



IPK projekt  
ZETA: Sniffer paketov  
Manuál

25. apríla 2021

Peter Močáry (xmocar00)

# Obsah

1	Úvod	2
2	Teoretické základy	2
3	Implementácia	3
4	Testovanie programu	3

# 1 Úvod

Cieľom projektu je implementácia sieťového analyzátoru, ktorý je schopný zachytávať a filtrvať pakety na zvolenom sieťovom rozhraní. Program vypisuje zachytené pakety na štandardný výstup. Tento projekt nás zoznami s problematikou zachytávania paketov a získavania dôležitých informácií z nich.

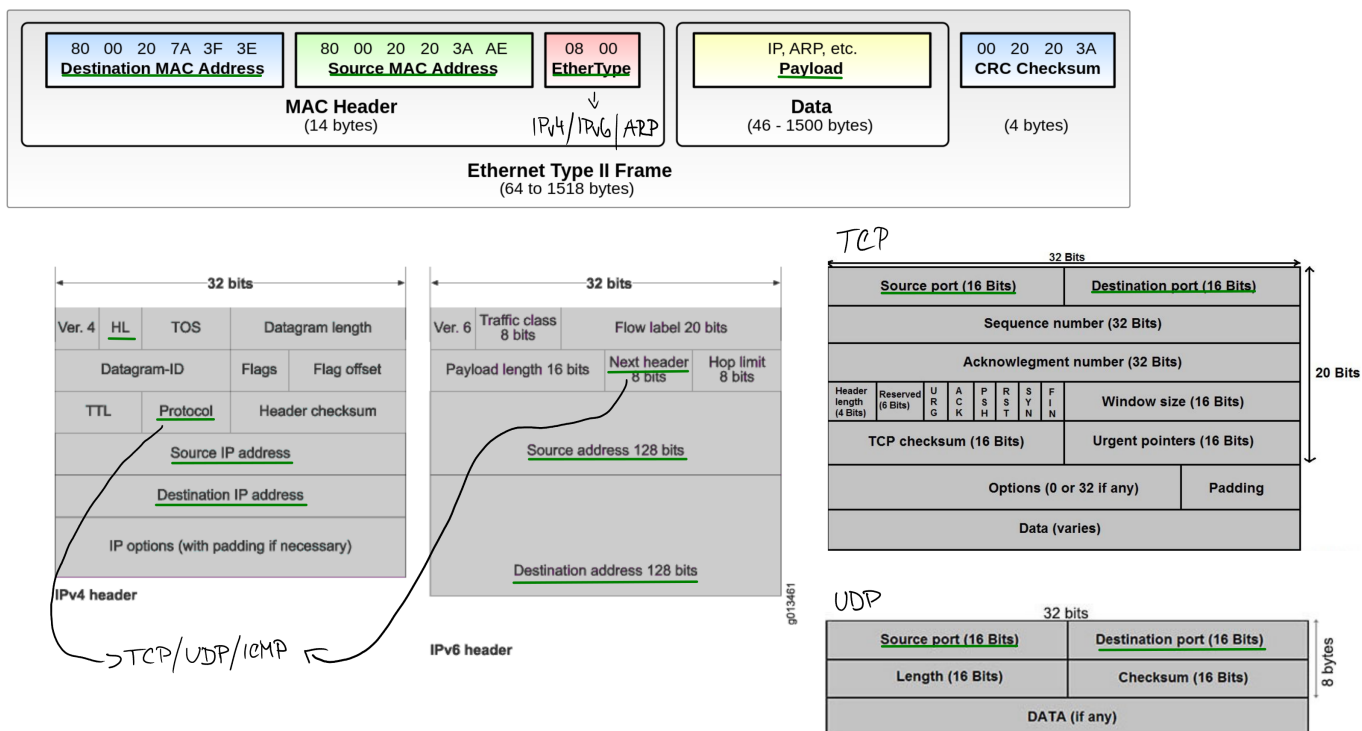
## 2 Teoretické základy

Pre pochopenie čo nás v projekte čaká si potrebujeme objasniť pár dôležitých pojmov. Na začiatku nás zaujíma čo to vlastne je paket?

*Packet* viz [5] je formátovaná jednotka dát prenášaná po sieti, ktorá nesie dáta od odosielateľa príjemcovi. Okrem dát však nesie aj hlavičku, ktorá v sebe skrýva potrebné informácie pre úspešnú dopravu k príjemcovi.

