ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА

Факультет прикладної математики та інформатики

Комп'ютерні інформаційні мережі

ЛАБОРАТОРНА РОБОТА №7

Виконав :

Ст *Гуменюк С. А.*

ПМІ -33

2024

Тема: Аналіз повідомлень канального рівня Ethernet засобами WireShark. Утиліти для діагностики мережі на канальному рівні

Мета роботи: Здобути практичні навички з інтерпретації Ethernet-кадрів та використання консольних утиліт для діагностики мережі на рівні мережевих інтерфейсів.

Хід роботи

1. Базова мережева конфігурація мого ПК

```
sonorma@hellcat:~$ sudo ifconfig wlp2s0
wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.50.66  netmask 255.255.255.0  broadcast 192.168.50.255
        inet6 fe80::cb28:85b7:b33c:2c94  prefixlen 64  scopeid 0x20<link>
        ether 14:13:33:36:7e:7d  txqueuelen 1000  (Ethernet)
        RX packets 71537  bytes 76474510 (72.9 MiB)
        RX errors 0  dropped 252  overruns 0  frame 0
        TX packets 31148  bytes 8183411 (7.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Активні TCP з'єднання:

```
sonorma@hellcat:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 hellcat:52684           server-18-66-231-:https ESTABLISHED
tcp        0      0 hellcat:47274           188.114.96.11:https     ESTABLISHED
tcp        0      0 hellcat:37654           52.123.135.7:https      ESTABLISHED
tcp        0      0 hellcat:39840           104.21.27.152:https     ESTABLISHED
tcp        0      0 hellcat:52214           52.111.236.12:https     ESTABLISHED
tcp        0      0 hellcat:36524           li1398-20.members:https ESTABLISHED
tcp        0      0 hellcat:45218           par10s21-in-f202.:https ESTABLISHED
tcp       76      0 hellcat:60978           151.101.245.91:https    CLOSE_WAIT
tcp        0      0 hellcat:36546           li1398-20.members:https ESTABLISHED
tcp        0      0 hellcat:34900           93.243.107.34.bc.:https ESTABLISHED
tcp        0      0 hellcat:52734           server-18-66-231-:https ESTABLISHED
tcp        0      0 hellcat:60524           149.154.167.41:https    ESTABLISHED
tcp        0      0 hellcat:49788           40.99.210.2:https       ESTABLISHED
tcp        0      0 hellcat:47550           140.227.186.35.bc:https ESTABLISHED
tcp        0      0 hellcat:32896           waw07s02-in-f3.1e:https ESTABLISHED
tcp        0      0 hellcat:53508           server-18-245-65-2:http TIME_WAIT
tcp        0      0 hellcat:48252           lb-140-82-112-25-:https ESTABLISHED
tcp        0      0 hellcat:49556           52.111.209.6:https      ESTABLISHED
tcp        0      0 hellcat:41616           172.64.41.4:https       ESTABLISHED
tcp        0      0 hellcat:36558           li1398-20.members:https ESTABLISHED
tcp        0      0 hellcat:38630           waw02s22-in-f3.1e1:http TIME_WAIT
tcp       76      0 hellcat:60960           151.101.245.91:https    CLOSE_WAIT
tcp        0      0 hellcat:42986           209.100.149.34.bc:https ESTABLISHED
tcp        0      0 hellcat:50574           ec2-34-237-73-95.:https ESTABLISHED
tcp        0      0 hellcat:54910           rd-in-f84.1e100.n:https ESTABLISHED
tcp        0      0 hellcat:38462           par10s21-in-f196.:https ESTABLISHED
tcp        0      0 hellcat:54914           a2-16-172-18.deplo:http ESTABLISHED
tcp        0      0 hellcat:41330           192.168.50.251:1716     ESTABLISHED
tcp        0      0 hellcat:36504           li1398-20.members:https ESTABLISHED
tcp        0      0 hellcat:47988           191.144.160.34.bc:https ESTABLISHED
tcp       64      0 hellcat:38558           876603927.war.cdn:https CLOSE_WAIT
tcp        0      0 hellcat:35686           rd-in-f84.1e100.n:https ESTABLISHED
tcp        0      0 hellcat:47224           104.22.26.181:https     ESTABLISHED
tcp        0      0 hellcat:35436           52.123.134.245:https    ESTABLISHED
tcp        0      0 hellcat:49370           waw07s03-in-f10.1:https TIME_WAIT
tcp        0      0 hellcat:34706           188.114.97.11:https     ESTABLISHED
tcp        0      0 hellcat:36508           li1398-20.members:https ESTABLISHED
tcp        0      0 hellcat:38446           par10s21-in-f196.:https ESTABLISHED
tcp        0      0 hellcat:46270           waw07s05-in-f10.1:https ESTABLISHED
tcp        0      0 hellcat:33720           server-3-165-206-:https ESTABLISHED
tcp        0      0 hellcat:36530           li1398-20.members:https ESTABLISHED
udp        0      0 hellcat:bootpc          RT-AX55-FCB8:bootps     ESTABLISHED
```

Основні стани TCP:

1. LISTEN - порт відкритий, очікує з'єднань
2. SYN_SENT - відправлено запит на з'єднання
3. SYN_RECEIVED - отримано запит, відправлено підтвердження
4. ESTABLISHED - з'єднання активне
5. FIN_WAIT_1/2 - очікування завершення з'єднання
6. TIME_WAIT - очікує очищення мережевих буферів
7. CLOSE_WAIT - віддалена сторона ініціювала закриття
8. LAST_ACK - очікує фінального підтвердження
9. CLOSED - з'єднання закрите

Команди netstat:
netstat -n:

- Числові адреси замість імен
- Швидша робота
- Без резолву DNS

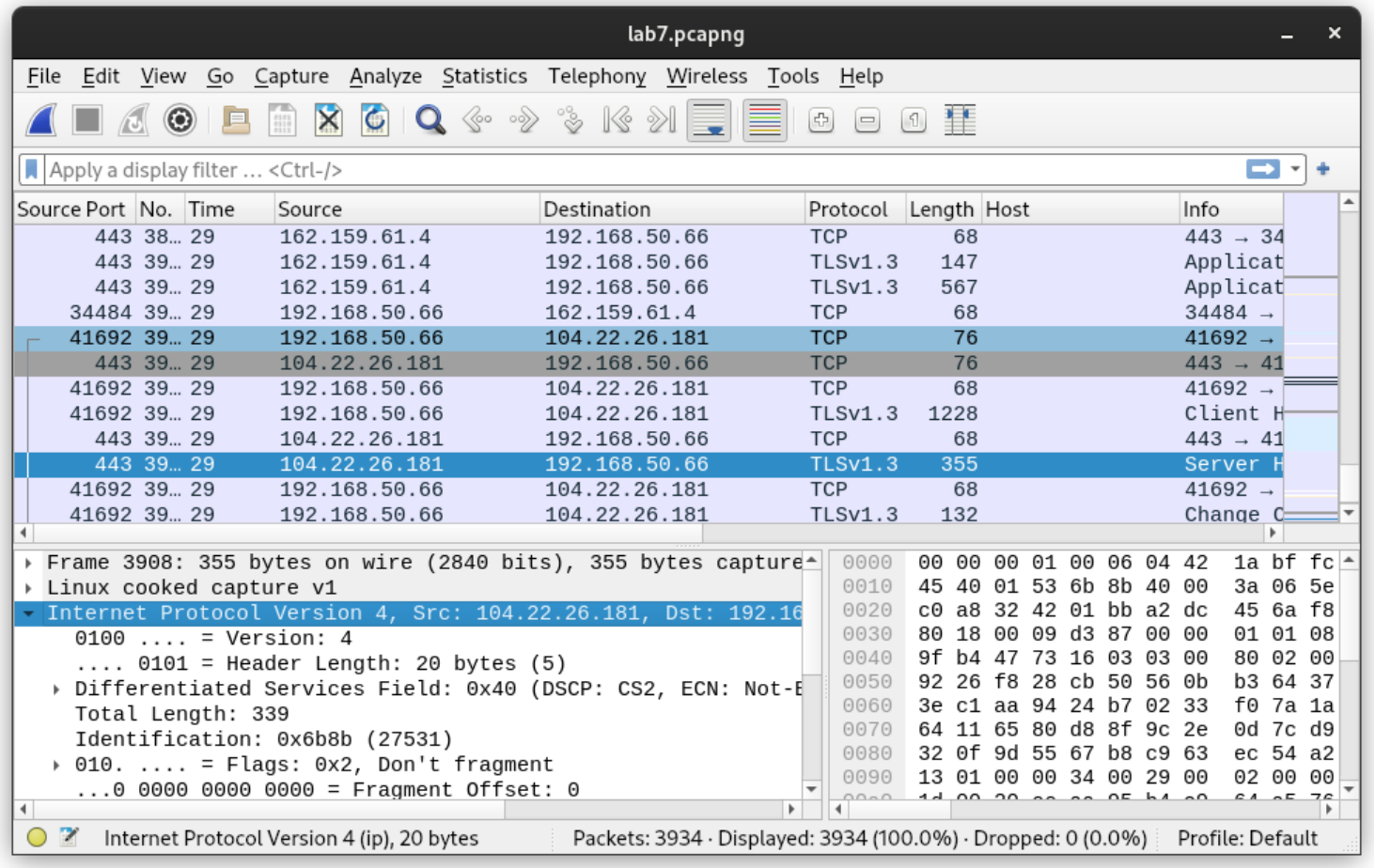
netstat -a:

- Всі з'єднання та порти
- Включає стан LISTEN
- Показує UDP-порти

3. Статистика

