



МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ  
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ  
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»  
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ  
Кафедра Інформаційної Безпеки

Практикум з Основ комп'ютерних мереж  

---

Протоколи мережного рівня – IP і ICMP

Перевірів:

\_\_\_\_\_

Виконав:

студент I курсу

групи ФБ-01

Сахній Н.Р.

Київ 2021

Запустимо **traceroute** і змусимо відправляти дейтаграми різної довжини. Послідовність дій відрізняється в залежності від того, на якій платформі виконується – Unix/Linux чи Windows.

## Linux/Unix

За допомогою команди **traceroute** розмір дейтаграми UDP, що посилається за призначенням, може бути явно встановлений шляхом зазначення кількості байтів дейтаграми. Це значення вводиться в команді **traceroute** відразу після імені або адреси призначення.

Наприклад, щоб **traceroute** відправила дейтаграму довжиною 2000 байт на адресу gaia.cs.umass.edu, команда має виглядати:

```
$ traceroute gaia.cs.umass.edu 2000
```

Виконаємо наступні дії:

1. Запустимо Wireshark і почнемо перехоплення пакетів.
2. Введемо 3 команди **traceroute**, одна з довжиною 56 байт, наступна з довжиною 2000 байт, і остання з довжиною 3500 байт.
3. Зупинимо перехоплення пакетів

## Дослідження перехоплених пакетів IP

The screenshot shows the Wireshark interface with a packet capture on interface eth0. The packet list shows a series of UDP packets from 192.168.1.144 to 128.119.245.12. Packet 23 is selected, showing details of an ICMP Echo (ping) request. The packet structure is: Ethernet II, Internet Protocol Version 4, ICMP Echo (ping) request. The packet length is 70 bytes. The source address is 192.168.1.144 and the destination address is 128.119.245.12. The packet data shows the ICMP header and the payload 'lh...8...\$FGHIJKLMVWXYZ'.

У перехоплених даних ми повинні побачити серію ICMP ехо-запитів або сегментів UDP, що були відправлені, та відповіді на них проміжних маршрутизаторів.

1. Виберемо перший ICMP ехо-запит, який був посланий моїм комп'ютером, і розкриємо деталі заголовку протоколу IP. Якою є IP адреса мого комп'ютера? Як показано на рисунку зверху ↑ IP адреса мого комп'ютера 192.168.1.144

2. Дивлячись на заголовок IP, сказати яким є значення поля протоколу вищого рівня.

Тут значення поля протоколу вищого рівня 17, яке означає, що на вищому рівні протокол UDP

3. Який розмір має IP заголовок? Скільки байтів містять дані корисного навантаження IP дейтаграми? Пояснити, як це визначено.

Розмір IP заголовка рівний 20 байтам. Дані корисного навантаження IP дейтаграми знаходяться як різниця довжини пакета та довжини заголовка:  $56 - 20 = 36$  (байтів)

4. Чи була ця IP дейтаграма фрагментована? Пояснити свою відповідь.

Ні, не була фрагментована, на що вказує флаг "More fragments" та "Зміщення пакета", які рівні нулю.

Далі, відсортуюємо пакети трасування за IP адресою відправника. Виберемо перший ICMP ехо-запит і розкриємо деталі заголовку протоколу IP.

5. Які поля IP дейтаграми завжди змінюються?

Identification (ідентифікує пакет), Header Checksum (забезпечує цілісність заголовку). Адже вони є унікальними для кожного пакета

6. Які поля IP дейтаграми не змінюються? Які поля не мають змінюватися? Які поля мають змінюватися? Чому?

Не змінюються: Version, Header Length, Total Length, Flags, Fragment Offset, Protocol, Source Address, Destination Address;

Не мають змінюватись: Version (бо ми використовуємо IPv4 для всіх запитів), Header Length (такі запити мають довжину 20 байт), Total Length (таке в тих запитах, що були відправлені з однаковою довжиною), Protocol (протокол вищого рівня для всіх пакетів буде UDP), Source Address та Destination Address (адже запити відбувається між двома незмінними вузлами);

Мають змінюватись: Identification (ідентифікує пакет, тому унікальне), Time to Live (має збільшуватись через кожні три запити), Header Checksum (забезпечує цілісність заголовку, унікальне).

Далі, знайдемо пакети ICMP відповідей.

