



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

Лабораторна робота № 5
З дисципліни: Комп'ютерні мережі

Протокол ІР

Виконала:
Студентка ІІІ курсу
Групи КА-74
Семіконь Я. В.
Перевірів: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз основних деталей роботи протоколу IP.

Wireshark, необхідними для дослідження мережових протоколів.Начало формы

Хід виконання роботи

```
Germes-Air:~ some321user_34$ traceroute gaia.cs.umass.edu 2000
traceroute to gaia.cs.umass.edu (128.119.245.12), 64 hops max, 2000 byte packets
 1 192.168.1.1 (192.168.1.1) 26.246 ms 20.575 ms *
 2 92-244-97-1.kievnet.com.ua (92.244.97.1) 71.582 ms 31.132 ms 11.204 ms
 3 * mx80-20g-unicorn.kievnet.com.ua (92.244.96.57) 28.840 ms *
 4 mx104-20g-mx80-wr.kievnet.com.ua (109.108.88.61) 19.797 ms 25.033 ms 79.042 ms
 5 ae3-235.rtl.kiv.ua.retn.net (87.245.237.110) 18.861 ms 65.477 ms 89.179 ms
 6 ae5-10.rtl.tc2.ams.nl.retn.net (87.245.234.113) 63.696 ms 85.779 ms 145.727 ms
 7 * * *
 8 * * *
 9 university.ear3.newyork1.level3.net (4.71.230.234) 186.150 ms 177.112 ms 144.871 ms
10 core1-rt-et-8-3-0.gw.umass.edu (192.80.83.109) 134.860 ms 154.000 ms 158.390 ms
11 n5-rt-1-1-et-0-0-0.gw.umass.edu (128.119.0.8) 129.390 ms 175.756 ms 132.094 ms
12 cics-rt-xe-0-0-0.gw.umass.edu (128.119.3.32) 161.185 ms 140.277 ms 141.191 ms
13 * * *
14 gaia.cs.umass.edu (128.119.245.12) 387.105 ms !Z 138.561 ms !Z 131.084 ms !Z
Germes-Air:~ some321user_34$ █
```

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
13	4.514192	192.168.1.1	192.168.1.102	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
18	4.558366	192.168.1.1	192.168.1.102	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
45	9.632759	92.244.97.1	192.168.1.102	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
50	9.687391	92.244.97.1	192.168.1.102	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
53	9.698618	92.244.97.1	192.168.1.102	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
71	14.727854	92.244.96.57	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
101	19.758152	109.108.88.61	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
106	19.810182	109.108.88.61	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
109	19.889269	109.108.88.61	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
112	19.908244	87.245.237.110	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
117	19.981237	87.245.237.110	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
120	20.070489	87.245.237.110	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
123	20.134223	87.245.234.113	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
128	20.300968	87.245.234.113	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
131	20.446706	87.245.234.113	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
261	50.648421	4.71.230.234	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
266	51.534673	4.71.230.234	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
269	51.679702	4.71.230.234	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
273	51.814561	192.80.83.109	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
280	52.438085	192.80.83.109	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
285	52.596540	192.80.83.109	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
288	52.726050	128.119.0.8	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
296	53.405781	128.119.0.8	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
299	53.537933	128.119.0.8	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
302	53.699265	128.119.3.32	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
308	54.272509	128.119.3.32	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
311	54.413666	128.119.3.32	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
347	69.808457	128.119.245.12	192.168.1.102	ICMP	590	Destination unreachable (Host administratively prohibited)
354	70.423105	128.119.245.12	192.168.1.102	ICMP	590	Destination unreachable (Host administratively prohibited)
357	70.554269	128.119.245.12	192.168.1.102	ICMP	590	Destination unreachable (Host administratively prohibited)

Контрольні запитання:

1. Визначте IP адреси вашої та цільової робочих станцій.

Вихідний IP: 192.168.1.102

Цільовий IP: 128.119.245.12

2. Яке значення в полі номера протоколу вищого рівня в заголовку IP першого пакету із запитом ICMP?

11	4.488941	192.168.1.102	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=82be) [Reassembled in #12]
12	4.488943	192.168.1.102	128.119.245.12	UDP	534	33469 → 33435 Len=1972
13	4.514192	192.168.1.1	192.168.1.102	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)

3. Скільки байт займає заголовок IP першого пакету із запитом ICMP? Скільки байт займає корисна інформація (payload) пакету? Поясніть як ви встановили кількість байт корисної інформації.

