

Міністерство освіти і науки України  
Львівський національний університет імені Івана Франка  
Факультет прикладної математики та інформатики  
Кафедра програмування

Звіт  
до лабораторної роботи №7  
з теми  
**“Аналіз IP-пакетів і повідомлень керуючих протоколів.  
Утиліти для діагностики мережі на мережевому рівні”**

Підготував:  
студент ПМІ-31  
Процьків Назарій

Львів 2023

## Хід роботи

1. Ознайомився з базовою мережевою конфігурацією свого комп'ютера, виконавши в консолі команду `ipconfig` та більше детальною конфігурацією за допомогою `ipconfig/all`:

```
C:\Users\Admin>ipconfig

Windows IP Configuration

Ethernet adapter Hamachi:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2620:9b::193b:a6f7
    Link-local IPv6 Address . . . . . : fe80::d530:dadd:388b:780d%2
    IPv4 Address. . . . . : 25.59.166.247
    Subnet Mask . . . . . : 255.0.0.0
    Default Gateway . . . . . : 2620:9b::1900:1
                                25.0.0.1

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::392c:56a9:52c0:5519%21
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Підключення через локальну мережу* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Підключення через локальну мережу* 12:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::d6ff:8b16:8024:3090%16
    IPv4 Address. . . . . : 192.168.222.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::aea4:7e96:9c75:5374%8
    IPv4 Address. . . . . : 192.168.223.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::28b7:3ab2:9099:c255%13
    IPv4 Address. . . . . : 192.168.1.9
    Subnet Mask . . . . . : 255.255.255.224
    Default Gateway . . . . . : 192.168.1.1
```

2. Команда `ipconfig/release` використовується для вивільнення поточного IP-адреси комп'ютера у мережі. При виклику цієї команди комп'ютер надсилає повідомлення до DHCP-сервера, який відповідає за призначення IP-адресу.

Після виклику команди /release комп'ютер втрачає свою поточну IP-адресу та будь-які інші налаштування мережі, пов'язані зі старою IP-адресою.

3. ipconfig/renew – команда, яка використовується для отримання нової IP-адреси від DHCP-сервера після того, як IP-адреса була вивільнена за допомогою команди /release.

Після виклику команди /renew комп'ютер надсилає запит до DHCP-сервера для отримання нової IP-адреси та інших налаштувань мережі.

Цією командою можна скористатись, коли потрібно змінити IP-адресу чи виправити проблеми з підключенням до мережі.

4. За допомогою команди netstat переглянув активні TCP-з'єднання

```
C:\Users\Admin>netstat
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	192.168.1.9:49414	20.199.120.182:https	ESTABLISHED
TCP	192.168.1.9:55222	149.154.167.51:http	TIME_WAIT
TCP	192.168.1.9:55228	bud02s38-in-f10:https	TIME_WAIT
TCP	192.168.1.9:55229	bud02s38-in-f10:https	TIME_WAIT
TCP	192.168.1.9:55230	149.154.167.51:https	ESTABLISHED
TCP	192.168.1.9:55238	149.154.175.100:http	TIME_WAIT
TCP	192.168.1.9:55241	lb-140-82-121-3-fra:https	ESTABLISHED
TCP	192.168.1.9:55245	158.120.16.74:https	ESTABLISHED
TCP	192.168.1.9:55246	158.120.16.201:12975	ESTABLISHED
TCP	192.168.1.9:55250	lb-140-82-121-3-fra:https	ESTABLISHED
TCP	192.168.1.9:55251	cdn-185-199-111-133:https	ESTABLISHED
TCP	192.168.1.9:55253	cdn-185-199-111-154:https	ESTABLISHED
TCP	192.168.1.9:55258	lu-in-f188:5228	ESTABLISHED
TCP	192.168.1.9:55259	104.26.9.101:https	ESTABLISHED
TCP	192.168.1.9:55260	104.26.9.101:https	ESTABLISHED
TCP	192.168.1.9:55263	cdn-185-199-109-133:https	ESTABLISHED

5. SYN\_SENT виникає, коли клієнт ініціює з'єднання, виславши сигнал SYN серверу.

ESTABLISHED позначає успішне встановлення з'єднання між клієнтом і сервером.

CLOSE\_WAIT вказує на те, що одна із сторін завершила передачу даних, але клієнт все ще може надсилати дані, чекаючи на сигнал від клієнта про готовність до закриття.

TIME\_WAIT виникає після закриття з'єднання.

5. При використанні netstat -n, відбувається вивід інформації, не виконуючи розгортання імен (hostname) та портів у числовому вигляді. Замість імен будуть показані числові представлення IP-адрес та номерів портів.