```
sonorma@hellcat:~$ netstat -s
Ip:
    Forwarding: 1
    47887 total packets received
    1 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    46239 incoming packets delivered
    32754 requests sent out
    28 outgoing packets dropped
    9 dropped because of missing route
    3 fragments dropped after timeout
    37 reassemblies required
    17 packets reassembled ok
    3 packet reassemblies failed
    609 outgoing packets fragmented ok
    1218 fragments created
Icmp:
    64 ICMP messages received
    0 input ICMP message failed
    ICMP input histogram:
        destination unreachable: 64
    110 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 110
IcmpMsg:
        InType3: 64
        OutType3: 110
Tcp:
    444 active connection openings
    2 passive connection openings
    2 failed connection attempts
    76 connection resets received
    24 connections established
    36840 segments received
    30093 segments sent out
    38 segments retransmitted
    0 bad segments received
    270 resets sent
```

4. Інформація про вибраний пакет:



Різниця в інтерпретації полів IPv4 заголовка:
Поле Version (0100 = 4)

- Біти 0100 дають число 4
- Використовується як є для позначення версії IPv4

Поле Header Length (0101 = 5)

- Біти 0101 дають число 5
- Вимірюється в 32-бітних словах (4 байти)
- Тому 5 * 4 = 20 байт реальної довжини заголовка
- Таке кодування економить місце, бо довжина завжди кратна 4

Тобто Version використовує пряме значення, а Header Length множиться на 4 для отримання реальної довжини в байтах.

