Síťové aplikace a správa sítí
Dokumentácia Generování NetFlow dat ze zachycené síťové komunikace

Emma Krompaščíková
xkromp00

Obsah

1 Zadanie

Popis: V rámci projektu implementujte NetFlow exportér, který ze zachycených síťových dat ve formátu pcap vytvoří záznamy NetFlow, které odešle na kolektor.

Použití:
Program musí podporovat 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.

Příklad použití:

./flow -f input.pcap -c 192.168.0.1:2055

Implementace:

Implementujte v jazyku C/C++, za pomoci knihovny libpcap.

Upřesnění zadání:

- Jako export stačí použít NetFlow v5. Pokud byste implementovali v9 se šablonami, bude to bonusově zohledněno v hodnocení projektu.
- Pro vytváření flow stačí podpora protokolů TCP, UDP, ICMP.
- Informace, které neznáte (srcAS, dstAS, next-hop, aj.) nastavte jako nulové.
- Při exportování používejte původní časové značky zachycené komunikace.
- Pro testování můžete využít nástroje ze sady nfdump (nfdump, nfcapd, nfreplay, ...).
- Pro vytvoření vlastního testovacího souboru můžete použít program *tcpdump*.
- Exportované NetFlow data by měla být čitelná nástrojem nfdump.

2 Teoretický úvod

NetFlow je otvorený protokol vyvinutý spoločnosťou Cisco Systems, určený pôvodne ako doplnková služba k Cisco smerovačom. Jeho hlavným účelom je monitorovanie sieťovej prevádzky na základe IP tokov, ktoré poskytuje administrátorom aj manažérom podrobný pohľad do prevádzky na ich sieti v reálnom čase.

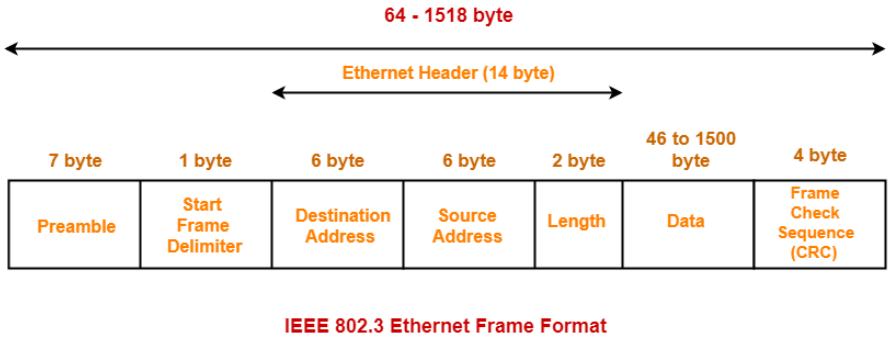
Potrebné tabuľky, ktoré som využila v projekte boli:

Netflow Header Format a Flow record tabuľky

Table B-3 Version 5 Header Format

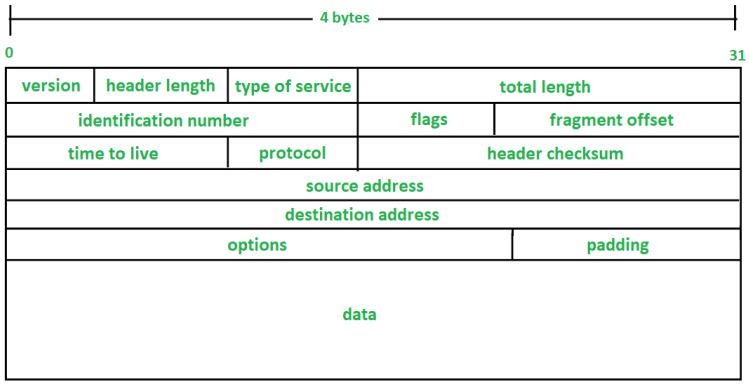
Bytes	Contents	Description
0-1	version	NetFlow export format version number
2-3	count	Number of flows exported in this packet (1-30)
4-7	SysUptime	Current time in milliseconds since the export device booted
8-11	unix_secs	Current count of seconds since 0000 UTC 1970
12-15	unix_nsecs	Residual nanoseconds since 0000 UTC 1970
16-19	flow_sequence	Sequence counter of total flows seen
20	engine_type	Type of flow-switching engine
21	engine_id	Slot number of the flow-switching engine
22-23	sampling_interval	First two bits hold the sampling mode; remaining 14 bits hold value of sampling interval

