



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

Лабораторна робота № 5
З дисципліни: Комп'ютерні мережі

Протокол ІР

Виконав:
Студент ІІІ курсу
Групи КА-74
Микитенко О.В.
Перевірив: Кухарєв С. О.

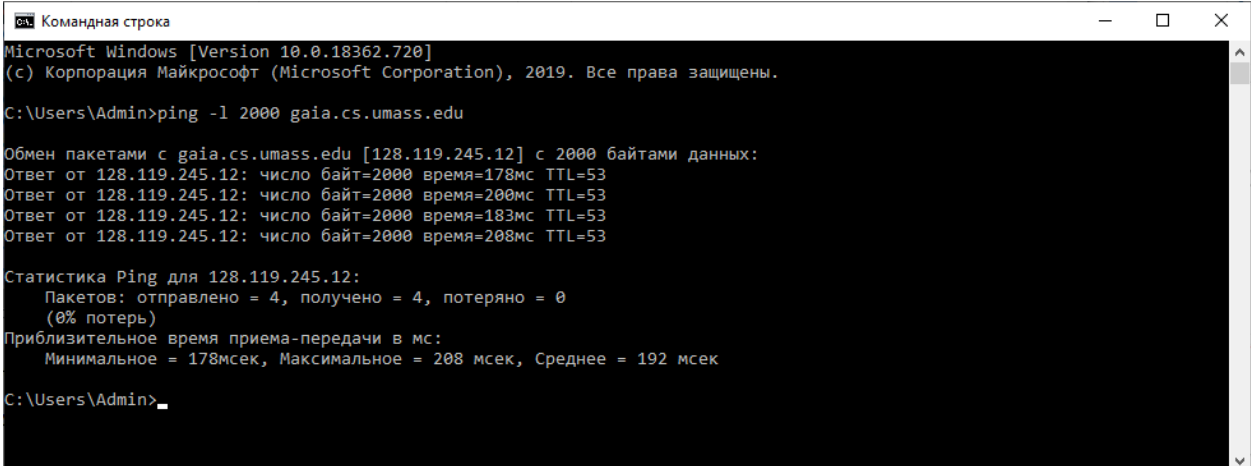
Київ 2020

Мета роботи: аналіз деталей роботи протоколу ICMP.

Хід роботи

Необхідно виконати наступні дії:

- ✓ Відкрийте командний термінал
- ✓ Запустіть Wireshark, почніть захоплення пакетів.
- ✓ Виконайте команду
 - windows: ping -l 2000 gaia.cs.umass.edu
 - linux: traceroute gaia.cs.umass.edu 2000
 - якщо відповіді від цільової робочої станції немає, можна використати іншу адресу, наприклад: 10.35.8.10 або 194.44.29.242 або IP адресу деякої робочої станції у локальній мережі (наприклад, зовнішню адресу вашої робочої станції)



```
Командная строка
Microsoft Windows [Version 10.0.18362.720]
(c) Корпорация Майкрософт (Microsoft Corporation), 2019. Все права защищены.

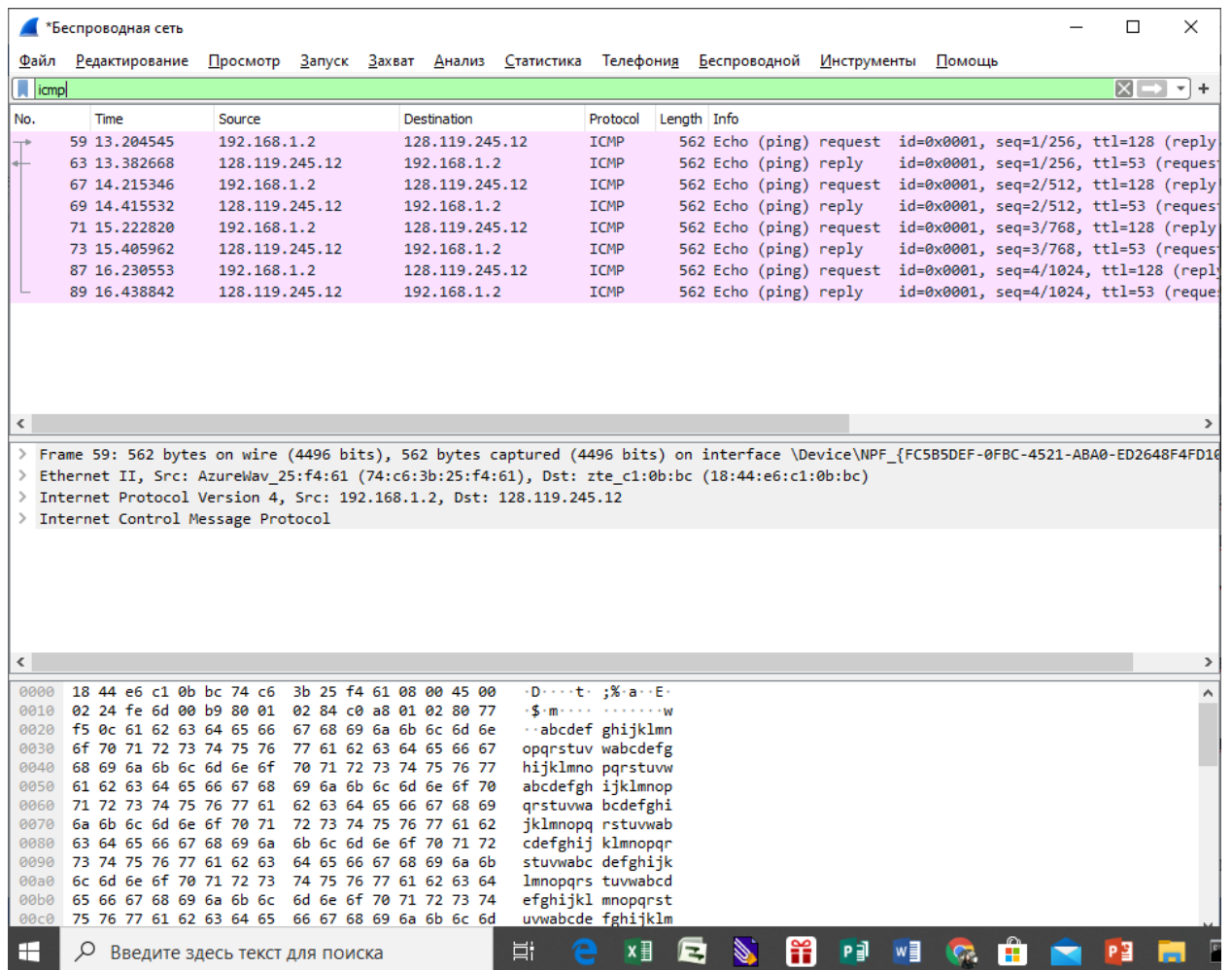
C:\Users\Admin>ping -l 2000 gaia.cs.umass.edu

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=178мс TTL=53
Ответ от 128.119.245.12: число байт=2000 время=200мс TTL=53
Ответ от 128.119.245.12: число байт=2000 время=183мс TTL=53
Ответ от 128.119.245.12: число байт=2000 время=208мс TTL=53

Статистика Ping для 128.119.245.12:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 178мсек, Максимальное = 208 мсек, Среднее = 192 мсек

C:\Users\Admin>
```

