**МІНІСТЕРСТВО ОСВІТИ І НАУКИ**

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»**



**ЛАБОРАТОРНА РОБОТА №1**

**ВАРІАНТ 9**

**Використання засобів командної оболонки для отримання відомостей про мережу**

**Виконав:**

**ст. гр. ІР-21**

**Касараба В.В.**

**Прийняла:**

**Доцент каф. КСА**

Влах-Вигриновська **Г.І.**

**Львів 2021**

**Завдання**

1. Відкрийте вікно **Командний рядок**.

2. Використовуючи команду **netstat** виконайте **Завдання 3.1** згідно свого варіанту. Завдання дивіться в таблиці **«Варіанти завдань»**. Номер варіанта визначається порядковим номером в журналі викладача. Завдання потрібно виконати на комп’ютері в аудиторії, де проводиться заняття, та на Вашому персональному (домашньому) комп’ютері, підключеному до **Інтернет**.

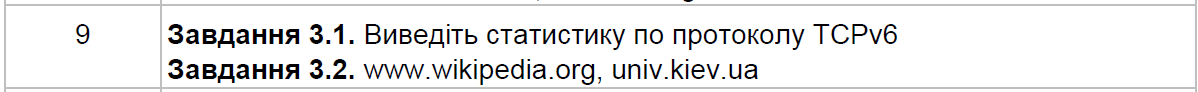
3. Використовуючи команду **ping** перевірте з'єднання на рівні протоколу IP з зазначеними в **Завданні 3.2** адресами та проаналізуйте отримані результати.

4. Використовуючи команду **tracert** визначте шлях до точки призначення. В якості точок призначення використайте адреси, зазначені в **Завданні 3.2**.

5. Використовуючи команду **pathping** отримайте інформацію про латентності мережі та втрати даних на проміжних вузлах між вихідним пунктом і пунктом призначення. В якості пунктів призначення використайте адреси, зазначені в **Завданні 3.2**.

6. Використовуючи команду **ipconfig** виведіть повну конфігурацію TCP/IP для всіх адаптерів.

7. Проаналізуйте отримані результати.



**Відповіді**

**№3.1**

**Використовуючи команду** ***netstat* виведіть статистику протоколу TCPv6.**

Для виведення статистики протоколу TCPv6 у командній оболонці Window з допомогою інтерпретатора команд Cmd.exe викликаємо команду *netstat -s -p tcpv6*, де параметр [-p протокол] означає виведення підключень для зазнеченого протоколу, а [-s] - виведення статистики по протоколу.

Аналіз:

Виконавши команду *netstat [-p протокол] [-s],* я вивів на еран відображення активних підключень TCP, портів, що прослуховуються комп'ютером, статистики Ethernet, таблиці маршрутизації IP, статистики для протоколу TCPv6. Уся статистика зображена на скріншотах нижче.



**№3.2**

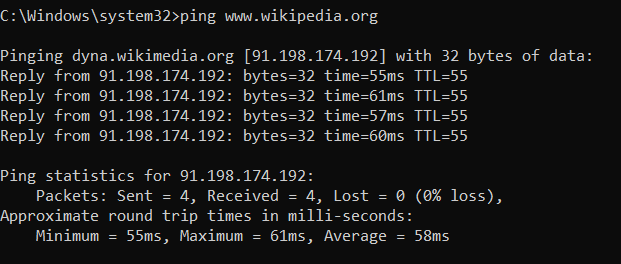
**Використовуючи команду ping перевірте з'єднання на рівні протоколу IP з адресами www.wikipedia.org, univ.kiev.ua та проаналізуйте отримані результати.**

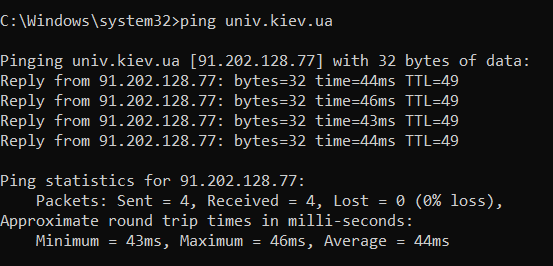
Для перевірки з'єднання на рівні протоколу IP з заданими адресами у командній оболонці Window з допомогою інтерпретатора команд Cmd.exe викликаємо команди *ping www.wikipedia.org* та *ping**univ.kiev.ua***.**

Аналіз:

Після кожної команди, ping відправив запити Echo-Request протоколу ICMP зазначеному вузлу мережі і зафіксував відповіді (ICMP Echo-Reply). Саме час між відправленням запиту й одержанням відповіді RTT дозволяє визначати двосторонні затримки RTT у маршруті й частоту втрати пакетів, тобто побічно визначати завантаженість каналів передачі даних і проміжних пристроїв.

