

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ  
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ  
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»**

**Інститут прикладного системного аналізу  
Кафедра математичних методів системного аналізу**

**Дисципліна: “Комп’ютерні мережі”**

**Лабораторна робота № 5**

**Тема роботи: “Протокол IP”**

Виконала: студентка  
3 курсу групи КА-77  
Деменкова В.В.

Прийняв: к.т.н. Кухарєв С.О.

**Київ – 2020**

## Лабораторна робота № 5. Протокол IP

**Мета роботи:** Аналіз основних деталей роботи протоколу IP.

### Отримані результати:

```
No.      Time      Source      Destination      Protocol Length Info
 54 5.341559 192.168.1.109 128.119.245.12  ICMP      562      Echo (ping) request id=0x0001, seq=88/22528, ttl=128
(reply in 57)
Frame 54: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{A1BA2240-64F3-4F12-995F-D42D06B55803},
id 0
Ethernet II, Src: HonHaiPr_b9:36:4d (a4:17:31:b9:36:4d), Dst: Tp-LinkT_de:11:f8 (b0:48:7a:de:11:f8)
Internet Protocol Version 4, Src: 192.168.1.109, 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: 0x271b (10011)
Flags: 0x00b9
...0 0101 1100 1000 = Fragment offset: 1480
Time to live: 128
Protocol: ICMP (1)
Header checksum: 0xd96b [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.109
Destination: 128.119.245.12
[2 IPv4 Fragments (2008 bytes): #53(1480), #54(528)]
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x7b1f [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence number (BE): 88 (0x0058)
Sequence number (LE): 22528 (0x5800)
[Response frame: 57]
Data (2000 bytes)
```

### Контрольні питання:

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

```
C:\Users\Doris>ping -l 2000 gaia.cs.umass.edu

Pinging gaia.cs.umass.edu [128.119.245.12] with 2000 bytes of data:
Reply from 128.119.245.12: bytes=2000 time=118ms TTL=46
Reply from 128.119.245.12: bytes=2000 time=131ms TTL=46
Reply from 128.119.245.12: bytes=2000 time=115ms TTL=46
Reply from 128.119.245.12: bytes=2000 time=121ms TTL=46

Ping statistics for 128.119.245.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 115ms, Maximum = 131ms, Average = 121ms
```

No.	Time	Source	Destination	Protocol	Length
54	5.341559	192.168.1.109	128.119.245.12	ICMP	562
57	5.459423	128.119.245.12	192.168.1.109	ICMP	562
59	6.346146	192.168.1.109	128.119.245.12	ICMP	562
61	6.477167	128.119.245.12	192.168.1.109	ICMP	562
70	7.350443	192.168.1.109	128.119.245.12	ICMP	562
81	7.466195	128.119.245.12	192.168.1.109	ICMP	562
111	8.356095	192.168.1.109	128.119.245.12	ICMP	562
113	8.477762	128.119.245.12	192.168.1.109	ICMP	562

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

53	5.341556	192.168.1.109	128.119.245.12	IPv4	1514	Fragmented
54	5.341559	192.168.1.109	128.119.245.12	ICMP	562	Echo (ping)
55	5.365858	8.8.4.4	192.168.1.109	DNS	93	Standard query
56	5.459234	128.119.245.12	192.168.1.109	IPv4	1514	Fragmented
57	5.459423	128.119.245.12	192.168.1.109	ICMP	562	Echo (ping)

  

No.	Time	Source	Destination	Protocol	Length	Info
54	5.341559	192.168.1.109	128.119.245.12	ICMP	562	Echo (ping)
57	5.459423	128.119.245.12	192.168.1.109	ICMP	562	Echo (ping)
59	6.346146	192.168.1.109	128.119.245.12	ICMP	562	Echo (ping)
61	6.477167	128.119.245.12	192.168.1.109	ICMP	562	Echo (ping)
70	7.350443	192.168.1.109	128.119.245.12	ICMP	562	Echo (ping)
81	7.466195	128.119.245.12	192.168.1.109	ICMP	562	Echo (ping)
111	8.356095	192.168.1.109	128.119.245.12	ICMP	562	Echo (ping)
113	8.477762	128.119.245.12	192.168.1.109	ICMP	562	Echo (ping)

