МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки комп’ютерної та програмної інженерії

Кафедра безпеки інформаційних технологій

**Технології забезпечення конфіденційності і цілісності інформаційних ресурсів**

**Лабораторна робота №1**

Тема: «Фізична основа кіберпростору – Інтернет. Мережеві утиліти та їх використання для моніторингу та діагностики мережі»

Тривалість заняття: 90 хв.

Київ 2023

**Тема**: «Фізична основа кіберпростору – Інтернет. Мережеві утиліти та їх використання для моніторингу та діагностики мережі

**Мета**: Вивчення основ адресації в комп’ютерних мережах.

**Теоретичні відомості**

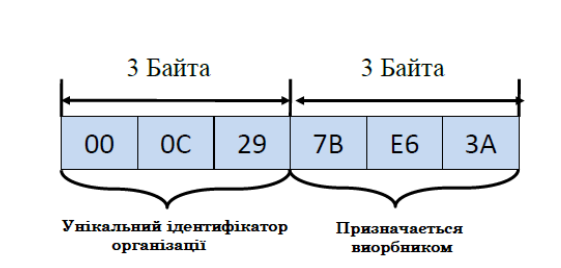
Одним із проявів наявності шкідливої програми може бути збільшена мережева активність. Шкідлива програма може відправляти листи, завантажувати інформацію з Інтернету, передавати комусь по мережі конфіденційну інформацію та багато іншого. При цьому необхідно пам’ятати, що легальні додатки також можуть використовувати Інтернет без дій користувача – наприклад, антивірусна програма може завантажувати оновлення бази сигнатур. Ось чому так важливо здійснювати контроль роботи мережі, а саме моніторинг і аналіз мережі. Незважаючи на те, що дані питання будуть розглядатися більш детально на наступних курсах, уже на даній лабораторній роботі розглядаються основи адресації в комп’ютерних мережах та використання декількох базових мережевих утиліт.

Кожен комп’ютер в мережі TCP/IP має адреси трьох рівнів:

1. На канальному рівні, локальну адресу вузла, яка визначається технологією, за допомогою якої побудована окрема мережа (в яку входить даний вузол). Для вузлів, що входять в локальні мережі, це МАС-адреса мережного адаптера або порту маршрутизатора, наприклад, 00-0С-29-7B-E6-3A.

2. IP-адреса, яка виражається одним 32-розрядним числом (4 байти), наприклад, 160.81.5.131 і використовується на мережному рівні. Вона призначається адміністратором під час конфігурування комп’ютерів і маршрутизаторів. IP-адреса складається з двох частин: адреси мережі і номера вузла (комп’ютера) в мережі. Адреса мережі може бути обрана адміністратором довільно, або призначена за рекомендацією спеціального підрозділу (Network Information Center, NIC), якщо мережа повинна працювати як складова частина мережі Інтернет. Зазвичай інтернет-провайдери отримують діапазони адрес у підрозділів NIC, а потім розподіляють їх між своїми абонентами. Номер вузла в протоколі IP призначається незалежно від локальної адреси вузла. Розподіл IPадреси на поле адреси мережі і номера вузла – гнучке, і межа між цими полями може встановлюватися досить таки довільно.

Кожен комп’ютер, підключений до мережі, має мережевий адаптер (мережеву карту) з присвоєним йому унікальним адресом, так званим MACадресом, який задається при виготовленні мережевого адаптера (виробниками устаткування) і в подальшому не змінюється. Довжина і інші особливості MACадреси залежать від використовуваної в локальній мережі технології. У мережах Ethernet MAC-адреса має довжину 6 байт, записаних в шістнадцятковому форматі і розділених дефісами (рис. 2.1): старші три байти – ідентифікатор фірми виробника, а молодші три байти призначаються унікальним чином самим виробником.



Для визначення локальної адреси за IP-адресою використовується протокол визначення адреси ARP (Address Resolution Protocol). Існує також протокол, що вирішує зворотну задачу – знаходження IP-адреси за відомим локальним адресом, так званий RARP – реверсивний ARP. Він використовується при старті бездискових станцій, які в початковий момент не знають свого IPадресу, але знають адресу свого мережного адаптера.