Для визначення розміру корисних даних:

1. Total Length (загальна довжина пакету) = 339 байт
2. Відняти IP заголовок = 20 байт

339 - 20 = 319 байт

Аналіз IP-адрес:
Відправник (Source): 104.22.26.181

- Це публічна IP-адреса
- Належить до глобальної мережі Інтернет

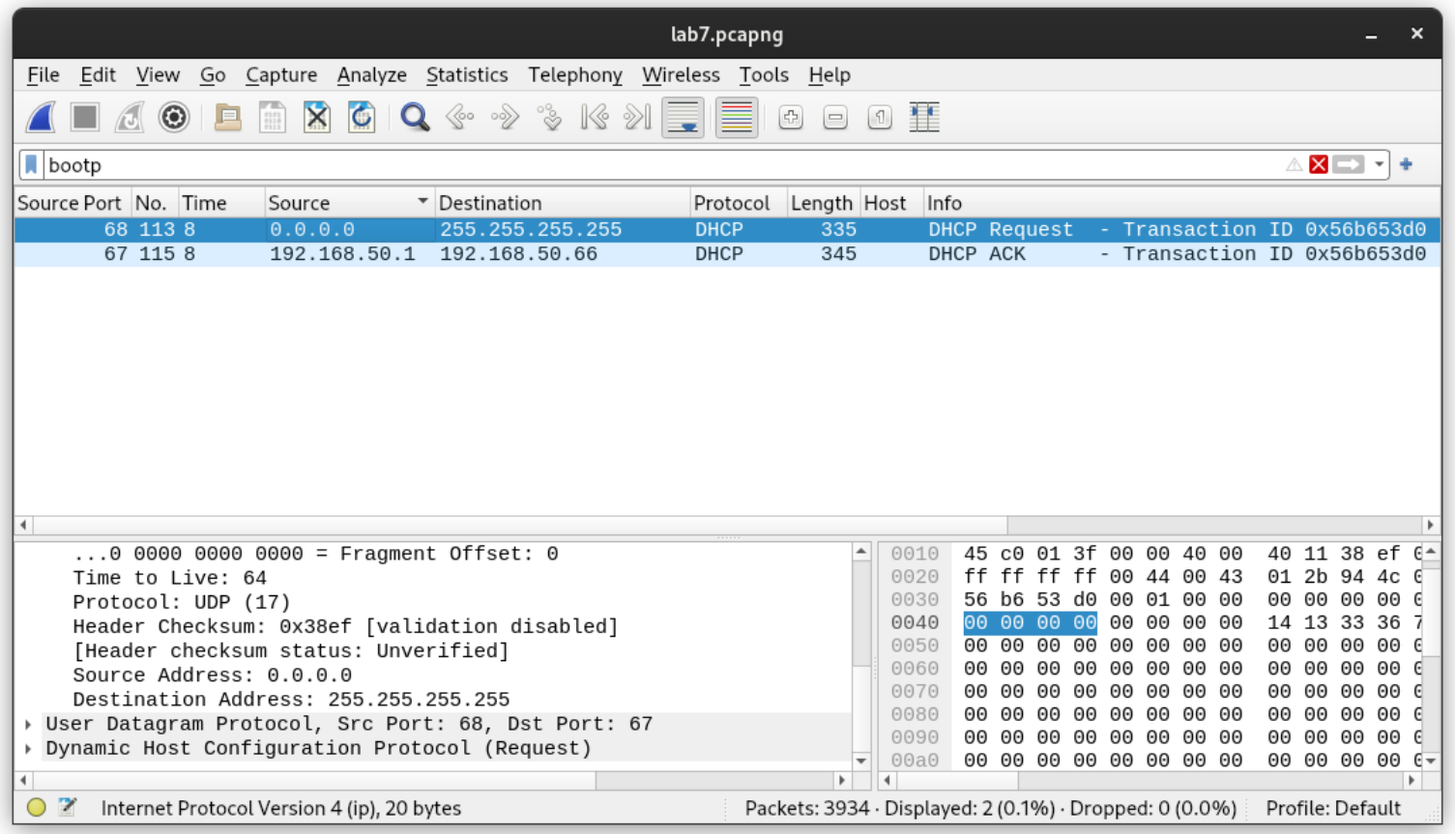
Одержувач (Destination): 192.168.50.66

- Це приватна IP-адреса з діапазону 192.168.0.0/16
- Використовується в локальних мережах
- Не маршрутизується в Інтернеті

Отже, пакет надсилається з публічної мережі Інтернет до комп'ютера в локальній мережі.

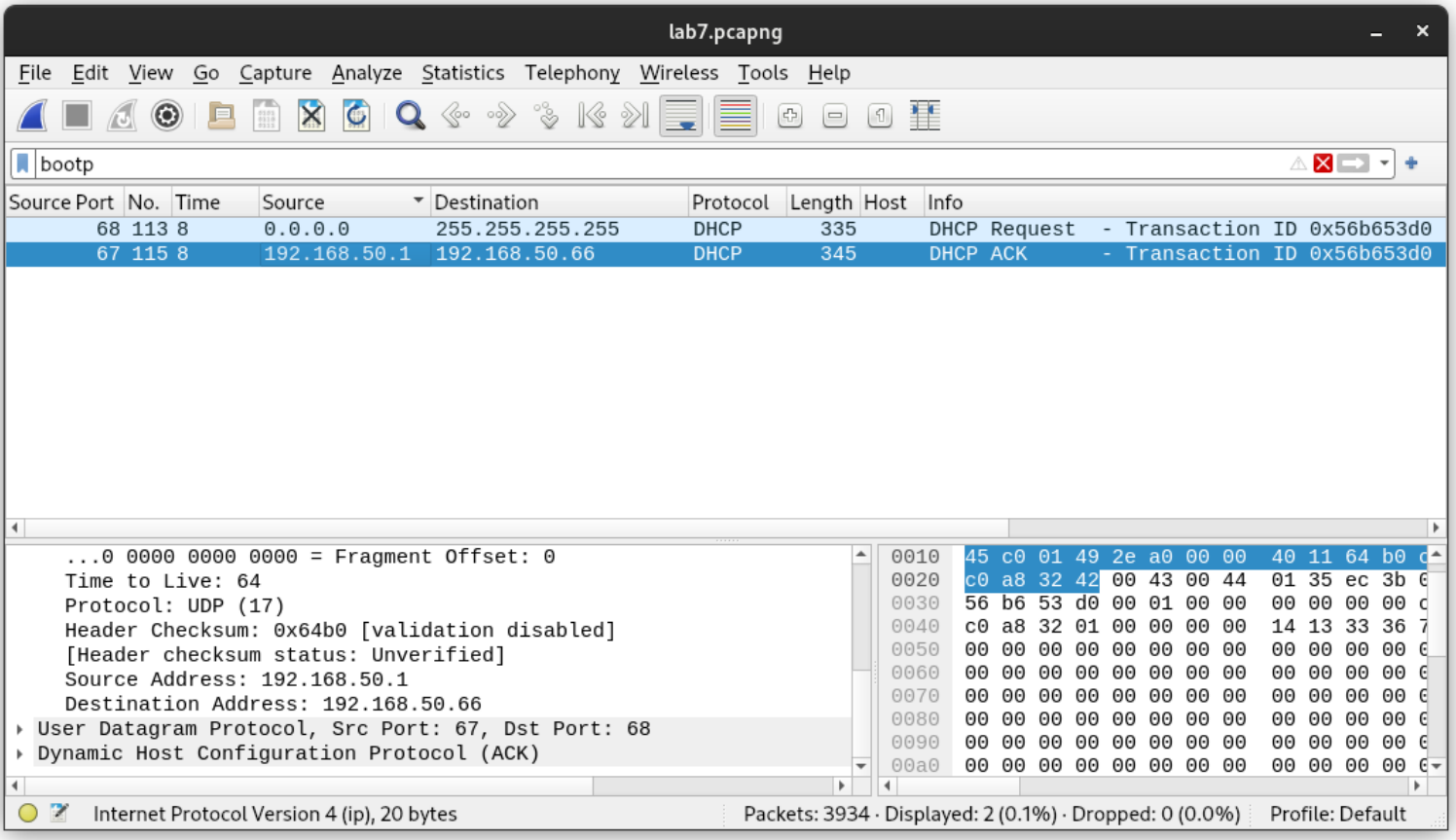
Поле Differentiated Services Field (DSCP) складається з двох частин:

- DSCP (6 біт) – визначає клас обслуговування пакета (QoS). У моєму випадку 010000 відповідає Class Selector 2 (CS2).
- ECN (2 біти) – використовується для сигналізації перевантаження мережі. У моєму випадку 00 означає, що пакет не підтримує ECN (Not ECN-Ca p-able).



В DHCP-запиті:

- IP-адреса відправника: 0.0.0.0 — клієнт ще не має IP-адреси.
- IP-адреса отримувача: 255.255.255.255 — широкомовна адреса для того, щоб запросити IP-адресу від DHCP-сервера, оскільки клієнт не знає його точну адресу.



У DHCP ACK:

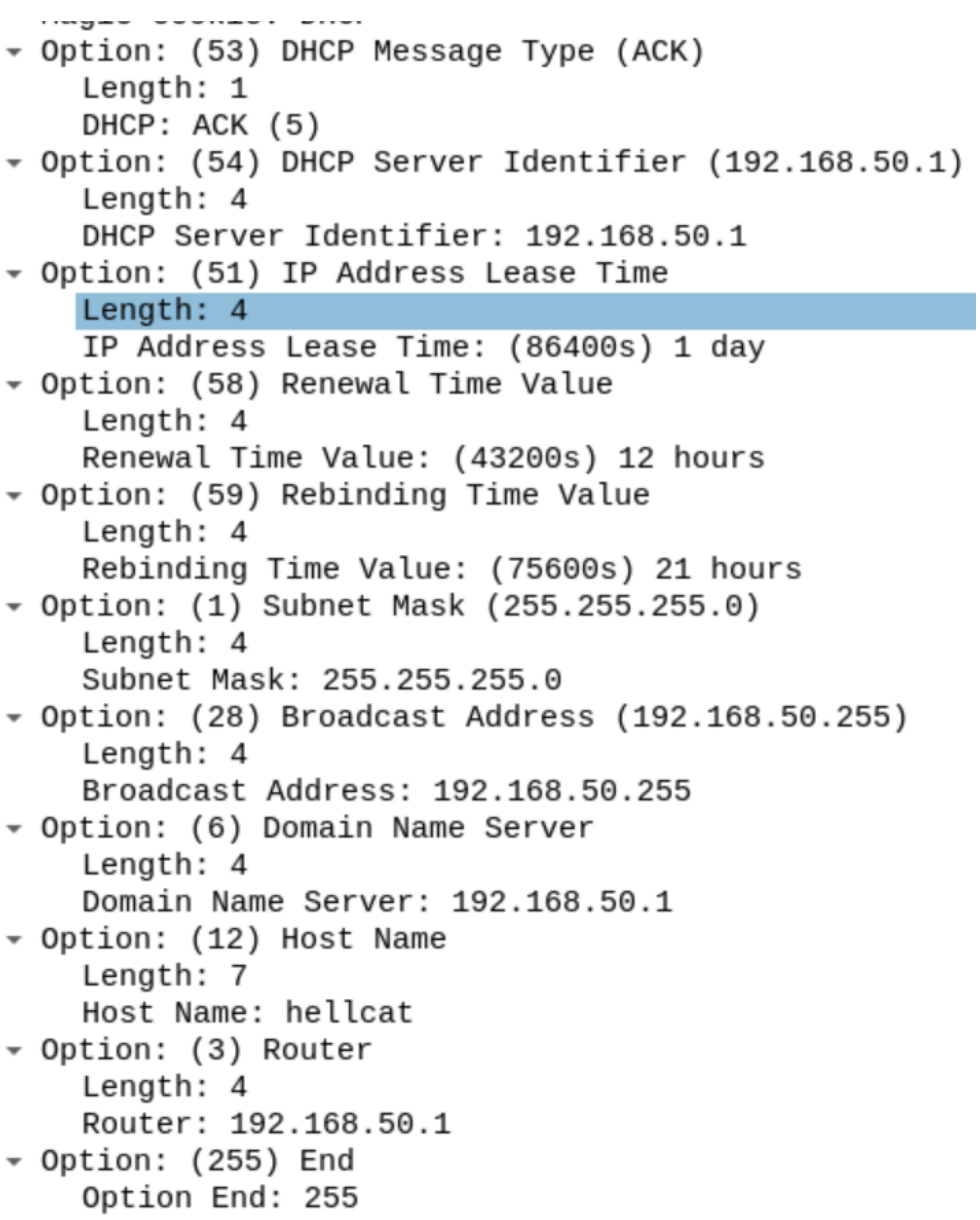
- IP-адреса відправника: 192.168.50.1 — це адреса DHCP-сервера, який підтверджує запит.
- IP-адреса отримувача: 192.168.50.66 — це нова адреса, виділена клієнту (DHCP ACK повідомляє клієнту про успішне призначення цієї IP-адреси).