Ďalej je potrebné vedieť, že dáta nám budú po sieti prichádzať obalení vo viacerých vrstvách. Prvou je tzv. *Ethernetový rámec* [1], ktorý tvorí kompatibilnú vrstvu obalujúcu všetky pakety, ktoré nás pre tento projekt zaujímajú. Ethernetový rámec ďalej môže obsahovať rôzne typy protokolov. Určiť druh nasledujúceho protokolu vieme z hlavičky Ethernetového rámca pomocou *EtherType* [7] časti. Z nich filtrujeme IPv4 [6], IPv6 [8] a ARP [3]. Avšak, táto vrstva nie je posledná. Internetové protokoly v sebe ešte ukrývajú TCP [2], UDP [4] a ICMP [9]. Každý protokol má svoju hlavičku a pre naše potreby nás budú zaujímať časti vyznačené na obrázku 1.

Našou úlohou teda bude prečítať z týchto hlavičiek všetko potrebné a vypísať dané informácie užívateľovi podľa toho aké argumenty programu zadal.



Obr. 1: Potrebné časti hlavičiek<sup>1</sup>

### 3 Implementácia

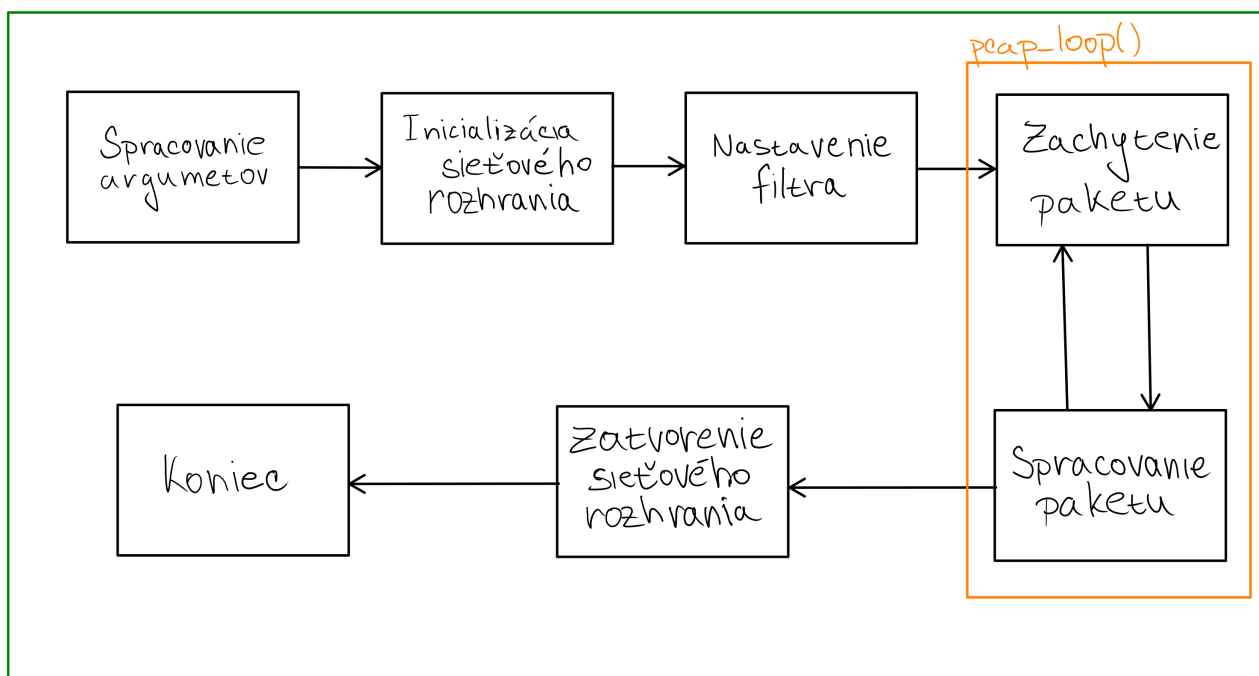
Projekt je implementovaný v jazyku C s využitím knižnice `libpcap` viz [?]. Program mmá jednoduchú štruktúru, ktorú môžete vidieť na obrázku 2.

Hneď po spracovaní argumentov programu zadaných užívateľom sa inicializuje sieťové rozhranie, ktoré má nastavené reagovanie na prečítaný packet ihneď ako ho prečíta pomocou funkcie `pcap_set_immediate_mode()`.