tabuľka ethernetovej hlavičky

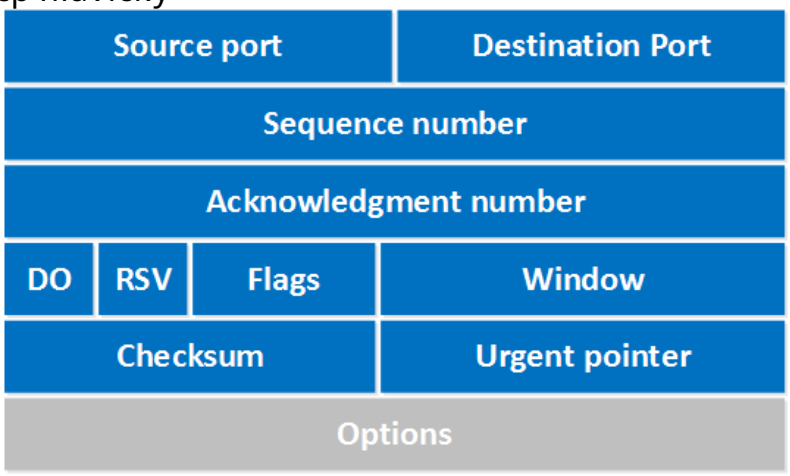


IEEE 802.3 Ethernet Frame Format

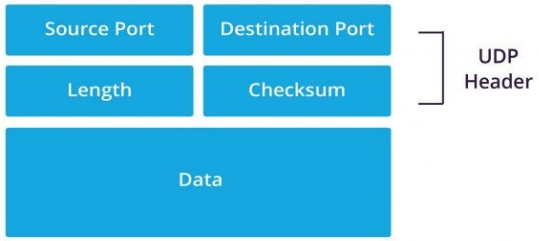
tabuľka IP hlavičky



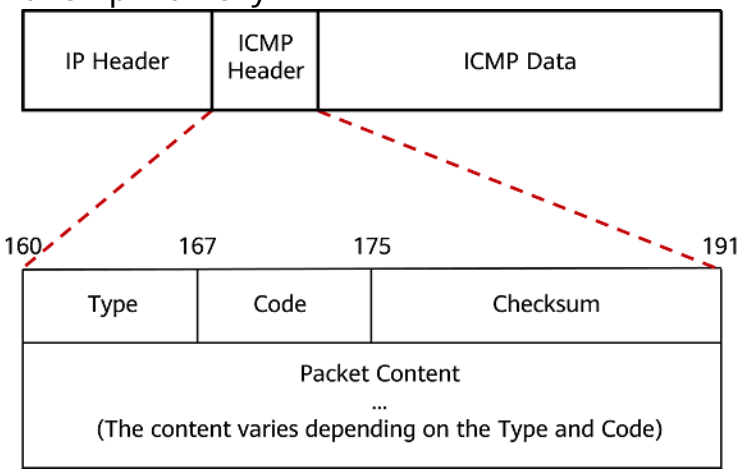
tabuľka tcp hlavičky



tabuľka udp hlavičky



tabuľka icmp hlavičky



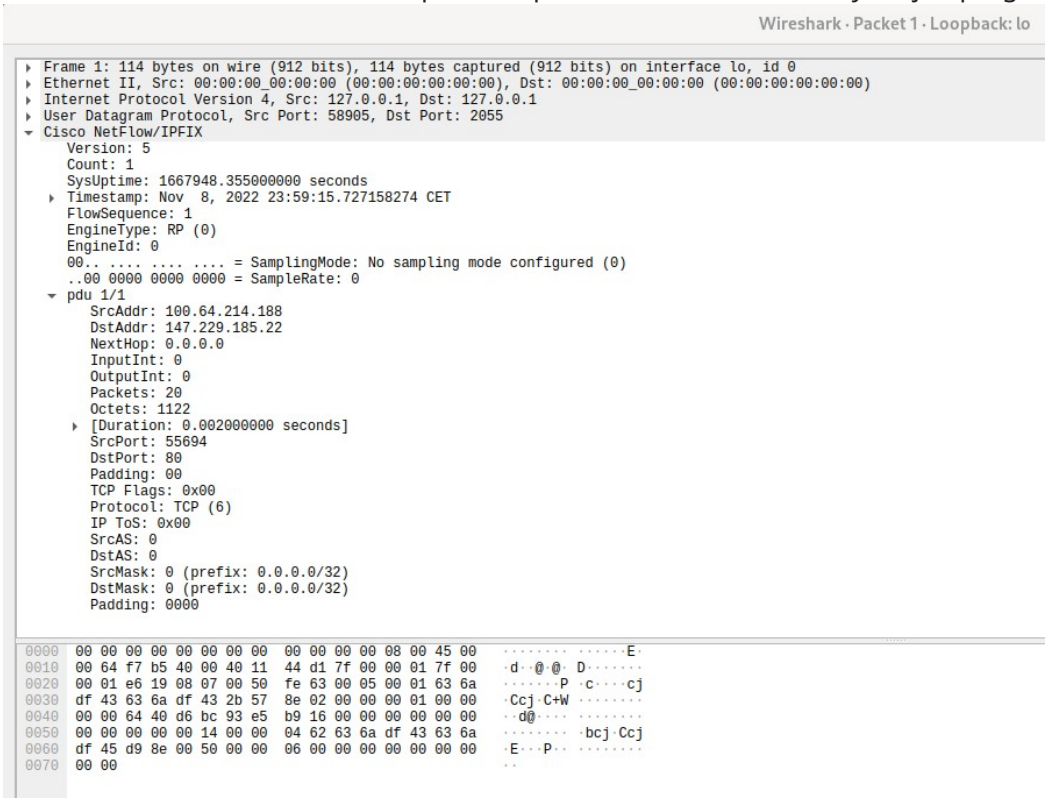
3 Použité nástroje

Na overenie funkčnosti som používala subor so zachytenými paketmi vo formáte .pcapng

Wireshark

Wireshark je počítačová aplikácia pre analýzu prevádzky v počítačových sieťach, ktorá sa používa na zisťovanie a odstraňovanie problémov v počítačových sieťach, vývoj komunikačných protokolov a softvéru a štúdium sieťovej komunikácie.

Vo Wiresharku som na rozhraní Loopback:lo pozorovala odoslané flowy mojím programom.



Dokážeme z toho ľahko vyčítať rôzne informácie, ako napríklad zdrojovú a cieľovú ip adresu, počet odoslaných paketov, či počet odoslaných bytov (Octest).

nfcadp

nfcadp je program na odchytávanie netflow premávky. Pomocou neho som kontorlovala, či boli pakety správne odoslané.

4 Použité knižnice