```
Magic cookie: DHCP
▾ Option: (53) DHCP Message Type (Request)
    Length: 1
    DHCP: Request (3)
▾ Option: (61) Client identifier
    Length: 7
    Hardware type: Ethernet (0x01)
    Client MAC address: AzureWav_36:7e:7d (14:13:33:36:7e:7d)
▾ Option: (55) Parameter Request List
    Length: 17
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (2) Time Offset
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (12) Host Name
    Parameter Request List Item: (15) Domain Name
    Parameter Request List Item: (26) Interface MTU
    Parameter Request List Item: (28) Broadcast Address
    Parameter Request List Item: (121) Classless Static Route
    Parameter Request List Item: (3) Router
    Parameter Request List Item: (33) Static Route
    Parameter Request List Item: (40) Network Information Service Domain
    Parameter Request List Item: (41) Network Information Service Servers
    Parameter Request List Item: (42) Network Time Protocol Servers
    Parameter Request List Item: (119) Domain Search
    Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
    Parameter Request List Item: (252) Private/Proxy autodiscovery
    Parameter Request List Item: (17) Root Path
▾ Option: (57) Maximum DHCP Message Size
    Length: 2
    Maximum DHCP Message Size: 576
▾ Option: (50) Requested IP Address (192.168.50.66)
    Length: 4
    Requested IP Address: 192.168.50.66
▾ Option: (12) Host Name
    Length: 7
    Host Name: hellcat
▾ Option: (255) End
    Option End: 255
```

1. **Magic cookie: DHCP** - стандартний заголовок DHCP-повідомлення
2. **Option (53) DHCP Message Type:** Тип повідомлення: Request (3) - це запит від клієнта
3. **Option (61) Client identifier:**
    - Тип обладнання: Ethernet (0x01)
    - MAC-адреса клієнта: AzureWav_36:7e:7d (14:13:33:36:7e:7d)
4. **Option (55) Parameter Request List:** Клієнт запитує наступні параметри:
    - Subnet Mask - маска підмережі
    - Time Offset - часовий зсув
    - Domain Name Server - DNS-сервер
    - Host Name - ім'я хоста
    - Domain Name - доменне ім'я
    - Interface MTU - максимальний розмір пакету
    - Broadcast Address - широкомовна адреса
    - Classless Static Route - статичні маршрути
    - Router - маршрутизатор
    - Static Route - статичний маршрут
    - Network Information Service Domain - домен NIS
    - Network Information Service Servers - сервери NIS
    - Network Time Protocol Servers - сервери NTP
    - Domain Search - пошук домену
    - Private/Classless Static Route - приватні статичні маршрути Microsoft
    - Private/Proxy autodiscovery - автовиявлення проксі
    - Root Path - кореневий шлях

