

**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 №5
з курсу «Комп'ютерні мережі»**

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

Київ – 2020р.

Мета роботи: аналіз деталей роботи протоколу IP.

Хід виконання роботи

```
[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.l111.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 130.46
0 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 m
s 57.107 ms
 9 te1-1-inria-rtr-021.noc.renater.fr (193.51.177.107) 56.805 ms 57.020 ms 5
6.897 ms
10 inria-rocquencourt-te1-4-inria-rtr-021.noc.renater.fr (193.51.184.177) 55.9
54 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$ traceroute gaia.cs.umass.edu 2000 ]
traceroute to gaia.cs.umass.edu (128.119.245.12), 64 hops max, 2000 byte packets
 1 192.168.1.1 (192.168.1.1) 4.968 ms 19.881 ms 51.562 ms
 2 * * 10.144.0.1 (10.144.0.1) 38.448 ms
 3 nat1.l111.dnipro.net (192.168.31.145) 424.642 ms * 80.195 ms
 4 g50.dnipro.net (192.168.31.177) 65.149 ms * 380.150 ms
 5 kiev-b1-link.telvia.net (213.248.101.50) 128.842 ms 106.633 ms 134.951 ms
 6 * win-bb4-link.telvia.net (62.115.141.162) 34.297 ms 28.939 ms
 7 win-b2-link.telvia.net (62.115.114.183) 29.953 ms 29.932 ms 30.177 ms
 8 level3-ic-336715-win-b4.c.telvia.net (62.115.11.51) 28.695 ms 30.947 ms 29
.038 ms
 9 ae-1-3501.ear3.newyork1.level3.net (4.69.150.202) 122.314 ms * *
10 university.ear3.newyork1.level3.net (4.71.230.234) 209.409 ms 157.281 ms
124.899 ms
11 core2-rt-et-8-3-0.gw.umass.edu (192.80.83.113) 124.167 ms 235.999 ms 903.
606 ms
12 n5-rt-1-1-et-10-0-0.gw.umass.edu (128.119.0.10) 1440.959 ms 125.326 ms 12
5.041 ms
13 cics-rt-xe-0-0-0.gw.umass.edu (128.119.3.32) 153.506 ms * 207.441 ms
14 * * *
15 gaia.cs.umass.edu (128.119.245.12) 207.663 ms !Z 714.183 ms !Z 307.889 ms
!Z
MacBook-Marina:~ alisakrutko$
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.1	192.168.1.102	ICMP	590	Time-to-live exceeded (Time to
2	0.021572	192.168.1.1	192.168.1.102	ICMP	590	Time-to-live exceeded (Time to
3	0.073179	192.168.1.1	192.168.1.102	ICMP	590	Time-to-live exceeded (Time to
4	10.117045	10.144.0.1	192.168.1.102	ICMP	110	Time-to-live exceeded (Time to
5	10.542596	192.168.31.145	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to
6	15.629087	192.168.31.145	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to
7	15.694243	192.168.31.177	192.168.1.102	ICMP	110	Time-to-live exceeded (Time to
8	21.080458	192.168.31.177	192.168.1.102	ICMP	110	Time-to-live exceeded (Time to
9	21.209410	213.248.101.50	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to
10	21.779765	213.248.101.50	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to
11	21.914773	213.248.101.50	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to
12	26.951396	62.115.141.162	192.168.1.102	ICMP	182	Time-to-live exceeded (Time to
13	27.221198	62.115.141.162	192.168.1.102	ICMP	182	Time-to-live exceeded (Time to
14	27.251264	62.115.114.183	192.168.1.102	ICMP	110	Time-to-live exceeded (Time to
15	27.441645	62.115.114.183	192.168.1.102	ICMP	110	Time-to-live exceeded (Time to
16	27.471903	62.115.114.183	192.168.1.102	ICMP	110	Time-to-live exceeded (Time to
17	27.500649	62.115.11.51	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to
18	27.681165	62.115.11.51	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to
19	27.710241	62.115.11.51	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to
20	27.832587	4.69.150.202	192.168.1.102	ICMP	170	Time-to-live exceeded (Time to
21	38.955845	4.71.230.234	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to
22	39.703827	4.71.230.234	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to
23	39.828776	4.71.230.234	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to
24	39.952966	192.80.83.113	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to
25	40.836484	192.80.83.113	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to
26	41.740343	192.80.83.113	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to
27	43.181397	128.119.0.10	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live e

Frame 1: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface en0, id 0

Контрольні запитання:

1. Визначте IP адреси вашої та цільової робочих станцій. IP адреси:

Моя: 192.168.1.1

Цільова: 192.168.1.102

2. Яке значення в полі номера протоколу вищого рівня в заголовку IP першого пакету із запитом ICMP?

1

3. Скільки байт займає заголовок IP першого пакету із запитом ICMP?

Скільки байт займає корисна інформація (payload) пакету? Поясніть як ви встановили кількість байт корисної інформації.

2008 bytes – payload.

