VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

NÁSTROJ PRO PRÁCI S DATY NETFLOW

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE MIROSLAV ŠOLTÉS
AUTHOR

BRNO 2011

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

NÁSTROJ PRO PRÁCI S DATY NETFLOW

NETFLOW DATA MANIPULATION TOOL

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE MIROSLAV ŠOLTÉS
AUTHOR

VEDOUCÍ PRÁCE Ing. MATĚJ GRÉGR
SUPERVISOR

BRNO 2011

Abstrakt

Tato bakalářská práce se zabývá návrhem a implementací nástroje pro práci s daty NetFlow. Obsahuje teoretický rozbor způsobu monitorování sítě za pomocí IP Flow, popis nástroje nfdump a jeho způsob ukládání dat NetFlow v9. Při návrhu nástroje je kladen důraz na efektivní manipulaci s daty.

Abstract

This bachelor thesis deals with design and implementation of NetFlow data manipulation tool. It contains analysis of IP Flow network monitoring, description of nfdump tool and format of Netflow v9 records saved by nfdump. The focus of this work lies in effective manipulation with NetFlow records.

Klíčová slova

NetFlow, záznam NetFlow v9, nfdump, Berkeley databáze

Keywords

NetFlow v9, record NetFlow v9, nfdump, Berkeley database

Citace

Šoltés Miroslav: Nástroj pro práci s daty NetFlow, bakalářská práce, Brno, FIT VUT v Brně, 2011

NÁSTROJ PRO PRÁCI S DATY NETFLOW

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením Ing. Matěje Grégra. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

……
Miroslav Šoltés
18.5.2011

Poděkování

Tímto bych chtěl rád poděkovat panu Ing. Matějovi Grégrovi za jeho rady, nápady i podporu pro vypracovaní této bakalářske práce.

Obsah

1 Úvod

Rozvoj informačných technológií priniesol, dnes už veľmi populárny Internet. Internet je celosvetová sieť spojená z menších navzájom poprepájaných sietí. Každým dňom sa táto mohutná sieť rozširuje, a tým sa zvyšuje aj počet používateľov. V dnešnej dobe existuje veľké množstvo aplikácií a služieb, ktoré využívajú Internet. Služby, ľudia väčšinou využívajú pri komunikácii so svojimi blízkymi, či už v reálnom čase pomocou instant messaging, alebo pomocou e-mailov. Veľmi populárne sa stali sociálne siete, ktoré ľudia využívajú každý deň. Sprístupnená je aj možnosť si so svojimi blízkymi zadarmo zatelefonovať, ba dokonca spustiť video hovor. Internet nám poskytuje možnosť dozvedieť sa informácie zo sveta, čo najrýchlejším spôsobom. Výhodou Internetu je aj možnosť vzdelávania sa, či už pomocou encyklopédií alebo streamingom prednášok zo školy.

Pre veľké spoločnosti je potrebné aby informácie o stave siete a dátami, ktoré si vymieňajú koncové body, boli k dispozícii. Je to z dôvodu toho, že v dnešnej dobe vzniká nespočetné množstvo útokov a bezpečnosť je preto nevyhnutná. Preto je dobré uchovávať si dlhodobé informácie aby bolo možné detekovať útok. Analýza siete nám pomáha odhaliť slabé miesta a tým pádom aj tieto miesta zabezpečiť. Ďalším dôvodom, zväčša pre poskytovateľov Internetu, je účtovanie a fakturizácia pre užívateľov.

Tieto všetky výhody monitorovania na sieti, bezpečnosti, sledovania a analýzy na sieti nám zabezpečila firma Cisco Systems [4]. Monitorovanie IP tokov využíva protokol NetFlow, ktorý vyvinula táto spoločnosť.

Hlavným cieľom bakalárskej práce bude analyzovať, či sa dá manipulovať s binárnymi dátami NetFlow, ktoré ukladá nástroj nfdump. Pokiaľ by sa táto manipulácia podarila, bol by to prínos k aktualizovaniu dát zo siete pre administrátorov. Táto bakalárska práca nadväzuje na semestrálny projekt, v ktorom bol popísaný protokol NetFlow, jeho architektúra a ktoré mechanizmy sa podieľajú a slúžia na generovanie záznamov NetFlow. Bol bližšie popísaný protokol NetFlow verzie 9, štruktura jeho záznamov a nástroj nfdump, ktorý dokáže pracovať s touto momentálne rozširujúcou sa verziou.