Так як оперувати довгими двійковими числами досить складно, число, яке визначає IP-адресу версії 4 (IPv4), розбивають на 4 октети – восьмирозрядних двійкових числа, а кожне з цих чисел представляють в десятковому вигляді. Октети відокремлюють один від одного крапками. Таким чином, 32-розрядна IP-адреса представляється у вигляді: 255.255.255.255 (десяткове число може змінюватися від 0 до 255 – максимального значення восьмирозрядного двійкового числа). Наприклад: 160.81.5.131 – десяткова форма представлення IP-адреси, 10100000.01010001.00000101.10000011 – двійкова форма представлення цієї ж адреси.

Далі показана структура IP-адреси в залежності від класу мережі.



Як вже зазначалося раніше, адреса складається з двох логічних частин – номера мережі і номера вузла в мережі. Яка частина адреси відноситься до номера мережі, а яка до номера вузла, визначається значеннями перших бітів адреси:

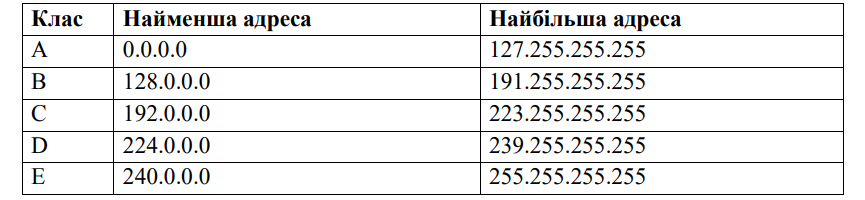
- Якщо адреса починається з 0, то мережу відносять до класу А (великі мережі загального користування), і номер мережі займає один байт, інші три байти інтерпретуються як номер вузла в мережі. Мережі класу А мають номери в діапазоні від 1 до 126. (номер 0 не використовується, а номер 127 зарезервований для спеціальних цілей).

- Якщо перші два біти адреси рівні 10, то мережа відноситься до класу В і є мережею середніх розмірів з числом вузлів 28 – 216. У мережах класу В під адресу мережі і під адресу вузла відводиться по 16 біт, тобто по 2 байти.

- Якщо адреса починається з послідовності 110, то це мережа класу C з числом вузлів не більше 28. Під адресу мережі відводиться 24 біти, а під адресу вузла – 8 біт.

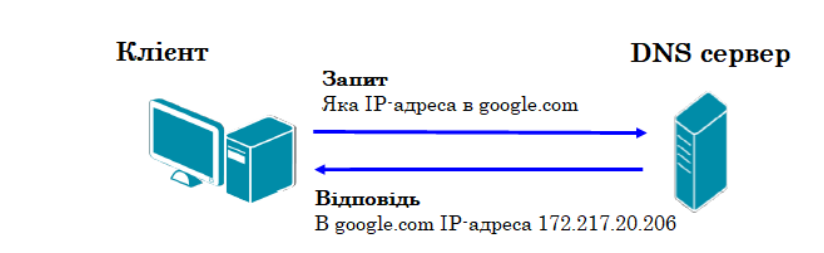
- Якщо адреса починається з послідовності 1110, то вона є адресою класу D і позначає особливу, групову адресу – multicast. Якщо в пакеті, як адреса призначення, вказано адресу класу D, то такий пакет повинні отримати всі вузли, яким присвоєно цю адресу.

- Якщо адреса починається з послідовності 11110, то це адреса класу Е, вона зарезервована для майбутнього використання.



У глобальних мережах і мережі Інтернет це служба DNS (Domain Name System) – розподілена база даних, що підтримує ієрархічну систему імен для ідентифікації вузлів в мережі Інтернет. Служба DNS призначена для автоматичного пошуку IP-адреси за відомим символьним імені вузла. Специфікація DNS визначається стандартами RFC 1034 і 1035. DNS вимагає статичноїної конфігурації своїх таблиць, які відображають імена комп’ютерів в IP-адресу.

Протокол DNS є службовим протоколом прикладного рівня. Цей протокол несиметричний – в ньому визначені DNS-сервери і DNS-клієнти. DNS-сервери зберігають частину розподіленої бази даних про відповідність символьних імен і IP-адрес. Ця база даних розподілена по адміністративним доменам мережі Інтернет. Клієнти сервера DNS знають IP-адреса сервера DNS свого адміністративного домену і за протоколом IP передають запит, в якому повідомляють через відоме символьне ім’я і просять повернути відповідну йому IP-адресу.