Nastavenie filtra prebieha vygenerovaním pseudokódu z argumentov, ktoré používateľ zadal. Ten je následne skompilovaný a nastavený ako filter paketov.

Nasleduje samotný „sniffing“ paketov, pre ktorý je využitá funkcia `pcap_loop()`, ktorá pri zachytení paketu zavolá obslužnú funkciu a vypíše požadovaný formát paketu na výstup viz obrázok 3.

Na záver nesmieme zabudnúť správne uzavrieť sieťové rozhranie a uvoľniť vymedzenú pamäť.



Obr. 2: Nastínenie fungovania programu (inšpirované [10])

### 4 Testovanie programu

Testovanie prebehlo na referenčnom virtualnom stroji za použitia programu Wireshark jednoduchým porovnávaním výsledkov „sniffera“ a Wiresharku.

<sup>1</sup>Dalšie použité zdroje viz [11] [12]

```

student@student-vm:/mnt/IPK-PROJ$ sudo ./ipk-sniffer -i ens33 -n 2
2021-04-24T23:14:14.615+02:00 IP: 172.16.176.129 : 49856 > IP: 172.16.176.2 : 53, length: 84
0x0000: 00 50 56 ee 42 71 00 0c 29 7c a5 bb 08 00 45 00 .PV.Bq..)|....E.
0x0010: 00 46 13 03 40 00 40 11 6e ff ac 10 b0 81 ac 10 .F..@.n.....
0x0020: b0 02 c2 c0 00 35 00 32 b8 e8 83 af 01 00 00 01 .....5.2.....
0x0030: 00 00 00 00 00 00 0c 64 65 74 65 63 74 70 6f 72 .....detectpor
0x0040: 74 61 6c 07 66 69 72 65 66 6f 78 03 63 6f 6d 00 tal.firefox.com.
0x0050: 00 01 00 01 ....

2021-04-24T23:14:14.615+02:00 IP: 172.16.176.129 : 50811 > IP: 172.16.176.2 : 53, length: 84
0x0000: 00 50 56 ee 42 71 00 0c 29 7c a5 bb 08 00 45 00 .PV.Bq..)|....E.
0x0010: 00 46 13 04 40 00 40 11 6e fe ac 10 b0 81 ac 10 .F..@.n.....
0x0020: b0 02 c6 7b 00 35 00 32 b8 e8 17 93 01 00 00 01 ...{.5.2.....
0x0030: 00 00 00 00 00 00 0c 64 65 74 65 63 74 70 6f 72 .....detectpor
0x0040: 74 61 6c 07 66 69 72 65 66 6f 78 03 63 6f 6d 00 tal.firefox.com.
0x0050: 00 1c 00 01 ....

student@student-vm:/mnt/IPK-PROJ$ █

```

Obr. 3: Ukážka správneho výstupu

**Capturing from ens33**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	2021/114 22:04:33,982190291	172.16.176.129	172.16.176.2	DNS	84	Standard query 0xc456 A detectportal.f
2	2021/114 22:04:33,982957873	172.16.176.129	172.16.176.2	DNS	84	Standard query 0xd8ac AAAA detectporta
3	2021/114 22:04:33,984174769	172.16.176.2	172.16.176.129	DNS	489	Standard query response 0xc456 A detec
4	2021/114 22:04:33,984837588	172.16.176.2	172.16.176.129	DNS	501	Standard query response 0xd8ac AAAA de
5	2021/114 22:04:33,997610873	172.16.176.129	34.107.221.82	TCP	74	58462 → 80 [SYN] Seq=0 Win=64240 Len=0
6	2021/114 22:04:34,004127755	172.16.176.129	172.16.176.2	DNS	95	Standard query 0x24f2 A content-sigmat

Frame 5: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface ens33, id 0

- Ethernet II, Src: VMware\_7c:a5:bb (00:0c:29:7c:a5:bb), Dst: VMware\_ee:42:71 (00:50:56:ee:42:71)
- Internet Protocol Version 4, Src: 172.16.176.129, Dst: 34.107.221.82
- Transmission Control Protocol, Src Port: 58462, Dst Port: 80, Seq: 0, Len: 0

```

0000  00 50 56 ee 42 71 00 0c 29 7c a5 bb 08 00 45 00  .PV.Bq..)|....E.
0010  00 3c 01 f3 40 00 40 06 dc 79 ac 10 b0 81 22 6b  .<..@.@..y...."k
0020  dd 52 e4 5e 00 50 ed 7e 15 95 00 00 00 00 a0 02  .R.^..P.~.....
0030  fa f0 5c 7e 00 00 02 04 05 b4 04 02 08 0a 11 b2  ..\~.....
0040  6e e1 00 00 00 00 01 03 03 07                    n.....

