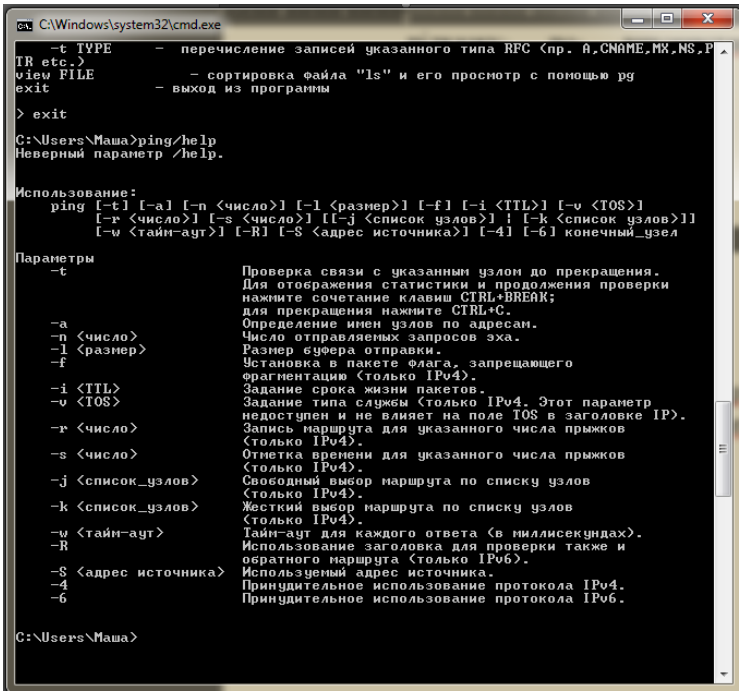

Рис. 13. Приклад виконання ping/help