```
sonorma@hellcat:~$ hostname
hellcat
```

5. **Option (57) Maximum DHCP Message Size:** Максимальний розмір повідомлення: 576 байт
6. **Option (50) Requested IP Address:** Запитувана IP-адреса: 192.168.50.66
7. **Option (12) Host Name:** Ім'я хоста: hellcat
8. **Option (255) End:** Позначає кінець DHCP-повідомлення



1. **Option (53) DHCP Message Type:** Тип повідомлення: ACK (5) - підтвердження від сервера
2. **Option (54) DHCP Server Identifier:** IP-адреса DHCP сервера: 192.168.50.1
3. **Option (51) IP Address Lease Time:** Час оренди IP-адреси: 86400 секунд (1 день)
4. **Option (58) Renewal Time Value:** Час оновлення: 43200 секунд (12 годин)
5. **Option (59) Rebinding Time Value:** Час перез'єднання: 75600 секунд (21 година)
6. **Option (1) Subnet Mask:** Маска підмережі: 255.255.255.0
7. **Option (28) Broadcast Address:** Широкомовна адреса: 192.168.50.255
8. **Option (6) Domain Name Server:** DNS-сервер: 192.168.50.1
9. **Option (12) Host Name:** Ім'я хоста: hellcat
10. **Option (3) Router:** Маршрутизатор (шлюз): 192.168.50.1
11. **Option (255) End:** Позначає кінець DHCP-повідомлення