V bakalárskej práci sa ďalej budem snažiť priblížiť štruktúru binárnych súborov, ktoré zaznamenáva nástroj nfdump. Následne bude rozobraný návrh a implementácia aplikácie, ktorá bude s danými dátami pracovať. Nasadenie aplikácie do praxe, by sa malo konzultovať s administrátorom siete na základe dosiahnutých výsledkov.

Kapitola 2 bola venovaná popisu protokolu NetFlow, jeho použitie a bola podrobne rozobraná štruktúra záznamu NetFlow verzie 9. V kapitole 3 sa zaoberám aplikáciou nfdump, jeho popisu a nástrojmi. Taktiež zložením binárneho súboru, ktorý je rozdelený na logické celky. Kapitola 4 je venovaný Oracle Berkeleyho databáze, jej popis a využitie. Návrh a implementácia nástroja pre prácu s dátami NetFlow je popísaná v kapitole 5. Kapitola 6 sa venuje testovaniu a dosiahnutými výsledkami. Možné rozšírenia aplikácie sú popísane v kapitole 7. Súčasťou bakalárskej práce sú aj prílohy.

2 NetFlow

Táto kapitola je zameraná na popis protokolu NetFlow. Je tu popísaná architektúra, princíp, použitie tohto protokolu a detekcia útokov.

2.1 Popis NetFlow

Tento protokol bol pôvodne vyvinutý pre firemné zariadenia spoločnosti Cisco systems. Hoci je to uzavretý protokol, máme k dispozícií špecifikáciu, zatiaľ poslednej verzie 9, v RFC 3954. Táto špecifikácia umožnila implementovať protokol aj na iné zariadenia, poprípade operačné systémy ako GNU/Linux, FreeBSD, OpenBSD.
NetFlow je protokol pre prenos záznamov o tokoch a zároveň je chápaný aj ako celý proces merania tokov [3].
Sieťový tok (IP tok) je definovaný ako postupnosť paketov zhodujúce sa v kľúčových vlastnostiach a prechádzajúci bodom pozorovania za určitý čas [1].
Medzi kľúčové vlastnosti patrí zdrojová a cieľová IP adresa, zdrojový a cieľový port, číslo protokolu, rozhranie a ToS (Type of Service), čo vidieť aj na obrázku 2.1.
IP tok obsahuje ďalšie údaje, ktoré zaznamenáva ako napríklad doba vzniku toku, dĺžka jeho trvania a iné. Podľa verzie protokolu záleží aké údaje obsahuje.

Obrázok 2.1: Identifikácia dátového toku [8]

2.2 Architektúra

Architektúra NetFlow je zložená z NetFlow exportéru a NetFlow kolektoru. Ich zásluhou sme schopný zachytiť tok a následne ho aj zálohovať.

2.2.1 Exportér

Exportérom môže byť sonda. Je to samostatné zariadenie pripojené pomocou rozbočovača k sledovanej linke. Taktiež exportér môže byť súčasťou nejakého aktívneho zariadenia typu router

alebo switch. Jeho hlavnou úlohou je monitorovať premávku na sieti a vytvárať IP toky. Pre každý IP tok exportér zaznamená jeho čas vzniku a ukončenia, počet bajtov a paketov. Zaznamenanie ďalších informácii záleží na verzii NetFlow protokolu. Po uplynutí určitého času alebo po nazbieraní určitého počtu tokov ich exportér prepošle na kolektor. Poslané toky sú z exportéru zmazané napríklad z dôvodu uvoľnenia pamäte pre ďalšie toky. Princíp fungovania exportéru môžeme rozdeliť do nasledujúcich bodov.

- Príjem paketu a extrakcia dát
- Založenie alebo aktualizovanie záznamu v NetFlow cache
- Exspirácia
- Export

Exspirácia je chápaná ako čas, ktorý po uplynutí exportuje toky dát na kolektor. Tok sa považuje za neaktívny, ak žiaden paket z toku nie je zachytený v bode pozorovania za určitý čas. Tok môže byť exportovaný na základe nasledujúcich podmienok [1].

