



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

Лабораторна робота № 4

З дисципліни: Комп'ютерні мережі

Основи роботи протоколу ICMP

Виконав:

Студент III курсу

Групи КА-72

Жакулін Н. В.

Перевірив: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз основних деталей роботи протоколу ICMP.

Хід виконання роботи

```
Командная строка
Microsoft Windows [Version 6.1.7601]
(с) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\Nikita>ping -n 10 www.ust.hk

Обмен пакетами с www.ust.hk [143.89.14.1] с 32 байтами данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 143.89.14.1:
    Пакетов: отправлено = 10, получено = 0, потеряно = 10
    (100% потеря)

C:\Users\Nikita>
```

1pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ICMP

No.	Time	Source	Destination	Protocol	Length	Info
3971	27.858394	192.168.0.103	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (no response found!)
4909	32.526780	192.168.0.103	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (no response found!)
5495	37.527973	192.168.0.103	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=25/6400, ttl=128 (no response found!)
6023	42.526180	192.168.0.103	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (no response found!)
6594	47.526394	192.168.0.103	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128 (no response found!)
7125	52.526664	192.168.0.103	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=128 (no response found!)
7653	57.526801	192.168.0.103	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=29/7424, ttl=128 (no response found!)
8196	62.526954	192.168.0.103	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=30/7680, ttl=128 (no response found!)
8744	67.526223	192.168.0.103	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=31/7936, ttl=128 (no response found!)
9290	72.528413	192.168.0.103	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=32/8192, ttl=128 (no response found!)

Frame 3971: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{8A2CE6CD-F596-41A8-9F9F-6404B65AB4DF}, id 0

Ethernet II, Src: LiteonTe_e9:5f:ac (70:f1:a1:e9:5f:ac), Dst: Tp-LinkT_72:eb:50 (18:d6:c7:72:eb:50)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 143.89.14.1

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x4d44 [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 23 (0x0017)

Sequence number (LE): 5888 (0x1700)

[No response seen]

0000 18 d6 c7 72 eb 50 70 f1 a1 e9 5f ac 08 00 45 00 ...ip ...E-

0010 00 3c 6e 8f 00 00 80 01 6d c8 c0 a8 00 67 8f 59 ...<n... m...g Y

0020 0e 01 08 00 4d 44 00 01 00 17 61 62 63 64 65 66 ...MD... abcdef

0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ...ghijklmn opqrstuv

0040 77 61 62 63 64 65 66 67 68 69 ...wabcdefg hi

Internet Control Message Protocol: Protocol

Packets: 10408 · Displayed: 10 (0.1%)

Profile: Default

22:59 31.03.2020

```

C:\Users\Nikita>tracert www.inria.fr

Трассировка маршрута к inria-cms.inria.fr [128.93.162.63]
с максимальным числом прыжков 30:

  1      1 ms      1 ms      1 ms  192.168.0.1
  2      1 ms      1 ms      1 ms  lo0.bras-dp-04.fregat.net [212.115.225.244]
  3      2 ms      1 ms      1 ms  10.0.11.25
  4      9 ms     10 ms     33 ms  212.115.254.185
  5      9 ms      9 ms     12 ms  185.23.164.129
  6     10 ms     22 ms      9 ms  ae2-232.RT.NTL.KIV.UA.retn.net [87.245.237.112]

  7     51 ms     51 ms     51 ms  ae0-9.RT.THV.PAR.FR.retn.net [87.245.233.186]
  8     64 ms     64 ms     55 ms  renater.par.franceix.net [37.49.236.19]
  9     61 ms     62 ms     55 ms  xe0-1-2-paris1-rtr-131.noc.renater.fr [193.51.177.88]
10     60 ms     63 ms     56 ms  te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
11     54 ms     54 ms     57 ms  inria-rocquencourt-te1-4-inria-rtr-021.noc.renater.fr [193.51.184.177]
12     55 ms     55 ms     55 ms  unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
13     57 ms     55 ms     55 ms  inria-cms.inria.fr [128.93.162.63]

Трассировка завершена.
  
```

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, analysis, and statistics.

The main packet list pane displays several ICMP Echo (ping) requests from source IP 192.168.0.103 to destination IP 128.93.162.63. The first few packets show successful responses, while subsequent ones indicate "Time-to-live exceeded" or "Destination unreachable".

The selected packet (No. 2650) is expanded, showing its details in the right-hand pane:

- 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: 192.168.0.103, Dst: 128.93.162.63.
- Internet Control Message Protocol**: Type: 8 (Echo (ping) request), Code: 0, Checksum: 0xf7ba [unverified] [in ICMP error packet], [Checksum Status: Unverified], Identifier (BE): 1 (0x0001).

The bottom pane shows the raw packet bytes in hexadecimal and ASCII format. The status bar at the bottom indicates "Packets: 7119 • Displayed: 84 (1.2%)" and "Profile: Default".

Контрольні запитання:

1. Які IP адреси вашої та цільової робочих станцій?
2. Чому ICMP пакет не вказує/використовує номери вихідного та цільового портів?
3. Дослідіть один з пакетів-запитів ICMP. Які тип та код зазначені у цьому пакеті?

Скільки байтів займають поля контрольної суми, номери послідовності та ідентифікатору?

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, номери послідовності та ідентифікатору?

5. Які IP адреси вашої та цільової робочих станцій?

6. Який номер протоколу IP використовується програмою?

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

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?

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?

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

Відповіді на контрольні запитання:

1. Моя IP адреса 192.168.0.103, цільова IP адреса 143.89.14.1.
2. Тому що протокол ICMP є протоколом мережевого рівня.
3. Тип 8, код 0. Контрольна сума, номер послідовності, номер ідентифікатору займають по два байти.
4. Відповіді не було. Якщо була б, то тип був 0, код 0, додалося б поле Response time. Контрольна сума, номер послідовності, номер ідентифікатору займають теж по два байти.
5. Моя IP адреса 192.168.0.103, цільова IP адреса 128.93.162.63.
6. IP протокол версії 4.
7. Поля не відрізняються.
8. Пакет ICMP з повідомленням про помилку має тип 11. Він не має полей ідентифікатор та номер послідовності.
9. Пакет ICMP з відповіддю має тип 0, а з повідомленням про помилку – код 11. Він не має полей ідентифікатор та номер послідовності. Час життя дейтаграми вичерпано.

6	10 ms	22 ms	9 ms	ae2-232.RT.NTL.KIV.UA.retn.net [87.245.237.112]
10. 7	51 ms	51 ms	51 ms	ae0-9.RT.THV.PAR.FR.retn.net [87.245.233.186]

Є можливість, але не завжди.

Висновок

У даній лабораторній роботі, за допомогою середовища захоплення та аналізу пакетів Wireshark, я ознайомилась зі структурою мережевого протоколу ICMP, що входить в стек протоколів TCP/IP. Перша команда не отримала відповіді, тому для надання відповіді на деякі питання знадобилося змінити хост-ім'я.