Як бачимо, в обох випадках при відправленні усіх чотирьох пакетів, ping отримав відповідь RTT, тому відсоток втрати пакетів рівний нулю. На скріншотах видно час, затрачений для отримання кожної з відповідей. Середній час очікування склав 58 мс.

****

****

**№4**

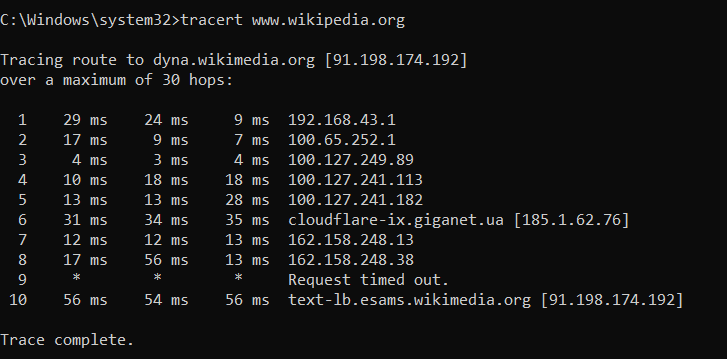
**Використовуючи команду *tracert* визначте шляхи до точок призначення www.wikipedia.org та univ.kiev.ua.**

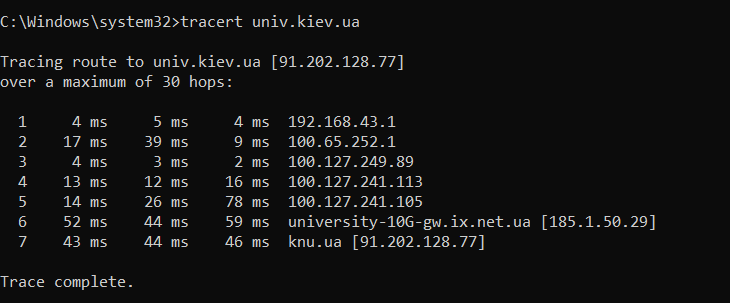
Для визначення шляхів до точок призначення у командній оболонці Window з допомогою інтерпретатора команд Cmd.exe викликаємо команди *tracert www.wikipedia.org* та *tracert univ.kiev.ua.*

Аналіз:

При кожному виконанні команд *tracert www.wikipedia.org* і *tracert univ.kiev.ua*я визначив маршрути слідування даних у мережах TCP/IP, а саме шлях до точки призначення за допомогою посилки в точку призначення «ехо-повідомлення» по протоколу Control Message Protocol (ICMP) з постійним збільшенням значеня терміну життя.

Виведений на скріншотах шлях – це список найближчих інтерфейсів маршрутизаторів, що знаходяться на шляху між вузлом джерелом і точкою призначення.





**№5**

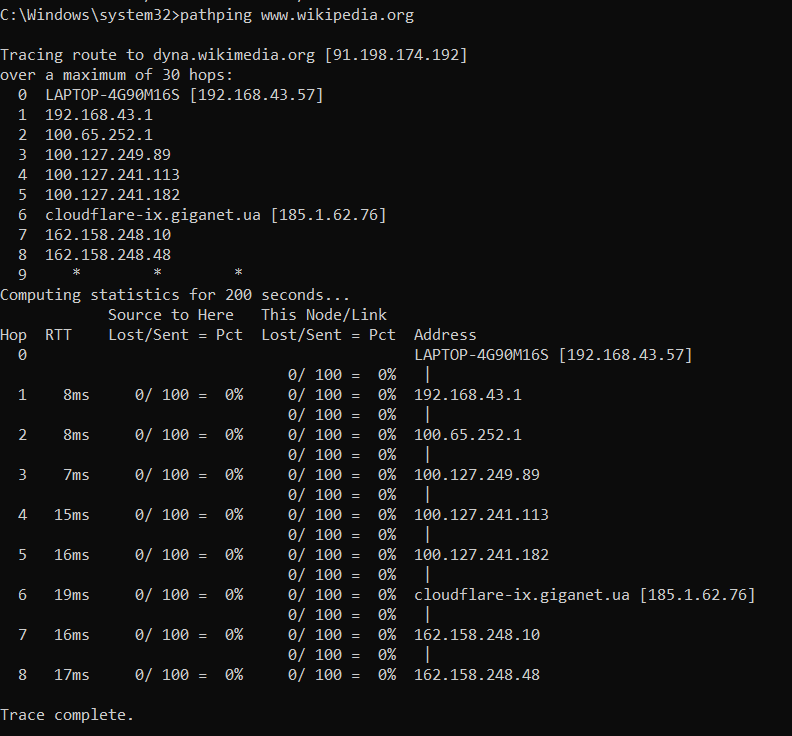
**Використовуючи команду *pathping* отримайте інформацію про латентності мережі та втрати даних на проміжних вузлах між вихідним пунктом і пунктом призначення. В якості пунктів призначення використайте адреси www.wikipedia.org та univ.kiev.ua.**

