



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

Лабораторна робота № 4
З дисципліни: Комп'ютерні мережі

Протоколи ICMP

Виконала:
Студентка III курсу
Групи КА-71
Висоцька М.А.
Перевірив: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз деталей роботи протоколу ICMP.

Контрольні питання

1. Які IP адреси вашої та цільової робочих станцій?
192.168.1.165 192.168.1.1
2. Чому ICMP пакет не вказує/використовує номери вихідного та цільового портів?

Тому, що він користується адресами робочих станцій.

```
Source: 192.168.1.165  
Destination: 143.89.14.1
```

3. Дослідіть один з пакетів-запитів ICMP. Які тип та код зазначені у цьому пакеті? Скільки байтів займають поля контрольної суми, номера послідовності та ідентифікатору?

```
Internet Control Message Protocol  
Type: 8 (Echo (ping) request)  
Code: 0  
Checksum: 0x4cfb [correct]  
[Checksum Status: Good]  
Identifier (BE): 1 (0x0001)  
Identifier (LE): 256 (0x0100)  
Sequence number (BE): 96 (0x0060)  
Sequence number (LE): 24576 (0x6000)  
> [No response seen]  
> Data (32 bytes)
```

4. Дослідіть відповідний пакет з відповіддю на пакет із пункту 3. Які тип та код зазначені у цьому пакеті? Які інші поля має цей пакет? Скільки байтів займають поля контрольної суми, номера послідовності та ідентифікатору?

```
[No response seen]  
[Expert Info (Warning/Sequence): No response seen to ICMP request]  
[No response seen to ICMP request]  
[Severity level: Warning]  
[Group: Sequence]  
> Data (32 bytes)
```

5. Які IP адреси вашої та цільової робочих станцій?

192.168.1.165 192.168.1.1

6. Який номер протоколу IP використовується програмою?

4

7. Чи відрізняється пакет із запитом програми traceroute від пакету із запитом програми ping? Якщо так, наведіть приклади.

Так. Ping не мають відповіді, а traceroute в тому ж файлі дають відповідь.

```
106 Echo (ping) request id=0x0001, seq=62/15872, ttl=3 (no response found!)  
131 8801 → 15688 Len=89  
147 8801 → 15688 Len=105  
147 8801 → 15688 Len=105  
131 8801 → 15688 Len=89  
70 Time-to-live exceeded (Time to live exceeded in transit)  
106 Echo (ping) request id=0x0001, seq=62/15872, ttl=3 (no response found!)
```

8. Проаналізуйте пакет ICMP з повідомленням про помилку. Чи є у ньому деякі додаткові поля, які не зазначаються у повідомленні з підтвердженням. Якщо є – які саме поля і яку інформацію вони вміщують?

Так є.

```
Internet Control Message Protocol
  Type: 11 (Time-to-live exceeded)
  Code: 0 (Time to live exceeded in transit)
  Checksum: 0xf4ff [correct]
  [Checksum Status: Good]
  Unused: 00000000
  Internet Protocol Version 4, Src: 192.168.1.165, Dst: 128.93.162.63
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0xe189 (57737)
    > Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 1
    > [Expert Info (Note/Sequence): "Time To Live" only 1]
    Protocol: ICMP (1)
    Header checksum: 0xf32d [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.165
    Destination: 128.93.162.63
  Internet Control Message Protocol
```

9. Проаналізуйте три останні відповіді протоколу ICMP, які отримала ваша робоча станція. Як ці пакети відрізняються від пакетів з повідомленням про помилку? Чому вони відрізняються?

```
Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0xffa0 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence number (BE): 94 (0x005e)
  Sequence number (LE): 24064 (0x5e00)
  [Request frame: 3853]
  [Response time: 54,911 ms]
  Data (64 bytes)
```

10. Знайдіть етап ретрансляції повідомлень з найбільшою середньою затримкою. Чи є можливість оцінити географічну відстань між маршрутизаторами на цьому етапі?

Так, за допомогою довжини даних.

Висновок

В ході виконання даної лабораторної роботи, були покращено навички використання програми Wireshark для захоплення пакетів. Було проаналізовано протоколи ICMP та було проведено аналіз деталей роботи даних протоколів.