

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

Лабораторна робота № 4
З дисципліни: Комп'ютерні мережі

Основи роботи протоколу ICMP

Виконала:
Студентка ІІІ курсу
Групи КА-74
Ковальчук О. О.
Перевірив: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз основних деталей роботи протоколу ICMP.

Хід виконання роботи

```
Командная строка
C:\Users\Olya> ping -n 10 www.ust.hk

Обмен пакетами с www.ust.hk [143.89.14.1] с 32 байтами данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 143.89.14.1:
    Пакетов: отправлено = 10, получено = 0, потеряно = 10
              (100% потеря)

C:\Users\Olya>
```

```
Командная строка
C:\Users\Olya>tracert www.inria.fr

Трассировка маршрута к inria-cms.inria.fr [128.93.162.63]
с максимальным числом прыжков 30:

 1  2 ms    2 ms    2 ms  192.168.0.1
 2  4 ms    4 ms    2 ms  malta20.zv.ua [10.200.20.1]
 3 12 ms   12 ms   11 ms  195-46-34-129.novograd.biz [195.46.34.129]
 4  7 ms    9 ms   24 ms  194.44.135.169
 5 18 ms   20 ms   22 ms  v3230.core1.waw1.he.net [216.66.84.117]
 6 43 ms   43 ms   45 ms  100ge16-2.core1.par2.he.net [184.105.213.121]
 7  *      43 ms   46 ms  renater.par.franceix.net [37.49.236.19]
 8 43 ms   45 ms   46 ms  xe1-0-1-paris1-rtr-131.noc.renater.fr [193.51.177.128]
 9 43 ms   45 ms   45 ms  te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
10 46 ms   44 ms   44 ms  inria-rocquencourt-te1-4-inria-rtr-021.noc.renater.fr [193.51.184.177]
11 46 ms   46 ms   44 ms  unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
12 43 ms   44 ms   45 ms  inria-cms.inria.fr [128.93.162.63]

Трассировка завершена.

C:\Users\Olya>
```

Контрольні запитання:

1. Які IP адреси вашої та цільової робочих станцій?

Wireshark packet capture showing ICMP Echo (ping) requests. The packet list shows 10 requests, all with "no response found!". The packet details pane shows the selected packet (No. 59) as an ICMP Echo request with sequence number 126. The packet bytes pane shows the raw data of the ICMP request.

No.	Time	Source	Destination	Protocol	Length	Info
22	13.639274	192.168.0.106	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=124/31744, ttl=128 (no response found!)
30	18.640126	192.168.0.106	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=125/32000, ttl=128 (no response found!)
59	23.640077	192.168.0.106	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=126/32256, ttl=128 (no response found!)
111	28.638374	192.168.0.106	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=127/32512, ttl=128 (no response found!)
131	33.638370	192.168.0.106	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=128/32768, ttl=128 (no response found!)
144	38.639463	192.168.0.106	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=129/33024, ttl=128 (no response found!)
177	43.638310	192.168.0.106	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=130/33280, ttl=128 (no response found!)
188	48.702879	192.168.0.106	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=131/33536, ttl=128 (no response found!)

Frame 59: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F69135E3-F800-4849-987E-D6BA2ECEC81A}, id 0
Ethernet II, Src: 5a:00:b4:e5:9c:fb (5a:00:b4:e5:9c:fb), Dst: Tp-LinkT_fb:ed:d2 (70:4f:57:fb:ed:d2)
Internet Protocol Version 4, Src: 192.168.0.106, Dst: 143.89.14.1
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x4cdd [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence number (BE): 126 (0x007e)
Sequence number (LE): 32256 (0x7e00)
[No response seen]
[Expert Info (Warning/Sequence): No response seen to ICMP request]
Data (32 bytes)

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

No corresponding response frame was seen (icmp.no_resp)

Пакеты: 235 · Показаны: 10 (4.3%) · Потеряно: 0 (0.0%) · Профиль: Default

Вихідний IP: 192.168.0.106

Цільовий IP: 143.89.14.1

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

Тому що, цей пакет потрібен для знаходження помилок при передачі запитів між вказаними адресами.

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?

Wireshark packet capture showing ICMP Echo (ping) requests. The packet list shows 10 requests, all with "no response found!". The packet details pane shows the selected packet (No. 59) as an ICMP Echo request with sequence number 126. The packet bytes pane shows the raw data of the ICMP request.

