

# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

## FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Počítačové komunikace a sítě – 2. projekt

### Sniffer paketů

# 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 pipeline 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 výjimku 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 nedostatku 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

```
rkvasn14@rkvasn14:~/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 de 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}....40
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 <...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....
rkvasn14@rkvasn14:~/Desktop$
```

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

```

xkvasn14@xkvasn14:~/Desktop$ sudo ./ipk-sniffer -i wlo1 -t -u -n 10
162.159.130.234 : 443 > 162.159.130.234 : 41124, length 369
0x0000 17 03 03 01 44 a0 ed df 46 c2 fc 78 3d 13 f2 09 ....D...F..x=...
0x0010 1a 35 92 8a 2c f1 c3 90 03 24 39 5f d7 38 21 8e .5.,,...$9_.8!.
0x0020 15 53 58 01 9e b5 28 09 0c d1 b5 bd 32 36 3d 46 .SX...(. ....26=F
0x0030 e6 f5 b8 cd 36 3b 01 e6 ae 20 eb fe af 17 4e 99 ....6;... ..N.
0x0040 f9 88 7d f1 ab af 97 7a 81 45 80 e1 22 c1 eb 86 ..). ...Z.E..."...
0x0050 a7 22 42 27 50 98 77 97 bb bb cf 4c 88 84 74 0d ."B'P.W....L..t.
0x0060 c8 7b 7c 19 03 04 35 97 a0 4e be fe 14 a4 40 b4 .{[...S..N....@.
0x0070 af 3b 4d 12 ec 1c b4 6b 8b 82 4b e4 0c 99 74 ca .;M....k..K...t.
0x0080 ba 1a 4f f4 fb 03 e8 3e a0 71 0c 61 36 75 b1 bf ..O....>.q.a6u...
0x0090 2f 04 fb e3 dd 2d 3d 83 cc ee 80 17 3b f4 f1 26 /. ...-=.....;..&
0x00a0 45 b0 c1 53 fa 8d 78 dc 31 1f 26 96 37 c8 7f 4c E..S..x.1.&.7..L
0x00b0 40 a9 d9 20 09 69 c7 d7 e7 ab 5b ae e5 68 d4 aa @... .i....[...h..
0x00c0 42 b2 d4 29 10 73 ea 06 46 4f 38 21 55 7d cd 52 B..).s..F08!U}.R
0x00d0 64 ab 02 f1 c4 05 ae 97 32 b9 6a 8f c3 4a 84 df d.....2.j...J..
0x00e0 6b 47 56 e4 ac 1a f6 a6 ea 23 0c 77 3d d9 68 70 kGV.....#.w=.hp
0x00f0 4f c4 4f 60 67 17 8d 5c 77 44 c8 87 c9 47 3e 47 O.O'g...|wD...G>G
0x0100 8f 3b 17 f0 a9 bf 9b 34 75 33 58 20 94 1d ff 80 .;.....4u3X ....
0x0110 b1 e5 35 a1 ed 0d ac f5 e6 9e e7 2c d4 d5 96 02 ..S.....,.....
0x0120 ac 2e 1a 6d 2c 54 00 22 71 79 30 f6 83 eb de 41 ...m,T."qy0...A
0x0130 dd bc 08 14 30 29 07 f5 c2 98 02 2f 16 dd e9 aa ....0)...../...
0x0140 da f1 24 57 13 1f ee 92 7e 00 00 00 00 00 00 ..SW.....-.....
0x0150 00 00 00 00 2d db 85 60 14 39 bc 38 36 00 00 .. ...'.9.86...
0x0160 36 00 00 00 01 00 00 00 5a 00 68 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 .....
0x0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
172.217.130.72 : 443 > 172.217.130.72 : 53866, length 243
0x0000 4f b6 1f bf 21 9c 14 a8 98 ef 0c 8c 4f fd 8f 71 O...!.....O...q
0x0010 09 a9 08 25 f3 ba fe 16 a7 cb 26 a3 36 5b e8 95 ...%.....&.6[...
0x0020 b7 c1 12 5d 64 77 8a 41 9a 3e ee fd b7 63 b5 d6 ...|dw.A.>...c...
0x0030 3a 99 f0 80 4e 49 3a bc 0c 81 72 7f 5f bf 69 e5 ...NI:...r...i.
0x0040 72 59 79 40 cc 3e ad 28 05 72 d0 5d 35 d3 74 3b rYy0.>.(.r.]5.t;
0x0050 25 fe 5e 45 eb b1 26 c0 b8 95 a2 11 ff 94 0a 5d %.^E.&.....]
0x0060 97 b2 ce 0a d2 a9 e7 48 ab a2 0a c3 74 08 16 b3 .....H.....t...
0x0070 6d 0b ab 39 c5 e5 e9 7d 58 a9 43 29 fe c8 a5 20 m..9....}X.C)...
0x0080 87 2f de ed af a8 ae 6f e3 1f aa ce 6d 03 ee 36 ./.....o.....m..6
0x0090 1c 13 7a a9 4d 0e ab 92 ff fa 8e 90 81 9b 89 18 ..z.M.....
0x00a0 be 3f 4b cb 63 ce 98 c6 a6 72 17 52 32 9d b1 58 .?K.c.....r.R2..X
0x00b0 f8 6c e5 de 26 14 d3 70 ce f5 2e ef 09 6a f4 76 .l..&..p.....j.v
0x00c0 cb ea 50 fa dc b0 3c e1 6e 9c 85 25 bc b7 bd 53 ..P...<.n...%...S
0x00d0 9d 0f fe 6a 5f 9e aa 00 00 00 00 00 b8 00 00 00 ...j.....
0x00e0 2e db 85 60 4a 6d c8 2d 58 00 00 00 58 00 00 00 ...'Jm.-X...X...
192.168.0.122 : 53866 > 192.168.0.122 : 443, length 74
0x0000 54 30 16 b9 02 c4 40 51 21 19 b9 a7 9b 3e 29 ce T0....@0!.....>).
0x0010 f0 4a 22 a9 39 e2 11 f9 cc 14 83 fe 18 6f 73 39 .J".9.....os9
0x0020 92 54 00 b2 0a 03 f4 5f 96 2d 12 4c 6a 9a 00 00 .T....._-Lj...
0x0030 00 00 00 00 c8 05 00 00 2e db 85 60 bb a0 03 2e .....
172.217.130.72 : 443 > 172.217.130.72 : 53866, length 1370
0x0000 42 33 8d 62 99 a7 aa aa 1f 3d 88 c6 d2 ac 6f 87 B3.b.....=...o.
0x0010 84 f0 eb 24 a8 df 94 41 25 e4 d9 27 7a 8f 7d f2 ...$. ...AK...'z.].
0x0020 85 ae 1d d8 dc a6 40 51 c3 78 1d a1 7a 49 3f 7c .....@Q.x...zI?|

```

Obrázek 2: S příkazem ./ipk-sniffer -i wlo1 -t -u -n 10