  

> Frame 54: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface  
 > Ethernet II, Src: HonHaiPr\_b9:36:4d (a4:17:31:b9:36:4d), Dst: Tp-LinkT\_de:11:f8 (b8:27:eb:11:f8:00)  
 > Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12

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

Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12

0100 .... = Version: 4

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

IP-пакеты состоят из заголовка и полезной нагрузки. Заголовок пакета IPv4 состоит из:

1. 4 бита содержат *версию* пакета: IPv4 или IPv6.
2. 4 бита содержат *длину интернет-заголовка*, которая измеряется отрезками по 4 байта (например, 5 означает 20 байт).
3. 8 бит содержат *тип обслуживания*, известный также как качество обслуживания (QoS), описывающее приоритеты пакета.
4. 16 бит содержат *длину* пакета в байтах.
5. 16 бит содержат *тег идентификации*, помогающий восстановить пакет из нескольких фрагментов.
6. 3 бита содержат нуль, флаг разрешения *фрагментации* пакета (DF: не фрагментировать), а также флаг разрешения дальнейшей фрагментации (MF: фрагментировать дальше).
7. 13 бит содержат *смещение фрагмента*, поле для идентификации положение фрагмента в исходном пакете.
8. 8 бит содержат *время жизни* (TTL), которое определяет количество переходов (через маршрутизаторы, компьютеры и сетевые устройства), разрешённых сделать пакету, прежде чем он исчезнет (например, пакету с TTL 16 разрешено пройти не более 16 маршрутизаторов, чтобы добраться до места назначения).
9. 8 бит содержат *протокол* (TCP, UDP, ICMP и т. д.).
10. 16 бит содержат *контрольную сумму заголовка*, используемую при обнаружении ошибок.
11. 32 бит содержат *IP-адрес источника*.
12. 32 бит содержат *адрес назначения*.

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

The image shows a Wireshark packet capture. The top pane displays a list of packets. The bottom pane shows the details of the selected packet (packet 54), which is an ICMP Echo (ping) request. The details pane shows the protocol as ICMP (1), the header checksum as 0xd96b [validation disabled], the source as 192.168.1.109, and the destination as 128.119.245.12. Below this, it shows two IPv4 fragments: #53 (1480 bytes) and #54 (528 bytes). The fragment count is 2, and the reassembled IPv4 length is 2008 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
54	5.341559	192.168.1.109	128.119.245.12	ICMP	562	Echo (ping) requ
57	5.459423	128.119.245.12	192.168.1.109	ICMP	562	Echo (ping) repl
59	6.346146	192.168.1.109	128.119.245.12	ICMP	562	Echo (ping) requ
61	6.477167	128.119.245.12	192.168.1.109	ICMP	562	Echo (ping) repl
70	7.350443	192.168.1.109	128.119.245.12	ICMP	562	Echo (ping) requ
81	7.466195	128.119.245.12	192.168.1.109	ICMP	562	Echo (ping) repl
111	8.356095	192.168.1.109	128.119.245.12	ICMP	562	Echo (ping) requ
113	8.477762	128.119.245.12	192.168.1.109	ICMP	562	Echo (ping) repl

Protocol: ICMP (1)  
Header checksum: 0xd96b [validation disabled]  
[Header checksum status: Unverified]  
Source: 192.168.1.109  
Destination: 128.119.245.12  
[2 IPv4 Fragments (2008 bytes): #53(1480), #54(528)]  
[Frame: 53, payload: 0-1479 (1480 bytes)]  
[Frame: 54, payload: 1480-2007 (528 bytes)]  
[Fragment count: 2]  
[Reassembled IPv4 length: 2008]  
[Reassembled IPv4 data: 08007b1f000100596162636465666768696a6b6c6d6e6f70 1

[Кадр: 53, полезна нагрукка: 0-1479 (1480 байт)]

[Кадр: 54, полезна нагрукка: 1480-2007 (528 байт)]

•	53	5.341556	192.168.1.109	128.119.245.12	IPv4	1514	Fragmented
→	54	5.341559	192.168.1.109	128.119.245.12	ICMP	562	Echo (ping)

4. Дослідіть пакет із пунктів 2/3. Чи фрагментований цей пакет? Ні

```
▼ 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
```

Поясніть як ви встановили фрагментацію пакету. Як можна встановити номер фрагменту, що передається у пакеті?