No.	Time	Source	Destination	Protocol	Length	Info
22	13.639274	192.168.0.106	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=124/31744, ttl=128 (no response found!)
30	18.640126	192.168.0.106	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=125/32000, ttl=128 (no response found!)
59	23.640077	192.168.0.106	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=126/32256, ttl=128 (no response found!)
111	28.638374	192.168.0.106	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=127/32512, ttl=128 (no response found!)
131	33.638370	192.168.0.106	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=128/32768, ttl=128 (no response found!)
144	38.639463	192.168.0.106	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=129/33024, ttl=128 (no response found!)
177	43.638310	192.168.0.106	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=130/33280, ttl=128 (no response found!)
188	48.702879	192.168.0.106	143.89.14.1	ICMP	74	Echo (ping) request id=0x0001, seq=131/33536, ttl=128 (no response found!)

Frame 59: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F69135E3-F800-4849-987E-D6BA2ECEC81A}, id 0
Ethernet II, Src: 5a:00:b4:e5:9c:fb (5a:00:b4:e5:9c:fb), Dst: Tp-LinkT_fb:ed:d2 (70:4f:57:fb:ed:d2)
Destination: Tp-LinkT_fb:ed:d2 (70:4f:57:fb:ed:d2)
Source: 5a:00:b4:e5:9c:fb (5a:00:b4:e5:9c:fb)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.0.106, Dst: 143.89.14.1
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x4cdd [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence number (BE): 126 (0x007e)
Sequence number (LE): 32256 (0x7e00)
[No response seen]
[Expert Info (Warning/Sequence): No response seen to ICMP request]
Data (32 bytes)

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

Checksum (icmp.checksum), 2 байты

Пакеты: 235 · Показаны: 10 (4.3%) · Потеряно: 0 (0.0%) · Профиль: Default

Тип: 8

Код: 0

Байти поля контрольної суми: 2 байти

Байти поля номера послідовності: 2 байти

Байти поля ідентифікатора: 2 байти

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? Відповідь не була отримана на жоден з 10 пакетів.
5. Які IP адреси вашої та цільової робочих станцій?

The screenshot shows the Wireshark network traffic analysis interface. The top menu bar includes options like "Беспроводная сеть", "Файл", "Редактирование", "Просмотр", "Запуск", "Захват", "Анализ", "Статистика", "Телефония", "Беспроводной", "Инструменты", and "Помощь". The main window displays a list of captured packets, with the selected packet (No. 3) showing details in the "Packet Details" pane. The "Packet List" pane shows a summary of the captured traffic, including ICMP Echo (ping) requests and responses. The "Packet Bytes" pane shows the raw data of the selected packet, including the Ethernet II header, Internet Protocol Version 4 header, and Internet Control Message Protocol header. The status bar at the bottom indicates that 161 packets were captured, 79 (49.1%) were shown, and 0 (0.0%) were lost.

No.	Time	Source	Destination	Protocol	Length	Info
3	2.727987	192.168.0.106	128.93.162.63	ICMP	106	Echo (ping) request id=0x0001, seq=76/19456, ttl=1 (no response found!)
4	2.730225	192.168.0.1	192.168.0.106	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
5	2.734945	192.168.0.106	128.93.162.63	ICMP	106	Echo (ping) request id=0x0001, seq=77/19712, ttl=1 (no response found!)
6	2.737419	192.168.0.1	192.168.0.106	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
7	2.745118	192.168.0.106	128.93.162.63	ICMP	106	Echo (ping) request id=0x0001, seq=78/19968, ttl=1 (no response found!)
8	2.747398	192.168.0.1	192.168.0.106	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
14	2.763611	192.168.0.1	192.168.0.106	ICMP	120	Destination unreachable (Port unreachable)
19	4.264385	192.168.0.1	192.168.0.106	ICMP	120	Destination unreachable (Port unreachable)

Frame 7: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{F69135E3-F800-4B49-9B7E-D6BA2ECEC81A}, id 0
> Ethernet II, Src: 5a:00:b4:e5:9c:fb (5a:00:b4:e5:9c:fb), Dst: Tp-LinkT_fb:ed:d2 (70:4f:57:fb:ed:d2)
> Internet Protocol Version 4, Src: 192.168.0.106, Dst: 128.93.162.63
> Internet Control Message Protocol

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

Internet Control Message Protocol: Protocol

Пакеты: 161 · Показаны: 79 (49.1%) · Потеряно: 0 (0.0%) · Профиль: Default

Вихідний IP: 192.168.0.1,

Цільовий IP: 128.93.162.63;

6. Який номер протоколу IP використовується програмою? Version 4;

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

Команда ping дає можливість перевірити доступність певного ресурсу мережі: подає на вказаний хост пакет заданого розміру, що згодом повертається назад. У нашому випадку відповідь не була отримана на жоден із 10 відправлених пакетів.

