

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА

Факультет прикладної математики та інформатики

Комп'ютерні інформаційні мережі

ЛАБОРАТОРНА РОБОТА №7

Виконав :

Ст Гуменюк С. А.

ПМІ -33

Тема: Аналіз повідомлень каналного рівня Ethernet засобами Wireshark.
Утиліти для діагностики мережі на каналному рівні

Мета роботи: Здобути практичні навички з інтерпретації Ethernet-кадрів та використання консольних утиліт для діагностики мережі на рівні мережевих інтерфейсів.

Хід роботи

1. Базова мережева конфігурація мого ПК

```
sonorma@hellcat:~$ sudo ifconfig wlp2s0
wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.50.66  netmask 255.255.255.0  broadcast 192.168.50.255
    inet6 fe80::cb28:85b7:b33c:2c94  prefixlen 64  scopeid 0x20<link>
    ether 14:13:33:36:7e:7d  txqueuelen 1000  (Ethernet)
    RX packets 71537  bytes 76474510 (72.9 MiB)
    RX errors 0  dropped 252  overruns 0  frame 0
    TX packets 31148  bytes 8183411 (7.8 MiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Активні TCP з'єднання:

```
sonorma@hellcat:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 hellcat:52684          server-18-66-231-:https ESTABLISHED
tcp      0      0 hellcat:47274          188.114.96.11:https ESTABLISHED
tcp      0      0 hellcat:37654          52.123.135.7:https ESTABLISHED
tcp      0      0 hellcat:39840          104.21.27.152:https ESTABLISHED
tcp      0      0 hellcat:52214          52.111.236.12:https ESTABLISHED
tcp      0      0 hellcat:36524          li1398-20.members:https ESTABLISHED
tcp      0      0 hellcat:45218          par10s21-in-f202.:https ESTABLISHED
tcp      76      0 hellcat:60978          151.101.245.91:https CLOSE_WAIT
tcp      0      0 hellcat:36546          li1398-20.members:https ESTABLISHED
tcp      0      0 hellcat:34900          93.243.107.34.bc.:https ESTABLISHED
tcp      0      0 hellcat:52734          server-18-66-231-:https ESTABLISHED
tcp      0      0 hellcat:60524          149.154.167.41:https ESTABLISHED
tcp      0      0 hellcat:49788          40.99.210.2:https ESTABLISHED
tcp      0      0 hellcat:47550          140.227.186.35.bc:https ESTABLISHED
tcp      0      0 hellcat:32896          waw07s02-in-f3.1e:https ESTABLISHED
tcp      0      0 hellcat:53508          server-18-245-65-2:http TIME_WAIT
tcp      0      0 hellcat:48252          lb-140-82-112-25-:https ESTABLISHED
tcp      0      0 hellcat:49556          52.111.209.6:https ESTABLISHED
tcp      0      0 hellcat:41616          172.64.41.4:https ESTABLISHED
tcp      0      0 hellcat:36558          li1398-20.members:https ESTABLISHED
tcp      0      0 hellcat:38630          waw02s22-in-f3.1e1:http TIME_WAIT
tcp      76      0 hellcat:60960          151.101.245.91:https CLOSE_WAIT
tcp      0      0 hellcat:42986          209.100.149.34.bc:https ESTABLISHED
tcp      0      0 hellcat:50574          ec2-34-237-73-95.:https ESTABLISHED
tcp      0      0 hellcat:54910          rd-in-f84.1e100.n:https ESTABLISHED
tcp      0      0 hellcat:38462          par10s21-in-f196.:https ESTABLISHED
tcp      0      0 hellcat:54914          a2-16-172-18.deplo:http ESTABLISHED
tcp      0      0 hellcat:41330          192.168.50.251:1716 ESTABLISHED
tcp      0      0 hellcat:36504          li1398-20.members:https ESTABLISHED
tcp      0      0 hellcat:47988          191.144.160.34.bc:https ESTABLISHED
tcp      64      0 hellcat:38558          876603927.war.cdn:https CLOSE_WAIT
tcp      0      0 hellcat:35686          rd-in-f84.1e100.n:https ESTABLISHED
tcp      0      0 hellcat:47224          104.22.26.181:https ESTABLISHED
tcp      0      0 hellcat:35436          52.123.134.245:https ESTABLISHED
tcp      0      0 hellcat:49370          waw07s03-in-f10.1:https TIME_WAIT
tcp      0      0 hellcat:34706          188.114.97.11:https ESTABLISHED
tcp      0      0 hellcat:36508          li1398-20.members:https ESTABLISHED
tcp      0      0 hellcat:38446          par10s21-in-f196.:https ESTABLISHED
tcp      0      0 hellcat:46270          waw07s05-in-f10.1:https ESTABLISHED
tcp      0      0 hellcat:33720          server-3-165-206-:https ESTABLISHED
tcp      0      0 hellcat:36530          li1398-20.members:https ESTABLISHED
udp      0      0 hellcat:bootpc         RT-AX55-FCB8:bootps ESTABLISHED
```

Основні стани TCP:

1. LISTEN - порт відкритий, очікує з'єднань
2. SYN_SENT - відправлено запит на з'єднання
3. SYN_RECEIVED - отримано запит, відправлено підтвердження
4. ESTABLISHED - з'єднання активне
5. FIN_WAIT_1/2 - очікування завершення з'єднання
6. TIME_WAIT - очікує очищення мережових буферів
7. CLOSE_WAIT - віддалена сторона ініціювала закриття
8. LAST_ACK - очікує фінального підтвердження
9. CLOSED - з'єднання закрито

Команди netstat:

netstat -n:

- Числові адреси замість імен
- Швидша робота
- Без резолву DNS

netstat -a:

- Всі з'єднання та порти
- Включає стан LISTEN
- Показує UDP-порти

3. Статистика

