



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

Лабораторна робота № 5
З дисципліни: Комп'ютерні мережі

Протоколи ІР

Виконав:
Студент ІІІ курсу
Групи КА-74
Джалаганія Б.І.
Перевірив: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз деталей роботи протоколу IP.

Хід виконання роботи

The image shows a Windows command prompt window titled "Командная строка" and a Wireshark network analyzer window titled "Беспроводная сеть".

Command Prompt Output:

```
(c) Корпорация Майкрософт (Microsoft Corporation), 2016. Все права защищены.  
C:\Users\olena>ping -l 2000 gaia.cs.umass.edu  
  
Обмен пакетами с gaia.cs.umass.edu [128.119.245.12] с 2000 байтами данных:  
Превышен интервал ожидания для запроса.  
Превышен интервал ожидания для запроса.  
Превышен интервал ожидания для запроса.  
Превышен интервал ожидания для запроса.  
  
Статистика Ping для 128.119.245.12:  
    Пакетов: отправлено = 4, получено = 0, потеряно = 4  
    (100% потеря)  
  
C:\Users\olena>ping -l 2000 gaia.cs.umass.edu  
  
Обмен пакетами с gaia.cs.umass.edu [128.119.245.12] с 2000 байтами данных:  
Превышен интервал ожидания для запроса.  
Превышен интервал ожидания для запроса.  
Превышен интервал ожидания для запроса.  
Превышен интервал ожидания для запроса.  
  
Статистика Ping для 128.119.245.12:  
    Пакетов: отправлено = 4, получено = 0, потеряно = 4  
    (100% потеря)  
  
C:\Users\olena>
```

Wireshark Output:

The Wireshark packet list shows four ICMP Echo (ping) requests to 128.119.245.12, all with "no response found!".

No.	Time	Source	Destination	Protocol	Length	Info
86	6.097872	77.47.197.26	128.119.245.12	ICMP	562	Echo (ping) request id=0x0001, seq=94/24864, ttl=128 (no response found!)
134	10.889093	77.47.197.26	128.119.245.12	ICMP	562	Echo (ping) request id=0x0001, seq=95/24320, ttl=128 (no response found!)
195	15.888345	77.47.197.26	128.119.245.12	ICMP	562	Echo (ping) request id=0x0001, seq=96/24576, ttl=128 (no response found!)
267	20.887408	77.47.197.26	128.119.245.12	ICMP	562	Echo (ping) request id=0x0001, seq=97/24832, ttl=128 (no response found!)

The packet details pane shows the selected packet is an Internet Control Message Protocol (ICMP) Echo (ping) request. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Frame 86: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{E7910711-2CFD-4CF3-A912-85868977E86D}, id 0
> Ethernet II, Src: AzureWav_87:73:0d (74:c6:3b:87:73:0d), Dst: Hangzhou_9d:38:c8 (00:0f:e2:9d:38:c8)
> Internet Protocol Version 4, Src: 77.47.197.26, Dst: 128.119.245.12
> Internet Control Message Protocol

Frame 86 (562 bytes) | Reassembled IPv4 (2008 bytes)
Internet Control Message Protocol: Protocol

Пакеты: 588 - Показаны: 4 (0.7%) - Потеряно: 0 (0.0%) | Профиль: Default

Контрольні запитання:

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

Моя: 77.47.197.26

Цільова: 128.119.245.12.

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

86.

No.	Time	Source	Destination	Protocol	Length	Info
15	0.758626	77.47.196.169	255.255.255.255	UDP	68	64514 → 7533 Len=
31	2.321172	77.47.197.218	77.47.197.255	NBNS	92	Name query NB RET
33	2.375235	77.47.197.26	239.255.255.250	IGMPv2	46	Membership Report
49	3.779781	77.47.196.169	255.255.255.255	UDP	68	64514 → 7533 Len=
51	3.801908	77.47.197.218	77.47.197.255	NBNS	92	Name query NB RET
52	3.875465	77.47.197.26	224.0.0.252	IGMPv2	46	Membership Report
63	4.548267	77.47.197.218	77.47.197.255	NBNS	92	Name query NB RET
80	5.497693	77.47.197.218	77.47.197.255	NBNS	92	Name query NB RET
85	6.097871	77.47.197.26	128.119.245.12	IPv4	1514	Fragmented IP pro
86	6.097872	77.47.197.26	128.119.245.12	ICMP	562	Echo (ping) reque
104	7.765820	77.47.196.169	255.255.255.255	UDP	68	64514 → 7533 Len=
116	8.760049	77.47.196.169	255.255.255.255	UDP	68	64514 → 7533 Len=
130	10.457913	92.118.37.68	77.47.197.26	TCP	60	45859 → 37291 [SY
132	10.794702	77.47.196.169	255.255.255.255	UDP	68	64514 → 7533 Len=
133	10.889089	77.47.197.26	128.119.245.12	IPv4	1514	Fragmented IP pro
134	10.889093	77.47.197.26	128.119.245.12	ICMP	562	Echo (ping) reque

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)
Differentiated Services Field: 0x00 (DSCP
  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 даних 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 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?

```

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.