```
C:\Users\Admin>netstat -n
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	192.168.1.9:49414	20.199.120.182:443	ESTABLISHED
TCP	192.168.1.9:55230	149.154.167.51:443	ESTABLISHED
TCP	192.168.1.9:55245	158.120.16.74:443	ESTABLISHED
TCP	192.168.1.9:55246	158.120.16.201:12975	ESTABLISHED
TCP	192.168.1.9:55251	185.199.111.133:443	ESTABLISHED
TCP	192.168.1.9:55258	74.125.131.188:5228	ESTABLISHED
TCP	192.168.1.9:55260	104.26.9.101:443	ESTABLISHED
TCP	192.168.1.9:55265	34.120.195.249:443	ESTABLISHED
TCP	192.168.1.9:55266	140.82.121.6:443	LAST_ACK
TCP	192.168.1.9:55275	104.26.9.101:443	ESTABLISHED
TCP	192.168.1.9:55276	104.18.12.180:443	ESTABLISHED
TCP	192.168.1.9:55280	142.251.39.8:443	ESTABLISHED
TCP	192.168.1.9:55281	172.217.19.110:443	ESTABLISHED
TCP	192.168.1.9:55284	104.126.37.128:443	ESTABLISHED
TCP	192.168.1.9:55293	74.125.131.155:443	ESTABLISHED
TCP	192.168.1.9:55296	216.239.34.181:443	ESTABLISHED
TCP	192.168.1.9:55299	142.250.201.195:443	ESTABLISHED
TCP	192.168.1.9:55311	13.107.42.14:443	ESTABLISHED
TCP	192.168.1.9:55313	94.153.123.155:443	TIME_WAIT
TCP	192.168.1.9:55317	142.250.201.206:443	ESTABLISHED
TCP	192.168.1.9:55318	142.250.201.206:443	ESTABLISHED
TCP	192.168.1.9:55321	35.186.247.156:443	TIME_WAIT
TCP	192.168.1.9:55322	172.67.74.223:443	ESTABLISHED
TCP	192.168.1.9:55325	172.67.74.223:443	TIME_WAIT

Параметр -n вказує netstat виводити інформацію про всі з'єднання та прослуховуючі порти, включаючи ті, які знаходяться в стані listening.

Використання цього параметра допомагає побачити всі активні мережеві з'єднання та порти на комп'ютері.

```
C:\Users\Admin>netstat -a
```

### Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	genuine:0	LISTENING
TCP	0.0.0.0:445	genuine:0	LISTENING
TCP	0.0.0.0:902	genuine:0	LISTENING
TCP	0.0.0.0:912	genuine:0	LISTENING
TCP	0.0.0.0:5040	genuine:0	LISTENING
TCP	0.0.0.0:5357	genuine:0	LISTENING
TCP	0.0.0.0:5432	genuine:0	LISTENING
TCP	0.0.0.0:7680	genuine:0	LISTENING
TCP	0.0.0.0:49664	genuine:0	LISTENING
TCP	0.0.0.0:49665	genuine:0	LISTENING
TCP	0.0.0.0:49666	genuine:0	LISTENING
TCP	0.0.0.0:49667	genuine:0	LISTENING
TCP	0.0.0.0:49668	genuine:0	LISTENING
TCP	0.0.0.0:49670	genuine:0	LISTENING
TCP	127.0.0.1:5939	genuine:0	LISTENING
TCP	127.0.0.1:61573	genuine:0	LISTENING
TCP	192.168.1.9:139	genuine:0	LISTENING

## 6. Запустив Wireshark, почав захоплення пакетів. Вибрав пакет для аналізу.

4107 32.283897 52.123.129.14 192.168.1.9 TLSv1.2 1514 Application Data

> Frame 4107: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0  
> Ethernet II, Src: Tp-LinkT\_82:e4:e4 (c0:25:e9:82:e4:e4), Dst: IntelCor\_e8:ea:0e (40:1c:00:00:00:00)

