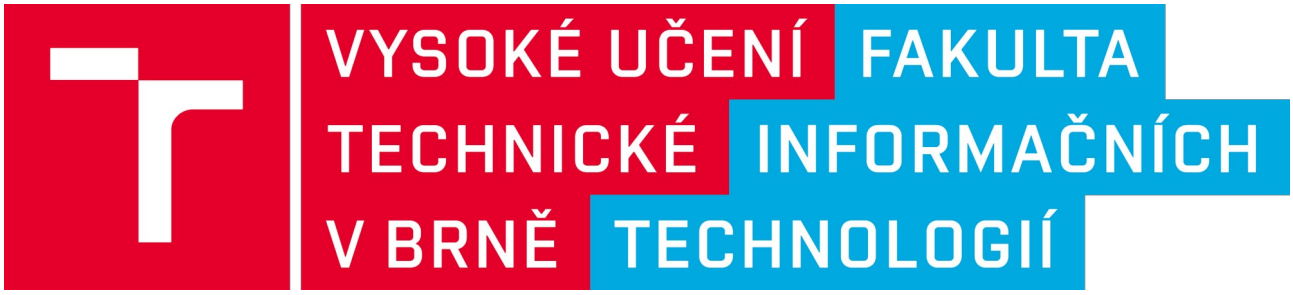


ISA - Síťové aplikace a správa sítí

Generování NetFlow dat ze zachycené síťové komunikace

Josef Kuba

07/11/22

Obsah

základní informace o programu

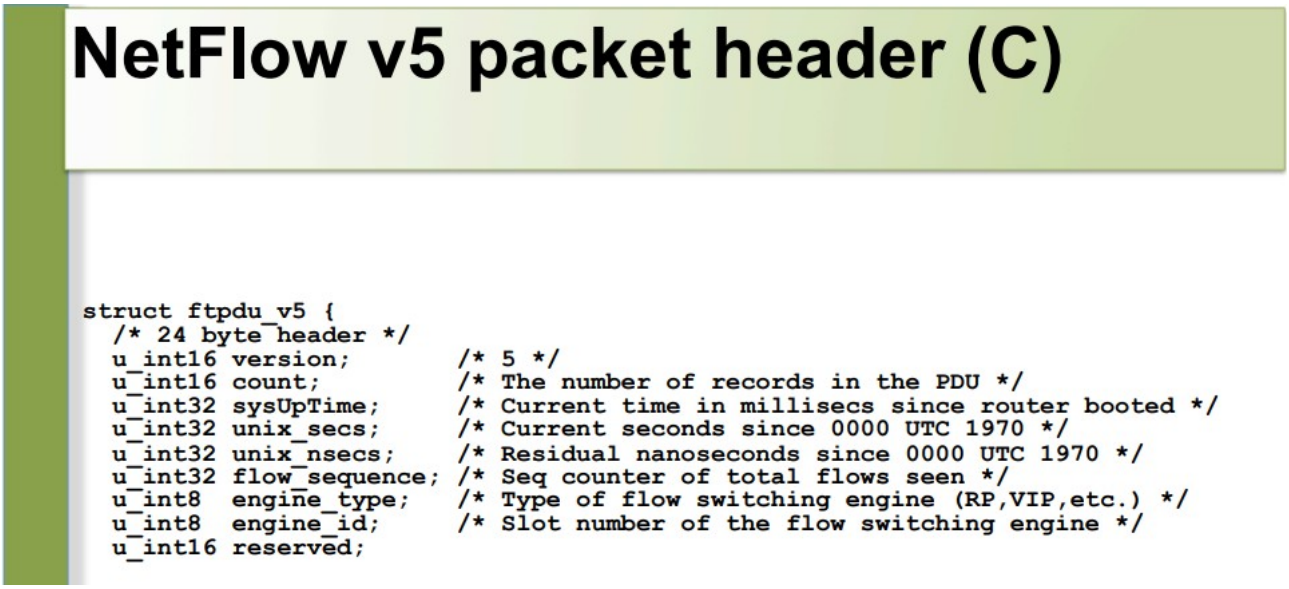
Netflow je software používaný na sběr informací o provozu v síti.