Якщо дані щодо запиту відповідності зберігаються в базі даного DNSсервера, то він відразу посилає відповідь клієнту, якщо ж ні – то він надсилає запит DNS-серверу іншого домену, який може сам обробити запит, або передати його іншому DNS-сервера. Всі DNS-сервери з’єднані ієрархічно, відповідно до ієрархії доменів мережі Інтернет. Клієнт опитує ці сервери імен, поки не знайде потрібні відображення. Цей процес прискорюється через те, що сервери імен постійно кешують інформацію, яка надається за запитами. Клієнтські комп’ютери можуть використовувати в своїй роботі IP-адреси декількох DNS-серверів, для підвищення надійності своєї роботи.

База даних DNS має структуру дерева, званого доменним простором імен, в якому кожен домен (вузол дерева) має ім’я і може містити піддомени. Ім’я домену ідентифікує його положення в цій базі даних по відношенню до батьківського домену, а точки в імені відділяють частини, відповідні вузлам домену, наприклад, www. ibm.ua.

Корінь бази даних DNS управляється центром Інтернет Network Information Center. Домени верхнього рівня призначаються для кожної країни, а також на організаційній основі. Імена цих доменів повинні слідувати міжнародним стандартом ISO 3166. Для позначення країн використовуються трьох буквенні та дво-літерні абревіатури, а для різних типів організацій використовуються наступні абревіатури:

- com – комерційні організації (наприклад, microsoft.com);

- edu – освітні (наприклад, mit.edu);

- gov – урядові організації (наприклад, nsf.gov);

- org – некомерційні організації (наприклад, pir.org);

- net – організації, що підтримують мережі (наприклад, nsf.net).

Кожен домен DNS адмініструється окремою організацією, яка зазвичай розбиває свій домен на піддомени і передає функції адміністрування цих піддоменів іншим організаціям. Кожен домен має унікальне ім’я, а кожен з піддоменів має унікальне ім’я усередині свого домену. Ім’я домена може містити до 63 символів. Кожен хост в мережі Інтернет однозначно визначається своїм повним доменним ім’ям (fully qualified domain name, FQDN), яке включає імена всіх доменів у напрямку від хоста до кореня. Приклад повного DNSімені: server.aics.acs.cctpu.edu.ua

Протокол DHCP (Dynamic Host Configuration Protocol) був розроблений для того, щоб звільнити адміністратора від необхідності призначення комп’ютерам IP-адрес вручну. У локальній мережі, що містить DHCP-сервер, кожен комп’ютер при включенні надсилає запит до цього сервера на отримання IP-адреси. Таким чином, основним призначенням DHCP є динамічне призначення IP-адрес. Однак, крім динамічного, DHCP може підтримувати і більш прості способи призначення адрес: ручний і автоматичний статичний.

При ручному призначенні адрес активну участь приймає адміністратор, який надає DHCP-серверу інформацію про відповідність IP-адрес фізичним адресами або іншим ідентифікаторам клієнтів. Ці адреси повідомляються клієнтам у відповідь на їх запити до DHCP-сервера.

При автоматичному статичному способі DHCP-сервер привласнює IPадресу (і, можливо, інші параметри конфігурації клієнта) з пулу (набору) наявних IP-адрес без втручання оператора. Межі пулу адрес, які призначаються задає адміністратор при конфігуруванні DHCP-сервера. Між ідентифікатором клієнта і його IP-адресою, як і при ручному призначенні, існує постійна відповідність. Вона встановлюється в момент первинного призначення сервером DHCP IP-адреси клієнта і таким чином при всіх наступних запитах сервер повертає той же самий IP-адрес.

При динамічному розподілі адрес DHCP-сервер видає адресу клієнту на обмежений час, що дає можливість згодом повторно використовувати IP-адреси іншими комп’ютерами. Динамічне розділення адрес дозволяє будувати IPмережу, кількість вузлів в якій набагато перевищує кількість наявних у розпорядженні адміністратора IP-адрес.

Всі мережеві операційні системи мають в своєму складі утиліти для тестування мережі. А оскільки більшість користується ОС Windows, тому далі будуть розглянуті декілька мережевих утиліт саме ОС Windows, які запускаються з командного рядка.

Утиліта ipconfig (IP configuration) призначена для настройки протоколу IP для операційної системи Windows. У даній лабораторній роботі ця утиліта буде використовуватися тільки для отримання інформації про з’єднання по локальній мережі. Для отримання цієї інформації введіть в командному рядку («Пуск» → «Виконати» → cmd): ipconfig /all У розділі «Адаптер Ethernet …» для даної лабораторної будуть необхідні поля «DHCP», «IP-адреса» і «DNS-сервери».

