

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 III курсу
Групи КА-74
Семіконь Я. В.
Перевірив: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз основних деталей роботи протоколу ICMP.

Wireshark, необхідними для дослідження мережевих протоколів.Начало формы

Хід виконання роботи

```
Last login: Tue May 5 13:44:19 on ttys000
[Germes-Air:~ some321user_34$ ping -c 10 www.ust.hk
PING www.ust.hk (143.89.14.1): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
Request timeout for icmp_seq 6
Request timeout for icmp_seq 7
Request timeout for icmp_seq 8

--- www.ust.hk ping statistics ---
10 packets transmitted, 0 packets received, 100.0% packet loss
Germes-Air:~ some321user_34$
```

No.	Time	Source	Destination	Protocol	Length	Info
3	1.067139	192.168.1.102	143.89.14.1	ICMP	98	Echo (ping) request id=0x5404, seq=0/0, ttl=64 (no response found!)
4	2.071952	192.168.1.102	143.89.14.1	ICMP	98	Echo (ping) request id=0x5404, seq=1/256, ttl=64 (no response found!)
5	3.075425	192.168.1.102	143.89.14.1	ICMP	98	Echo (ping) request id=0x5404, seq=2/512, ttl=64 (no response found!)
6	4.080249	192.168.1.102	143.89.14.1	ICMP	98	Echo (ping) request id=0x5404, seq=3/768, ttl=64 (no response found!)
7	5.082020	192.168.1.102	143.89.14.1	ICMP	98	Echo (ping) request id=0x5404, seq=4/1024, ttl=64 (no response found!)
8	6.081901	192.168.1.102	143.89.14.1	ICMP	98	Echo (ping) request id=0x5404, seq=5/1280, ttl=64 (no response found!)
9	7.081777	192.168.1.102	143.89.14.1	ICMP	98	Echo (ping) request id=0x5404, seq=6/1536, ttl=64 (no response found!)
10	8.084837	192.168.1.102	143.89.14.1	ICMP	98	Echo (ping) request id=0x5404, seq=7/1792, ttl=64 (no response found!)
11	9.087849	192.168.1.102	143.89.14.1	ICMP	98	Echo (ping) request id=0x5404, seq=8/2048, ttl=64 (no response found!)
14	10.088192	192.168.1.102	143.89.14.1	ICMP	98	Echo (ping) request id=0x5404, seq=9/2304, ttl=64 (no response found!)

```
[Germes-Air:~ some321user_34$ traceroute -I www.inria.fr
traceroute to inria-cms.inria.fr (128.93.162.63), 64 hops max, 72 byte packets
 1 192.168.1.1 (192.168.1.1) 3.155 ms 1.755 ms 11.190 ms
 2 92-244-97-1.kievnet.com.ua (92.244.97.1) 2.173 ms 5.953 ms 6.411 ms
 3 mx80-20g-unicorn.kievnet.com.ua (92.244.96.57) 3.725 ms 2.042 ms 4.340 ms
 4 mx104-20g-mx80-wr.kievnet.com.ua (109.108.88.61) 11.592 ms 4.949 ms 3.107
ms
 5 ae3-235.rt.ntl.kiv.ua.retn.net (87.245.237.110) 2.726 ms 1.861 ms 6.759 m
s
 6 ae0-9.rt.thv.par.fr.retn.net (87.245.233.186) 77.432 ms 49.884 ms 40.247
ms
 7 * * *
 8 193.51.180.44 (193.51.180.44) 56.050 ms 63.933 ms 49.527 ms
 9 te1-1-inria-rtr-021.noc.renater.fr (193.51.177.107) 51.007 ms 60.703 ms 8
2.922 ms
10 inria-rocquencourt-te1-4-inria-rtr-021.noc.renater.fr (193.51.184.177) 52.6
68 ms 66.639 ms 45.643 ms
11 unit240-reth1-vfw-ext-dcl.inria.fr (192.93.122.19) 47.715 ms 57.412 ms 49
.411 ms
12 inria-cms.inria.fr (128.93.162.63) 48.922 ms 52.402 ms 56.479 ms
Germes-Air:~ some321user_34$
```

Контрольні питання

1. Які IP адреси вашої та цільової робочих станцій?

Наша станція: 192.168.1.102

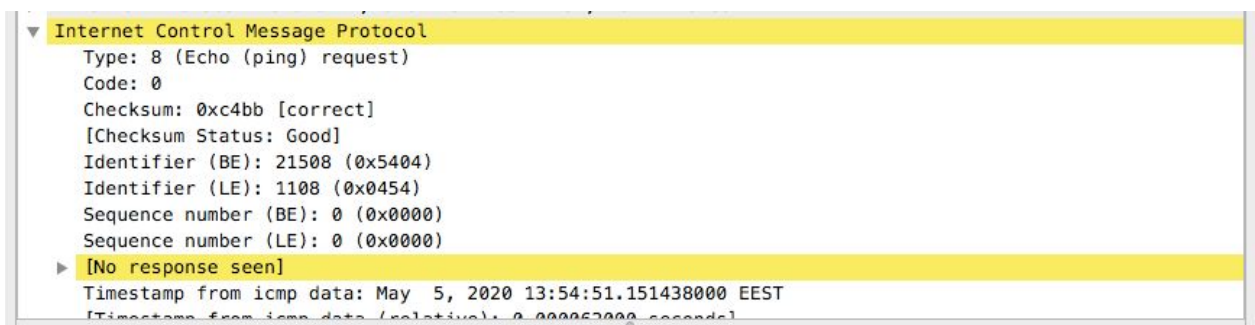
Цільова: 143.89.14.1

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

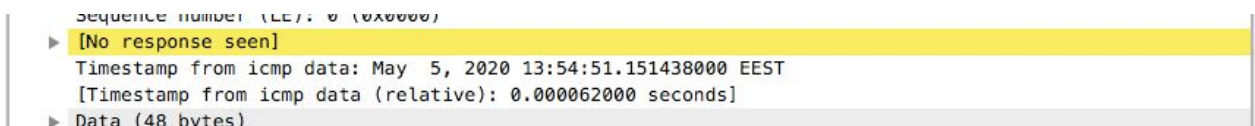
Тому що, цей пакет потрібен для знаходження помилок при передачі запитів між вказаними адресами.