•	53	5.341556	192.168.1.109	128.119.245.12	IPv4	1514	Fragmented
→	54	5.341559	192.168.1.109	128.119.245.12	ICMP	562	Echo (ping)
	55	5.365858	8.8.4.4	192.168.1.109	DNS	93	Standard qu
	56	5.459234	128.119.245.12	192.168.1.109	IPv4	1514	Fragmented
←	57	5.459423	128.119.245.12	192.168.1.109	ICMP	562	Echo (ping)

[2 IPv4 Fragments (2008 bytes): #53(1480), #54(528)]

[\[Frame: 53, payload: 0-1479 \(1480 bytes\)\]](#)

[\[Frame: 54, payload: 1480-2007 \(528 bytes\)\]](#)

[Fragment count: 2]

[Reassembled IPv4 length: 2008]

[Reassembled IPv4 data: 08007b1f000100586162636465666768696a6b6c6d6e6f70...]

[Количество фрагментов: 2]

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

IPv4	1514	Fragmented	IP protocol (proto=ICMP 1, off=0, ID=271b)	[Reassembled in #54]
IPv4	1514	Fragmented	IP protocol (proto=ICMP 1, off=0, ID=2cd9)	[Reassembled in #57]
IPv4	1514	Fragmented	IP protocol (proto=ICMP 1, off=0, ID=271c)	[Reassembled in #59]
IPv4	1514	Fragmented	IP protocol (proto=ICMP 1, off=0, ID=2e53)	[Reassembled in #61]
IPv4	1514	Fragmented	IP protocol (proto=ICMP 1, off=0, ID=271d)	[Reassembled in #70]
IPv4	1514	Fragmented	IP protocol (proto=ICMP 1, off=0, ID=3124)	[Reassembled in #81]
IPv4	1514	Fragmented	IP protocol (proto=ICMP 1, off=0, ID=271e)	[Reassembled in #111]
IPv4	1514	Fragmented	IP protocol (proto=ICMP 1, off=0, ID=3184)	[Reassembled in #113]

[Reassembled in #111]

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

```
IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=2cd9)
ICMP      562 Echo (ping) reply      id=0x0001, seq=88/22528, ttl=46 (
IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=271c)
ICMP      562 Echo (ping) request id=0x0001, seq=89/22784, ttl=128
IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=2e53)
```

```
Header checksum: 0x0267 [validation disabled]
```

```
Header checksum: 0xb66b [validation disabled]
```

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

```
Identification: 0x271b (10011)
```

```
Header checksum: 0xd96b [validation disabled]
```

```
[2 IPv4 Fragments (2008 bytes): #53(1480), #54(528)]
```

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

```
Total Length: 548
```

```
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
```

```
Source: 192.168.1.109
```

```
Destination: 128.119.245.12
```

```
Protocol: ICMP (1)
```

#### Общее содержание ICMP пакета

- IP Header (синим цветом):
  - *Protocol* устанавливается значение — 1 (ICMP) и *Type of Service* — 0

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

Ідентифікація (*Identification*) — шістнадцятибітове поле, що зберігає ціле число, яке описує даний пакет. Це число являє собою послідовний номер.

Закономірність – збільшення на 1.

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

```
> Flags: 0x00b9
...0 0101 1100 1000 = Fragment offset: 1480
Time to live: 128
Protocol: ICMP (1)
Header checksum: 0xd96b [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.109
Destination: 128.119.245.12
```

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?

*Identification* змінюється, а *TTL* - ні, бо за допомогою ідентифікатора визначається той чи інший пакет, а час життя визначається джерелом передачі.

**Висновок:** В данній лабораторій роботі було проаналізовано основні деталі роботи протоколу IP з використанням команди `ping -l 2000 gaia.cs.umass.edu`. Досліджено перший пакет із запитом ICMP. Встановлено номер фрагменту, що передається у пакеті. Розглянуто послідовність пакетів IP із повідомленнями `TTL_exceeded` від найближчого маршрутизатора.