



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-73
Яблуновський О. В.
Перевірив: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз деталей роботи протоколу ICMP.

Хід виконання роботи

```
Sashka--PK:~ mac$ 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

```
Sashka--PK:~ mac$
```

The image shows a Wireshark packet capture window titled 'dump1.pcapng'. The filter is set to 'icmp'. The packet list shows 10 ICMP Echo (ping) requests from source 192.168.1.209 to destination 143.89.14.1. Each request is 98 bytes long. The packet details pane for the selected packet (No. 8) shows the following structure:

- Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
- Ethernet II, Src: Apple_2f:ad:e0 (b8:e8:56:2f:ad:e0), Dst: ASUSTekC_cc:d0:98 (08:60:6e:cc:d0:98)
- Internet Protocol Version 4, Src: 192.168.1.209, Dst: 143.89.14.1
- Internet Control Message Protocol

```
Sashka--PK:~ mac$ traceroute -I www.inria.fr
traceroute to inria-cms.inria.fr (128.93.162.63), 64 hops max, 72 byte packets
 1 www.asusnetwork.net (192.168.1.1)  2.185 ms  1.296 ms  0.900 ms
 2 49-8-5-195.ip.ukrtel.net (195.5.8.49)  5.795 ms  9.296 ms  9.581 ms
 3 10.80.19.54 (10.80.19.54)  12.521 ms  12.247 ms  12.399 ms
 4 ae5.rt.dsf.dnk.ua.retn.net (87.245.239.76)  26.383 ms  24.453 ms  21.704 ms
 5 ae10-11.rt.thv.par.fr.retn.net (87.245.232.252)  54.201 ms  51.490 ms  51.711 ms
 6 renater.par.franceix.net (37.49.236.19)  54.640 ms  55.470 ms  60.042 ms
 7 xe-0-0-16-paris1-rtr-131.noc.renater.fr (193.51.177.68)  54.840 ms  55.337 ms  55.404 ms
 8 te1-1-inria-rtr-021.noc.renater.fr (193.51.177.107)  55.014 ms  55.922 ms  55.043 ms
 9 inria-rocquencourt-te1-4-inria-rtr-021.noc.renater.fr (193.51.184.177)  54.870 ms  54.868 ms  54.884 ms
10 unit240-reth1-vfw-ext-dc1.inria.fr (192.93.122.19)  55.293 ms  55.218 ms  55.275 ms
11 inria-cms.inria.fr (128.93.162.63)  58.318 ms  58.631 ms  58.371 ms
Sashka--PK:~ mac$
```

57	4.404789	193.51.177.107	192.168.1.209	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
58	4.404932	192.168.1.209	128.93.162.63	ICMP	86	Echo (ping) request id=0xd53a, seq=24/6144, ttl=8 (no response found!)
59	4.459828	193.51.177.107	192.168.1.209	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
60	4.460003	192.168.1.209	128.93.162.63	ICMP	86	Echo (ping) request id=0xd53a, seq=25/6400, ttl=9 (no response found!)
61	4.514693	193.51.184.177	192.168.1.209	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
62	4.515911	192.168.1.209	128.93.162.63	ICMP	86	Echo (ping) request id=0xd53a, seq=26/6656, ttl=9 (no response found!)
63	4.570652	193.51.184.177	192.168.1.209	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
64	4.570793	192.168.1.209	128.93.162.63	ICMP	86	Echo (ping) request id=0xd53a, seq=27/6912, ttl=9 (no response found!)
65	4.625534	193.51.184.177	192.168.1.209	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
66	4.625705	192.168.1.209	128.93.162.63	ICMP	86	Echo (ping) request id=0xd53a, seq=28/7168, ttl=10 (no response found!)
67	4.680819	192.93.122.19	192.168.1.209	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
68	4.682149	192.168.1.209	128.93.162.63	ICMP	86	Echo (ping) request id=0xd53a, seq=29/7424, ttl=10 (no response found!)
69	4.737196	192.93.122.19	192.168.1.209	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
70	4.737327	192.168.1.209	128.93.162.63	ICMP	86	Echo (ping) request id=0xd53a, seq=30/7680, ttl=10 (no response found!)
71	4.792456	192.93.122.19	192.168.1.209	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
72	4.792629	192.168.1.209	128.93.162.63	ICMP	86	Echo (ping) request id=0xd53a, seq=31/7936, ttl=11 (reply in 73)
73	4.850833	128.93.162.63	192.168.1.209	ICMP	86	Echo (ping) reply id=0xd53a, seq=31/7936, ttl=51 (request in 72)
74	4.851639	192.168.1.209	128.93.162.63	ICMP	86	Echo (ping) request id=0xd53a, seq=32/8192, ttl=11 (reply in 75)
75	4.910106	128.93.162.63	192.168.1.209	ICMP	86	Echo (ping) reply id=0xd53a, seq=32/8192, ttl=51 (request in 74)
76	4.910275	192.168.1.209	128.93.162.63	ICMP	86	Echo (ping) request id=0xd53a, seq=33/8448, ttl=11 (reply in 77)
77	4.968534	128.93.162.63	192.168.1.209	ICMP	86	Echo (ping) reply id=0xd53a, seq=33/8448, ttl=51 (request in 76)

Контрольні питання

1. Які IP адреси вашої та цільової робочих станцій?

Моя: 192.168.1.209

Цільова: 143.89.14.1

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

Тому, що він користується адресами робочих станцій.

Source: 192.168.1.209

Destination: 143.89.14.1

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?