Internet Protocol Version 4, Src: 52.123.129.14, Dst: 192.168.1.9

0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
> Differentiated Services Field: 0x80 (DSCP: CS4, ECN: Not-ECT)  
Total Length: 1500  
Identification: 0xb55d (46429)  
> 010. .... = Flags: 0x2, Don't fragment  
...0 0000 0000 0000 = Fragment Offset: 0  
Time to Live: 122  
Protocol: TCP (6)  
Header Checksum: 0xce03 [validation disabled]  
[Header checksum status: Unverified]  
Source Address: 52.123.129.14  
Destination Address: 192.168.1.9

> Transmission Control Protocol, Src Port: 443, Dst Port: 51939, Seq: 811754, Ack: 1870,  
> [6 Reassembled TCP Segments (8230 bytes): #4089(1135), #4090(1460), #4092(1460), #4105(1460)]

> Transport Layer Security

0000 40 1c 83 e8 ea 0e c0 25 e9 82 e4 e4 08 00 4b 80 @.....% .....  
0010 05 dc b5 5d 40 00 7a 06 ce 03 34 7b 81 0e c0 a8 ...]@z:..4{...  
0020 01 09 01 bb ca e3 3b ed cf 11 96 a0 df b7 50 18 .....;...P...  
0030 f9 78 43 44 00 00 76 a6 4a 91 e7 2f ed 02 67 a5 -xCD-v- J-/-g...  
0040 fb 15 11 76 1d d0 ac a8 bf 6c 19 3c 7e f7 25 37 --v-...-1<~%7...  
0050 31 1c 64 6d 3a 51 e6 44 70 3b 94 88 86 e9 51 0c 1-dm:Q-D p;...Q...  
0060 f3 e4 52 43 f2 7b 9c 0c 3b 5d 2e 16 10 33 6d cc --RC{...;]...3m...  
0070 14 ce 9f 70 16 96 8c aa ac d2 a5 eb a5 a3 76 4d --p-...-...vM...  
0080 bd df 15 b1 db ad 2b e8 05 ef 5f 50 10 14 cf f6 --...+...P-...  
0090 f7 21 b3 a0 58 6c 55 7b 81 ad 24 70 bc c4 5b 7b -q-XIU[ - \$p- [{  
00a0 11 21 55 6f 05 53 4c 7d 58 d4 ef ca 57 82 e9 56 -[Uo-SL] X--W-V...  
00b0 aa ef 69 eb 4e 9b a0 84 6b 58 89 bf a9 53 0b b2 -i-N-...kX--S-...  
00c0 8b 0b 71 ec af 0c bf de 34 09 80 83 a0 76 c6 3a -q-...-4-...v-...  
00d0 30 57 f4 24 7f d3 55 d7 83 1a 44 d9 ba 3f 06 48 0W-\$-U- -D-? H...  
00e0 ed f5 65 2d 11 88 00 78 c3 7b 54 d1 61 e8 a2 27 --e-...x -(T-a-...  
00f0 cb ec 96 dc 43 1a 61 50 c3 7b ca 6b 13 33 d0 9d --C-aP -(k-3-...  
0100 e1 59 19 18 82 89 2f 33 ba b9 c7 af 3c 60 2f 78 -Y-.../3 -...</x...  
0110 86 e3 e5 11 ba b4 74 c0 e3 b5 2f 7a da b8 a9 ea .....t-;/z-...  
0120 ed b0 dc 84 9f 91 ff 34 e7 5a cf d1 fe 37 fb 57 .....4-Z-...7-W...  
0130 ba 8b f6 ae 19 ab fb 93 d0 3a 8e 83 39 6e fa af .....-...9n-...  
0140 73 c3 8b 18 95 80 c0 a8 eb 6a 7e 86 2b c8 5c 6a s-...-j~+~\j...  
0150 f9 cc 02 58 78 df b3 d0 2b 70 a4 7b 40 40 8c 4d --X-...+pJ{@@M...  
0160 7b 5b 8e da 84 30 c4 0a a5 e8 a4 2b 10 40 b4 44 {[...0-...+@D...  
0170 aa ca 30 08 b4 89 ab 8a d0 c7 ae 4c bf 6d 6d 85 -0-...-...L-m-...  
0180 6b ba f8 45 1c 2a 04 e8 e3 33 46 84 1e f3 72 b7 k-E-\*...-3F-...r...  
0190 de 41 31 aa 23 88 f0 98 8c 24 da 4d e1 8d be 0a -A1-#-...-\$-M-...  
01a0 3a 8e 7f 50 26 61 96 b2 9f ac 4a 1e bb 57 a0 ed :-P&a-...-W-...