The screenshot displays a Wireshark interface with a packet list on the left and a packet details pane on the right.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
11	4.488941	192.168.1.102	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=82be) [Reassembled in #12]
12	4.488943	192.168.1.102	128.119.245.12	UDP	534	33469 → 33435 Len=1972
13	4.514192	192.168.1.1	192.168.1.102	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
14	4.515431	192.168.1.102	192.168.1.1	DNS	84	Standard query 0xfc0 PTR 1.1.168.192.in-addr.arpa

Packet Details Pane (Selected Packet 11):

- Ethernet II, Src: Realtek_8C:8E:8F, Dst: Realtek_8C:8E:8F
- Internet Protocol Version 4, Src: 192.168.1.102, Destination: 128.119.245.12
- TCP Segment, Seq: 33469, Win: 0, Len: 0
- [Raw] (application/octet-stream)
- Header checksum: 0xfcd8 [validation disabled]
[Header checksum status: Unverified]
- Source: 192.168.1.102
- Destination: 128.119.245.12
- ▼ [2 IPv4 Fragments (1980 bytes): #11(1480), #12(500)]
 - [Frame: 11, payload: 0-1479 (1480 bytes)]
 - [Frame: 12, payload: 1480-1979 (500 bytes)]
 - [Fragment count: 2]
 - [Reassembled IPv4 length: 1980]
 - [Reassembled IPv4 data: 82bd829b07bcb38a00000000000000000000000000000000...]

Заголовок IP займає 20 байтів.

Payload=1980;

4. Дослідіть пакет із пунктів 2/3. Чи фрагментований цей пакет? Поясніть як ви встановили фрагментацію пакету. Як можна встановити номер фрагменту, що передається у пакеті?

▼ Flags: 0x00b9

```

0... .. = Reserved bit: Not set
.0... .. = Don't fragment: Not set
..0. .... = More fragments: Not set
0 0101 1100 1000 = Fragment offset: 1480

```

▼ Time to live: 1

MF (More Fragments) = 0. Отже, пакет не фрагментований.

5. Знайдіть наступний фрагмент дейтаграми ІР. Яка інформація дозволяє встановити наявність наступних фрагментів, що мають слідувати за другим фрагментом?

```

▼ Flags: 0x00b9
  0... .. = Reserved bit: Not set
  .0.. .. = Don't fragment: Not set
  ..0. .. = More fragments: Not set
  ...0 0101 1100 1000 = Fragment offset: 1480
▼ Time to live: 1

```

6. Які поля протоколу IP відрізняють перший фрагмент від другого?

Identification, Header checksum

7. Розгляньте послідовність пакетів IP із запитами ICMP вашої робочої станції. Які поля заголовку IP завжди змінюються?

Завжди змінюється Identification

8. Розгляньте послідовність пакетів IP із запитами ICMP вашої робочої станції. Які поля заголовку IP мають зберігати свої значення? Які поля мають змінюватися? Чому?

Identification має змінюватись, щоб розрізняти фрагменти і уникати проблем подвоєння, загублення. Всі інші зберігають свої значення.

9. Розгляньте послідовність пакетів IP із запитами ICMP вашої робочої станції. Опишіть закономірність зміни значень поля Identification рівня IP.

Кожного разу додається одиниця до коду.

10. Розгляньте послідовність пакетів IP із повідомленнями TTL-exceeded від найближчого маршрутизатора. Які значення встановлені у полях Identification та TTL?

```

▼ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.102
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
▼ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
  1100 00.. = Differentiated Services Codepoint: Class Selector 6 (48)
  .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 576
  Identification: 0x9bf2 (39922)
▼ Flags: 0x0000
  0... .. = Reserved bit: Not set
  .0.. .. = Don't fragment: Not set
  ..0. .. = More fragments: Not set
  ...0 0000 0000 0000 = Fragment offset: 0
  Time to live: 64
  Protocol: ICMP (1)
  Header checksum: 0x5853 [validation disabled]
  [Header checksum status: Unverified]

```

Identification: 0x9bf2 (39922)

Time to live: 64

11. Розгляньте послідовність пакетів IP із повідомленнями TTL-exceeded від найближчого маршрутизатора. Які значення встановлені у полях Identification та TTL? Чи змінюються ці значення для різних пакетів у послідовності? Чому?

Time to live: не змінюється

Identification: змінюється, щоб розрізняти фрагменти

Висновок

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