

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС
«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ**

**Практична робота №4
з курсу «Комп'ютерні мережі»**

**Виконала: студентка 3 курсу
групи КА-74
Крутько А.О.
Прийняв: Кухарев С.О.**

Київ – 2020р.

Мета роботи: аналіз деталей роботи протоколу ICMP.

Хід виконання роботи

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

Wi-Fi: en0 (icmp)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	143.89.14.1	ICMP	98	Echo (ping) request id=0xb502,
2	1.005375	192.168.1.102	143.89.14.1	ICMP	98	Echo (ping) request id=0xb502,
3	2.010573	192.168.1.102	143.89.14.1	ICMP	98	Echo (ping) request id=0xb502,
4	3.010759	192.168.1.102	143.89.14.1	ICMP	98	Echo (ping) request id=0xb502,
5	4.012663	192.168.1.102	143.89.14.1	ICMP	98	Echo (ping) request id=0xb502,
6	5.013727	192.168.1.102	143.89.14.1	ICMP	98	Echo (ping) request id=0xb502,
7	6.017954	192.168.1.102	143.89.14.1	ICMP	98	Echo (ping) request id=0xb502,
8	7.021625	192.168.1.102	143.89.14.1	ICMP	98	Echo (ping) request id=0xb502,
9	8.025335	192.168.1.102	143.89.14.1	ICMP	98	Echo (ping) request id=0xb502,
10	9.025505	192.168.1.102	143.89.14.1	ICMP	98	Echo (ping) request id=0xb502,
11	12.030002	192.168.1.102	143.89.14.1	ICMP	70	Destination unreachable (Port unreachable)

- ▶ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
- ▶ Ethernet II, Src: Apple_1a:7f:60 (a8:66:7f:1a:7f:60), Dst: Tp-LinkT_ad:c0:5c (f8:d1:11:ad:c0:5c)
- ▶ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 143.89.14.1
- ▶ Internet Control Message Protocol

0000 f8 d1 11 ad c0 5c a8 66 7f 1a 7f 60 08 00 45 00f....F.

```
alisakrutko — -bash — 80x24

--- www.ust.hk ping statistics ---
10 packets transmitted, 0 packets received, 100.0% packet loss
MacBook-Marina:~ alisakrutko$ 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) 1.795 ms 1.148 ms 1.032 ms
 2 10.144.0.1 (10.144.0.1) 10.443 ms 10.478 ms 10.540 ms
 3 nat1.l11.dnipro.net (192.168.31.145) 9.933 ms * 55.038 ms
 4 g50.dnipro.net (192.168.31.177) 80.269 ms 804.194 ms 56.321 ms
 5 ae2-265.rt.ntl.kiv.ua.retn.net (87.245.237.54) 114.273 ms 111.807 ms 230.306 ms
 6 ae0-9.rt.thv.par.fr.retn.net (87.245.233.186) 132.959 ms 61.489 ms 130.460 ms
 7 * renater.par.franceix.net (37.49.236.19) 97.538 ms 56.464 ms
 8 xe-0-0-16-paris1-rtr-131.noc.renater.fr (193.51.177.68) 56.181 ms 58.061 ms 57.107 ms
 9 te1-1-inria-rtr-021.noc.renater.fr (193.51.177.107) 56.805 ms 57.020 ms 56.897 ms
10 inria-rocquencourt-te1-4-inria-rtr-021.noc.renater.fr (193.51.184.177) 55.954 ms 57.034 ms 56.151 ms
11 unit240-reth1-vfw-ext-dc1.inria.fr (192.93.122.19) 56.946 ms 56.265 ms 56.894 ms
12 inria-cms.inria.fr (128.93.162.63) 56.880 ms 57.937 ms 57.123 ms
MacBook-Marina:~ alisakrutko$
```