Команда tracert також надсилає пакет до вказаного ресурсу, ще й послідовно запитує і вимірює час затримку між маршрутизаторами на шляху пакета. Таким чином, можна визначити інтервал найбільших затримок. Також, при використанні команди tracert з адресом, що вказаним символьно, автоматично перевіряється робота DNS сервісу, який вертає запитую IP адресу заданого ресурсу мережі.

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?

Wireshark packet capture showing an ICMP Echo (ping) request. The packet is highlighted in blue. The packet details pane shows the ICMP Echo (ping) request with fields: Type: 8 (Echo (ping) request), Code: 0, Checksum: 0xf792 [correct], Identifier (BE): 1 (0x0001), Identifier (LE): 256 (0x0100), Sequence number (BE): 108 (0x006c), Sequence number (LE): 27648 (0x6c00). The packet bytes pane shows the raw data of the ICMP Echo request.

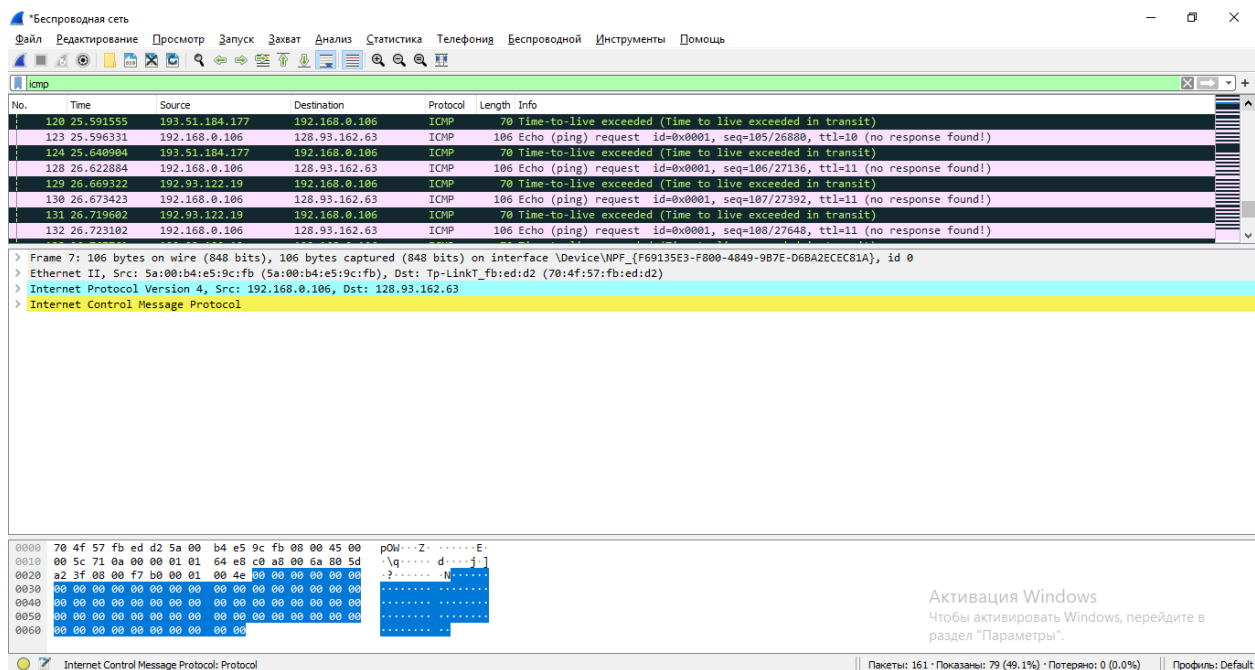
Є поле No response seen, у якому зазначено, що не було відповіді на запит ICMP.

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?

Wireshark packet capture showing three ICMP Echo (ping) replies. The packets are highlighted in blue. The packet details pane shows the ICMP Echo (ping) reply with fields: Type: 0 (Echo (ping) reply), Code: 0, Checksum: 0xf791 [correct], Identifier (BE): 1 (0x0001), Identifier (LE): 256 (0x0100), Sequence number (BE): 109 (0x006d), Sequence number (LE): 27904 (0x6d00). The packet bytes pane shows the raw data of the ICMP Echo reply.

Тому що, у пакетах з помилкою не було отримано відповіді.

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



Є така можливість.

Висновок

В ході виконання даної лабораторної роботи, були покращено навички використання програми Wireshark для захоплення пакетів. Було проаналізовано основні деталі роботи протоколу ICMP.