```

ens33: <live capture in progress> Packets: 296 · Displayed: 296 (100.0%) Profile: Default

student@student-vm: /mnt/IPK-PROJ

```

2021-04-24T22:04:33.997+02:00 IP: 172.16.176.129 : 58462 > IP: 34.107.221.82 : 80, length: 74
0x0000: 00 50 56 ee 42 71 00 0c 29 7c a5 bb 08 00 45 00  .PV.Bq..)|....E.
0x0010: 00 3c 01 f3 40 00 40 06 dc 79 ac 10 b0 81 22 6b  .<..@.@..y...."k
0x0020: dd 52 e4 5e 00 50 ed 7e 15 95 00 00 00 00 a0 02  .R.^..P.~.....
0x0030: fa f0 5c 7e 00 00 02 04 05 b4 04 02 08 0a 11 b2  ..\~.....
0x0040: 6e e1 00 00 00 00 01 03 03 07                    n.....

```

Obr. 4: Test TCP

Capturing from ens33

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
50	2021/114 22:15:46,149684097	VMware_7c:a5:bb	VMware_ee:42:71	ARP	42	Who has 172.16.176.2? Tell 172.16.176.
51	2021/114 22:15:46,149995266	VMware_ee:42:71	VMware_7c:a5:bb	ARP	60	172.16.176.2 is at 00:50:56:ee:42:71
52	2021/114 22:16:04,987884634	172.16.176.129	172.16.176.2	DNS	89	Standard query 0x146f A connectivity-c
53	2021/114 22:16:04,990430407	172.16.176.2	172.16.176.129	DNS	249	Standard query response 0x146f A conne
54	2021/114 22:16:04,992185911	172.16.176.129	35.232.111.17	TCP	74	49544 → 80 [SYN] Seq=0 Win=64240 Len=0
55	2021/114 22:16:05,119333405	35.232.111.17	172.16.176.129	TCP	60	80 → 49544 [SYN, ACK] Seq=0 Ack=1 Win=

Frame 52: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface ens33, id 0

- Ethernet II, Src: VMware\_7c:a5:bb (00:0c:29:7c:a5:bb), Dst: VMware\_ee:42:71 (00:50:56:ee:42:71)
- Internet Protocol Version 4, Src: 172.16.176.129, Dst: 172.16.176.2
- User Datagram Protocol, Src Port: 59169, Dst Port: 53
- Domain Name System (query)

0000	00 50 56 ee 42 71 00 0c 29 7c a5 bb 08 00 45 00	.PV.Bq..) ....E.
0010	00 4b 24 e5 40 00 40 11 5d 18 ac 10 b0 81 ac 10	.K\$.@.@.].....
0020	b0 02 e7 21 00 35 00 37 b8 ed 14 6f 01 00 00 01	...!.5.7...o....
0030	00 00 00 00 00 00 12 63 6f 6e 6e 65 63 74 69 76	.....connectiv
0040	69 74 79 2d 63 68 65 63 6b 06 75 62 75 6e 74 75	ity-check.kubuntu
0050	03 63 6f 6d 00 00 01 00 01	.com.....

ens33: <live capture in progress>

Packets: 63 · Displayed: 63 (100.0%) Profile: Default

+

student@student-vm: /mnt/IPK-PROJ

Q

≡

-

□

×

```

student@student-vm:/mnt/IPK-PROJ$ sudo ./ipk-sniffer -i ens33
2021-04-24T22:16:04.987+02:00 IP: 172.16.176.129 : 59169 > IP: 172.16.176.2 : 53, length: 89
0x0000: 00 50 56 ee 42 71 00 0c 29 7c a5 bb 08 00 45 00 .PV.Bq..)|....E.
0x0010: 00 4b 24 e5 40 00 40 11 5d 18 ac 10 b0 81 ac 10 .K$.@.@.].....
0x0020: b0 02 e7 21 00 35 00 37 b8 ed 14 6f 01 00 00 01 ...!.5.7...o....
0x0030: 00 00 00 00 00 00 12 63 6f 6e 6e 65 63 74 69 76 .....connectiv
0x0040: 69 74 79 2d 63 68 65 63 6b 06 75 62 75 6e 74 75 ity-check.ubuntu
0x0050: 03 63 6f 6d 00 00 01 00 01 .com.....

student@student-vm:/mnt/IPK-PROJ$