7. Якими є значення полів ідентифікації  
Identification 0x9080 (36992),  
Time to Live: 64

```
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0x6587 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.1
Destination Address: 192.168.1.144
▼ Internet Control Message Protocol
  Type: 11 (Time-to-live exceeded)
  Code: 0 (Time to live exceeded in transit)
  Checksum: 0x2cf2 [correct]
  [Checksum Status: Good]
  Unused: 00000000
  ▼ Internet Protocol Version 4, Src: 192.168.1.144, Dst: 128.119.245.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 56
      Identification: 0x0de7 (3559)
0000 00 0c 29 e2 8f c7 bc ee 7b 6c 68 68 08 00 45 c0  ..)....
0010 00 54 90 80 00 00 40 01 65 87 c0 a8 01 01 c0 a8  .T....
```

8. Чи ці значення не змінюються для всіх ICMP пакетів, що були послані на мій комп'ютер найближчим роутером? Чому?

Identification змінюється, адже це значення унікальне для кожного пакета.

TTL пакетів, що послані найближчим роутером не змінюється і є якомога більші, тому що пакет повинен точно повернутися до нас, поки не став не діючим.

## Фрагментація

Відсортуюмо лістинг пакетів за часом.

No.	Time	Source	Destination	Protocol	Length	Info
254	10.853383528	192.168.1.1	192.168.1.144	DNS	130	Standard query response 0xid17 AAAA gaia.cs.uma
255	10.853668378	192.168.1.144	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=
256	10.853840200	192.168.1.144	128.119.245.12	UDP	534	43954 → 33434 Len=1972
257	10.853947159	192.168.1.144	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=
258	10.854053092	192.168.1.144	128.119.245.12	UDP	534	38999 → 33435 Len=1972
259	10.854157201	192.168.1.144	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=
260	10.854270039	192.168.1.144	128.119.245.12	UDP	534	52686 → 33436 Len=1972
261	10.854398974	192.168.1.144	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=
262	10.854513932	192.168.1.144	128.119.245.12	UDP	534	36253 → 33437 Len=1972
263	10.854643911	192.168.1.144	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=
264	10.854756392	192.168.1.144	128.119.245.12	UDP	534	48143 → 33438 Len=1972
265	10.854852876	192.168.1.144	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=
266	10.854962487	192.168.1.144	128.119.245.12	UDP	534	46834 → 33439 Len=1972
267	10.855068747	192.168.1.144	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=
268	10.855190644	192.168.1.144	128.119.245.12	UDP	534	33829 → 33440 Len=1972
269	10.855314330	192.168.1.144	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=
270	10.855422201	192.168.1.144	128.119.245.12	UDP	534	51818 → 33441 Len=1972
271	10.855525010	192.168.1.144	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=
272	10.855631895	192.168.1.144	128.119.245.12	UDP	534	56222 → 33442 Len=1972
273	10.855742570	192.168.1.144	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=

Frame 255: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface eth0, id 0

Ethernet II, Src: VMware\_e2:8f:c7 (00:0c:29:e2:8f:c7), Dst: ASUSTekC\_6c:68:68 (bc:ee:7b:6c:68:68)

Internet Protocol Version 4, Src: 192.168.1.144, 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: 1500

Identification: 0x1270 (4720)

Flags: 0x20, More fragments

0... .... = Reserved bit: Not set

.0.. .... = Don't fragment: Not set

..1. .... = More fragments: Set

Fragment Offset: 0

Time to Live: 1

Protocol: UDP (17)

Header Checksum: 0x49e5 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.144

Destination Address: 128.119.245.12

[Reassembled IPv4 in frame: 256]

Data (1480 bytes)

0010 05 dc 12 70 20 00 01 11 49 e5 c0 a8 01 90 80 77 ...p...

0020 f5 0c ab b2 82 9a 07 bc cd d9 40 41 42 43 44 45 .....

0030 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 FGHIJKLM

0040 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 VWXYZ[\]

0050 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 fghijklm

0060 76 77 78 79 7a 7b 7c 7d 7e 7f 40 41 42 43 44 45 vwxyz{}

0070 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 FGHIJKLM

Flags (3 bits) (ip.flags), 1 byte(s) Packets: 911 · Displayed: 911 (100.0%) · Dropped: 0 (0.0%) Profile: Default

9. Знайдемо перший ICMP Echo Request. Чи було це повідомлення фрагментованим на декілька дейтаграм?

Знайдено перший пакет↑, що був відправлений після команди “traceroute 2000”. Воно фрагментоване на декілька дейтаграм.

10. Виведемо перший фрагмент фрагментованої IP дейтаграми. Яка інформація підкаже, що ця дейтаграма була фрагментована? Якої довжини ця IP дейтаграма?