```

0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Destination: 128.119.245.12
[2 IPv4 Fragments (2008 bytes): #85(1480), #86(528)]
  [Frame: 85, payload: 0-1479 (1480 bytes)]
  [Frame: 86, payload: 1480-2007 (528 bytes)]
  [Fragment count: 2]

```

4. Дослідіть пакет із пунктів 2/3. Чи фрагментований цей пакет? Поясніть як ви встановили фрагментацію пакету. Як можна встановити номер фрагменту, що передається у пакеті?

Пакет фрагментований.

```

Flags: 0x00b9
 0... .... = Reserved bit: Not set
.0... .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 0101 1100 1000 = Fragment offset: 1480
Time to live: 128
Protocol: ICMP (1)

```

За допомогою Flags, який передається.

5. Знайдіть наступний фрагмент датаграми IP. Яка інформація дозволяє встановити наявність наступних фрагментів, що мають слідувати за другим фрагментом?

```

Flags: 0x00b9
 0... .... = Reserved bit: Not set
.0... .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 0101 1100 1000 = Fragment offset: 1480
Time to live: 128
Protocol: ICMP (1)

```

6. Як поля протоколу IP відрізняють перший фрагмент від другого?

Фрагменти відрізняються Flags- у кожного фрагменту він різний.

7. Розгляньте послідовність пакетів IP із запитом ICMP вашої робочої станції. Які поля заголовку IP завжди змінюються?

Завжди змінюється поле Identification.

8. Розгляньте послідовність пакетів IP із запитами ICMP вашої робочої станції. Які поля заголовку IP мають зберігати свої значення? Які поля мають змінюватися? Чому?

```
Internet Protocol Version 4, Src: 77.47.197.26, Dst: 128.119.245.12
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 548
    Identification: 0x21d4 (8660)
  > Flags: 0x00b9
    ...0 0101 1100 1000 = Fragment offset: 1480
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x8e7e [validation disabled]
    [Header checksum status: Unverified]
    Source: 77.47.197.26
    Destination: 128.119.245.12
```

Окрім поля Identification, воно повинно змінюватися, бо кожного разу ми ідентифікуємо інший запит.

9. Розгляньте послідовність пакетів IP із запитами ICMP вашої робочої станції. Опишіть закономірність зміни значень поля Identification рівня IP.

Кожного разу додається одиниця до коду.

10. Розгляньте послідовність пакетів IP із повідомленнями TTL-exceeded від найближчого маршрутизатора. Які значення встановлені у полях Identification та TTL?

```
...0 0101 1100 1000 = Fragment offset: 1480
Time to live: 128
Protocol: ICMP (1)
Header checksum: 0x8e7f [validation disabled]
[Header checksum status: Unverified]
Source: 77.47.197.26
```

11. Розгляньте послідовність пакетів IP із повідомленнями TTL-exceeded від найближчого маршрутизатора. Які значення встановлені у полях Identification та TTL? Чи змінюються ці значення для різних пакетів у послідовності? Чому?

Так змінюються, тому що validation disabled різний для всіх протоколів.

Висновок

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