```

Obr. 5: Test UDP

**Capturing from ens33**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	2021/114 22:26:53,217517670	172.16.176.129	172.16.176.2	DNS	70	Standard query 0xb2b5 A google.com
2	2021/114 22:26:53,218204020	172.16.176.129	172.16.176.2	DNS	70	Standard query 0x335d AAAA google.com
3	2021/114 22:26:53,220166481	172.16.176.2	172.16.176.129	DNS	334	Standard query response 0xb2b5 A googl
4	2021/114 22:26:53,220728976	172.16.176.2	172.16.176.129	DNS	346	Standard query response 0x335d AAAA go
5	2021/114 22:26:53,221710562	172.16.176.129	172.217.23.238	ICMP	98	Echo (ping) request id=0x0002, seq=1/
6	2021/114 22:26:53,234704633	172.217.23.238	172.16.176.129	ICMP	98	Echo (ping) reply id=0x0002, seq=1/

Frame 5: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface ens33, id 0  
 Ethernet II, Src: VMware\_7c:a5:bb (00:0c:29:7c:a5:bb), Dst: VMware\_ee:42:71 (00:50:56:ee:42:71)  
 Internet Protocol Version 4, Src: 172.16.176.129, Dst: 172.217.23.238  
 Internet Control Message Protocol

```

0000  00 50 56 ee 42 71 00 0c 29 7c a5 bb 08 00 45 00  .PV.Bq..)|...E.
0010  00 54 7f 9e 40 00 40 01 99 b1 ac 10 b0 81 ac d9  .T..@.@.....
0020  17 ee 08 00 ac e8 00 02 00 01 0d 7f 84 60 00 00  .....`..
0030  00 00 f7 61 03 00 00 00 00 00 10 11 12 13 14 15  ...a.....
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  &'()*+,-./012345
0060  36 37                                     67
  
```

ens33: <live capture in progress> Packets: 16 · Displayed: 16 (100.0%) Profile: Default

student@student-vm: /mnt/IPK-PROJ

```

2021-04-24T22:26:53.221+02:00 IP: 172.16.176.129 > IP: 172.217.23.238, length: 98
0x0000: 00 50 56 ee 42 71 00 0c 29 7c a5 bb 08 00 45 00  .PV.Bq..)|...E.
0x0010: 00 54 7f 9e 40 00 40 01 99 b1 ac 10 b0 81 ac d9  .T..@.@.....
0x0020: 17 ee 08 00 ac e8 00 02 00 01 0d 7f 84 60 00 00  .....`..
0x0030: 00 00 f7 61 03 00 00 00 00 00 10 11 12 13 14 15  ...a.....
0x0040: 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  .....!"#$%
0x0050: 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0x0060: 36 37                                     67
  
```

Obr. 6: TEST ICMP



**Capturing from ens33 (arp)**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	2021/114 22:34:14.629571993	VMware_7c:a5:bb	VMware_ee:42:71	ARP	42	Who has 172.16.176.2? Tell 172.16.176.
2	2021/114 22:34:14.629759488	VMware_ee:42:71	VMware_7c:a5:bb	ARP	60	172.16.176.2 is at 00:50:56:ee:42:71
3	2021/114 22:34:43.045677373	VMware_7c:a5:bb	VMware_ee:42:71	ARP	42	Who has 172.16.176.2? Tell 172.16.176.
4	2021/114 22:34:43.045953615	VMware_ee:42:71	VMware_7c:a5:bb	ARP	60	172.16.176.2 is at 00:50:56:ee:42:71
5	2021/114 22:34:57.362848203	VMware_ee:42:71	Broadcast	ARP	60	Who has 172.16.176.129? Tell 172.16.17
6	2021/114 22:34:57.362920787	VMware_7c:a5:bb	VMware_ee:42:71	ARP	42	172.16.176.129 is at 00:0c:29:7c:a5:bb
7	2021/114 22:35:24.005660297	VMware_7c:a5:bb	VMware_ee:42:71	ARP	42	Who has 172.16.176.2? Tell 172.16.176.

Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface ens33, id 0  
 Ethernet II, Src: VMware\_ee:42:71 (00:50:56:ee:42:71), Dst: VMware\_7c:a5:bb (00:0c:29:7c:a5:bb)  
 Address Resolution Protocol (reply)

```

0000  00 0c 29 7c a5 bb 00 50 56 ee 42 71 08 06 00 01  ..)|...P V.Bq....
0010  08 00 06 04 00 02 00 50 56 ee 42 71 ac 10 b0 02  ....PV.Bq....
0020  00 0c 29 7c a5 bb ac 10 b0 81 00 00 00 00 00 00  ..)|.....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
  
```

student@student-vm: /mnt/IPK-PROJ

```

student@student-vm:/mnt/IPK-PROJ$ sudo ./ipk-sniffer -i ens33 --arp -n 10
2021-04-24T22:34:14.629+02:00 IP: 00:0c:29:7c:a5:bb > IP: 00:50:56:ee:42:71, length: 42
0x0000: 00 50 56 ee 42 71 00 0c 29 7c a5 bb 08 06 00 01  .PV.Bq..)|.....
0x0010: 08 00 06 04 00 01 00 0c 29 7c a5 bb ac 10 b0 81  ....)|.....
0x0020: 00 00 00 00 00 00 ac 10 b0 02  ....
2021-04-24T22:34:14.629+02:00 IP: 00:50:56:ee:42:71 > IP: 00:0c:29:7c:a5:bb, length: 60
0x0000: 00 0c 29 7c a5 bb 00 50 56 ee 42 71 08 06 00 01  ..)|...PV.Bq....
0x0010: 08 00 06 04 00 02 00 50 56 ee 42 71 ac 10 b0 02  ....PV.Bq....
0x0020: 00 0c 29 7c a5 bb ac 10 b0 81 00 00 00 00 00 00  ..)|.....
0x0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
2021-04-24T22:34:43.045+02:00 IP: 00:0c:29:7c:a5:bb > IP: 00:50:56:ee:42:71, length: 42
0x0000: 00 50 56 ee 42 71 00 0c 29 7c a5 bb 08 06 00 01  .PV.Bq..)|.....
0x0010: 08 00 06 04 00 01 00 0c 29 7c a5 bb ac 10 b0 81  ....)|.....
0x0020: 00 00 00 00 00 00 ac 10 b0 02  ....
  
```

Obr. 7: TEST ARP

**Capturing from ens33**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	2021/114 22:43:01,612839433	fe80::9099:8138:f79...	ff02::1:ff00:0	ICMPv6	86	Neighbor Solicitation for :: from 00:0c:
2	2021/114 22:43:02,629691791	fe80::9099:8138:f79...	ff02::1:ff00:0	ICMPv6	86	Neighbor Solicitation for :: from 00:0c:
3	2021/114 22:43:03,653630928	fe80::9099:8138:f79...	ff02::1:ff00:0	ICMPv6	86	Neighbor Solicitation for :: from 00:0c:
4	2021/114 22:43:29,874432619	fe80::9099:8138:f79...	ff02::1:ff00:0	ICMPv6	86	Neighbor Solicitation for :: from 00:0c:
5	2021/114 22:43:30,885647608	fe80::9099:8138:f79...	ff02::1:ff00:0	ICMPv6	86	Neighbor Solicitation for :: from 00:0c:
6	2021/114 22:43:31,909634612	fe80::9099:8138:f79...	ff02::1:ff00:0	ICMPv6	86	Neighbor Solicitation for :: from 00:0c:

Frame 4: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface ens33, id 0

- Ethernet II, Src: VMware\_7c:a5:bb (00:0c:29:7c:a5:bb), Dst: IPv6mcast\_ff:00:00:00 (33:33:ff:00:00:00)
- Internet Protocol Version 6, Src: fe80::9099:8138:f792:4b2, Dst: ff02::1:ff00:0
- Internet Control Message Protocol v6

```

0000  33 33 ff 00 00 00 00 0c 29 7c a5 bb 86 dd 60 00  33.....)|....`
0010  00 00 00 20 3a ff fe 80 00 00 00 00 00 00 90 99  ... :.....
0020  81 38 f7 92 04 b2 ff 02 00 00 00 00 00 00 00 00  .8.....
0030  00 01 ff 00 00 00 87 00 9d c3 00 00 00 00 00 00  .....
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 01 01  .....
0050  00 0c 29 7c a5 bb                                ..)|..