Оскільки це перший фрагмент фрагментованої IP дейтаграми, то на фрагментованість вказує флаг 1 у полі More fragments: Set; Total Length: 1500 байт

11. Виведемо другий фрагмент. Яка інформація покаже, що це не перший фрагмент? Чи існують ще якісь фрагменти? Чому?

```
Identification: 0x1270 (4720)
▼ Flags: 0x00
  0... .... = Reserved bit: Not set
  .0... .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
Fragment Offset: 1480
```

Те, що це фрагмент тієї ж IP дейтаграми вказує однакове значення Identification: 0x1270 (4720), а те, що він другий і після нього більше немає фрагментів вказує флаг 0 у полі More fragments: Not set та поле Fragment Offset: 1480

12. Скільки фрагментів було створено з оригінальної дейтаграми?

З оригінальної дейтаграми створено 2 фрагменти.

13. Яке поле змінюється в IP заголовку у фрагментах?

Total Length (для першого 1500 байтів, а для другого 520), Flags (у першому фрагменті має значення 20, а в другому 00), Fragment Offset (у першому 0, а в другому 1480) та Header checksum (унікальне значення).

## Дослідження протоколу ICMP

Далі ми розглянемо деякі аспекти протоколу ICMP:

- ICMP повідомлення, які генеруються програмою *ping*;
- ICMP повідомлення, які генерується програмою *traceroute*;
- Формат та зміст ICMP повідомлень.

### ICMP та ping

Почнемо дослідження ICMP за допомогою програми *ping*. Програма *ping* – це простий засіб, який дозволяє будь-якому користувачеві перевірити досяжність деякої IP адреси. Програма *ping* відправляє пакет ICMP (ехо-запит) на цільову IP адресу, яку ми перевіряємо, та або відповідає, надсилаючи нам пакет ICMP (ехо-відповідь), або не відповідає.

Виконаймо наступне:

1. Запустимо командне вікно (Unix/Linux – shell).
2. Запустимо Wireshark і почнемо перехоплення пакетів.
3. В командному рядку наберемо команду

```
$ ping -c 10 <hostname>
```

де *hostname* – це доменне ім'я або IP адреса хосту.

Пояснити, що означає аргумент 10:

Означає, що TTL пакета дорівнює 10

4. Спостерігаємо за результатами, які виводить програма *ping*. Після завершення роботи програми треба зупинити перехоплення пакетів Wireshark.

По результатам *ping* – тесту дати відповіді на наступні запитання:

```
(snz24@cybernaz)~$ ping -c 10 youtube.com
PING youtube.com (172.217.18.78) 56(84) bytes of data.
64 bytes from bud02s26-in-f14.1e100.net (172.217.18.78): icmp_seq=1 ttl=119 time=109 ms
64 bytes from bud02s26-in-f14.1e100.net (172.217.18.78): icmp_seq=2 ttl=119 time=37.5 ms
64 bytes from bud02s26-in-f14.1e100.net (172.217.18.78): icmp_seq=3 ttl=119 time=36.0 ms
64 bytes from bud02s26-in-f14.1e100.net (172.217.18.78): icmp_seq=4 ttl=119 time=18.2 ms
64 bytes from bud02s26-in-f14.1e100.net (172.217.18.78): icmp_seq=5 ttl=119 time=17.8 ms
64 bytes from bud02s26-in-f14.1e100.net (172.217.18.78): icmp_seq=6 ttl=119 time=20.4 ms
64 bytes from bud02s26-in-f14.1e100.net (172.217.18.78): icmp_seq=7 ttl=119 time=61.9 ms
64 bytes from bud02s26-in-f14.1e100.net (172.217.18.78): icmp_seq=8 ttl=119 time=17.6 ms
64 bytes from bud02s26-in-f14.1e100.net (172.217.18.78): icmp_seq=9 ttl=119 time=17.8 ms
64 bytes from bud02s26-in-f14.1e100.net (172.217.18.78): icmp_seq=10 ttl=119 time=20.6 ms

--- youtube.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9019ms
rtt min/avg/max/mdev = 17.570/35.669/108.807/27.868 ms
```