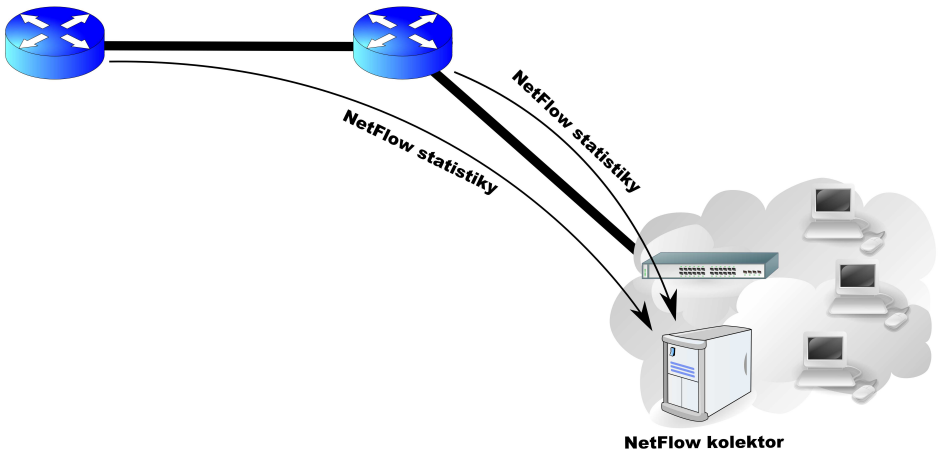
- Ak exportér dokáže detekovať koniec toku. Napríklad ak FIN alebo RST bit je nastavený v TCP spojení, tok je exportovaný.
- Ak tok je neaktívny v určitom časovom intervale. Tento neaktívny interval by mal byť konfigurovateľný na exportéry s minimálnou hodnotou 0 pre okamžitú exspiráciu.
- Ak čas toku je dlhotrvajúci, exportér by mal exportovať toky pravidelne.
- Ak má exportér nejaké obmedzenia, napríklad málo pamäte, toky sú exspirované permanentne.

Exportér môže využívať aj vzorkovanie (sampling) pre výber iba niektorých paketov. Je to výhodne z hľadiska menších nárokov na hardware.

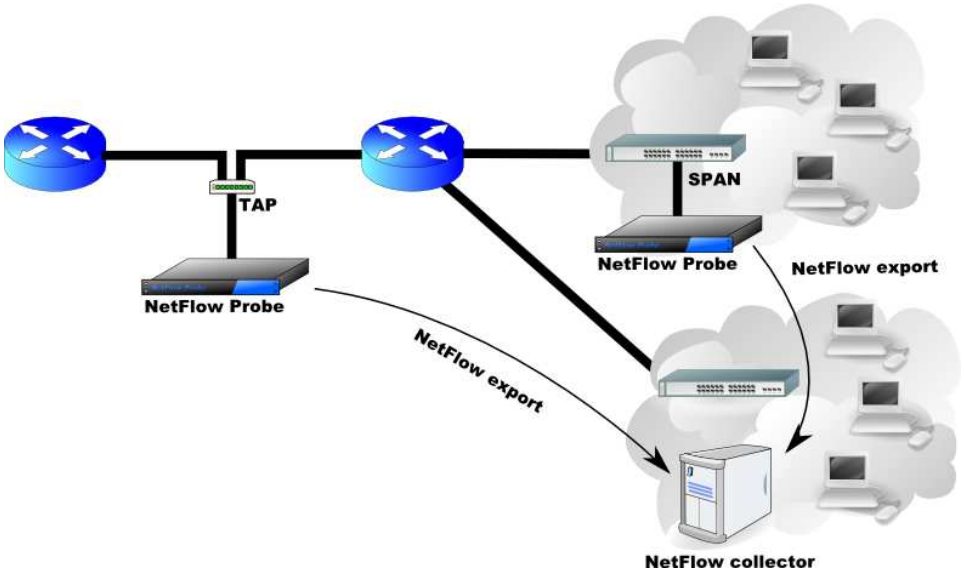
2.2.2 Kolektor

Kolektor ukladá informácie o dátových tokoch do databáze alebo na disk z jedného alebo viac exportérov. Komunikácia medzi exportérom a kolektorom prebieha pomocou UDP protokolu, čo nezaisťuje doručenie paketov na kolektor. Tieto informácie o dátových tokoch môžu byť dostupné v grafickej reprezentácii pomocou grafov alebo tabuliek. Máme tak možnosť jednoduchšie analyzovať premávku paketov v sieti. Tak ako exportér, tak aj kolektor môže používať vzorkovanie (sampling) a filtrovať tak pakety.

