

**«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ «КПІ»
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ**

**Лабораторна робота №5
з курсу «Комп'ютерні мережі»**

**Виконав: студент 3 курсу
групи КА-73**

Приходько А.І.

Прийняв: Кухарєв С.О.

Київ 2020 р.

No.	Time	Source	Destination	Protocol	Length	Info
176	195.120382	192.168.1.106	10.35.8.10	ICMP	562	Echo (ping) request id=0x0001, seq=53/13568, ttl=128 (no response found!)
181	199.663423	192.168.1.106	10.35.8.10	ICMP	562	Echo (ping) request id=0x0001, seq=54/13824, ttl=128 (no response found!)
255	204.670875	192.168.1.106	10.35.8.10	ICMP	562	Echo (ping) request id=0x0001, seq=55/14080, ttl=128 (no response found!)
260	209.670917	192.168.1.106	10.35.8.10	ICMP	562	Echo (ping) request id=0x0001, seq=56/14336, ttl=128 (no response found!)

> Frame 176: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{105EB1FF-1E88-49D2-B75B-A6018706E6FA}, id 0
 > Ethernet II, Src: IntelCor_95:51:8c (bc:a8:a6:95:51:8c), Dst: CameoCom_ec:b9:7d (00:18:e7:ec:b9:7d)
 > Internet Protocol Version 4, Src: 192.168.1.106, Dst: 10.35.8.10
 > Internet Control Message Protocol

```

0000  00 18 e7 ec b9 7d bc a8 a6 95 51 8c 08 00 45 00  ....}.Q...E-
0010  02 24 13 21 00 b9 80 01 50 c0 c0 a8 01 6a 0a 23  -$.!....P....j.#
0020  08 0a 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e  --.abcdef ghijklmn
0030  6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67  opqrstuv wabcdefg
0040  68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77  hijklmno pqrstuvw
0050  61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70  abcdefgh ijklmnop
0060  71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwv bcdefghi
  
```

Frame (562 bytes) Reassembled IPv4 (2008 bytes)

(Термінал:

Значок Windows + R -> Cmd)

Frame 176: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface
 \Device\NPF_{105EB1FF-1E88-49D2-B75B-A6018706E6FA}, id 0

Ethernet II, Src: IntelCor_95:51:8c (bc:a8:a6:95:51:8c), Dst: CameoCom_ec:b9:7d (00:18:e7:ec:b9:7d)

Internet Protocol Version 4, Src: 192.168.1.106, Dst: 10.35.8.10

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 548

Identification: 0x1321 (4897)

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)

Header checksum: 0x50c0 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.106

Destination: 10.35.8.10

[2 IPv4 Fragments (2008 bytes): #175(1480), #176(528)]

[Frame: 175, payload: 0-1479 (1480 bytes)]

[Frame: 176, payload: 1480-2007 (528 bytes)]

[Fragment count: 2]

[Reassembled IPv4 length: 2008]

[Reassembled IPv4 data: 08007b42000100356162636465666768696a6b6c6d6e6f70...]

Internet Control Message Protocol

Контрольні запитання:

1. Визначте IP адреси вашої та цільової робочих станцій.

192.168.1.106,

10.35.8.10 .

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

Protocol: 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.

20 байт, 2008 байт = 1480 + 528 ;

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?

Так, фрагментований. Встановлено за номером фрейма.

[2 IPv4 Fragments (2008 bytes): #175(1480), #176(528)]

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

More fragments: Not set

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

Відрізняють назва фрейму; Upper Layer Protocol, Fragment offset.

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

Identification та Header checksum ;

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

Поля, які зберігають свої значення:

- 1) Version (ми використовуємо IPv4 для всіх пакетів)
- 2) header length (всі пакети – ICMP)
- 3) source IP, destination IP (Ми пінгуємо одну і ту ж адресу)
- 4) Differentiated Services (всі ICMP пакети одного службового типу)
- 5) Time to live

Поля, які змінюють свої значення:

- 6) Upper Layer Protocol (всі заголовки ICMP мають унікальні поля, що змінюються)
- 7) Identification (IP пакети мають мати різні id)
- 8) Header checksum (оскільки заголовки змінюються, то контрольна сума

9. Розгляньте послідовність пакетів IP із запитами ICMP вашої робочої станції.

Опишіть закономірність зміни значень поля Identification рівня IP.

Значення кожен раз збільшується на 1 ;

10. Розгляньте послідовність пакетів IP із повідомленнями

TTL-exceeded від найближчого маршрутизатора. Які значення встановлені у полях Identification та TTL?

Даних послідовностей пакетів не було. (Утиліта ping не змінює TTL для різних запитів) ;

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?

Для кожної ICMP TTL-exceeded відповіді змінюється поле Identification. Якщо дві IP датаграми мають однакове поле Identification, то дані датаграми є фрагментами однієї великої IP датаграми. Поле TTL завжди мусить бути однакове, адже у заданого маршрутизатора він один.

Висновок:

В лабораторній роботі я ознайомився з деталями роботи протоколу IP, який відповідає за адресацію пакетів. Протокол IP розпізнає формат заголовка пакета (адресну частину та іншу службову інформацію включно). IP-пакети складаються з даних верхнього рівня та IP-заголовку.