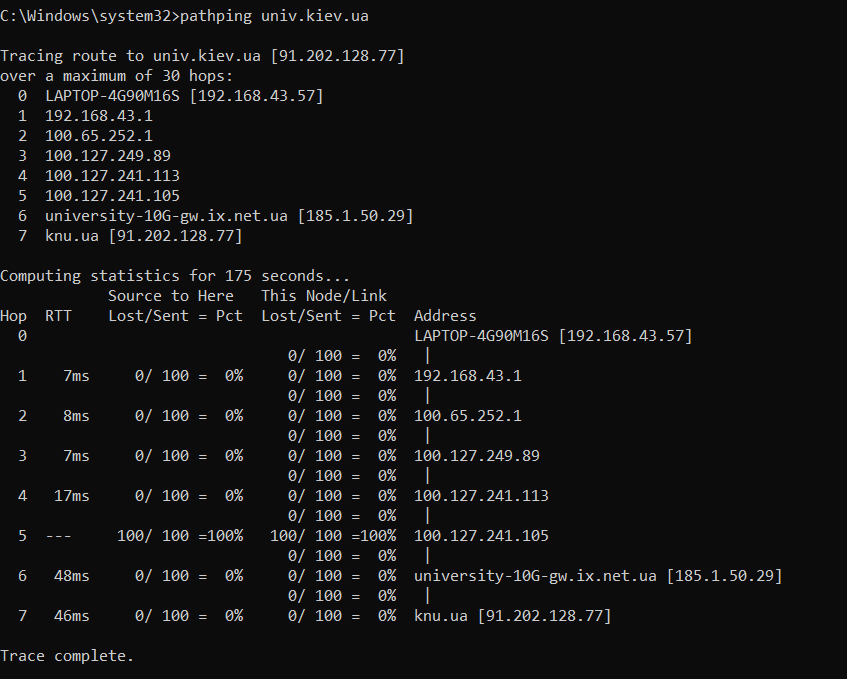
Для отримання інформації про латентності мережі та втрати даних на проміжних вузлах між вихідним пунктом і пунктом призначення у командній оболонці Window з допомогою інтерпретатора команд Cmd.exe викликаємо команди *pathping* *www.wikipedia.org* та *pathping* *univ.kiev.ua.*

Аналіз:

Команда *pathping* протягом деякого періоду часу відправляла численні повідомлення з «ехо-запитом» кожному маршрутизатору, що знаходиться між вихідним пунктом і пунктом призначення, а потім на підставі пакетів, отриманих від кожного з них, обчислила результати.

На скріншотах ми можемо побачити час, затрачений на очікування відвовіді RTT від кожного маршутизатора, та коефіцієнт втрати пакетів для кожного маршутеризатора. Майже у кожному випадку, відсоток втрачених пакетів дорівнює нулю, а лише в одному втрата пакетів рівна 100%, що означає що маршуризатор 100.127.241.105 швидше за все має певні блокування ехо-запитів брандмауера з міркувань безпеки.

