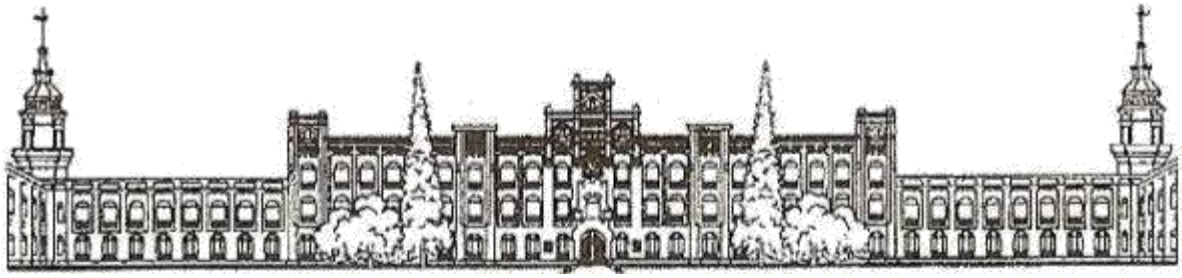


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ННК
«ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»
КАФЕДРА ММСА

Лабораторна робота № 5
З дисципліни: Комп'ютерні мережі

Протоколи IP

Виконала:
Студентка III курсу
Групи КА-73
Ярошенко В. О.
Перевірив: Кухарєв С. О.

Київ 2020

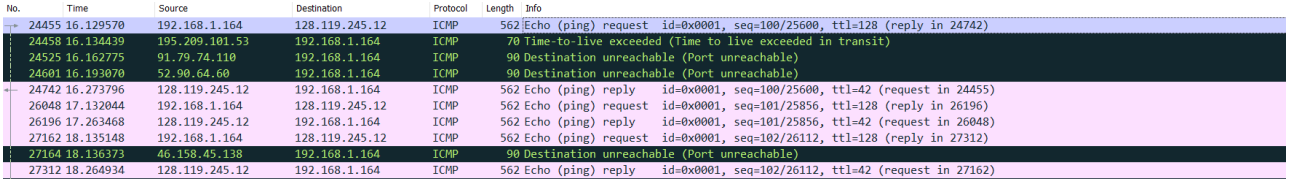
```
C:\WINDOWS\system32>ping -l 2000 gaia.cs.umass.edu

Обмен пакетами с gaia.cs.umass.edu [128.119.245.12] с 2000 байтами данных:
Ответ от 128.119.245.12: число байт=2000 время=144мс TTL=42
Ответ от 128.119.245.12: число байт=2000 время=131мс TTL=42
Ответ от 128.119.245.12: число байт=2000 время=129мс TTL=42
Ответ от 128.119.245.12: число байт=2000 время=144мс TTL=42

Статистика Ping для 128.119.245.12:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 129мсек, Максимальное = 144 мсек, Среднее = 137 мсек

C:\WINDOWS\system32>
```

```
No.     Time           Source                Destination           Protocol Length Info
  24455 16.129570      192.168.1.164         128.119.245.12        ICMP     562    Echo (ping) request  id=0x0001, seq=100/25600, ttl=128
(reply in 24742)
Frame 24455: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{3CE8ED40-6CFE-47DB-8508-9072AD0B8C48}
id 0
Ethernet II, Src: IntelCor_d6:66:72 (3c:f8:62:d6:66:72), Dst: ASUSTekC_76:a6:80 (2c:4d:54:76:a6:80)
Internet Protocol Version 4, Src: 192.168.1.164, Dst: 128.119.245.12
Internet Control Message Protocol
No.     Time           Source                Destination           Protocol Length Info
  24742 16.273796      128.119.245.12        192.168.1.164         ICMP     562    Echo (ping) reply    id=0x0001, seq=100/25600, ttl=42
(request in 24455)
Frame 24742: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{3CE8ED40-6CFE-47DB-8508-9072AD0B8C48}
id 0
Ethernet II, Src: ASUSTekC_76:a6:80 (2c:4d:54:76:a6:80), Dst: IntelCor_d6:66:72 (3c:f8:62:d6:66:72)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.164
Internet Control Message Protocol
No.     Time           Source                Destination           Protocol Length Info
  26048 17.132044      192.168.1.164         128.119.245.12        ICMP     562    Echo (ping) request  id=0x0001, seq=101/25856, ttl=128
(reply in 26196)
Frame 26048: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{3CE8ED40-6CFE-47DB-8508-9072AD0B8C48}
id 0
Ethernet II, Src: IntelCor_d6:66:72 (3c:f8:62:d6:66:72), Dst: ASUSTekC_76:a6:80 (2c:4d:54:76:a6:80)
Internet Protocol Version 4, Src: 192.168.1.164, Dst: 128.119.245.12
Internet Control Message Protocol
No.     Time           Source                Destination           Protocol Length Info
  26196 17.263468      128.119.245.12        192.168.1.164         ICMP     562    Echo (ping) reply    id=0x0001, seq=101/25856, ttl=42
(request in 26048)
Frame 26196: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{3CE8ED40-6CFE-47DB-8508-9072AD0B8C48}
id 0
Ethernet II, Src: ASUSTekC_76:a6:80 (2c:4d:54:76:a6:80), Dst: IntelCor_d6:66:72 (3c:f8:62:d6:66:72)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.164
Internet Control Message Protocol
No.     Time           Source                Destination           Protocol Length Info
  27162 18.135148      192.168.1.164         128.119.245.12        ICMP     562    Echo (ping) request  id=0x0001, seq=102/26112, ttl=128
(reply in 27312)
Frame 27162: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{3CE8ED40-6CFE-47DB-8508-9072AD0B8C48}
id 0
Ethernet II, Src: IntelCor_d6:66:72 (3c:f8:62:d6:66:72), Dst: ASUSTekC_76:a6:80 (2c:4d:54:76:a6:80)
Internet Protocol Version 4, Src: 192.168.1.164, Dst: 128.119.245.12
Internet Control Message Protocol
No.     Time           Source                Destination           Protocol Length Info
  27312 18.264934      128.119.245.12        192.168.1.164         ICMP     562    Echo (ping) reply    id=0x0001, seq=102/26112, ttl=42
(request in 27162)
Frame 27312: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{3CE8ED40-6CFE-47DB-8508-9072AD0B8C48}
id 0
Ethernet II, Src: ASUSTekC_76:a6:80 (2c:4d:54:76:a6:80), Dst: IntelCor_d6:66:72 (3c:f8:62:d6:66:72)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.164
Internet Control Message Protocol
No.     Time           Source                Destination           Protocol Length Info
  28618 19.138296      192.168.1.164         128.119.245.12        ICMP     562    Echo (ping) request  id=0x0001, seq=103/26368, ttl=128
(reply in 28858)
Frame 28618: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{3CE8ED40-6CFE-47DB-8508-9072AD0B8C48}
id 0
Ethernet II, Src: IntelCor_d6:66:72 (3c:f8:62:d6:66:72), Dst: ASUSTekC_76:a6:80 (2c:4d:54:76:a6:80)
Internet Protocol Version 4, Src: 192.168.1.164, Dst: 128.119.245.12
Internet Control Message Protocol
No.     Time           Source                Destination           Protocol Length Info
  28858 19.282788      128.119.245.12        192.168.1.164         ICMP     562    Echo (ping) reply    id=0x0001, seq=103/26368, ttl=42
```