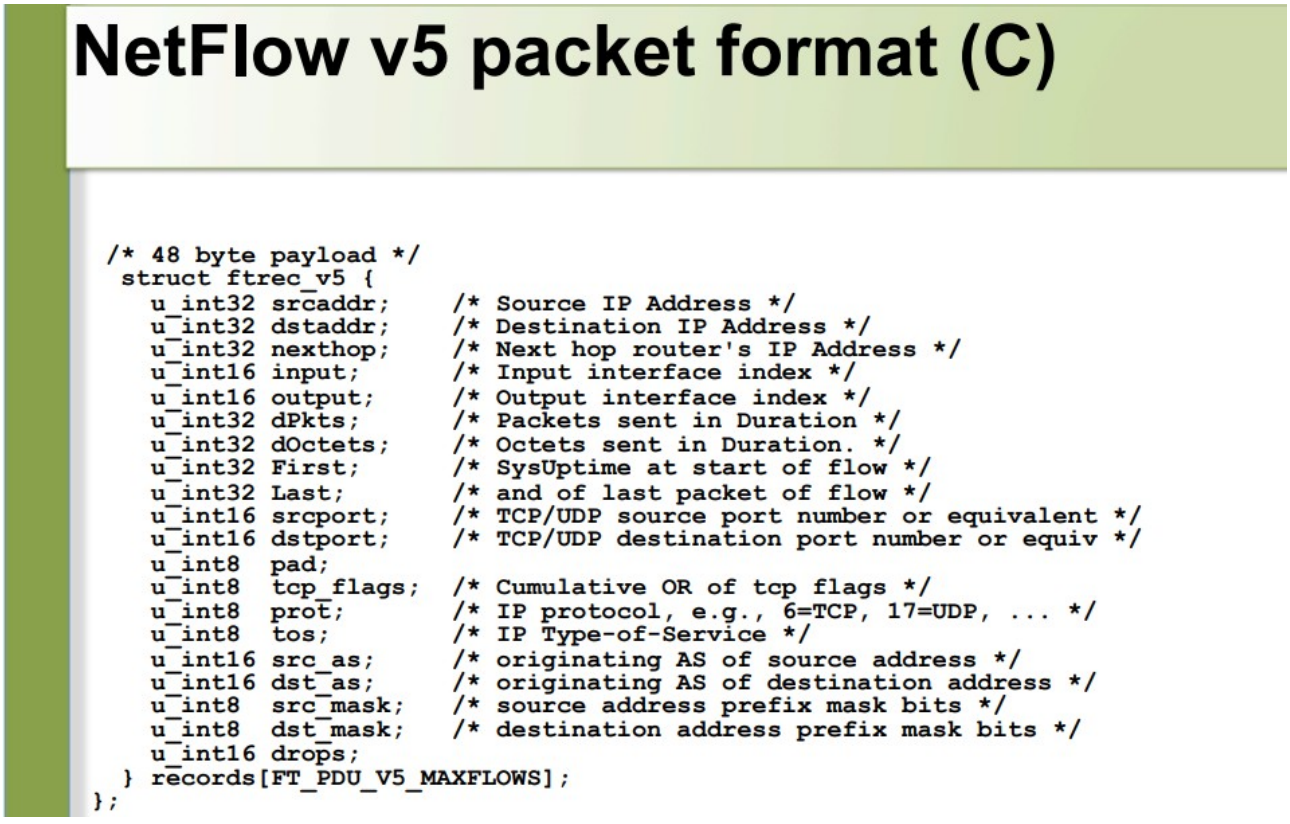
Program načítá (podle zadání TCP, UDP, ICMP) pakety, které zařazuje do flow a odesílá na kolektor. Zdroj je zadán přepínačem -f nebo defaultně STDIN.

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 danný 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.





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 (převedl 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 uložená v MojeMapa a odesílám flows pomocí funce 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.
Nfcapd, 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/IPv4
https://www.google.com/search?q=tcp+header&source=lnms&tbm=isch&sa=X&ved=2ahUKEwiqrIKOyJz7AhWAVvEDHf30DSgQ_AUoAXoECAIQAw&cshid=1667841208734914&biw=1920&bih=973&dpr=1#imgrc=Wu4y0W59XZRa1M
q=udp+header&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjD9JefyJz7AhXdSvEDHXAADroQ_AUoAXoECAIQAw&biw=1920&bih=973&dpr=1#imgrc=V1Rb9t5pq8h4AM
https://www.google.com/search?q=icmp+header&source=lnms&tbm=isch&sa=X&ved=2ahUKEwii3_zsyJz7AhXnQPEDHYSEAiwQ_AUoAXoECAIQAw&biw=1920&bih=973&dpr=1#imgrc=X3uHmLJp92Oc6M