Wi-Fi: en0 (icmp)

icmp tcp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.93.162.63	ICMP	86	Echo (ping) request id=0x8314, s
2	0.000978	192.168.1.1	192.168.1.102	ICMP	114	Time-to-live exceeded (Time to li
3	0.031670	192.168.1.102	128.93.162.63	ICMP	86	Echo (ping) request id=0x8314, s
4	0.032641	192.168.1.1	192.168.1.102	ICMP	114	Time-to-live exceeded (Time to li
5	0.032844	192.168.1.102	128.93.162.63	ICMP	86	Echo (ping) request id=0x8314, s
6	0.033716	192.168.1.1	192.168.1.102	ICMP	114	Time-to-live exceeded (Time to li
7	0.033916	192.168.1.102	128.93.162.63	ICMP	86	Echo (ping) request id=0x8314, s
8	0.044204	10.144.0.1	192.168.1.102	ICMP	110	Time-to-live exceeded (Time to li
9	0.072400	192.168.1.102	128.93.162.63	ICMP	86	Echo (ping) request id=0x8314, s
10	0.082701	10.144.0.1	192.168.1.102	ICMP	110	Time-to-live exceeded (Time to li
11	0.082887	192.168.1.102	128.93.162.63	ICMP	86	Echo (ping) request id=0x8314, s
12	0.093278	10.144.0.1	192.168.1.102	ICMP	110	Time-to-live exceeded (Time to li
13	0.093475	192.168.1.102	128.93.162.63	ICMP	86	Echo (ping) request id=0x8314, s
14	0.103244	192.168.31.145	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to li
15	0.153593	192.168.1.102	128.93.162.63	ICMP	86	Echo (ping) request id=0x8314, s
16	5.158751	192.168.1.102	128.93.162.63	ICMP	86	Echo (ping) request id=0x8314, s
17	5.213574	192.168.31.145	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to li
18	5.213871	192.168.1.102	128.93.162.63	ICMP	86	Echo (ping) request id=0x8314, s
19	5.293924	192.168.31.177	192.168.1.102	ICMP	110	Time-to-live exceeded (Time to li
20	5.413421	192.168.1.102	128.93.162.63	ICMP	86	Echo (ping) request id=0x8314, s
21	6.217441	192.168.31.177	192.168.1.102	ICMP	110	Time-to-live exceeded (Time to li
22	6.217690	192.168.1.102	128.93.162.63	ICMP	86	Echo (ping) request id=0x8314, s
23	6.272625	192.168.31.177	192.168.1.102	ICMP	110	Time-to-live exceeded (Time to li

▶ Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface en0, id 0

Ethernet II, Src: Intel(R) Ethernet Controller (10:00:00:00:00:00), Dst: 01:00:5E:00:00:00 (01:00:5E:00:00:00)

0010	00 48 83 15 00 00 01 01	51 f5 c0 a8 01 66 80 5d	H.....Q...f.]
0020	a2 3f 08 00 74 ea 83 14	00 01 00 00 00 00 00 00	?..t.....
0030	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0040	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0050	00 00 00 00 00 00 00 00	

Контрольні питання

1. Які IP адреси вашої та цільової робочих станцій?

Моя: 192.168.1.102

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: 192.168.1.102
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: 0x2762 [correct]
  [Checksum Status: Good]
  Identifier (BE): 46338 (0xb502)
  Identifier (LE): 693 (0x02b5)
  Sequence number (BE): 0 (0x0000)
  Sequence number (LE): 0 (0x0000)
  ► [No response seen]
  Timestamp from icmp data: May 16, 2020 13:08:24.857651000 EEST
  [Timestamp from icmp data (relative): 0.000056000 seconds]
  ► Data (48 bytes)
```

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?