Контрольні запитання:

1. Визначте IP адреси вашої та цільової робочих станцій. IP адреси:
Моя: 192.168.1.164
Цільва: 128.119.245.12.

2. Яке значення в полі номера протоколу вищого рівня в заголовку IP першого пакету із запитом ICMP?
26048.



No.	Time	Source	Destination	Protocol	Length	Info
24455	16.129570	192.168.1.164	128.119.245.12	ICMP	562	Echo (ping) request id=0x0001, seq=100/25600, ttl=128 (reply in 24742)
24458	16.134439	195.209.101.53	192.168.1.164	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
24525	16.162775	91.79.74.110	192.168.1.164	ICMP	90	Destination unreachable (Port unreachable)
24601	16.193070	52.90.64.60	192.168.1.164	ICMP	90	Destination unreachable (Port unreachable)
24742	16.273796	128.119.245.12	192.168.1.164	ICMP	562	Echo (ping) reply id=0x0001, seq=100/25600, ttl=42 (request in 24455)
26048	17.132044	192.168.1.164	128.119.245.12	ICMP	562	Echo (ping) request id=0x0001, seq=101/25856, ttl=128 (reply in 26196)
26196	17.263468	128.119.245.12	192.168.1.164	ICMP	562	Echo (ping) reply id=0x0001, seq=101/25856, ttl=42 (request in 26048)
27162	18.135148	192.168.1.164	128.119.245.12	ICMP	562	Echo (ping) request id=0x0001, seq=102/26112, ttl=128 (reply in 27312)
27164	18.136373	46.158.45.138	192.168.1.164	ICMP	90	Destination unreachable (Port unreachable)
27312	18.264934	128.119.245.12	192.168.1.164	ICMP	562	Echo (ping) reply id=0x0001, seq=102/26112, ttl=42 (request in 27162)

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.

```
Time to live: 128
Protocol: ICMP (1)
Header checksum: 0x39fc [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.164
Destination: 128.119.245.12
[2 IPv4 Fragments (2008 bytes): #26047(1480), #26048(528)]
   [Frame: 26047, payload: 0-1479 (1480 bytes)]
   [Frame: 26048, 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
```

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
```

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

Фрагменти відрізняються Flags- у кожного фрагменту він різний.

7. Розгляньте послідовність пакетів IP із запитами 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?

```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x88 (DSCP: AF41, ECN: Not-ECT)
Total Length: 548
Identification: 0xd93e (55614)
Flags: 0x00b9
...0 0101 1100 1000 = Fragment offset: 1480
Time to live: 42
Protocol: ICMP (1)
Header checksum: 0x7c89 [validation disabled]
[Header checksum status: Unverified]
Source: 128.119.245.12
Destination: 192.168.1.164
```

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 0000 0000 0000 = Fragment offset: 0
Time to live: 246
Protocol: ICMP (1)
Header checksum: 0xd8e9 [validation disabled]
[Header checksum status: Unverified]
Source: 195.209.101.53
Destination: 192.168.1.164
```

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, було проаналізовано протоколи IP та було проведено аналіз деталей роботи даних протоколів.