```
sonorma@hellcat:~$ ping google.com
PING google.com (142.250.203.206) 56(84) bytes of data.
64 bytes from waw02s22-in-f14.1e100.net (142.250.203.206): icmp_seq=1 ttl=117 time=22.8 ms
64 bytes from waw02s22-in-f14.1e100.net (142.250.203.206): icmp_seq=2 ttl=117 time=22.6 ms
64 bytes from waw02s22-in-f14.1e100.net (142.250.203.206): icmp_seq=3 ttl=117 time=48.6 ms
64 bytes from waw02s22-in-f14.1e100.net (142.250.203.206): icmp_seq=4 ttl=117 time=23.1 ms
64 bytes from waw02s22-in-f14.1e100.net (142.250.203.206): icmp_seq=5 ttl=117 time=41.9 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 22.601/31.790/48.563/11.176 ms
```

```
sonorma@hellcat:~$ nslookup google.com
Server:         192.168.50.1
Address:        192.168.50.1#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.203.206
Name:   google.com
Address: 2a00:1450:401b:80e::200e
```

Source Port	No.	Time	Source	Destination	Protocol	Length	Host	Info
	47	1	192.168.50.66	142.250.203.206	ICMP	98		Echo (ping) request id=0xfa1e, seq=1/256, ttl=64 (reply in 48)
	48	1	142.250.203.206	192.168.50.66	ICMP	98		Echo (ping) reply id=0xfa1e, seq=1/256, ttl=117 (request in 47)
	465	2	192.168.50.66	142.250.203.206	ICMP	98		Echo (ping) request id=0xfa1e, seq=2/512, ttl=64 (reply in 466)
	466	2	142.250.203.206	192.168.50.66	ICMP	98		Echo (ping) reply id=0xfa1e, seq=2/512, ttl=117 (request in 465)
	469	3	192.168.50.66	142.250.203.206	ICMP	98		Echo (ping) request id=0xfa1e, seq=3/768, ttl=64 (reply in 470)
	470	3	142.250.203.206	192.168.50.66	ICMP	98		Echo (ping) reply id=0xfa1e, seq=3/768, ttl=117 (request in 469)
	477	4	192.168.50.66	142.250.203.206	ICMP	98		Echo (ping) request id=0xfa1e, seq=4/1024, ttl=64 (reply in 478)
	478	4	142.250.203.206	192.168.50.66	ICMP	98		Echo (ping) reply id=0xfa1e, seq=4/1024, ttl=117 (request in 477)
	490	5	192.168.50.66	142.250.203.206	ICMP	98		Echo (ping) request id=0xfa1e, seq=5/1280, ttl=64 (reply in 491)
	491	5	142.250.203.206	192.168.50.66	ICMP	98		Echo (ping) reply id=0xfa1e, seq=5/1280, ttl=117 (request in 490)

TTL (Time To Live) в пакетах різний, тому що:

1. **Різні системи ставлять різні стартові значення TTL:**
   - Linux дає TTL=64 (це видно в запитах)
   - Windows зазвичай ставить TTL=128
   - Роутери можуть ставити TTL=255
2. **В нашому прикладі:**
   - Наш комп (192.168.50.66) працює на Linux, тому відправляє пакети з TTL=64
   - Сервер Google (142.250.203.206) ставить інший TTL, і коли пакет йде назад через роутери, значення зменшується до 117

Тобто кожен ставить своє початкове значення TTL, а потім воно зменшується на 1, коли проходить через кожен роутер на шляху. Тому в запиті і відповіді значення різні.
За TTL можна дізнатись, скільки роутерів між нами і сервером - просто відняти отримане значення від початкового.