****



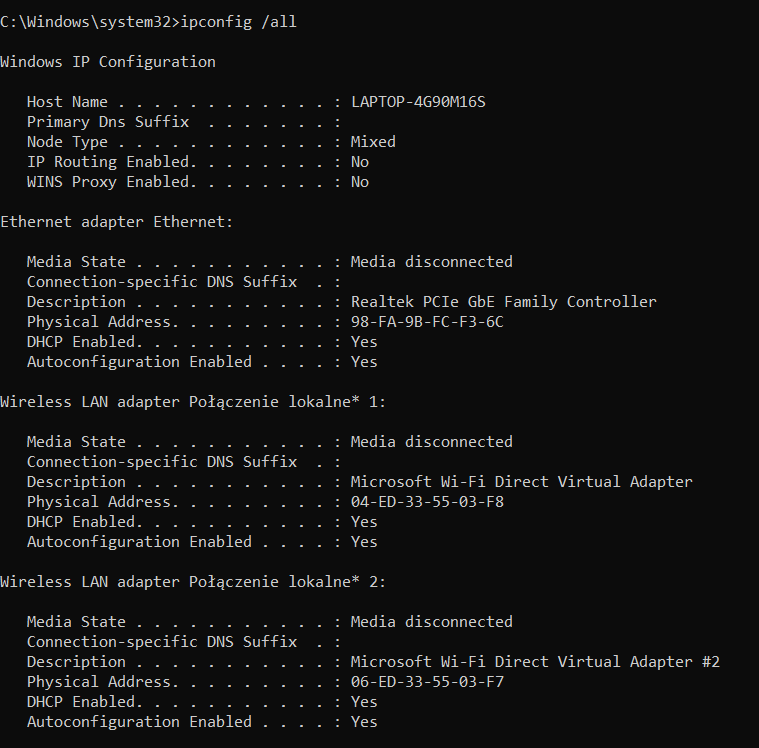
**№6**

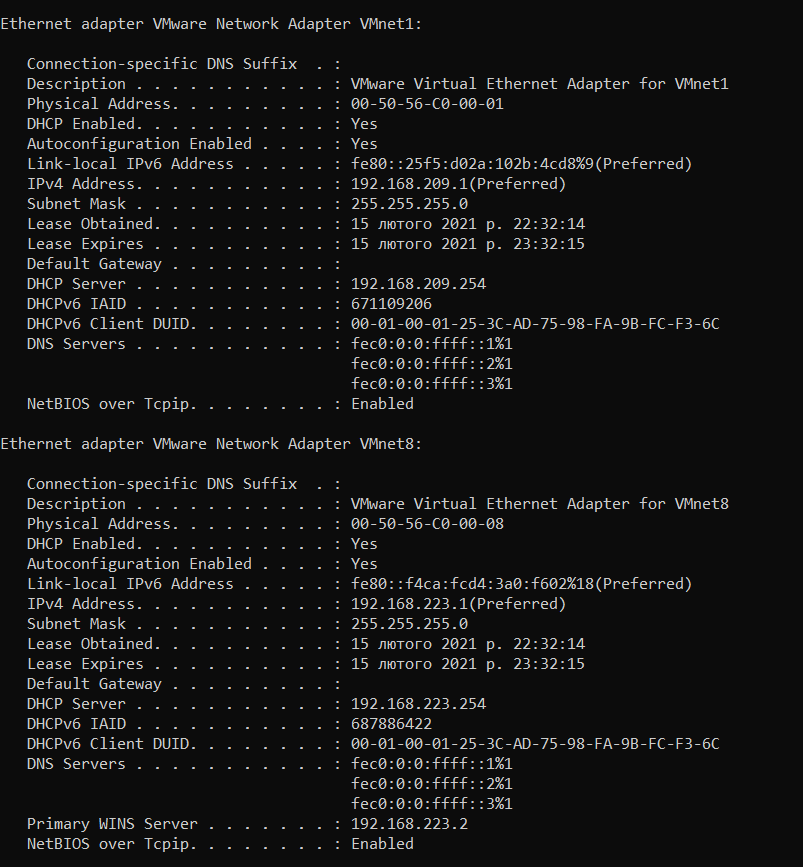
**Використовуючи команду *ipconfig* виведіть повну конфігурацію TCP/IP для всіх адаптерів.**

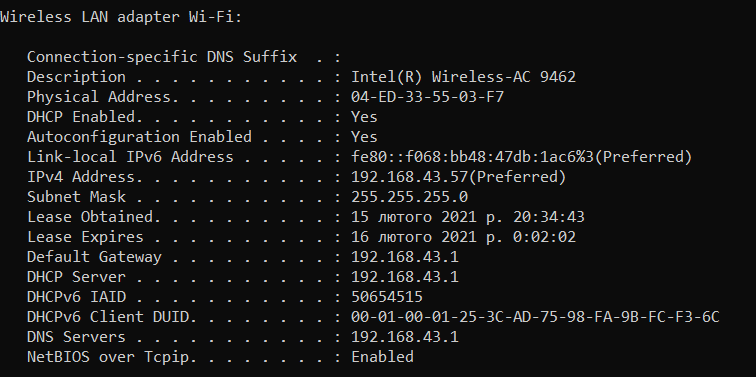
Для отримання повної конфігурації TCP/IP для всіх адаптерів у командній оболонці Window з допомогою інтерпретатора команд Cmd.exe викликаємо команду *ipconfig /all.*