```
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xeb1b [correct]
[Checksum Status: Good]
Identifier (BE): 31444 (0x7ad4)
Identifier (LE): 54394 (0xd47a)
Sequence number (BE): 0 (0x0000)
Sequence number (LE): 0 (0x0000)
[No response seen]
Timestamp from icmp data: Mar 30, 2020 19:56:52.533422000 EEST
[Timestamp from icmp data (relative): 0.000055000 seconds]
Data (48 bytes)
Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f...
[Length: 48]
```

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?

```
[No response seen]
[Expert Info (Warning/Sequence): No response seen to ICMP request]
[No response seen to ICMP request]
[Severity level: Warning]
[Group: Sequence]
Timestamp from icmp data: Mar 30, 2020 19:56:52.533422000 EEST
[Timestamp from icmp data (relative): 0.000055000 seconds]
```

5. Які IP адреси вашої та цільової робочих станцій?

Моя: 192.168.1.209

Цільова: 128.93.162.63

6. Який номер протоколу IP використовується програмою?

Номер 8.

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

Так. Ping не мають відповіді, а traceroute в тому ж файлі дають відповідь.

```
86 Echo (ping) request id=0xd53a, seq=1/256, ttl=1 (no response found!)
114 Time-to-live exceeded (Time to live exceeded in transit)
```

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?

Так є.

- ▼ 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: 192.168.1.209, Dst: 128.93.162.63
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 72
 - Identification: 0xd89e (55454)
 - Flags: 0x0000
 - ...0 0000 0000 0000 = Fragment offset: 0
 - Time to live: 1
 - Protocol: ICMP (1)
 - Header checksum: 0xfc00 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 192.168.1.209
 - Destination: 128.93.162.63

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?

- ▼ Internet Control Message Protocol
 - Type: 0 (Echo (ping) reply)
 - Code: 0
 - Checksum: 0x2aa4 [correct]
 - [Checksum Status: Good]
 - Identifier (BE): 54586 (0xd53a)
 - Identifier (LE): 15061 (0x3ad5)
 - Sequence number (BE): 33 (0x0021)
 - Sequence number (LE): 8448 (0x2100)
 - [\[Request frame: 76\]](#)
 - [Response time: 58.259 ms]
- ▼ Data (44 bytes)
 - Data: 00...
 - [Length: 44]

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.