```
sonorma@hellcat:~$ ping -t 1 -c 5 google.com
PING google.com (142.250.203.206) 56(84) bytes of data.
From RT-AX55-FCB8 (192.168.50.1) icmp_seq=1 Time to live exceeded
From RT-AX55-FCB8 (192.168.50.1) icmp_seq=2 Time to live exceeded
From RT-AX55-FCB8 (192.168.50.1) icmp_seq=3 Time to live exceeded
From RT-AX55-FCB8 (192.168.50.1) icmp_seq=4 Time to live exceeded
From RT-AX55-FCB8 (192.168.50.1) icmp_seq=5 Time to live exceeded

--- google.com ping statistics ---
5 packets transmitted, 0 received, +5 errors, 100% packet loss, time 4006ms
```

12… 391	192.168.50.1	192.168.50.66	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
12… 392	192.168.50.66	142.250.203.206	ICMP	98	Echo (ping) request id=0x0094, seq=2/512, ttl=1 (no response found!)
12… 392	192.168.50.1	192.168.50.66	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
12… 393	192.168.50.66	142.250.203.206	ICMP	98	Echo (ping) request id=0x0094, seq=3/768, ttl=1 (no response found!)
12… 393	192.168.50.1	192.168.50.66	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
12… 394	192.168.50.66	142.250.203.206	ICMP	98	Echo (ping) request id=0x0094, seq=4/1024, ttl=1 (no response found!)
12… 394	192.168.50.1	192.168.50.66	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
12… 395	192.168.50.66	142.250.203.206	ICMP	98	Echo (ping) request id=0x0094, seq=5/1280, ttl=1 (no response found!)
12… 395	192.168.50.1	192.168.50.66	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)

```
Internet Protocol Version 4, Src: 192.168.50.1, Dst: 192.168.50.66
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
▸ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
  Total Length: 112
  Identification: 0xd49b (54427)
▸ 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: ICMP (1)
  Header Checksum: 0xbf9d [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.50.1
  Destination Address: 192.168.50.66
Internet Control Message Protocol
  Type: 11 (Time-to-live exceeded)
  Code: 0 (Time to live exceeded in transit)
  Checksum: 0xf4ff [correct]
  [Checksum Status: Good]
  Unused: 00000000
▾ Internet Protocol Version 4, Src: 192.168.50.66, Dst: 142.250.203.206
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x339b (13211)
```

В попередньому пінгу ми отримували відповідь від серверу гугл, але зараз пи отримуємо відповідь від нашого маршутизатор що TTL закінчився