- ✓ Зупиніть захоплення пакетів.
- ✓ Перегляньте деталі захоплених пакетів. Для цього налаштуйте вікно деталей пакету: згорніть деталі протоколів усіх рівнів крім IP/ICMP (за допомогою знаків +/-).



- ✓ Приготуйте відповіді на контрольні запитання, роздрукуйте необхідні для цього пакети.
- ✓ Закрийте Wireshark, закрийте командний термінал.

Контрольні питання

1. Визначте IP адреси вашої та цільової робочих станцій.

Мій: 192.168.1.2

Цільовий: 128.119.245.12

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

```
Time to live: 128
Protocol: ICMP (1)
Header checksum: 0x0284 [validation]
```

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.

```
Internet Protocol Version 4, Src: 192.168.1.2, 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
  ...

[2 IPv4 Fragments (2008 bytes): #58(1480), #59(528)]
  [Frame: 58, payload: 0-1479 (1480 bytes)]
  [Frame: 59, payload: 1480-2007 (528 bytes)]
  [Fragment count: 2]
```

Payload = 548 – 20 = 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?

Встановлений біт MF (More Fragments) = 0, це говорить про те, що даний пакет не є фрагментом. Отже, пакет не 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
```

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

IP використовує наступні поля для відстеження утворених фрагментів: -
Ідентифікація: 16-бітне поле, яке однозначно визначає фрагмент вихідного пакета IP - Flag: 3-бітне поле, яке визначає спосіб фрагментації пакета. Воно використовується з полями "Зміщення фрагменту" та "Ідентифікація" для полегшення відновлення фрагментів у вихідний пакет.

```
Identification: 0x1afe (6910)
  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: 53
    Protocol: ICMP (1)
    Header checksum: 0x30f4 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.119.245.12
    Destination: 192.168.1.2
  [2 IPv4 Fragments (2008 bytes): #62(1480), #63(528)]
    [Frame: 62, payload: 0-1479 (1480 bytes)]
    [Frame: 63, payload: 1480-2007 (528 bytes)]
    [Fragment count: 2]
    [Reassembled IPv4 length: 2008]
    [Reassembled IPv4 data: 00008376000100016162636465666768696a6b6c6d6e6f70...]
  Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x8376 [correct]
    [Checksum Status: Good]
```

6. Які поля протоколу IP відрізняють перший фрагмент від другого?
Identification, Header checksum.
7. Розгляньте послідовність пакетів IP із запитамі ICMP вашої робочої станції. Які поля заголовку IP завжди змінюються?
Завжди змінюється поле Identification.
8. Розгляньте послідовність пакетів IP із запитамі ICMP вашої робочої станції. Які поля заголовку IP мають зберігати свої значення? Які поля мають змінюватися? Чому?
Identification має змінюватись, щоб розрізняти фрагменти і уникати проблем подвоєння, загублення. Всі інші зберігають свої значення.
9. Розгляньте послідовність пакетів IP із запитамі ICMP вашої робочої станції. Опишіть закономірність зміни значень поля Identification рівня IP.
Кожного разу додається одиниця до коду.
9. Розгляньте послідовність пакетів IP із повідомленнями TTL-exceeded від найближчого маршрутизатора. Які значення встановлені у полях Identification та TTL?

```
Identification: 0xfe6d (65133)
  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: 0x0284 [validation disabled]
    [Header checksum status: Unverified]
```

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?

Time to live: не змінюється

Identification: змінюється, щоб розрізняти фрагменти

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.