## ↑Результат роботи програми ping у Shell↑

No.	Time	Source	Destination	Protocol	Length	Info
5	0.160494985	192.168.1.144	172.217.18.78	ICMP	98	Echo (ping) request id=0xa250, seq=1/256, ttl=64
6	0.269282314	172.217.18.78	192.168.1.144	ICMP	98	Echo (ping) reply id=0xa250, seq=1/256, ttl=64
9	1.161843487	192.168.1.144	172.217.18.78	ICMP	98	Echo (ping) request id=0xa250, seq=2/512, ttl=64
10	1.199300373	172.217.18.78	192.168.1.144	ICMP	98	Echo (ping) reply id=0xa250, seq=2/512, ttl=64
13	2.164367487	192.168.1.144	172.217.18.78	ICMP	98	Echo (ping) request id=0xa250, seq=3/768, ttl=64
14	2.200340513	172.217.18.78	192.168.1.144	ICMP	98	Echo (ping) reply id=0xa250, seq=3/768, ttl=64
17	3.166099130	192.168.1.144	172.217.18.78	ICMP	98	Echo (ping) request id=0xa250, seq=4/1024, ttl=64
18	3.184213633	172.217.18.78	192.168.1.144	ICMP	98	Echo (ping) reply id=0xa250, seq=4/1024, ttl=64
21	4.167300097	192.168.1.144	172.217.18.78	ICMP	98	Echo (ping) request id=0xa250, seq=5/1280, ttl=64
22	4.185090561	172.217.18.78	192.168.1.144	ICMP	98	Echo (ping) reply id=0xa250, seq=5/1280, ttl=64
27	5.170213649	192.168.1.144	172.217.18.78	ICMP	98	Echo (ping) request id=0xa250, seq=6/1536, ttl=64
28	5.190604961	172.217.18.78	192.168.1.144	ICMP	98	Echo (ping) reply id=0xa250, seq=6/1536, ttl=64
34	5.275017626	192.168.1.144	192.168.1.1	ICMP	582	Destination unreachable (Port unreachable)
35	6.172983419	192.168.1.144	172.217.18.78	ICMP	98	Echo (ping) request id=0xa250, seq=7/1792, ttl=64
36	6.234827905	172.217.18.78	192.168.1.144	ICMP	98	Echo (ping) reply id=0xa250, seq=7/1792, ttl=64
40	6.371153337	192.168.1.144	192.168.1.1	ICMP	582	Destination unreachable (Port unreachable)
41	7.175272528	192.168.1.144	172.217.18.78	ICMP	98	Echo (ping) request id=0xa250, seq=8/2048, ttl=64
42	7.192816514	172.217.18.78	192.168.1.144	ICMP	98	Echo (ping) reply id=0xa250, seq=8/2048, ttl=64
46	7.332795746	192.168.1.144	192.168.1.1	ICMP	582	Destination unreachable (Port unreachable)
47	8.177247539	192.168.1.144	172.217.18.78	ICMP	98	Echo (ping) request id=0xa250, seq=9/2304, ttl=64
48	8.195030875	172.217.18.78	192.168.1.144	ICMP	98	Echo (ping) reply id=0xa250, seq=9/2304, ttl=64
58	8.409657865	192.168.1.144	192.168.1.1	ICMP	104	Destination unreachable (Port unreachable)
59	9.179176815	192.168.1.144	172.217.18.78	ICMP	98	Echo (ping) request id=0xa250, seq=10/2560, ttl=64
60	9.199718476	172.217.18.78	192.168.1.144	ICMP	98	Echo (ping) reply id=0xa250, seq=10/2560, ttl=64

  

Internet Protocol Version 4, Src: 192.168.1.144, Dst: 172.217.18.78

0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 84  
Identification: 0xf27f (62079)  
Flags: 0x40, Don't fragment  
Fragment Offset: 0  
Time to Live: 64  
Protocol: ICMP (1)  
Header Checksum: 0xc6c9 [validation disabled]  
[Header checksum status: Unverified]  
Source Address: 192.168.1.144  
1. Destination Address: 172.217.18.78

Internet Control Message Protocol

Type: 8 (Echo (ping) request)  
Code: 0  
Checksum: 0x7d42 [correct]  
[Checksum Status: Good]

0010 00 54 f2 7f 40 00 00 01 c6 c9 c0 a8 01 90 ac d9 .T..@..@.  
0020 12 4e 00 00 7d 42 a2 50 00 01 bc d5 4f 60 00 00 .N..}B.P  
0030 00 00 06 63 07 00 00 00 00 00 10 11 12 13 14 15 ...c....  
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 .....!"#\$  
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()\*+,-./  
0060 36 37 67

Type (icmp.type), 1 byte(s)
Packets: 64 · Displayed: 25 (39.1%) · Dropped: 0 (0.0%) · Profile: Default

## ↑Результат роботи програми ping у вікні Wireshark↑

1. Якою є IP адреса мого комп'ютера? Якою є IP адреса хоста призначення?  
Source Address: 192.168.14.144, Destination Address: 172.217.18.78

2. Чому ICMP пакети не мають порта відправника та порта призначення?  
Номери портів використовуються для того, щоб забезпечити роботу доставки process-to-process, але ICMP не є протоколом транспортного рівня, він є протоколом обміну повідомленнями на мережевому рівні

3. Яким є тип і код ICMP пакету, що був відправлений мною?  
Type: 8 і Code: 0, що являються так званим ICMP ехо-запитом

4. Яким є тип і код ICMP пакету, що був отриманий мною у відповідь?  
Type: 0 і Code: 0, що являються так званою ICMP ехо-відповіддю