Аналіз:

Дану команду використовують для виводу деталей поточного з'єднання і управління клієнтськими сервісами DHCP і DNS. Додатковий параметр [/all] дозволяє вивести повну конфігурації TCP/IP для всіх адаптерів. Результат виконання команди зображений на скрішотах нижче.







**Висновок:**

На даній лабораторній роботі я вивчив основні можливості командної оболонки та утиліт для дослідження мережевих параметрів. Спочатку я ознайомився з командними оболонками, а саме Cmd.exe на моїй операційній системі, дослідив можливість використання вкладених командних оболонок, ознайомився з використанням синтаксису команд, навчився використовувати декілька команд одним записом, та вивчив символи умовної обробки.

Виконуючи цю лабораторну роботу, я перевірив роботу локальної мережі засобами ОС.

Спочатку я використав команду для *netstat -s -p tcpv6* виведення статистики протоколу TCPv6, де параметр [-p протокол] означає виведення підключень для зазнеченого протоколу, а [-s] - виведення статистики по протоколу. Після виконання команди, на еран було відображено активні підключень TCP, порти, що прослуховуються комп'ютером, статистики Ethernet, таблиці маршрутизації IP, статистики для протоколу TCPv6.

Потім я використав команду *ping* для перевірки з'єднання на рівні протоколу IP з адресами www.wikipedia.org, univ.kiev.ua. Після кожної команди *ping www.wikipedia.org* і *ping univ.kiev.ua*, ping відправив запити Echo-Request протоколу ICMP зазначеному вузлу мережі і зафіксував відповіді (ICMP Echo-Reply). Саме час між відправленням запиту й одержанням відповіді RTT дозволяє визначати двосторонні затримки RTT у маршруті й частоту втрати пакетів, тобто побічно визначати завантаженість каналів передачі даних і проміжних пристроїв. В обох випадках при відправленні усіх чотирьох пакетів, ping отримав відповідь RTT, тому відсоток втрати пакетів рівний нулю. Середній час очікування склав 58 мс.

Команду *tracert* я використав для визначення шляхів до точок призначення www.wikipedia.org та univ.kiev.ua. При кожному виконанні команд *tracert www.wikipedia.org* і *tracert univ.kiev.ua*я визначив маршрути слідування даних у мережах TCP/IP, а саме шлях до точки призначення за допомогою посилки в точку призначення «ехо-повідомлення» по протоколу Control Message Protocol (ICMP) з постійним збільшенням значеня терміну життя.

Використовуючи команди *pathping* *www.wikipedia.org* та *pathping* *univ.kiev.ua,* я отримав інформацію про латентності мережі та втрати даних на проміжних вузлах між вихідним пунктом і пунктом призначення. Команда *pathping* протягом деякого періоду часу відправляла численні повідомлення з «ехо-запитом» кожному маршрутизатору, що знаходиться між вихідним пунктом і пунктом призначення, а потім на підставі пакетів, отриманих від кожного з них, обчислила результати. На скріншотах під відповідним завданням ми можемо побачити час, затрачений на очікування відвовіді RTT від кожного маршутизатора, та коефіцієнт втрати пакетів для кожного маршутеризатора. Майже у кожному випадку, відсоток втрачених пакетів дорівнює нулю, а лише в одному втрата пакетів рівна 100%, що означає що маршуризатор 100.127.241.105 швидше за все має певні блокування ехо-запитів брандмауера з міркувань безпеки

На кінець, використовуючи команду *ipconfig /all,* я вивів повну конфігурацію TCP/IP для всіх адаптерів. Дану команду використовують для виводу деталей поточного з'єднання і управління клієнтськими сервісами DHCP і DNS. Додатковий параметр [/all] дозволяє вивести повну конфігурації TCP/IP для всіх адаптерів.

Отже, на даній лабораторній роботі я вивчив основні можливості командної оболонки та утиліт для дослідження мережевих параметрів, та перевірив роботу локальної мережі засобами ОС з допомогою консольних команд *netstat, ping, tracert, pathping* та *ipconfig.*