VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Počítačové komunikace a sítě – 2. projekt

Sniffer paketů

25. dubna 2021

Jaroslav Kvasnička

1 Uvedení do problematiky a Implementace

Pro Implementaci byl zvolen jazyk c++ pro jeho jednoduchost a dostupné knihovny. Sniffer se skládá z jednoho hlavního souboru ipk-sniffer.cpp. Vnitřek programu tvoří několik funkcí s hlavním tělem main. V těle main se nachází pipelina k sniffování packetů. Je to řada několika referencí na jednotlivé funkce a jak ji postupně program prochází, vyhodnocuje jednotlivé kroky a v případě chyby nebo špatných argumentů vyhodí vyjímku a program končí. Program by měl správně vyhodnocovat jednotlivé argumenty a podle nich se zařídit při sniffování packetů a vypisování jejich dat jak v hexa tak v ascii formátu. Hlavnička je tvojena IP adresami s Porty. Čas v hlavičce nebyl implementován z důvodu nedostaktu času.

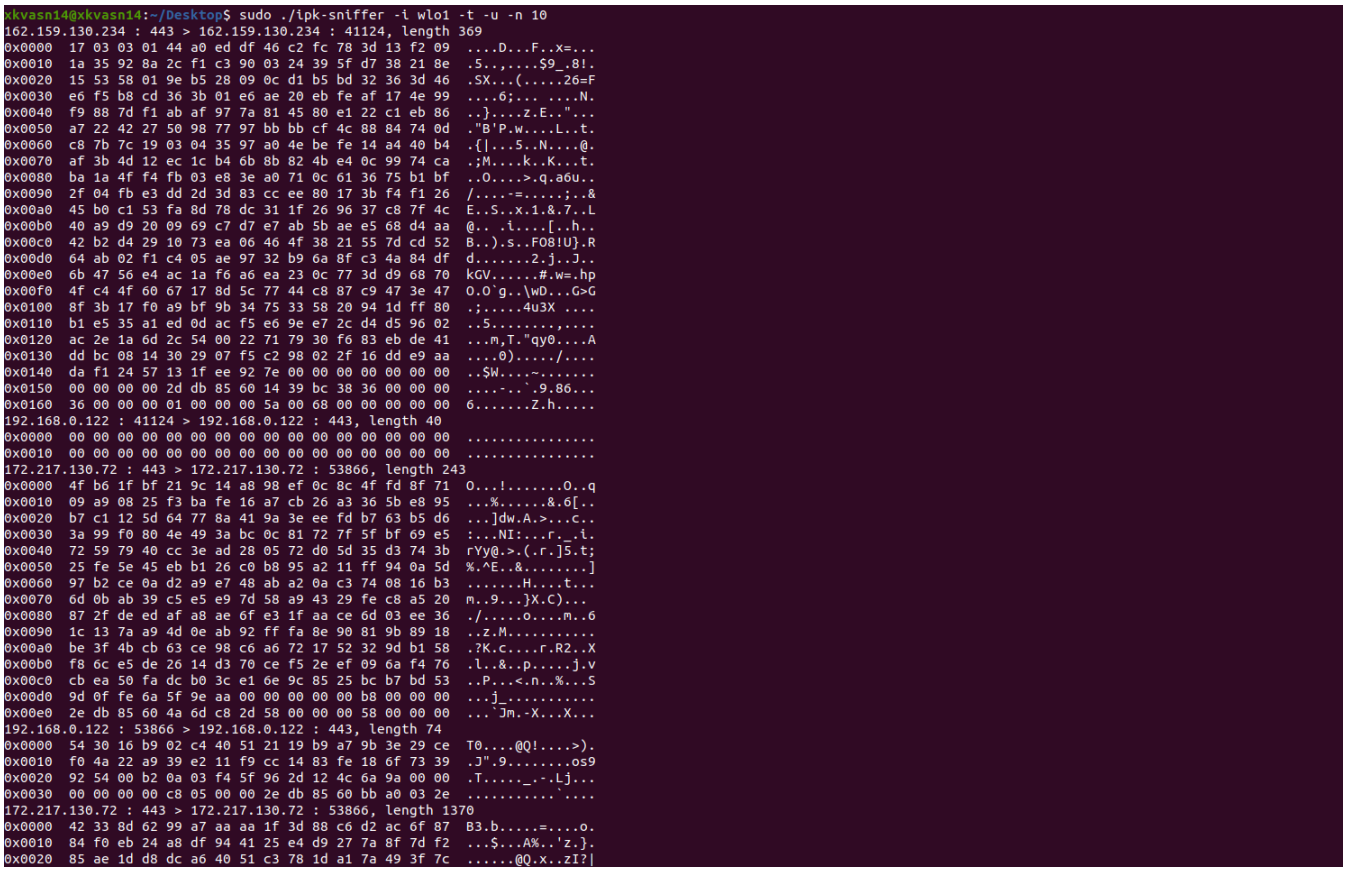
2 Problémy

Program se potýká s několika nedostatky, jako například nedokončení funkčnosti pro vypisování arp. Funkčnost TCP je plná nicméně funkčnost UDP se zdá proměnlivá. Při testování se několikrát stalo, že se program, při vypisování dat z části vyhrazené pro udp, zastavil. Obrázek č.2 nasvědčuje správné funkčnosti UDP, nicméně se může stát při testování, že nastane několik chyb a program skončí.