7. Клацнув на рядку Internet Protocol version 4 в області “Ієрархічний вміст пакета”. В області “Бітове подання” підсвітилися біти, які відповідають заголовку ІР-пакета:

4107 32.283897	52.123.129.14	192.168.1.9	TLSv1.2	1514 Application Data
> Frame 4107: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on inter				
> Ethernet II, Src: Tp-LinkT_82:e4:e4 (c0:25:e9:82:e4:e4), Dst: IntelCor_e8:ea:0e (40:1c				
✓ Internet Protocol Version 4, Src: 52.123.129.14, Dst: 192.168.1.9				
0100 .... = Version: 4				

8. Довжина заголовка: це 4-бітне поле, що вказує на розмір ІР-заголовка у 32-бітних блоках. Мінімальна довжина ІР-заголовка складає 20 байтів, тому у цьому полі можна бачити значення 5, бо 20 байтів це  $5 * 32$  біт. Максимальне можливе значення з 4 біт = 15, що відповідає довжині заголовка у 60 байтів, враховуючи 32-бітні інкременти. Це саме поле також називається IHL.

✓ Internet Protocol Version 4, Src: 52.123.129.14, Dst: 192.168.1.9

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

- > Differentiated Services Field: 0x80 (DSCP: CS4, ECN: Not-ECT)

Total Length: 1500

Identification: 0xb55d (46429)

- > 010. .... = Flags: 0x2, Don't fragment

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 122

Protocol: TCP (6)

Header Checksum: 0xce03 [validation disabled]

[Header checksum status: Unverified]

Source Address: 52.123.129.14

Destination Address: 192.168.1.9

9. Для знаходження розміру корисних даних у пакеті ІРv4, скористався полем Total Length у заголовку ІРv4. Це 16-бітне поле, яке вказує на загальну довжину пакета.

Загальний розмір пакета визначається як сума розміру заголовка та розміру корисних даних. Таким чином, розмір корисних даних можна знайти віднімаючи розмір заголовка від загальної довжини пакета.

- $1500 - 20 = 1480$  байт

10. Адреса відправника(52.123.129.14) – глобальна адреса, яка може вказувати на зовнішній пристрій

Адреса отримувача(192.168.1.9) - адреса мого Wifi-адаптера.

11. DSCP є розширенням ToS і використовує 6 бітів для кодування рівнів обслуговування. DSCP може включати як біти ToS, так і нові біти.

Загалом, DSCP складається з шести бітів, які використовуються для визначення класу обслуговування.

- a. Class Selector: Перші три біти вказують на клас обслуговування і можуть імітувати значення старих бітів ToS.
- b. Drop Probability (Ймовірність втрат): Це два біти, які можуть вказувати ймовірність втрат для пакета.
- c. Explicit Congestion Notification (ECN): Останній біт використовується для реалізації ECN, що дозволяє обмінюватися інформацією про перенавантаження в мережі.

```
▼ Differentiated Services Field: 0x80 (DSCP: CS4, ECN: Not-ECT)
  1000 00.. = Differentiated Services Codepoint: Class Selector 4 (32)
  .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 1500
Identification: 0xb55d (46429)
```

13. Цей пункт в мене не вийшло зробити, я пробував кілька разів, але зовсім не появлялись ніякі пакети протоколу DHCP. Тому я розглянув як цю секцію завдань (з цього по 17 пункт) зробив інший студент і пояснив це.

За допомогою фільтра bootp відобразив пакети протоколу DHCP.

bootp						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x16b8905c

14. IP-адреси відправника та отримувача у DHCP-запиті:

- a. Source: Зазвичай вказується 0.0.0.0 або IP-адреса самого клієнта, оскільки DHCP-клієнт ще не отримав IP-адресу від DHCP-сервера.
- b. Destination: Зазвичай вказується 255.255.255.255, оскільки DHCP-клієнт спрямовує свій запит на весь локальний підмережевий діапазон і намагається звернутися до будь-якого доступного DHCP-сервера.

```
▼ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
```

15. IP-адреси відправника та отримувача у DHCP-відповіді:

- c. Source: Це IP-адреса DHCP-сервера, який відправляє підтвердження клієнту.
- d. Destination: Це IP-адреса DHCP-клієнта, якому призначається IP-адреса та інші мережеві параметри.



