



# ISA - Síťové aplikace a správa sítí

Generování NetFlow dat ze zachycené síťové komunikace

*Josef Kuba*

*07/11/22*

## Obsah

|                                    |   |
|------------------------------------|---|
| základní informace o programu..... | 3 |
| Použití.....                       | 5 |
| Implementace.....                  | 5 |
| Zdroje.....                        | 5 |
| Kódy.....                          | 5 |
| Literatura:.....                   | 6 |

## základní informace o programu

Netflow je software používaný na sběr informací o provozu v síti.

Program načítá (podle zadání TCP, UDP, ICMP) pakety, které zařazuje do flow a odesílá na kolektor. Zdroj je zadán přepínačem -f nebo defaultně STDIN.

Flow je jednoznačně rozlišitelná pomocí šestice zdrojová ip adresa, cílová ip adresa, zdrojový port, cílový port, ToS (type of service) a protokol (TCP, UDP a ICMP). Pakety jsou po jednom načítány a informace z nich jsou uládány do flows.

Pokud dojde k překročení intervalu active nebo inactive je daný flow odeslán na kolektor. Intervaly jsou určeny přepínači -a pro active a -i pro inactive . Pokud dojde k přeplnění cache je nejstarší flow odeslána. Maximální počet flows uchovávaných v cachi je určeno přepínačem -m.

Po zpracování všech paketů se odešle zbytek flows uložených cache a program se ukončí.

## NetFlow v5 packet header (C)

```
struct ftpdu_v5 {
    /* 24 byte header */
    u_int16 version;          /* 5 */
    u_int16 count;            /* The number of records in the PDU */
    u_int32 sysUpTime;        /* Current time in millisecs since router booted */
    u_int32 unix_secs;        /* Current seconds since 0000 UTC 1970 */
    u_int32 unix_nsecs;       /* Residual nanoseconds since 0000 UTC 1970 */
    u_int32 flow_sequence;    /* Seq counter of total flows seen */
    u_int8  engine_type;      /* Type of flow switching engine (RP,VIP,etc.) */
    u_int8  engine_id;        /* Slot number of the flow switching engine */
    u_int16 reserved;
};
```

## NetFlow v5 packet format (C)

```
/* 48 byte payload */
struct ftrec_v5 {
    u_int32 srcaddr;          /* Source IP Address */
    u_int32 dstaddr;          /* Destination IP Address */
    u_int32 nexthop;          /* Next hop router's IP Address */
    u_int16 input;            /* Input interface index */
    u_int16 output;           /* Output interface index */
    u_int32 dPkts;            /* Packets sent in Duration */
    u_int32 dOctets;          /* Octets sent in Duration */
    u_int32 First;            /* SysUptime at start of flow */
    u_int32 Last;             /* and of last packet of flow */
    u_int16 srcport;          /* TCP/UDP source port number or equivalent */
    u_int16 dstport;          /* TCP/UDP destination port number or equiv */
    u_int8  pad;
    u_int8  tcp_flags;        /* Cumulative OR of tcp flags */
    u_int8  prot;             /* IP protocol, e.g., 6=TCP, 17=UDP, ... */
    u_int8  tos;              /* IP Type-of-Service */
    u_int16 src_as;           /* originating AS of source address */
    u_int16 dst_as;           /* originating AS of destination address */
    u_int8  src_mask;         /* source address prefix mask bits */
    u_int8  dst_mask;         /* destination address prefix mask bits */
    u_int16 drops;
}; records[FT_PDU_V5_MAXFLOWS];
```

## Použití

Program podporuje následující syntax pro spuštění:

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

kde

-f <file> jméno analyzovaného souboru nebo STDIN,

-c <neflow\_collector:port> IP adresa, nebo hostname NetFlow kolektoru. volitelně i UDP port (127.0.0.1:2055, pokud není specifikováno),

-a <active\_timer> - interval v sekundách, po kterém se exportují aktivní záznamy na kolektor (60, pokud není specifikováno),

-i <seconds> - interval v sekundách, po jehož vypršení se exportují neaktivní záznamy na kolektor (10, pokud není specifikováno),

-m <count> - velikost flow-cache. Při dosažení max. velikosti dojde k exportu nejstaršího záznamu v cachi na kolektor (1024, pokud není specifikováno).

Všechny parametry jsou brány jako volitelné. Pokud některý z parametrů není uveden, použije se místo něj výchozí hodnota.

## Implementace

Pro načtení argumentů jsem využil knihovnu getopt. Nahrané argumenty jsem zpracoval (převedel na číslo - NumOrEnd gethostbyname převedení adresy).

