

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

Лабораторна робота № 4
З дисципліни: Комп'ютерні мережі

Протокол ІСМР

Виконала:
Студентка ІІІ курсу
Групи КА-77
Яцько Я. В.
Перевірів: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз основних деталей роботи протоколу ICMP.

Хід виконання роботи

The image displays two screenshots of the Wireshark network protocol analyzer, showing ICMP traffic analysis.

Top Screenshot: The main packet list shows a series of ICMP Echo (ping) requests from source 192.168.1.106 to destination 143.89.14.1. All requests are marked as "no response found!". The packet details pane shows the structure of an ICMP Echo request, including Type 8, Code 0, Checksum 0x4d5a, Identifier (BE) 1 (0x0001), Identifier (LE) 256 (0x0100), Sequence number (BE) 1 (0x0001), and Sequence number (LE) 256 (0x0100). The packet data section shows the raw hex data and its ASCII representation.

Bottom Screenshot: This screenshot shows a different set of ICMP traffic. It includes Echo requests, "Time-to-live exceeded" messages, and Echo replies. The packet details pane for Frame 6 shows an ICMP Echo request with Type 8, Code 0, Checksum 0xf7f6, Identifier (BE) 1 (0x0001), Identifier (LE) 256 (0x0100), Sequence number (BE) 8 (0x0008), and Sequence number (LE) 2048 (0x0800). The packet data section shows the raw hex data and its ASCII representation.

Контрольні питання

1. Які IP адреси вашої та цільової робочих станцій?

Source	Destination
192.168.1.106	143.89.14.1

2. Чому ICMP пакет не вказує/використовує номери вихідного та цільового портів?

Тому, що він користується адресами робочих станцій.

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: 0x4d5a [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 1 (0x0001)

Sequence number (LE): 256 (0x0100)

> [No response seen]

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]

✓ Data (32 bytes)

Data: 6162636465666768696a6b6c6d6e6f707172737475767761...

[Length: 32]

5. Які IP адреси вашої та цільової робочих станцій?

Моя: 192.168.1.106

Цільова: 128.93.162.63

6. Який номер протоколу IP використовується програмою?

Номер 8.

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.

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.

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?

Вони не містять поля NetBIOS Name Service

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 проведено аналіз деталей роботи даних протоколів.