```
sonorma@hellcat:~$ netstat -s
Ip:
    Forwarding: 1
    47887 total packets received
    1 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    46239 incoming packets delivered
    32754 requests sent out
    28 outgoing packets dropped
    9 dropped because of missing route
    3 fragments dropped after timeout
    37 reassemblies required
    17 packets reassembled ok
    3 packet reassemblies failed
    609 outgoing packets fragmented ok
    1218 fragments created
Icmp:
    64 ICMP messages received
    0 input ICMP message failed
    ICMP input histogram:
        destination unreachable: 64
    110 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 110
IcmpMsg:
    InType3: 64
    OutType3: 110
Tcp:
    444 active connection openings
    2 passive connection openings
    2 failed connection attempts
    76 connection resets received
    24 connections established
    36840 segments received
    30093 segments sent out
    38 segments retransmitted
    0 bad segments received
    270 resets sent
```

4. Інформація про вибраний пакет:

The screenshot shows the Wireshark interface with a packet capture named 'lab7.pcapng'. The packet list pane shows several packets, with packet 3908 selected. The packet details pane shows the following information:

- Frame 3908: 355 bytes on wire (2840 bits), 355 bytes captured
- Linux cooked capture v1
- Internet Protocol Version 4, Src: 104.22.26.181, Dst: 192.168.50.66
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x40 (DSCP: CS2, ECN: Not-ECT)
 - Total Length: 339
 - Identification: 0x6b8b (27531)
 - 010. = Flags: 0x2, Don't fragment
 - ...0 0000 0000 0000 = Fragment Offset: 0

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 00 00 00 01 00 06 04 42 1a bf fc
0010 45 40 01 53 6b 8b 40 00 3a 06 5e
0020 c0 a8 32 42 01 bb a2 dc 45 6a f8
0030 80 18 00 09 d3 87 00 00 01 01 08
0040 9f b4 47 73 16 03 03 00 80 02 00
0050 92 26 f8 28 cb 50 56 0b b3 64 37
0060 3e c1 aa 94 24 b7 02 33 f0 7a 1a
0070 64 11 65 80 d8 8f 9c 2e 0d 7c d9
0080 32 0f 9d 55 67 b8 c9 63 ec 54 a2
0090 13 01 00 00 34 00 29 00 02 00 00
00a0 1d 00 20 00 00 05 b4 00 64 05 76
```