Утиліта ping (Packet Internet Groper) є одним з головних засобів, що використовуються для налагодження мереж, і служить для примусового виклику відповіді конкретної машини. Для цього використовується дейтаграмма ECHO\_REQUEST протоколу ICMP.

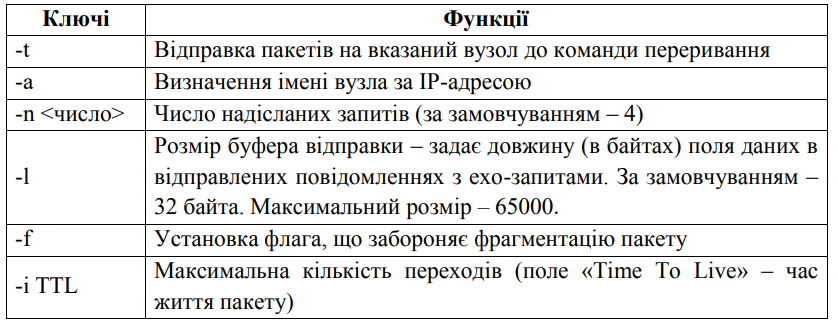
Дана утиліта дозволяє перевіряти роботу програм TCP/IP на віддалених машинах, адреси пристроїв в локальній мережі, адресу і маршрут для віддаленого мережевого пристрою. У виконанні команди ping беруть участь система маршрутизації, схеми дозволу адрес і мережеві шлюзи. Це утиліта низького рівня, яка не вимагає наявності серверних процесів на машині, яка перевіряється, тому успішний результат при проходженні запиту зовсім не означає, що виконуються які-небудь сервісні програми високого рівня, а говорить про те, що мережа знаходиться в робочому стані, живлення машини, яка перевіряється, включено, і машина не відмовила («не зависла»).

У ОС Windows утиліта ping є в комплекті поставки і являє собою програму, що запускається з командного рядка.

Запити утиліти ping передаються по протоколу ICMP (Internet Control Message Protocol). Отримавши такий запит, програмне забезпечення, що реалізує протокол IP у адресата, посилає відлуння-відповідь (ехо-відповідь). Якщо машина, яка перевіряється, в момент отримання запиту була завантажена більш пріоритетною роботою (наприклад, обробкою і перенаправленням великого обсягу трафіку), то відповідь буде відправлена не відразу, а як тільки закінчиться виконання більш пріоритетного завдання. Тому слід врахувати, що затримка, розрахована утилітою ping, викликана не тільки пропускною здатністю каналу передачі даних до машини, яка перевіряється, але і завантаженістю цієї машини.

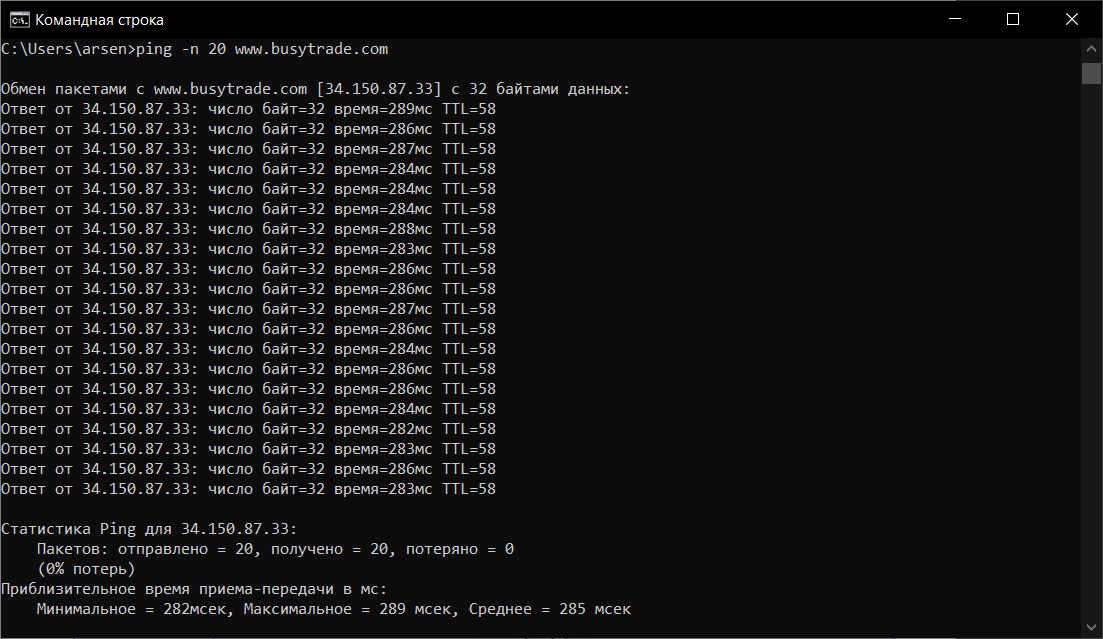
Відлуння-запити надсилаються задану кількість разів (ключ -n). За замовчуванням передається чотири запити, після чого виводяться статистичні дані.

