
**Vysoké učení technické v Brně**
**Fakulta informačních technologií**
Počítačové komunikace a sítě
2019 / 2020

# Varianta ZETA: Sniffer paketů

Roman Ondráček (xondra58@stud.fit.vutbr.cz)
3. května 2020

# Obsah

# Úvod

Tento dokument byl vytvořen jako dokumentace druhého projektu do předmětu Počítačové komunikace a sítě a popisuje daný projekt, implementační detaily, testování a zdroje informací. Cílem projektu je síťový analyzátor napsaný v jazyce C++11, který je chopný na určitém síťovém rozhraní zachytávat a filtrovat pakety. Pro zachycení a filtrování paketů je použita knihovna `libpcap`[1]. Při implementaci byly hojně používány manuálnové stránky.

# 1 Implementace

Tato část popisuje samotný způsob implementace programu v jazyce C++11.

## 1.1 Práce s parametry

Vzhledem k tomu, že zadání požadovalo načítání krátkých i dlouhých parametrů, byla použita knihovna `getopt`[2]. Která ve standardní POSIXové implementaci sice umí pouze krátké parametry, ale na většině systémů je nainstalována GNU implementace.

## 1.2 Získání dostupných síťových rozhraní

Pro získání všech dostupných síťových rozhraní je použita funkce `pcap_findalldevs`[3] z knihovny `libpcap`. Poté ve smyčce se vypisují rozhraní, na kterých lze spustit zachytávání a filtrování paketů.

## 1.3 Zachytávání a filtrování paketů

Pro otevření síťového rozgraní pro zachytávání paketů je použita funkce `pcap_open_live`[4]. Podle použitých argumentů se v funkci `composePcapFilter` sestaví filtrovací výraz, který se poté sestaví pomocí funkce `pcap_compile`[5]. Sestavený filter se poté nastaví pomocí funkce `pcap_setfilter`[6]. Samotné zachytávání paketů se spustí pomocí funkce `pcap_loop`[7] a při každém zachycením se spustí funkce `processPacket`, která se stará o parsování jednotlivých protokolů na různých síťových vrstvách.

# 2 Testování

Moje implementace byla testována na Debianu testing a její výstupy byly porovnány s výstupy open-source síťového analyzátoru WireShark[8].