Різниця в інтерпретації полів IPv4 заголовка:

Поле Version (0100 = 4)

- Біти 0100 дають число 4
- Використовується як є для позначення версії IPv4

Поле Header Length (0101 = 5)

- Біти 0101 дають число 5
- Вимірюється в 32-бітних словах (4 байти)
- Тому $5 * 4 = 20$ байт реальної довжини заголовка
- Таке кодування економить місце, бо довжина завжди кратна 4

Тобто Version використовує пряме значення, а Header Length множиться на 4 для отримання реальної довжини в байтах.

Для визначення розміру корисних даних:

1. Total Length (загальна довжина пакету) = 339 байт
2. Відняти IP заголовок = 20 байт

$339 - 20 = 319$ байт

Аналіз IP-адрес:

Відправник (Source): 104.22.26.181

- Це публічна IP-адреса
- Належить до глобальної мережі Інтернет

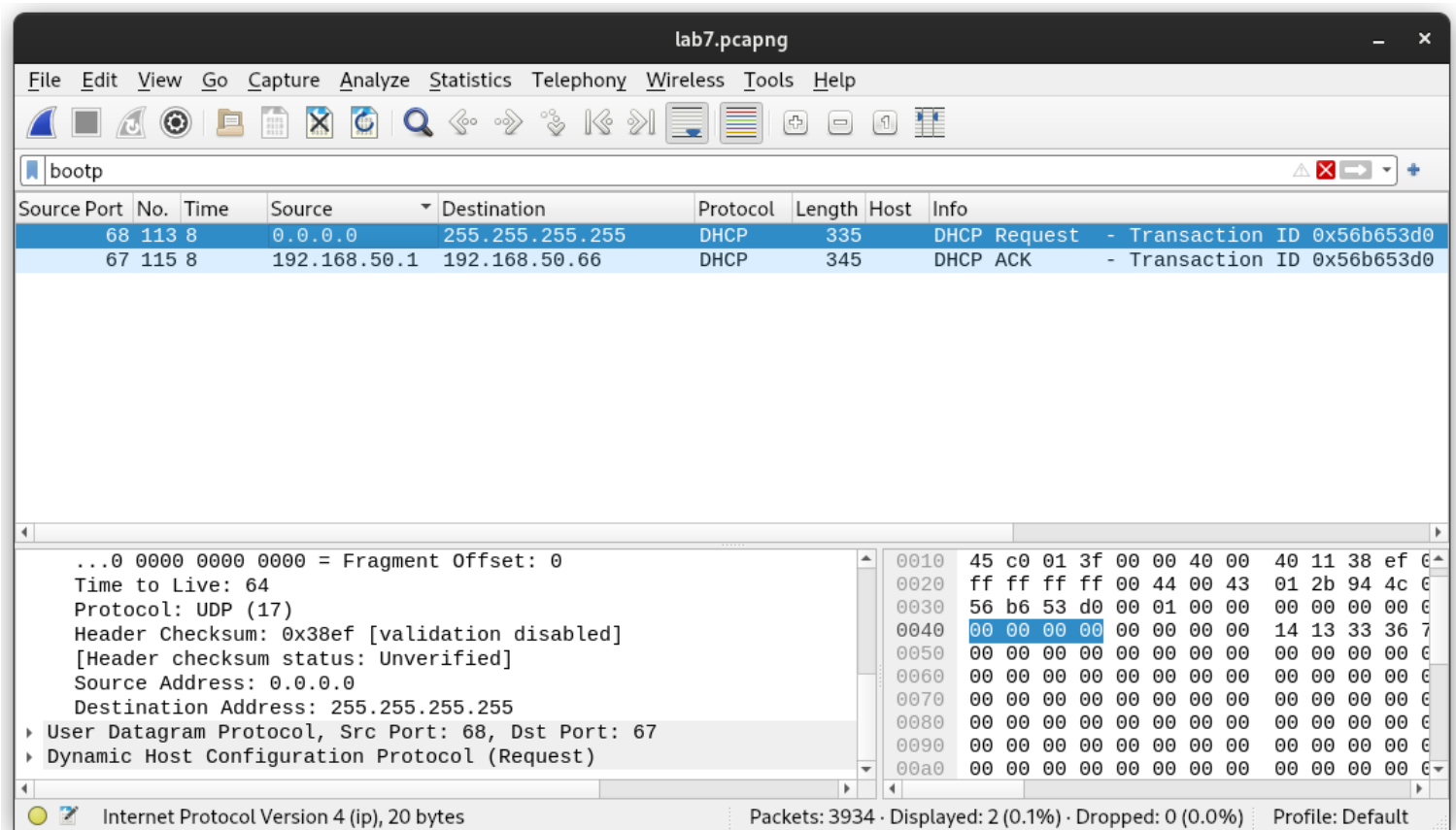
Одержувач (Destination): 192.168.50.66

- Це приватна IP-адреса з діапазону 192.168.0.0/16
- Використовується в локальних мережах
- Не маршрутизується в Інтернеті

Отже, пакет надсилається з публічної мережі Інтернет до комп'ютера в локальній мережі.

Поле Differentiated Services Field (DSCP) складається з двох частин:

- DSCP (6 біт) – визначає клас обслуговування пакета (QoS). У вашому прикладі 010000 відповідає Class Selector 2 (CS2).
- ECN (2 біти) – використовується для сигналізації перевантаження мережі. У вашому прикладі 00 означає, що пакет не підтримує ECN (Not ECN-Capable).



lab7.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

bootp

Source Port	No.	Time	Source	Destination	Protocol	Length	Host	Info
68	113	8	0.0.0.0	255.255.255.255	DHCP	335		DHCP Request - Transaction ID 0x56b653d0
