

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА
Факультет прикладної математики та інформатики

**Комп'ютерні інформаційні
мережі**

ЛАБОРАТОРНА РОБОТА №4

**Аналіз повідомлень канального рівня Ethernet засобами
Wireshark**

Виконав:

Студент групи ПМі-31

Яцуляк Андрій

2023

Мета: Здобути практичні навички з інтерпретації Ethernet-кадрів. Ознайомитися на основі опрацьованого теоретичного лекційного матеріалу з форматом кадру Ethernet II (порядок полів, їх розмір та призначення).

Хід роботи

1. Від'єднайтеся від мережі..
2. Запустив аналізатор мережевих пакетів Wireshark від імені адміністратора.
3. З'єднайтесь з мережею.
4. Захопіть кадри впродовж приблизно 30 секунд, здійснюючи активність в браузері або передаючи файли локальною мережею.
5. Вибрав кадр № 7189, розмір - 66 байт(528 біт):

7179	24.445785	192.168.1.5	142.250.75.4	QUIC	74 Protected Payload (KP0), DCID=eb6e346741b8f72b
7180	24.445986	192.168.1.5	142.250.75.4	QUIC	76 Protected Payload (KP0), DCID=eb6e346741b8f72b
7181	24.446085	192.168.1.5	142.250.75.4	QUIC	78 Protected Payload (KP0), DCID=eb6e346741b8f72b
7182	24.463868	142.250.75.4	192.168.1.5	QUIC	67 Protected Payload (KP0)
7183	24.464252	142.250.75.4	192.168.1.5	QUIC	67 Protected Payload (KP0)
7184	24.464252	142.250.75.4	192.168.1.5	QUIC	292 Protected Payload (KP0)
7185	24.464320	142.250.75.4	192.168.1.5	QUIC	67 Protected Payload (KP0)
7186	24.464320	142.250.203.142	192.168.1.5	QUIC	67 Protected Payload (KP0)
7187	24.464699	192.168.1.5	142.250.75.4	QUIC	80 Protected Payload (KP0), DCID=eb6e346741b8f72b
7188	24.464741	142.250.75.4	192.168.1.5	QUIC	67 Protected Payload (KP0)
7189	24.492253	142.250.75.4	192.168.1.5	QUIC	66 Protected Payload (KP0)
7190	24.827150	192.168.1.5	142.250.75.14	QUIC	71 Protected Payload (KP0), DCID=fb33596e262f3776
7191	24.921094	192.168.1.5	142.250.75.14	QUIC	71 Protected Payload (KP0), DCID=fb33596e262f3776
7192	24.922948	fe80::272:63ff:fe3c::	ff02::1	ICMPv6	90 Multicast Listener Query
7193	24.923151	fe80::86f5:3a79:80c::	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
7194	24.946137	142.250.75.14	192.168.1.5	QUIC	67 Protected Payload (KP0)
7195	25.247895	fe80::86f5:3a79:80c::	ff02::16	ICMPv6	130 Multicast Listener Report Message v2

> Frame 7189: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{DA8BD077-0000-0000-0000-000000000000}	0000	90 0f 0c 88 42 5f 00 72 63 3c 09 e0 08 00 45 000..r c.....E..
> Ethernet II, Src: NetcoreT_3c:09:e0 (00:72:63:3c:09:e0), Dst: CloudNet_88:42:5f (90:0f:0c:88:42:5f)	0010	00 34 00 00 40 00 3a 11 a5 0d 8e fa 4b 04 c0 a8	.4...@... ..K...
> Internet Protocol Version 4, Src: 142.250.75.4, Dst: 192.168.1.5	0020	01 05 01 bb e5 b3 00 20 e5 d8 5d 4b 31 f1 c5 ba]K1...
> User Datagram Protocol, Src Port: 443, Dst Port: 58803	0030	85 a7 66 56 a8 4c e8 d8 27 df 20 13 b1 47 c9 fd	..fV.L... '...G...
> QUIC IETF	0040	01 71	..q

6. Час захоплення: 13.10.2023 10:44:42

Ієрархія протоколів стеку TCP/IP:

- Ethernet-кадр
- IP-пакет
- UDP-сегмент
- QUIC-повідомлення

```

v Frame 7189: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{DA8BD773-E797-474F-B302-58BD357A142E}
  Section number: 1
  > Interface id: 0 (\Device\NPF_{DA8BD773-E797-474F-B302-58BD357A142E})
  Encapsulation type: Ethernet (1)
  Arrival Time: Oct 13, 2023 10:44:42.564731000 FLE Daylight Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1697183082.564731000 seconds
  [Time delta from previous captured frame: 0.027512000 seconds]
  [Time delta from previous displayed frame: 0.027512000 seconds]
  [Time since reference or first frame: 24.492253000 seconds]
  Frame Number: 7189
  Frame Length: 66 bytes (528 bits)
  Capture Length: 66 bytes (528 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:udp:quic]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
  > Ethernet II, Src: NetcoreT_3c:09:e0 (00:72:63:3c:09:e0), Dst: CloudNet_88:42:5f (90:0f:0c:88:42:5f)
  > Internet Protocol Version 4, Src: 142.250.75.4, Dst: 192.168.1.5
  > User Datagram Protocol, Src Port: 443, Dst Port: 58803

```

7. Заголовок кадру та його складові:

Отримувач: мережевий адаптер (MAC 90:0f:0c:99:42:5f)

Відправник: маршрутизатор (MAC 00:72:63:3c:09:e0)

Вкладений протокол, що передається: IPv4

```

> Frame 7189: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{DA8BD773-E797-474F-B302-58BD357A142E}
v Ethernet II, Src: NetcoreT_3c:09:e0 (00:72:63:3c:09:e0), Dst: CloudNet_88:42:5f (90:0f:0c:88:42:5f)
  > Destination: CloudNet_88:42:5f (90:0f:0c:88:42:5f)
  > Source: NetcoreT_3c:09:e0 (00:72:63:3c:09:e0)
  Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 142.250.75.4, Dst: 192.168.1.5
  > User Datagram Protocol, Src Port: 443, Dst Port: 58803
  > QUIC IETF

```

8. За першою половиною MAC-адреси отримав інформацію про виробників пристроїв передавача та отримувача:

Введіть тас-адресу для перевірки

90:0f:0c

ПЕРЕВІРИТИ

Виробником пристрою з тас-адресою 90:0f:0c є компанія:

Ім'я компанії: CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD.

Адреса компанії: B22 Building, NO.51 Tongle Road, Shajing Town, Jiangnan District, Nanning, Guangxi Province, China Nanning Guangxi CN 530007

Унікальний ідентифікатор організації: 900F0C

Розмір діапазону: MA-L 

9. Відшукав за допомогою фільтра кадри, які переносять повідомлення протоколу ARP:

No.	Time	Source	Destination	Protocol	Length	Info
2	0.001165	CloudNet_88:42:5f	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.5
3	0.008859	NetcoreT_3c:09:e0	CloudNet_88:42:5f	ARP	42	192.168.1.1 is at 00:72:63:3c:09:e0
42	0.060823	CloudNet_88:42:5f	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.5
48	0.065816	NetcoreT_3c:09:e0	CloudNet_88:42:5f	ARP	42	192.168.1.1 is at 00:72:63:3c:09:e0
288	0.243901	CloudNet_88:42:5f	Broadcast	ARP	42	Who has 192.168.1.5? (ARP Probe)
295	0.293360	CloudNet_88:42:5f	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.5
296	0.297043	NetcoreT_3c:09:e0	CloudNet_88:42:5f	ARP	42	192.168.1.1 is at 00:72:63:3c:09:e0
490	1.248007	CloudNet_88:42:5f	Broadcast	ARP	42	Who has 192.168.1.5? (ARP Probe)
558	2.248260	CloudNet_88:42:5f	Broadcast	ARP	42	Who has 192.168.1.5? (ARP Probe)
599	3.248755	CloudNet_88:42:5f	Broadcast	ARP	42	ARP Announcement for 192.168.1.5

> Frame 599: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{DABD0773}		0000	ff ff ff ff ff 90 0f 0c 88 42 5f 08 06 00 01B_....
▼ Ethernet II, Src: CloudNet_88:42:5f (90:0f:0c:88:42:5f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)		0010	08 00 06 04 00 01 90 0f 0c 88 42 5f c0 a8 01 05B_....
> Destination: Broadcast (ff:ff:ff:ff:ff:ff)		0020	00 00 00 00 00 00 c0 a8 01 05
> Source: CloudNet_88:42:5f (90:0f:0c:88:42:5f)				
> Type: ARP (0x0806)				
> Address Resolution Protocol (ARP Announcement)				

10. В моєму випадку поля Padding немає. Поле **Padding** у пакетах, які переносять повідомлення протоколу ARP, використовується для того, щоб розмір пакета був кратним 4 байтам. Це необхідно для того, щоб пакети могли безпечно передаватися через мережу. ARP-повідомлення є невеликими за розміром, але вони можуть містити додаткову інформацію, наприклад, тип протоколу, для якого запитується адреса. Якщо розмір пакета не буде кратним 4 байтам, то він може бути сприйнятий як пошкоджений або помилковий. Це може призвести до того, що пакет буде відкинутий або до того, що дані в пакеті будуть втрачені або пошкоджені. Або ж, якщо розмір пакета не буде кратним 4 байтам, то він може бути розділений на кілька блоків, що призведе до додаткових витрат на передачу даних. Поле **Padding** заповнюється

нулями, тому воно не містить жодної корисної інформації. Однак воно є важливим для забезпечення надійності передачі ARP-повідомлень.

11. **Кінцевик** - це той пристрій, який відправляє або приймає мережеві пакети, включаючи дані, які пересилаються через мережу. У мережевому пакеті з адресою призначення broadcast, не передбачається конкретний кінцевий адресат. Пакет із цією адресою призначення призначений для розсилки даних всім пристроям в мережі, і він визначається за допомогою спеціальної адреси - FF:FF:FF:FF:FF:FF, яка означає "всі пристрої в даній мережі". Оскільки broadcast-пакети не адресовані конкретному пристрою, то немає необхідності вказувати кінцевий вузол. Це дозволяє мережевим пристроям ефективно передавати такі пакети всім пристроям в мережі.

Висновок. Під час виконання лабораторної роботи я здобув практичні навички з інтерпретації Ethernet-кадрів. Ознайомився на основі опрацьованого теоретичного лекційного матеріалу з форматом кадру Ethernet II (порядок полів, їх розмір та призначення).