3 Testování

```
xkvasn14@xkvasn14:~/Desktop$ sudo ./ipk-sniffer -i wlo1 -t -n 10
192.168.0.122 : 45056 > 192.168.0.122 : 443, length 40
0x0000  a0 00 00 00 a2 da 85 60 e7 66 0b 2f 42 00 00 00  .......`.f./B...
0x0010  42 00 00 00 01 00 00 00 5a 00 68 00 00 00 00 00  B.......Z.h.....
192.168.0.122 : 43124 > 192.168.0.122 : 443, length 52
0x0000  00 00 00 00 98 00 00 00 a2 da 85 60 85 57 25 30  ...........`.W%0
0x0010  38 00 00 00 38 00 00 00 01 00 00 00 5a 00 68 00  8...8.......Z.h.
0x0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
162.159.129.232 : 443 > 162.159.129.232 : 45056, length 40
0x0000  00 00 00 00 00 00 00 00 a0 00 00 00 a2 da 85 60  ...............`
0x0010  76 b6 5f 31 42 00 00 00 42 00 00 00 01 00 00 00  v._1B...B.......
142.250.27.188 : 443 > 142.250.27.188 : 43124, length 52
0x0000  00 00 00 00 a0 00 00 00 a2 da 85 60 8c 3c e1 37  ...........`.<.7
0x0010  42 00 00 00 42 00 00 00 01 00 00 00 5a 00 68 00  B...B.......Z.h.
0x0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
192.168.0.122 : 42058 > 192.168.0.122 : 443, length 52
0x0000  00 00 00 00 d0 00 00 00 a3 da 85 60 27 c4 bd 02  ...........`'...
0x0010  75 00 00 00 75 00 00 00 01 00 00 00 5a 00 68 00  u...u.......Z.h.
0x0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
162.159.130.234 : 443 > 162.159.130.234 : 41124, length 103
0x0000  17 03 03 00 3a 11 a7 af d6 75 10 38 86 6e 04 1c  ....:....u.8.n..
0x0010  08 90 3d eb 5e d3 50 2f 88 4a 48 00 be 3f b7 ea  ..=.^.P/.JH..?..
0x0020  3f 2f cb cd a0 44 55 50 7d cf e1 bb f3 82 34 51  ?/...DUP}.....4Q
0x0030  36 cd 2e c1 26 dd 92 79 e8 ad 95 76 17 ed 76 00  6...&..y...v..v.
0x0040  00 00 00 00 a3 da 85 60 7c 7e be 02 36 00 00 00  .......`|~..6...
0x0050  36 00 00 00 01 00 00 00 5a 00 68 00 00 00 00 00  6.......Z.h.....
192.168.0.122 : 41124 > 192.168.0.122 : 443, length 40
0x0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
52.14.65.80 : 443 > 52.14.65.80 : 42058, length 52
0x0000  00 00 00 00 c8 00 00 00 a3 da 85 60 0a 97 3c 11  ...........`..<.
0x0010  6b 00 00 00 6b 00 00 00 01 00 00 00 5a 00 68 00  k...k.......Z.h.
0x0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
162.159.130.234 : 443 > 162.159.130.234 : 41124, length 93
0x0000  17 03 03 00 30 d7 9d d1 b0 b8 a9 19 22 06 ad 51  ....0.......".."Q
0x0010  66 d6 46 f1 79 34 7e 31 df a9 7c c0 74 d3 50 0a  f.F.y4~1..|.t.P.
0x0020  3c 90 88 64 cc 08 71 fd de 0d 5c b6 57 17 b1 ff  <..d..q...\.W...
0x0030  64 16 e4 f2 8a 00 00 00 90 00 00 00 a3 da 85 60  d..............`
0x0040  5d 30 3d 11 36 00 00 00 36 00 00 00 01 00 00 00  ]0=.6...6.......
192.168.0.122 : 41124 > 192.168.0.122 : 443, length 40
0x0000  60 01 00 00 a3 da 85 60 c6 56 e2 1e 00 01 00 00  `......`.V......
0x0010  00 01 00 00 01 00 00 00 5a 00 68 00 00 00 00 00  ........Z.h.....
xkvasn14@xkvasn14:~/Desktop$
```

Obrázek 1: S příkazem ./ipk-sniffer -i wlo1 -t -n 10



Obrázek 2: S příkazem ./ipk-sniffer -i wl01 -t -u -n 10