



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»
КАФЕДРА ММСА

Лабораторна робота № 4
З дисципліни: Комп'ютерні мережі

Протоколи ІСМР

Виконав:
Студент III курсу
Групи КА-77
Морозов Р.Д.
Перевірив: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз деталей роботи протоколу ICMP.

Хід виконання роботи

```
Last login: Tue Mar 31 15:35:36 on ttys000

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
[MacBook-Pro-Roman:~ roman$ ping -c 10 www.ust.hk
PING www.ust.hk (143.89.14.1): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
Request timeout for icmp_seq 6
Request timeout for icmp_seq 7
Request timeout for icmp_seq 8

--- www.ust.hk ping statistics ---
10 packets transmitted, 0 packets received, 100.0% packet loss
MacBook-Pro-Roman:~ roman$
```

The image shows a Wireshark packet capture window titled "Wi-Fi: en0". The packet list on the left shows 10 ICMP Echo (ping) requests from source 192.168.1.3 to destination 143.89.14.1. The selected packet (No. 12) is expanded in the packet details pane, showing the following structure:

- Frame 12: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
- Ethernet II, Src: Apple_a4:d0:fe (f0:18:98:a4:d0:fe), Dst: Tp-LinkT_98:e9:b2 (84:16:f9:98:e9:b2)
- Internet Protocol Version 4, Src: 192.168.1.3, Dst: 143.89.14.1
- Internet Control Message Protocol**
 - Type: 8 (Echo (ping) request)
 - Code: 0
 - Checksum: 0x6c65 [correct]
 - [Checksum Status: Good]
 - Identifier (BE): 28945 (0x7111)
 - Identifier (LE): 4465 (0x1171)
 - Sequence number (BE): 0 (0x0000)
 - Sequence number (LE): 0 (0x0000)
- [No response seen]**

The packet bytes pane at the bottom shows the raw data: 0000 84 16 f9 98 e9 b2 f0 18 98 a4 d0 fe 08 00 45 00 ...E...

At the bottom of the window, a status bar indicates: Packets: 305 · Displayed: 10 (3.3%) · Dropped: 0 (0.0%) · Profile: Default

```

[MacBook-Pro-Roman:~ roman$ traceroute -I www.inria.fr
traceroute to inria-cms.inria.fr (128.93.162.63), 64 hops max, 72 byte packets
 1 192.168.1.1 (192.168.1.1) 8.116 ms 2.750 ms 2.134 ms
 2 46-119-95-252.broadband.kyivstar.net (46.119.95.252) 4.876 ms 2.725 ms 2.733 ms
 3 81-23-23-74.ip.kyivstar.net (81.23.23.74) 5.089 ms 6.322 ms 3.241 ms
 4 be5877.rcr22.kbp01.atlas.cogentco.com (149.6.190.65) 5.034 ms 3.816 ms 4.834 ms
 5 be2047.ccr22.bts01.atlas.cogentco.com (154.54.60.205) 26.576 ms 20.118 ms 22.981 ms
 6 ae2.cr2-bts1.ip4.gtt.net (213.254.226.153) 22.967 ms 22.227 ms 19.962 ms
 7 et-3-3-0.cr4-par7.ip4.gtt.net (213.200.119.214) 41.520 ms 41.817 ms 42.846 ms
 8 renater-gw-ix1.gtt.net (77.67.123.206) 61.491 ms 48.797 ms 47.403 ms
 9 te1-1-inria-rtr-021.noc.renater.fr (193.51.177.107) 48.094 ms 50.767 ms 48.115 ms
10 inria-rocquencourt-te1-4-inria-rtr-021.noc.renater.fr (193.51.184.177) 49.300 ms 49.32
8 ms 49.169 ms
11 unit240-reth1-vfw-ext-dc1.inria.fr (192.93.122.19) 51.436 ms 48.707 ms 48.096 ms
12 inria-cms.inria.fr (128.93.162.63) 52.830 ms 48.845 ms 48.855 ms
MacBook-Pro-Roman:~ roman$