## 16. Option 53: DHCP Message Type (Request)

Значення 3 вказує, що це DHCP-запит типу "Request". Клієнт просить підтвердження або оновлення своєї конфігурації IP.

### Option 61: Client Identifier

Вказує ідентифікатор клієнта, включаючи тип апаратного забезпечення (Ethernet) та MAC-адресу клієнта.

### Option 50: Requested IP Address

Вказує IP-адресу, яку клієнт запитує. У цьому випадку, 192.168.0.101.

### Option 12: Host Name

Вказує ім'я хоста клієнта. У цьому випадку, "DESKTOP-21Q2D8Q".

### Option 81: Client Fully Qualified Domain Name

Вказує повністю кваліфіковане доменне ім'я клієнта. У цьому випадку, "DESKTOP-21Q2D8Q".

### Option 60: Vendor Class Identifier

Вказує ідентифікатор вендора, у цьому випадку "MSFT 5.0".

### Option 55: Parameter Request List

Вказує список запитуваних параметрів від DHCP-сервера.

### Option 255: End

Вказує завершення списку опцій.



- ```

✓ Option: (53) DHCP Message Type (Request)
  Length: 1
  DHCP: Request (3)
✓ Option: (61) Client identifier
  Length: 7
  Hardware type: Ethernet (0x01)
  Client MAC address: IntelCor_71:31:21 (e4:a4:71:71:31:21)
✓ Option: (50) Requested IP Address (192.168.0.101)
  Length: 4
  Requested IP Address: 192.168.0.101
✓ Option: (12) Host Name
  Length: 15
  Host Name: DESKTOP-2IQ2D8Q
✓ Option: (81) Client Fully Qualified Domain Name
  Length: 18
  > Flags: 0x00
  A-RR result: 0
  PTR-RR result: 0
  Client name: DESKTOP-2IQ2D8Q
✓ Option: (60) Vendor class identifier
  Length: 8
  Vendor class identifier: MSFT 5.0
✓ Option: (55) Parameter Request List
  Length: 14
  Parameter Request List Item: (1) Subnet Mask
  Parameter Request List Item: (3) Router
  Parameter Request List Item: (6) Domain Name Server
  Parameter Request List Item: (15) Domain Name
  Parameter Request List Item: (31) Perform Router Discover
  Parameter Request List Item: (33) Static Route
  Parameter Request List Item: (43) Vendor-Specific Information
  Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
  Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
  Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
  Parameter Request List Item: (119) Domain Search
  Parameter Request List Item: (121) Classless Static Route
  Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
  Parameter Request List Item: (252) Private/Proxy autodiscovery
✓ Option: (255) End
  Option End: 255

```

16. За допомогою команди `hostname` переконався, що ім'я мого комп'ютеру співпадає з іменем у DHCP-запиті.

```
C:\>hostname
DESKTOP-2IQ2D8Q
```

## 17. Option 53: DHCP Message Type (ACK)

Значення 5 вказує, що це DHCP-підтвердження типу "АСК" (Acknowledgment). Це повідомлення підтверджує прийняття та надання ІР-адреси клієнту.

## Option 54: DHCP Server Identifier

Вказує IP-адресу DHCP-сервера, який надає підтвердження. У цьому випадку, 192.168.0.1.

Option 51: IP Address Lease Time

Вказує час, на який надається IP-адреса клієнту. У цьому випадку, 7200 секунд (2 години).

Option 1: Subnet Mask

Вказує маску підмережі для IP-адреси, яку клієнт отримав. У цьому випадку, 255.255.255.0.

Option 3: Router

Вказує IP-адресу маршрутизатора (шлюзу), який використовуватиметься клієнтом. У цьому випадку, 192.168.0.1.

Option 6: Domain Name Server

Вказує IP-адреси серверів DNS, які клієнт повинен використовувати. У цьому випадку, 192.168.0.1 та 0.0.0.0 (вказує, що DNS-сервер не визначено).