67	115	8	192.168.50.1	192.168.50.66	DHCP	345		DHCP ACK - Transaction ID 0x56b653d0

...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0x38ef [validation disabled]
[Header checksum status: Unverified]
Source Address: 0.0.0.0
Destination Address: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)

Internet Protocol Version 4 (ip), 20 bytes

Packets: 3934 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%) Profile: Default

В DHCP-запиті:

- IP-адреса відправника: 0.0.0.0 — клієнт ще не має IP-адреси.
- IP-адреса отримувача: 255.255.255.255 — широкомовна адреса для того, щоб запросити IP-адресу від DHCP-сервера, оскільки клієнт не знає його точну адресу.

lab7.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

bootp

Source Port	No.	Time	Source	Destination	Protocol	Length	Host	Info
68	113	8	0.0.0.0	255.255.255.255	DHCP	335		DHCP Request - Transaction ID 0x56b653d0
67	115	8	192.168.50.1	192.168.50.66	DHCP	345		DHCP ACK - Transaction ID 0x56b653d0

...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 64
 Protocol: UDP (17)
 Header Checksum: 0x64b0 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 192.168.50.1
 Destination Address: 192.168.50.66
 ▶ User Datagram Protocol, Src Port: 67, Dst Port: 68
 ▶ Dynamic Host Configuration Protocol (ACK)

Internet Protocol Version 4 (ip), 20 bytes Packets: 3934 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%) Profile: Default

У DHCP ACK:

- IP-адреса відправника: 192.168.50.1 — це адреса DHCP-сервера, який підтверджує запит.
- IP-адреса отримувача: 192.168.50.66 — це нова адреса, виділена клієнту (DHCP ACK повідомляє клієнту про успішне призначення цієї IP-адреси).