```

ens33: <live capture in progress> Packets: 6 · Displayed: 6 (100.0%) Profile: Default

```

^Cstudent@student-vm:/mnt/IPK-PROJ$ sudo ./ipk-sniffer -i ens33 -n 10
2021-04-24T22:43:29.874+02:00 IP: fe80::9099:8138:f792:4b2 > IP: ff02::1:ff00:0, length: 86
0x0000: 33 33 ff 00 00 00 00 0c 29 7c a5 bb 86 dd 60 00  33.....)|....`
0x0010: 00 00 00 20 3a ff fe 80 00 00 00 00 00 00 90 99  ... :.....
0x0020: 81 38 f7 92 04 b2 ff 02 00 00 00 00 00 00 00 00  .8.....
0x0030: 00 01 ff 00 00 00 87 00 9d c3 00 00 00 00 00 00  .....
0x0040: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 01  .....
0x0050: 00 0c 29 7c a5 bb                                ..)|..

```

Obr. 8: TEST ICMPv6

## Literatúra

- [1] Ethernet frame. [online], Posledná modifikácia: 03. február 2021, [vid. 2021-04-20]. Dostupné z: [https://en.wikipedia.org/wiki/Ethernet\\_frame](https://en.wikipedia.org/wiki/Ethernet_frame)
- [2] Transmission Control Protocol. [online], Posledná modifikácia: 05. apríl 2021, [vid. 2021-04-21]. Dostupné z: [https://en.wikipedia.org/wiki/Transmission\\_Control\\_Protocol](https://en.wikipedia.org/wiki/Transmission_Control_Protocol)
- [3] Address Resolution Protocol. [online], Posledná modifikácia: 07. apríl 2021, [vid. 2021-04-20]. Dostupné z: [https://en.wikipedia.org/wiki/Address\\_Resolution\\_Protocol](https://en.wikipedia.org/wiki/Address_Resolution_Protocol)
- [4] User Datagram Protocol. [online], Posledná modifikácia: 08. apríl 2021, [vid. 2021-04-21]. Dostupné z: [https://en.wikipedia.org/wiki/User\\_Datagram\\_Protocol](https://en.wikipedia.org/wiki/User_Datagram_Protocol)
- [5] Network Packet. [online], Posledná modifikácia: 11. apríl 2021, [vid. 2021-04-20]. Dostupné z: [https://en.wikipedia.org/wiki/Network\\_packet](https://en.wikipedia.org/wiki/Network_packet)
- [6] IPv4. [online], Posledná modifikácia: 12. apríl 2021, [vid. 2021-04-21]. Dostupné z: <https://en.wikipedia.org/wiki/IPv4>
- [7] EtherType. [online], Posledná modifikácia: 16. január 2021, [vid. 2021-04-20]. Dostupné z: <https://en.wikipedia.org/wiki/EtherType>
- [8] IPv6. [online], Posledná modifikácia: 17. apríl 2021, [vid. 2021-04-21]. Dostupné z: <https://en.wikipedia.org/wiki/IPv6>
- [9] Internet Control Message Protocol. [online], Posledná modifikácia: 19. apríl 2021, [vid. 2021-04-21]. Dostupné z: [https://en.wikipedia.org/wiki/Internet\\_Control\\_Message\\_Protocol](https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol)
- [10] Garcia, L. M.: Programming with Libcap – Sniffing the Network From Our Own Application. *Hakin9*, ročník 3, č. 2, 2 2008: s. 39 – 43, ISSN 1733 – 7186. Dostupné z: <http://recursos.aldeabacknocking.com/libpcapHakin9LuisMartinGarcia.pdf>
- [11] Juniper Networks, I.: IPv6 Overview. [online], Posledná modifikácia: 13. august 2014, [vid. 2021-04-23]. Dostupné z: [https://www.juniper.net/documentation/en\\_US/junose15.1/topics/concept/ipv6-overview.html](https://www.juniper.net/documentation/en_US/junose15.1/topics/concept/ipv6-overview.html)
- [12] Liang, K.: Explaining TCP/IP. [online], Posledná modifikácia: 18. jún 2018, [vid. 2021-04-23]. Dostupné z: [https://kelvin.ink/2018/06/18/ExplainingTCP\\_IP/](https://kelvin.ink/2018/06/18/ExplainingTCP_IP/)