Протокол ICMP - це протокол мережевого рівня, а порти використовуються на транспортному рівні.

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?



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.



5. Які IP адреси вашої та цільової робочих станцій?

66	5.520866	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=1/256, ttl=1 (no response found!)
67	5.522985	192.168.1.1	192.168.1.102	ICMP	114 Time-to-live exceeded (Time to live exceeded in transit)
70	5.530440	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=2/512, ttl=1 (no response found!)
71	5.532002	192.168.1.1	192.168.1.102	ICMP	114 Time-to-live exceeded (Time to live exceeded in transit)
72	5.532230	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=3/768, ttl=1 (no response found!)
73	5.543210	192.168.1.1	192.168.1.102	ICMP	114 Time-to-live exceeded (Time to live exceeded in transit)
74	5.543457	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=4/1024, ttl=2 (no response found!)
75	5.545462	92.244.97.1	192.168.1.102	ICMP	114 Time-to-live exceeded (Time to live exceeded in transit)
78	5.550071	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=5/1280, ttl=2 (no response found!)
79	5.555849	92.244.97.1	192.168.1.102	ICMP	114 Time-to-live exceeded (Time to live exceeded in transit)
80	5.556091	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=6/1536, ttl=2 (no response found!)
81	5.562347	92.244.97.1	192.168.1.102	ICMP	114 Time-to-live exceeded (Time to live exceeded in transit)
82	5.562507	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=7/1792, ttl=3 (no response found!)
83	5.566072	92.244.96.57	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
86	5.578297	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=8/2048, ttl=3 (no response found!)
87	5.580216	92.244.96.57	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
88	5.580335	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=9/2304, ttl=3 (no response found!)
89	5.584582	92.244.96.57	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
90	5.584704	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=10/2560, ttl=4 (no response found!)
91	5.596180	109.108.88.61	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
94	5.601446	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=11/2816, ttl=4 (no response found!)
95	5.606268	109.108.88.61	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
96	5.606427	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=12/3072, ttl=4 (no response found!)
97	5.609424	109.108.88.61	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
98	5.609548	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=13/3328, ttl=5 (no response found!)
99	5.612169	87.245.237.110	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
102	5.616281	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=14/3584, ttl=5 (no response found!)
103	5.618049	87.245.237.110	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)

Наша: 192.168.1.102

Цільова: 128.93.162.63

6. Який номер протоколу IP використовується програмою?

Version 4;

▼ Internet Protocol Version 4, Src: 192.168.1.102, 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: 72	
Identification: 0x8463 (33891)	
► Flags: 0x0000	
...0 0000 0000 0000 = Fragment offset: 0	
► Time to live: 1	
Protocol: ICMP (1)	
Header checksum: 0x50a7 [validation disabled]	
[Header checksum status: Unverified]	
Source: 192.168.1.102	

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

Так, відрізняється.

Ping: перевірка доступності мережевих ресурсів. (в нашому випадку відповіді ми не отримали)

Traceroute : посилає пакет до ресурсу та вимірює час затримки. + DNS повертає IP адресу заданному ресурсу мережі. (в нашому випадку відповіді отримані)

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? бачимо поле *no response seen*

```

▶ Frame 66: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
▶ Ethernet II, Src: Apple_a0:e6:ff (70:56:81:a0:e6:ff), Dst: EdimaxTe_61:bc:ac (80:1f:02:61:bc:ac)
▶ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.93.162.63
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x739c [correct]
  [Checksum Status: Good]
  Identifier (BE): 33890 (0x8462)
  Identifier (LE): 25220 (0x6284)
  Sequence number (BE): 1 (0x0001)
  Sequence number (LE): 256 (0x0100)
▶ [No response seen]
▶ Data (44 bytes)
0000  80 1f 02 61 bc ac 70 56 81 a0 e6 ff 08 00 45 00  ..a..pV .....E-
0010  00 48 84 63 00 00 01 01 50 a7 c0 a8 01 66 80 5d  ..H.c... P....f.]
0020  a2 3f 08 00 73 9c 84 62 00 01 00 00 00 00 00 00  ..?..s..b .....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....

```

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?

95	5.606268	109.108.88.61	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
96	5.606427	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=12/3072, ttl=4 (no response found!)
97	5.609424	109.108.88.61	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
98	5.609548	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=13/3328, ttl=5 (no response found!)
99	5.612169	87.245.237.110	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
102	5.616281	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=14/3584, ttl=5 (no response found!)
103	5.618049	87.245.237.110	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
104	5.618158	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=15/3840, ttl=5 (no response found!)
105	5.624815	87.245.237.110	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
106	5.624939	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=16/4096, ttl=6 (no response found!)
107	5.702163	87.245.233.186	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
110	6.048621	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=17/4352, ttl=6 (no response found!)
111	6.098317	87.245.233.186	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
112	6.098503	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=18/4608, ttl=6 (no response found!)
113	6.138629	87.245.233.186	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
114	6.138791	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=19/4864, ttl=7 (no response found!)
123	11.142525	192.168.1.102	128.93.162.63	ICMP	86 Echo (ping) request id=0x8462, seq=20/5120, ttl=7 (no response found!)

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? Так, за допомогою довжини даних.

Висновок

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