```

Wi-Fi: en0

No.	Time	Source	Destination	Protocol	Length	Info
42	4.962164	192.168.1.3	128.93.162.63	ICMP	86	Echo (ping) request id=0x9187, seq=1
43	4.969892	192.168.1.1	192.168.1.3	ICMP	114	Time-to-live exceeded (Time to live e
44	4.970726	192.168.1.3	128.93.162.63	ICMP	86	Echo (ping) request id=0x9187, seq=2
45	4.973348	192.168.1.1	192.168.1.3	ICMP	114	Time-to-live exceeded (Time to live e
46	4.973515	192.168.1.3	128.93.162.63	ICMP	86	Echo (ping) request id=0x9187, seq=3
47	4.975544	192.168.1.1	192.168.1.3	ICMP	114	Time-to-live exceeded (Time to live e
48	4.975639	192.168.1.3	128.93.162.63	ICMP	86	Echo (ping) request id=0x9187, seq=4
49	4.980448	46.119.95.252	192.168.1.3	ICMP	114	Time-to-live exceeded (Time to live e
50	4.980998	192.168.1.3	128.93.162.63	ICMP	86	Echo (ping) request id=0x9187, seq=5
51	4.983667	46.119.95.252	192.168.1.3	ICMP	114	Time-to-live exceeded (Time to live e
52	4.983727	192.168.1.3	128.93.162.63	ICMP	86	Echo (ping) request id=0x9187, seq=6
53	4.986411	46.119.95.252	192.168.1.3	ICMP	114	Time-to-live exceeded (Time to live e
54	4.986468	192.168.1.3	128.93.162.63	ICMP	86	Echo (ping) request id=0x9187, seq=7
55	4.991484	81.23.23.74	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live e
56	4.992066	192.168.1.3	128.93.162.63	ICMP	86	Echo (ping) request id=0x9187, seq=8
57	4.998257	81.23.23.74	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live e
58	4.998441	192.168.1.3	128.93.162.63	ICMP	86	Echo (ping) request id=0x9187, seq=9
59	5.001553	81.23.23.74	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live e
60	5.001689	192.168.1.3	128.93.162.63	ICMP	86	Echo (ping) request id=0x9187, seq=10
61	5.006559	149.6.190.65	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live e
62	5.007571	192.168.1.3	128.93.162.63	ICMP	86	Echo (ping) request id=0x9187, seq=11
63	5.011275	149.6.190.65	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live e

▶ Frame 42: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface en0, id 0
 ▶ Ethernet II, Src: Apple_a4:d0:fe (f0:18:98:a4:d0:fe), Dst: Tp-LinkT_98:e9:b2 (84:16:f9:98:e9:b2)
 ▶ Internet Protocol Version 4, Src: 192.168.1.3, Dst: 128.93.162.63
 ▶ **Internet Control Message Protocol**
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0x6677 [correct]
 [Checksum Status: Good]
 Identifier (BE): 37255 (0x9187)
 Identifier (LE): 34705 (0x8791)
 Sequence number (BE): 1 (0x0001)
 Sequence number (LE): 256 (0x0100)
 ▶ [No response seen]

0000 84 16 f9 98 e9 b2 f0 18 98 a4 d0 fe 08 00 45 00E..

wireshark_Wi-Fi_20200331175257_ht4Hml.pcapng Packets: 123 · Displayed: 72 (58.5%) Profile: Default

Контрольні питання

1. Які IP адреси вашої та цільової робочих станцій?

Моя: 192.168.1.3

Цільова: 143.89.14.1

2. Чому ICMP пакет не вказує/використовує номери вихідного та цільового портів?

Тому що протокол ICMP не є транспортним протоколом, що орієнтованим на з'єднання. Це протокол мережевого рівня.

3. Дослідіть один з пакетів-запитів ICMP. Які тип та код зазначені у цьому пакеті? Скільки байтів займають поля контрольної суми, номера послідовності та ідентифікатору?

Type: 8 (Echo (ping) request)

Code: 0

Контрольна сума – 2 байти

Номера послідовності – 2 байти

Номера ідентифікатору – 2 байти

4. Дослідіть відповідний пакет з відповіддю на пакет із пункту 3. Які тип та код зазначені у цьому пакеті? Які інші поля має цей пакет? Скільки байтів займають поля контрольної суми, номера послідовності та ідентифікатору?

Відповіді немає. Якби була отримана, тип змінився б на 0 (Echo (ping) reply), додалось поле Response time, розмір такий самий.

5. Які IP адреси вашої та цільової робочих станцій?

Моя: 192.168.1.3

Цільова: 128.93.162.63

6. Який номер протоколу IP використовується програмою?

Internet Protocol Version 4

7. Чи відрізняється пакет із запитом програми traceroute від пакету із запитом програми ping? Якщо так, наведіть приклади.

Ні, не відрізняються.

8. Проаналізуйте пакет ICMP з повідомленням про помилку. Чи є у ньому деякі додаткові поля, які не зазначаються у повідомленні з підтвердженням. Якщо є – які саме поля і яку інформацію вони вміщують?

Type: 11 (Time-to-live exceeded)

Code: 0 (Time to live exceeded in transit)

9. Проаналізуйте три останні відповіді протоколу ICMP, які отримала ваша робоча станція. Як ці пакети відрізняються від пакетів з повідомленням про помилку? Чому вони відрізняються?

Type: 0 (Echo (ping) reply)

Вони відрізняються тим, що ніколи не дійшли до місця призначення; їх скинули.

10. Знайдіть етап ретрансляції повідомлень з найбільшою середньою затримкою. Чи є можливість оцінити географічну відстань між маршрутизаторами на цьому етапі?

Так, за допомогою довжини даних.

Висновок

В ході виконання даної лабораторної роботи, були покращено навички використання програми Wireshark для захоплення пакетів. Було проаналізовано протоколи ICMP та було проведено аналіз деталей роботи даних протоколів.