```
sonorma@hellcat:~$ traceroute google.com
traceroute to google.com (142.250.203.206), 30 hops max, 60 byte packets
 1  RT-AX55-FCB8 (192.168.50.1)  1.982 ms  2.923 ms  2.897 ms
 2  172.17.188.3 (172.17.188.3)  16.567 ms  16.544 ms  16.521 ms
 3  rsm.uar.net (194.44.212.174)  3.762 ms  3.738 ms  3.714 ms
 4  194.44.212.36 (194.44.212.36)  12.298 ms  22.927 ms  12.253 ms
 5  194.44.4.254 (194.44.4.254)  11.608 ms  10.611 ms  19.580 ms
 6  74.125.245.57 (74.125.245.57)  12.161 ms  12.487 ms 74.125.245.73 (74.125.245.73)  10.107 ms
 7  74.125.245.84 (74.125.245.84)  9.522 ms 74.125.245.62 (74.125.245.62)  10.400 ms 74.125.245.64 (74.125.245.64)  11.710 ms
 8  142.251.242.39 (142.251.242.39)  25.515 ms 142.251.242.37 (142.251.242.37)  24.236 ms 72.14.239.111 (72.14.239.111)  10.492 ms
 9  192.178.99.103 (192.178.99.103)  23.012 ms 216.239.35.132 (216.239.35.132)  23.671 ms 142.251.242.41 (142.251.242.41)  23.979 ms
10  209.85.252.109 (209.85.252.109)  23.407 ms 209.85.250.175 (209.85.250.175)  23.156 ms 216.239.58.77 (216.239.58.77)  24.302 ms
11  209.85.252.109 (209.85.252.109)  23.347 ms 209.85.250.175 (209.85.250.175)  22.604 ms  23.536 ms
12  waw02s22-in-f14.1e100.net (142.250.203.206)  23.177 ms  23.893 ms  23.104 ms
```

Пакет пройшов 11 маршутизаторів для досягнення серверву google.com

Source Port	No.	Time	Source	Destination	Protocol	Length	Host	Info
60248	76	2	192.168.50.1	192.168.50.66	ICMP	102		Time-to-live exceeded (Time to live exceeded in transit)
35329	78	2	192.168.50.1	192.168.50.66	ICMP	102		Time-to-live exceeded (Time to live exceeded in transit)
48773	79	2	192.168.50.1	192.168.50.66	ICMP	102		Time-to-live exceeded (Time to live exceeded in transit)
48153	80	2	172.17.188.3	192.168.50.66	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
41940	82	2	172.17.188.3	192.168.50.66	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
54753	83	2	172.17.188.3	192.168.50.66	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
36909	84	2	194.44.212.174	192.168.50.66	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
48994	87	2	194.44.212.174	192.168.50.66	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
45368	98	2	194.44.212.252	192.168.50.66	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
48452	100	2	194.44.212.36	192.168.50.66	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
51518	102	2	74.125.245.73	192.168.50.66	ICMP	102		Time-to-live exceeded (Time to live exceeded in transit)
42025	104	2	194.44.4.254	192.168.50.66	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
34024	105	2	194.44.212.36	192.168.50.66	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
40625	108	2	194.44.4.254	192.168.50.66	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
54157	109	2	194.44.4.254	192.168.50.66	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
41939	112	2	74.125.245.57	192.168.50.66	ICMP	110		Time-to-live exceeded (Time to live exceeded in transit)
56193	114	2	74.125.245.73	192.168.50.66	ICMP	102		Time-to-live exceeded (Time to live exceeded in transit)
51013	116	2	74.125.245.86	192.168.50.66	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
35109	118	2	72.14.239.111	192.168.50.66	ICMP	182		Time-to-live exceeded (Time to live exceeded in transit)
60987	120	2	74.125.245.86	192.168.50.66	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
33135	121	2	74.125.245.64	192.168.50.66	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
52861	128	2	194.44.212.174	192.168.50.66	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
57746	129	2	142.251.242.41	192.168.50.66	ICMP	182		Time-to-live exceeded (Time to live exceeded in transit)
48419	130	2	142.251.242.35	192.168.50.66	ICMP	182		Time-to-live exceeded (Time to live exceeded in transit)
46455	131	2	192.178.99.101	192.168.50.66	ICMP	102		Time-to-live exceeded (Time to live exceeded in transit)
32816	134	2	216.239.58.79	192.168.50.66	ICMP	110		Time-to-live exceeded (Time to live exceeded in transit)
45396	135	2	142.251.242.35	192.168.50.66	ICMP	70		Time-to-live exceeded (Time to live exceeded in transit)
54670	136	2	192.178.99.99	192.168.50.66	ICMP	102		Time-to-live exceeded (Time to live exceeded in transit)
53959	137	2	209.85.250.175	192.168.50.66	ICMP	102		Time-to-live exceeded (Time to live exceeded in transit)
33787	138	2	216.239.58.77	192.168.50.66	ICMP	110		Time-to-live exceeded (Time to live exceeded in transit)
53321	139	2	142.250.203.206	192.168.50.66	ICMP	70		Destination unreachable (Port unreachable)
58094	140	2	216.239.58.77	192.168.50.66	ICMP	110		Time-to-live exceeded (Time to live exceeded in transit)
57951	141	2	209.85.250.175	192.168.50.66	ICMP	102		Time-to-live exceeded (Time to live exceeded in transit)
54743	142	2	142.250.203.206	192.168.50.66	ICMP	70		Destination unreachable (Port unreachable)
58646	151	2	142.250.203.206	192.168.50.66	ICMP	70		Destination unreachable (Port unreachable)
35993	152	2	142.250.203.206	192.168.50.66	ICMP	70		Destination unreachable (Port unreachable)

Traceroute працює так:

1. **Спочатку відправляє пакет з TTL=1**
   - Перший роутер зменшує TTL до 0
   - Пакет "помирає" і роутер відправляє назад повідомлення "Time Exceeded"
   - Так ми дізнаємось IP першого роутера
2. **Потім відправляє пакет з TTL=2**
   - Перший роутер зменшує TTL до 1
   - Другий роутер зменшує TTL до 0 і відправляє "Time Exceeded"
   - Тепер знаємо IP другого роутера
3. **І так далі, збільшуючи TTL на 1:**
   - TTL=3 - дізнаємось третій роутер
   - TTL=4 - четвертий
   - І так поки не дійдемо до цілі
4. **Коли доходимо до потрібного хоста:**
   - Він відповідає Echo Reply замість Time Exceeded
   - Це значить, що ми знайшли всі роутери по дорозі

Тобто traceroute хитро використовує TTL - навмисно робить так, щоб пакети "помирали" на кожному роутері по черзі. По відповідях від роутерів будується карта всього маршруту.
Якщо глянути в Wireshark, там буде видно як TTL збільшується в кожному новому запиті, і як міняються адреси роутерів, що відповідають.

Так, можна дізнатись маршрут за допомогою ping, якщо робити як в traceroute - змінювати TTL вручну.

Алгоритм такий:

1. **Спочатку пінгуємо з TTL=1:**
   - ping -c 1 -t 1 8.8.8.8
   - Отримуємо "Time Exceeded" від першого роутера - тепер знаємо його IP
2. **Далі з TTL=2:**
   - ping -c 1 -t 2 8.8.8.8
   - Бачимо IP другого роутера
3. **Збільшуємо TTL на 1 і повторюємо, поки не дійдемо до цілі і так далі.**

Це працює так само як traceroute, просто треба вручну міняти TTL і запускати ping кілька разів. Traceroute просто робить це все автоматично і показує результат гарніше.

Параметри в команді:

- -n 1 / -c 1: відправити 1 пакет
- -i / -t: встановити TTL
- 8.8.8.8: адреса призначення (тут DNS Google як приклад)

```
sonorma@hellcat:~$ ping -c 1 -t 1 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 192.168.50.1 icmp_seq=1 Time to live exceeded

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms

sonorma@hellcat:~$ ping -c 1 -t 2 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 172.17.188.3 icmp_seq=1 Time to live exceeded

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms

sonorma@hellcat:~$ ping -c 1 -t 3 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 194.44.212.174 icmp_seq=1 Time to live exceeded

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms

sonorma@hellcat:~$ ping -c 1 -t 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 194.44.212.36 icmp_seq=1 Time to live exceeded

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```