## 2.1 Ukázkový výstup

```
sudo ./ipk-sniffer -i eno1 -p 80 -t -n 4
22:46:57.609842 ASUS-B85-PRO-GAMER:35012 > www.fit.vutbr.cz:80

0x0000  d8 58 d7 00 1d c1 08 62  66 4c 53 fd 86 dd 60 08        .X.....bfLS...‘.
0x0010  2f fc 00 28 06 40 20 01  04 70 5b b2 00 00 00 00        /..(.@ ..p[.....
0x0020  00 00 00 00 06 71 20 01  06 7c 12 20 08 09 00 00        .....q ..|. ....
0x0030  00 00 93 e5 09 17 88 c4  00 50 da ea ba 55 00 00        .........P...U..
0x0040  00 00 a0 02 fd 20 64 65  00 00 02 04 05 a0 04 02        ..... de........
0x0050  08 0a 2b 71 9d 7c 00 00  00 00 01 03 03 07              ..+q.|........

22:46:57.619431 www.fit.vutbr.cz:80 > ASUS-B85-PRO-GAMER:35012

0x0000  08 62 66 4c 53 fd d8 58  d7 00 1d c1 86 dd 60 02        .bfLS..X......‘.
0x0010  8c 56 00 28 06 38 20 01  06 7c 12 20 08 09 00 00        .V.(.8 ..|. ....
0x0020  00 00 93 e5 09 17 20 01  04 70 5b b2 00 00 00 00        ...... ..p[.....
0x0030  00 00 00 00 06 71 00 50  88 c4 0c d2 8c 56 da ea        .....q.P.....V..
0x0040  ba 56 a0 12 ff ff 8d 49  00 00 02 04 05 a0 01 03        .V.....I........
0x0050  03 04 04 02 08 0a e4 11  f2 08 2b 71 9d 7c              ..........+q.|

22:46:57.619464 ASUS-B85-PRO-GAMER:35012 > www.fit.vutbr.cz:80

0x0000  d8 58 d7 00 1d c1 08 62  66 4c 53 fd 86 dd 60 08        .X.....bfLS...‘.
0x0010  2f fc 00 20 06 40 20 01  04 70 5b b2 00 00 00 00        /.. .@ ..p[.....
0x0020  00 00 00 00 06 71 20 01  06 7c 12 20 08 09 00 00        .....q ..|. ....
0x0030  00 00 93 e5 09 17 88 c4  00 50 da ea ba 56 0c d2        .........P...V..
0x0040  8c 57 80 10 01 fb 64 5d  00 00 01 01 08 0a 2b 71        .W....d]......+q
0x0050  9d 85 e4 11 f2 08                                       ......

22:46:57.619557 ASUS-B85-PRO-GAMER:35012 > www.fit.vutbr.cz:80

0x0000  d8 58 d7 00 1d c1 08 62  66 4c 53 fd 86 dd 60 08        .X.....bfLS...‘.
0x0010  2f fc 00 70 06 40 20 01  04 70 5b b2 00 00 00 00        /..p.@ ..p[.....
0x0020  00 00 00 00 06 71 20 01  06 7c 12 20 08 09 00 00        .....q ..|. ....
0x0030  00 00 93 e5 09 17 88 c4  00 50 da ea ba 56 0c d2        .........P...V..
0x0040  8c 57 80 18 01 fb 64 ad  00 00 01 01 08 0a 2b 71        .W....d.......+q
0x0050  9d 85 e4 11 f2 08 47 45  54 20 2f 20 48 54 54 50        ......GET / HTTP
0x0060  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e        /1.1..Host: www.
0x0070  66 69 74 2e 76 75 74 62  72 2e 63 7a 0d 0a 55 73        fit.vutbr.cz..Us
0x0080  65 72 2d 41 67 65 6e 74  3a 20 63 75 72 6c 2f 37        er-Agent: curl/7
0x0090  2e 36 38 2e 30 0d 0a 41  63 63 65 70 74 3a 20 2a        .68.0..Accept: *
0x00a0  2f 2a 0d 0a 0d 0a                                       /*....
```

# Reference


[1] TCPDUMP/LIBPCAP public repository [online]. The Tcpdump Group, 2020 [cit. 2020-05-03]. Dostupné z: https://www.tcpdump.org/

[2] Getopt(3) - Linux manual page [online]. Linux Programmer's Manual, 2020 [cit. 2020-05-03]. Dostupné z: http://man7.org/linux/man-pages/man3/getopt.3.html

[3] Manpage of PCAP_FINDALLDEVS [online]. The Tcpdump Group, 2020 [cit. 2020-05-03]. Dostupné z: https://www.tcpdump.org/manpages/pcap_findalldevs.3pcap.html

[4] Manpage of PCAP_FINDALLDEVS [online]. The Tcpdump Group, 2020 [cit. 2020-05-03]. Dostupné z: https://www.tcpdump.org/manpages/pcap_open_live.3pcap.html

[5] Manpage of PCAP_COMPILE [online]. The Tcpdump Group, 2020 [cit. 2020-05-03]. Dostupné z: https://www.tcpdump.org/manpages/pcap_compile.3pcap.html

[6] Manpage of PCAP_SETFILTER [online]. The Tcpdump Group, 2020 [cit. 2020-05-03]. Dostupné z: https://www.tcpdump.org/manpages/pcap_compile.3pcap.html

[7] Manpage of PCAP_LOOP [online]. The Tcpdump Group, 2020 [cit. 2020-05-03]. Dostupné z: https://www.tcpdump.org/manpages/pcap_loop.3pcap.html

[8] Wireshark · Go Deep. [online]. The Wireshark Foundation, 2020 [cit. 2020-05-03]. Dostupné z: https://www.wireshark.org/