Зверніть увагу: оскільки з утиліти ping можуть починатися більшість хакерських атак, деякі сервери з метою безпеки не посилають ехо-відповіді (наприклад, www.microsoft.com). Не чекайте марно, введіть команду переривання (CTRL + C).

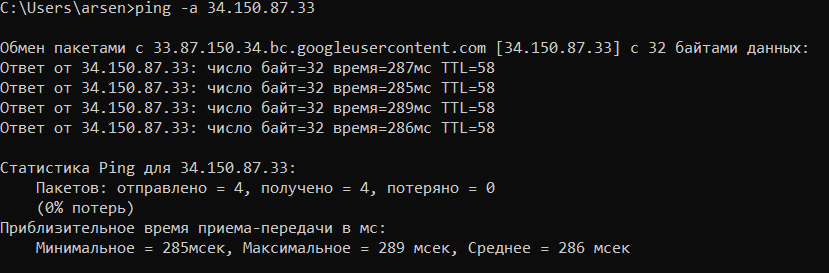


На практиці більшість опцій в форматі команди можна опустити, тоді в командному рядку може бути прописано: ping ім’я вузла (для зациклення виведення інформації про з’єднання використовується опція -t; для виведення інформації n-раз використовується опція -n ).

Приклад:



Приклад визначення імені вузла за IP-адресою:

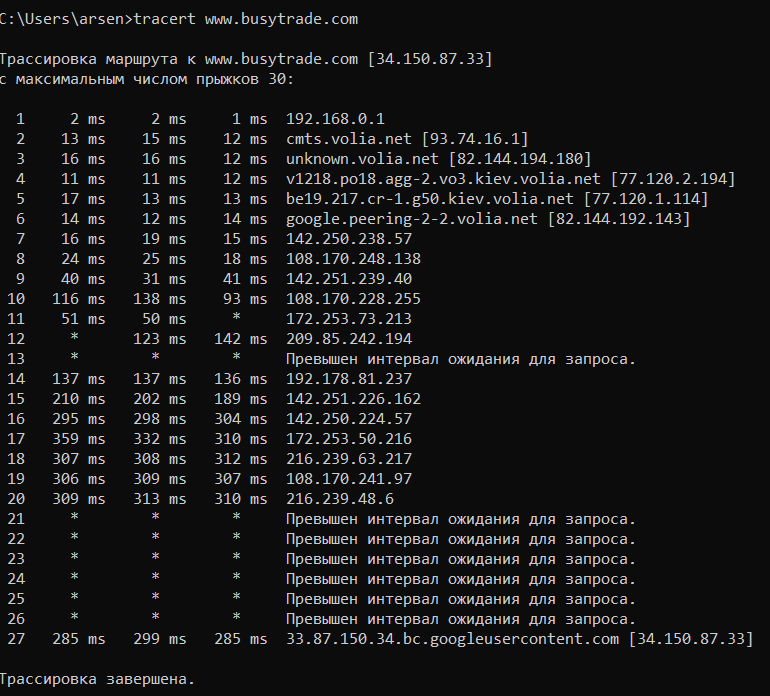


Утиліта tracert

Ця команда подібна команді ping, обидві посилають в точку призначення ехо-пакети і потім чекають їх повернення. Відмінність пакетів команди traceroute від пакетів ping полягає в тому, що вони мають різний термін життя (Time to Live, TTL) і за допомогою цього, утиліта tracert дозволяє виявляти послідовність маршрутизаторів, через які проходить IP-пакет на шляху до пункту свого призначення.

Формат команди: tracert імя\_машини де імя\_машини може бути ім’ям вузла або IP-адресою машини. Вихідна інформація являє собою список машин, починаючи з першого шлюзу і закінчуючи вузлом призначення.