libpcap – knižnica na zachytávanie paketov a spracúvanie
getopt – spracúvanie argumentov
netinet – spracúvanie hlavičiek paketov

5 Implementácia

Z knižnice libpcac používam funkciu pcap_open_offline() na načítavanie paketov zo súboru.
Používam pcac_loop() - na prechádzanie jednotlivých paketov v súbore.
Vo funkcii packet_handler() spracúvam jednotlivé pakety.
Vo funkcii udpSend() zostavujem UDP paket, ktorý posielam na Netflow collector.
Používam pomocné debuggovacie fukncie debugging_flow_key() a extended_debugging_flow() na pomoc pri vypisovaní jednotlivých informácií z flowov.
Spracúvam argumenty cez getopt.

6 (Ne)Funkčnosť

Môj Netflow exporter dokáže:

- čítať pakety z pcap súboru,
- rozobrať jednotlivé hlavičky a vyčítať z nich informácie
- zostaviť flow hlavičku
- agregovať pakety do tokov
- odoslať UDP paket na kolektor
- dobre spracovať argumenty
- podporuje UPD, TCP a ICMP

Na druhú stranu, má aj neodstatky:

- v každom flow pakete odosiela jeden tok,
- tok odosiela okamžite, nečaká na žiaden timer
- neberie ohľad na velikost flow-cache.