Option 255: End

Вказує завершення блоку опцій в DHCP-повідомленні. Після цієї опції не слід вказувати інші опції. "Padding" використовується для забезпечення того, що загальна довжина DHCP-повідомлення буде кратної певному розміру.

18. Реалізував перехоплення ICMP-пакетів за допомогою консольної утиліти ping.

```
C:\Users\Admin>ping youtube.com

Pinging youtube.com [172.217.19.110] with 32 bytes of data:
Reply from 172.217.19.110: bytes=32 time=26ms TTL=117
Reply from 172.217.19.110: bytes=32 time=54ms TTL=117
Reply from 172.217.19.110: bytes=32 time=220ms TTL=117
Request timed out.

Ping statistics for 172.217.19.110:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 220ms, Average = 100ms
```

19. Бачу непорожній результат при фільтруванні:



За допомогою задання TLL=1 я спробував отримати інший тип повідомлень

```
C:\Users\Admin>ping -i 1 youtube.com
```

```
Pinging youtube.com [142.250.186.206] with 32 bytes of data:  
Reply from 192.168.1.1: TTL expired in transit.  
Reply from 192.168.1.1: TTL expired in transit.  
Reply from 192.168.1.1: TTL expired in transit.  
Reply from 192.168.1.1: TTL expired in transit.
```

```
Ping statistics for 142.250.186.206:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Отримав повідомлення типу 11

|    |          |                   |                   |      |                                                                           |
|----|----------|-------------------|-------------------|------|---------------------------------------------------------------------------|
| 37 | 2.562505 | 192.168.1.1       | 192.168.1.9       | ICMP | 102 Time-to-live exceeded (Time to live exceeded in transit)              |
| 38 | 2.567255 | 192.168.1.1       | 192.168.1.9       | ICMP | 102 Time-to-live exceeded (Time to live exceeded in transit)              |
| 39 | 3.176685 | Tp-LinkT_82:e4:e4 | Broadcast         | ARP  | 42 Who has 192.168.1.9? Tell 192.168.1.1                                  |
| 40 | 3.176701 | IntelCor_e8:ea:0e | Tp-LinkT_82:e4:e4 | ARP  | 42 192.168.1.9 is at 40:1c:83:e8:ea:0e                                    |
| 41 | 3.565563 | 192.168.1.9       | 142.250.186.206   | ICMP | 74 Echo (ping) request id=0x0001, seq=20/5120, ttl=1 (no response found!) |

  

|                                                                                                       |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |          |          |          |
|-------------------------------------------------------------------------------------------------------|------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----------|----------|----------|
| > Frame 38: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF{...} | 0000 | 40 | 1c | 83 | e8 | ea | 0e | c0 | 25 | e9 | 82 | e4 | e4 | 08 | 00 | 45 | 00 | ...      | %        | .....E   |
| > Ethernet II, Src: Tp-LinkT_82:e4:e4 (c0:25:e9:82:e4:e4), Dst: IntelCor_e8:ea:0e (40:1c:83:e8:ea:0e) | 0010 | 00 | 58 | b6 | a6 | 00 | 00 | 40 | 01 | 3f | e4 | c0 | a8 | 01 | 01 | c0 | a8 | ...      | X        | .....?   |
| > Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.9                                     | 0020 | 01 | 09 | 0b | 00 | f4 | ff | 00 | 00 | 00 | 00 | 45 | 00 | 00 | 3c | b8 | 87 | ...      | .....E   | <...     |
| 0100 .... = Version: 4                                                                                | 0030 | 00 | 00 | 01 | 01 | f5 | bf | c0 | a8 | 01 | 09 | 8e | fa | ba | ce | 08 | 00 | ...      | .....    | .....    |
| .... 0101 = Header Length: 20 bytes (5)                                                               | 0040 | 4d | 48 | 00 | 01 | 00 | 13 | 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 6a | MH       | ....ab   | cdefghij |
| > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)                                       | 0050 | 6b | 6c | 6d | 6e | 6f | 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 61 | 62 | 63 | klmnopqr | stuvwabc | defghi   |
| Total Length: 88                                                                                      | 0060 | 64 | 65 | 66 | 67 | 68 | 69 |    |    |    |    |    |    |    |    |    |    |          |          |          |
| Identification: 0xb6a6 (46758)                                                                        |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |          |          |          |
| > 000. .... = Flags: 0x0                                                                              |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |          |          |          |
| ...0 0000 0000 0000 = Fragment Offset: 0                                                              |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |          |          |          |
| Time to Live: 64                                                                                      |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |          |          |          |
| Protocol: ICMP (1)                                                                                    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |          |          |          |
| Header Checksum: 0x3fe4 [validation disabled]                                                         |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |          |          |          |
| [Header checksum status: Unverified]                                                                  |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |          |          |          |
| Source Address: 192.168.1.1                                                                           |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |          |          |          |
| Destination Address: 192.168.1.9                                                                      |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |          |          |          |
| > Internet Control Message Protocol                                                                   |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |          |          |          |

22. Коли TTL встановлено на 1, це означає, що пакет може пройти лише через один маршрутизатор. Якщо цей маршрутизатор відправляє пакет назовні мережі (наприклад, ретранслює його на іншу мережу), він може обрати новий IP-адресу для цього пакета.

23. Визначив маршрут, яким проходять пакети від мого ноутбука до отримувача. Проходять 9 додаткових маршрутизаторів.

