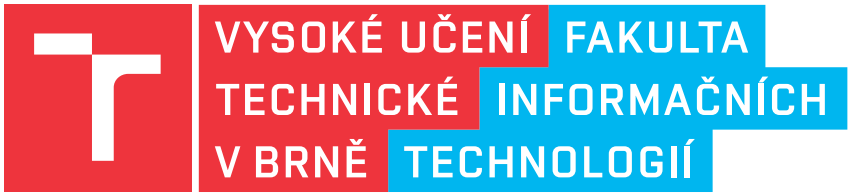


# Projektová dokumentácia

## Generování NetFlow dat ze zachycené síťové komunikace

Síťové aplikace a správa sítí

14. novembra 2022 Johann A. Gawron (xgawro00)

# Obsah

# 1 Úvod

Zadaním bolo vytvoriť Netflow sondu resp. exportér, ktorý spracuje súbor typu .pcap, v ktorom sú zachytené metadáta z internetovej komunikácie, selektívne vyberá a agreguje ich do formátu netflow.

Netflow je otvorený štandard primárne používaný spoločnosťou Cisco, ktorého hlavným cieľom je monitorovanie sieťového provozu na základe IP tokov v reálnom čase. Skladá sa z Netflow hlavičky a Netflow záznamu.

## 1.1 Štruktúra Netflow v5 záznamu

- srcaddr
- dstaddr
- nexthop
- input
- output
- dPkts
- dOctets
- First
- Last
- srcport
- dstport
- pad1
- tcp_flags
- prot
- tos
- src_as
- dst_as
- src_mask
- dst_mask
- pad2

# 2 Implementácia

Pre projekt bola zvolená Netflow v5. Program podporuje 3 protkoly: TCP, UDP a ICMP. teda iba tie dané zadaním.

## 2.1 Identifikácia toku

Pre identifikáciu toku sa používa zoradená petica údajov (Zdrojová IP adresa, Cieľová IP adresa, Zdrojový port, Cieľový port, IP protokol), ktorá je uložená pomocou štruktúry tuple v podobe kľúču pre mapu, v ktorej sú uložené vo forme kľúč, [hlavička, záznam].

## 2.2 Chod programu

Program načíta súbor pcap pre offline čítanie a následne iteruje cez packety. Popri tejto iterácii sa kontrolujú podmienky tvorby tokov ako active timer, timeout, TCP RESET alebo FIN príznak prípadne naplnenie cache tokov alebo koniec súboru pcap.

## 2.3 Export tokov

V mojej implementácii projektu sa toky odosielajú po jednom. Každá Netflow hlavička má práve jeden Netflow záznam.

# 3 Spúšťanie programu

```
./flow
>-f [-f <file>] [-c <netflow_collector>[:<port>]] [-a <active_timer>]
[-i <inactive_timer>] [-m <count>] [-h]

-f    - meno analyzovaného pcap súboru alebo STDIN
-c    - IP adresa alebo hostname Netflow kolektoru, volitelne aj UDP port
-a    - interval v sekundách, pre active export
-i    - interval v sekundách, pre inactive export
-m    - veľkosť flow cache
-h    - help
```

## 3.1 Príklad spustenia

```
>./flow -f file.pcap -c localhost:2055 -a 60 -i 10 -m 1024
```

**Použitá Literatúra**


- https://en.wikipedia.org/wiki/NetFlow — NetFlow na Wikipedia.org
- https://www.ibm.com/docs/en/npi/1.3.0?topic=versions-netflow-v5-formats — Definícia Netflow v5 formátov
- https://www.mutekh.org/doc/Network_library_module_reference.html — Network library module reference