```
► Frame 11: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface en0, id 0
► Ethernet II, Src: Apple_1a:7f:60 (a8:66:7f:1a:7f:60), Dst: Tp-LinkT_ad:c0:5c (f8:d1:11:ad:c0:5c)
► Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.1
▼ Internet Control Message Protocol
  Type: 3 (Destination unreachable)
  Code: 3 (Port unreachable)
  Checksum: 0xfca1 [correct]
  [Checksum Status: Good]
  Unused: 00000000
  ► Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.102
  ► User Datagram Protocol, Src Port: 53, Dst Port: 65494
```

5. Які IP адреси вашої та цільової робочих станцій?

Моя: 192.168.1.102

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.

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.

The image shows a Wireshark packet capture analysis. The top section displays a warning: "[No response seen]" and "[Expert Info (Warning/Sequence): No response seen to ICMP request]". Below this, a packet list shows an ICMP Echo (ping) request (ID 0xd53a, seq=1/256, ttl=1) and a Time-to-live exceeded message (Time to live exceeded in transit). The packet details pane shows the structure of the ICMP message, including the Type (11), Code (0), Checksum (0xbf0c), and the Internet Protocol Version 4 header (Src: 192.93.122.19, Dst: 192.168.1.102). The packet bytes pane shows the raw data of the ICMP message, including the Type (11), Code (0), Checksum (0xbf0c), and the Internet Protocol Version 4 header (Src: 192.93.122.19, Dst: 192.168.1.102).

```
▼ [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]

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)

8 192.93.122.19 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in t
1 192.168.1.102 128.93.162.63 ICMP 86 Echo (ping) request id=0x8314, seq=34/8704, ttl=
2 128.93.162.63 192.168.1.102 ICMP 86 Echo (ping) reply id=0x8314, seq=34/8704, ttl=
3 192.168.1.102 128.93.162.63 ICMP 86 Echo (ping) request id=0x8314, seq=35/8960, ttl=
7 128.93.162.63 192.168.1.102 ICMP 86 Echo (ping) reply id=0x8314, seq=35/8960, ttl=
5 192.168.1.102 128.93.162.63 ICMP 86 Echo (ping) request id=0x8314, seq=36/9216, ttl=
2 128.93.162.63 192.168.1.102 ICMP 86 Echo (ping) reply id=0x8314, seq=36/9216, ttl=46 ...

► Frame 64: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface en0, id 0
► Ethernet II, Src: Tp-LinkT_ad:c0:5c (f8:d1:11:ad:c0:5c), Dst: Apple_1a:7f:60 (a8:66:7f:1a:7f:60)
► Internet Protocol Version 4, Src: 192.93.122.19, Dst: 192.168.1.102
▼ Internet Control Message Protocol
  Type: 11 (Time-to-live exceeded)
  Code: 0 (Time to live exceeded in transit)
  Checksum: 0xbf0c [correct]
  [Checksum Status: Good]
  Unused: 00000000
► Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.93.162.63
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xaabd [unverified] [in ICMP error packet]
  [Checksum Status: Unverified]
  Identifier (BE): 33556 (0x8314)
  Identifier (LE): 5251 (0x1483)
  Sequence number (BE): 33 (0x0021)
  Sequence number (LE): 8448 (0x2100)
```

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?

```
178732  128.93.162.63  192.168.1.102  ICMP  86 Echo (ping) reply  id=0x8314, seq=36/9216, ttl=
  ▶ Frame 70: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface en0, id 0
  ▶ Ethernet II, Src: Tp-LinkT_ad:c0:5c (f8:d1:11:ad:c0:5c), Dst: Apple_1a:7f:60 (a8:66:7f:1a:7f:60)
  ▶ Internet Protocol Version 4, Src: 128.93.162.63, Dst: 192.168.1.102
  ▼ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x7cc7 [correct]
    [Checksum Status: Good]
    Identifier (BE): 33556 (0x8314)
    Identifier (LE): 5251 (0x1483)
    Sequence number (BE): 36 (0x0024)
    Sequence number (LE): 9216 (0x2400)
    [Request frame: 69]
    [Response time: 56.966 ms]
  ▼ Data (44 bytes)
    Data: 0000000000000000000000000000000000000000000000000000000000000000...
    [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.