V další části jsem se inspiroval svým kódem z projektu (IPK 2 packet sniffer) kde jsem využil konstrukci na zpracování packetu (funkce my\_callback, handle\_ethernet, handle\_IP).

Funkce z knihovny pcap pcap\_loop mi předá ukazatel na paket který předá funkci my\_callback, ve které volá funkci handle\_ethernet. V této funkci si uložím informace o čase kdy byl packet zachycen a uložím si data do struktury ether\_header abych je mohl načíst (data z této struktury zachytávají chyby). V ukazateli daném pcap\_loop se posunu o velikost ether\_header a nahraji data do struktury my\_ip ze které už získávám potřebné informace a ukládám je do globální struktury MyPacket a zároveň předem zmíněnou šestici do MyKey.

Nejprve kontroluji timery (active, inactive) každé flow co je uložena v MojeMapa a odesílám flows pomocí funcce SendAndRemoveByKey. Tuto funkci používám (jak název napovídá) k odeslání flows na kolektor a vymazání záznamu z mapy.

Dále ve funkci my\_callback ukládám tyto získané informace z MyPacket do globální map (MojeMapa). Pokud neexistuje klíč vytvoří se nová flow a pokud ne tak se upraví informace o flow. Nakonec ve funkci my\_callback kontroluji zda nebyl překročen maximální počet uložených flows. Odesílání flow jsem se inspiroval z Elearningu (echo-udp-client2.c).

Použití existujících programů

Existující programy jsem používal pro kontrolu výsledků.

Nfcpad, nfdump a Wireshark.

# Zdroje

## Kódy

Načtení argumentů: <https://www.man7.org/linux/man-pages/man3/getopt.3.html>

Čtení z paketu: <http://yuba.stanford.edu/~casado/pcap/disect2.c>

Netflow paket formát: <https://nsrc.org/workshops/2010/aroc-guatemala/raw-attachment/wiki/Agenda/netflow-slides.pdf>

Odesílání: echo-udp-client2.c

Převedení dat: <https://cplusplus.com/reference/cstring/memcpy/>

## Literatura:

<https://en.wikipedia.org/wiki/NetFlow>

[https://en.wikipedia.org/wiki/Ethernet\\_frame](https://en.wikipedia.org/wiki/Ethernet_frame)

<https://en.wikipedia.org/wiki/IPv4>

[https://www.google.com/search?](https://www.google.com/search?q=tcp+header&source=lnms&tbm=isch&sa=X&ved=2ahUKEwiqrIKOyJz7AhWAVvEDHf30DSgQAUoAXoECAIQAw&cshid=1667841208734914&biw=1920&bih=973&dpr=1#imgrc=Wu4y0W59XZR1M)

[q=tcp+header&source=lnms&tbm=isch&sa=X&ved=2ahUKEwiqrIKOyJz7AhWAVvEDHf30DSgQAUoAXoECAIQAw&cshid=1667841208734914&biw=1920&bih=973&dpr=1#imgrc=Wu4y0W59XZR1M](https://www.google.com/search?q=tcp+header&source=lnms&tbm=isch&sa=X&ved=2ahUKEwiqrIKOyJz7AhWAVvEDHf30DSgQAUoAXoECAIQAw&cshid=1667841208734914&biw=1920&bih=973&dpr=1#imgrc=Wu4y0W59XZR1M)

[q=udp+header&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjD9JefyJz7AhXdSvEDHXAAADroQAUoAXoECAIQAw&biw=1920&bih=973&dpr=1#imgrc=V1Rb9t5pq8h4AM](https://www.google.com/search?q=udp+header&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjD9JefyJz7AhXdSvEDHXAAADroQAUoAXoECAIQAw&biw=1920&bih=973&dpr=1#imgrc=V1Rb9t5pq8h4AM)

[https://www.google.com/search?](https://www.google.com/search?q=icmp+header&source=lnms&tbm=isch&sa=X&ved=2ahUKEwii3_zsyJz7AhXnQPEDHYSEAiWQAUoAXoECAIQAw&biw=1920&bih=973&dpr=1#imgrc=X3uHmLJp92Oc6M)

[q=icmp+header&source=lnms&tbm=isch&sa=X&ved=2ahUKEwii3\\_zsyJz7AhXnQPEDHYSEAiWQAUoAXoECAIQAw&biw=1920&bih=973&dpr=1#imgrc=X3uHmLJp92Oc6M](https://www.google.com/search?q=icmp+header&source=lnms&tbm=isch&sa=X&ved=2ahUKEwii3_zsyJz7AhXnQPEDHYSEAiWQAUoAXoECAIQAw&biw=1920&bih=973&dpr=1#imgrc=X3uHmLJp92Oc6M)