Приклад:

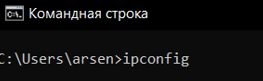


Пакети надсилаються по три на кожен вузол. Для кожного пакету на екрані відображається величина інтервалу часу між відправленням пакета і отриманням відповіді. Символ \* означає, що відповідь на даний пакет не була отримана. Якщо вузол не відповідає, то при перевищенні інтервалу очікування відповіді видається повідомлення «Перевищено інтервал очікування для запиту». Інтервал очікування відповіді може бути змінений за допомогою опції -w команди tracert.

Команда tracert працює шляхом установки поля часу життя (числа переходів) вихідного пакета таким чином, щоб цей час спливав до досягнення пакетом пункту призначення. Коли час життя закінчиться, поточний шлюз відправить повідомлення про помилку на машину-джерело. Кожне збільшення поля часу життя дозволяє пакету пройти на один маршрутизатор далі.

При реєстрації доменних імен другого рівня обов’язковою умовою є надання вірних відомостей про власника цього домену: для юридичних осіб – назва організації, для фізичних осіб – ПІБ і паспортні дані. Також обов’язковим є надання контактної інформації. Частина цієї інформації стає вільно доступною для будь-якого користувача мережі Інтернет через сервіс Whois. Отримати необхідну інформацію про власника домену можна через Whoisклієнт, наприклад, в Unix це консольна команда whois, в ОС Windows – це додаток SmartWhois. Але найпростіше відправити запит можна через веб-форму on-line сервісу Whois, наприклад через форму на сторінці https://www.whois.com

**Завдання**

1. Включити комп’ютер.
2. Ознайомитись з теоретичними відомостями.
3. Використовуючи утиліту( утиліти які вам потрібно використовувати в лабораторній роботі є вбудованими в Windows, тобто їх не потрібно додатково скачувати) ipconfig визначити IP адресу і фізичну адресу основного мережевого інтерфейсу свого комп’ютера, IP адресу шлюзу, IP адресу DNS-серверів і чи використовується DHCP(опис що таке DNS та DHCP можна знайти в теоретичних відомостях) Результати представити у вигляді таблиці та розмістити після таблиці зображення вікна (скріншот робочого столу). Для цього вам потрібно відкрити пошук в Windows ввести туди командний рядок, та відкрити його. В командний рядок вам потрібно ввести таку команду 
4. Перевірити стан зв’язку з [www.chinavasion.com](http://www.chinavasion.com), 104.26.6.231, [www.imobile.com.cn](http://www.imobile.com.cn), 47.94.88.155, [www.vancl.com](http://www.vancl.com), 120.92.34.213, [www.shop.com](http://www.shop.com), 104.84.62.138, [www.amazon.com](http://www.amazon.com), 18.66.225.227. Отримані дані занести в таблцю та додати скріншоти виконання перевірки стану зв’язку. Для перевірки стану зв’язку вам потрібно вводити наступні команди в командний рядок :





І так далі, змінюючи то інтернет адрессу, то IP-адрессу.

1. Провести трасування таких вузлів: [www.chinavasion.com](http://www.chinavasion.com), [www.imobile.com.cn](http://www.imobile.com.cn), [www.vancl.com](http://www.vancl.com), [www.shop.com](http://www.shop.com), [www.amazon.com](http://www.amazon.com). Отримані дані занести до таблиці та додати скріншоти трасування. Для проведення трасування вам потрібно вводити в командий рядок таку команду



І так далі замінюючи інтернет адресу на потрібну вас адрессу

1. За результатами трасування зробити графіки зміни середнього часу проходження пакету.
2. Звіт має містити скріншоти виконання введених вами команд в командний рядок.
3. Дати відповідь на конрольні питання
4. Зробити висновки та занести їх до звіту.

**Контрольні питання**

1. Назвіть три рівні адресації в комп’ютерних мережах, та наведіть приклади адрес до кожного з рівнів.
2. Поясніть, що таке MAC-адреса, та опишіть її структуру.
3. Опишіть структуру IP-адреси та поясніть що таке маска підмережі і для чого вона використовується?
4. Назвіть основні критерії віднесення ІР-адреси до певного класу мережі.
5. Назвіть та опишіть IP-адреси спеціального призначення.
6. Поясніть, що таке служба DNS?
7. Поясніть, що таке протокол DHCP?
8. Для чого призначена утиліта ipconfig?
9. Назвіть основне призначення утиліти ping та опишіть алгоритм її роботи.
10. Назвіть основну відмінність утиліт ping та traceroute.