```

C:\Users\Admin>tracert youtube.com

Tracing route to youtube.com [142.250.186.206]
over a maximum of 30 hops:

  1    15 ms    9 ms    10 ms  192.168.1.1
  2     9 ms    14 ms    *      178-137-19-253.broadband.kyivstar.net [178.137.19.253]
  3    16 ms    58 ms    11 ms  74.125.32.161
  4    13 ms    14 ms    13 ms  74.125.32.160
  5    19 ms    21 ms    40 ms  108.170.248.155
  6     *       25 ms    29 ms  142.251.242.39
  7   200 ms    24 ms    29 ms  142.250.37.193
  8   218 ms    37 ms    41 ms  142.250.239.81
  9    32 ms    28 ms    35 ms  waw07s05-in-f14.1e100.net [142.250.186.206]

Trace complete.

```

24. Утиліта `tracert` використовує ICMP-пакети для відстеження маршруту до пункту призначення. Кожен пакет має поле TTL (Time to Live), яке визначає, скільки маршрутизаторів може пройти пакет перед викиданням. Починаючи з  $TTL = 1$ , кожен маршрутизатор, через який проходить пакет, зменшує TTL на одиницю, і якщо TTL стає рівним нулю, маршрутизатор відкидає пакет та надсилає повідомлення про помилку назад.

|     |           |                 |                 |      |                                                                             |
|-----|-----------|-----------------|-----------------|------|-----------------------------------------------------------------------------|
| 478 | 25.811108 | 192.168.1.9     | 142.250.186.206 | ICMP | 106 Echo (ping) request id=0x0001, seq=65/16640, ttl=5 (no response found!) |
| 479 | 25.821754 | 108.170.248.155 | 192.168.1.9     | ICMP | 70 Time-to-live exceeded (Time to live exceeded in transit)                 |
| 480 | 25.823482 | 192.168.1.9     | 142.250.186.206 | ICMP | 106 Echo (ping) request id=0x0001, seq=66/16896, ttl=5 (no response found!) |
| 481 | 25.887203 | 108.170.248.155 | 192.168.1.9     | ICMP | 70 Time-to-live exceeded (Time to live exceeded in transit)                 |
| 482 | 25.889279 | 192.168.1.9     | 142.250.186.206 | ICMP | 106 Echo (ping) request id=0x0001, seq=67/17152, ttl=5 (no response found!) |
| 483 | 25.906978 | 108.170.248.155 | 192.168.1.9     | ICMP | 70 Time-to-live exceeded (Time to live exceeded in transit)                 |

25. Утиліта `ping`, зазвичай, не надає повний маршрут, який пакет проходить від джерела до призначення. Проте, існують параметри та інші інструменти, які дозволяють отримати додаткову інформацію про маршрут. Команда "`ping -r 5 youtube.com`" вказує, що пакет Ping буде містити інформацію про проміжні маршрутизатори для перших 5 етапів маршруту. Важливо врахувати, що якщо маршрут має більше 5 проміжних маршрутизаторів, інформація про них не буде включена в вивід.