Pre hardwarové nároky a pomerne vysokú cenu exportéru, ktorý je aktívnym zariadením ako router, boli implementované do siete sondy, ktoré sú samostatným zariadením, určené iba pre monitorovanie na sieti. Sondy poskytujú vo väčšine prípadov nižšiu cenu a môžu byť nasadené aj v malých a stredných sietiach. Na obrázku 2.2 je znázornená situácia keď exportérom je aktívne zariadenie a ten preposiela štatistiky NetFlow kolektoru. Ďalší prípad nastáva, keď exportérom sú sondy a v sieti sa využívajú aj ďalšie technológie ako TAP a SPAN, čo vidíme na obrázku 2.3.



Obrázok 2.2: Export dát z NetFlow exportéru [12]



Obrázok 2.3: Export dát z NetFlow sondy [12]

SPAN (Switch port analyzer) analyzuje sieťovú premávku prechádzajúcu cez porty a preposiela kópiu premávky do ďalšieho portu rozbočovača, ktorý bol pripojený na sondu alebo bezpečnostné zariadenie. SPAN odráža prijatú, odoslanú alebo obojakú premávku na jeden alebo viac zdrojových portov do cieľového portu na analýzu [6].

TAP je hardvérové zariadenie, ktoré poskytuje prístup k dátam tečúcich cez počítačovú sieť. Obsahuje najmenej tri porty A, B a port na monitorovanie. TAP vôbec neblokuje premávku a zároveň ju kopíruje do portu na monitorovanie. Tento port nám slúži na umožnenie zberu dát [13].

2.3 Verzie NetFlow

V súčasnosti poznáme už niekoľko verzií protokolu NetFlow. Najviac používaná je najmä NetFlow verzia 5. Pomaly sa rozširuje aj verzia 9, ktorá dokáže monitorovať viacero údajov ako napríklad VLAN (Virtual LAN), BGP (Border Gateway Protocol), IPv6, a ďalšie.
Momentálne sa vyvíja nová verzia tohto protokolu IPFIX, ktorá bude založená na najnovšej verzii 9. Prehľad verzií protokolu NetFlow [12]:

Verzia	Popis
v1	Prvá, ale už zastarala verzia
v2 – v4	Neboli nikdy zverejnené
v5	Najrozšírenejšia, vyhradená pre toky s IPv4 adresou
v6	Pridané informácie o zapuzdrení
v7	Obsahuje informácie o smerovači
v8	Agregácia tokov
v9	Aktuálna verzia protokol s novým formátom, obsahuje nové položky a využíva šablóny pre záznamy
IPFIX	Nadstavba na verziu 9, IETF štandard

2.4 Použitie NetFlow

Protokol NetFlow je založený na monitorovaní siete. Pre administrátorov je veľmi výhodný z hľadiska znalosti premávky na sieti. Administrátor tak môže sledovať aplikácie, ktoré používajú užívatelia v danej sieti a pomocou analýzy zistiť v ktorom čase je premávka na sieti najviac využívaná. Prevádzkovatelia Internetu využívajú tento protokol taktiež aj pre účtovanie a fakturizáciu pre užívateľov.

NetFlow má výhodu taktiež čo sa týka aj bezpečnosti [5]. Dá sa použiť taktiež k detekcii rôznych útokov.

- TCP SYN flood – detekcia mnoho jedno paketových tokov s nastavenými príznakmi TCP SYN flagmi.
- Červ (worm) – detekcia mnoho odchádzajúceho toku z bežnej stanice
- Vírus – detekcia odchýlky od bežnej komunikácie
- Prenos na neobvyklých portoch
- Zvýšené prenosy na SMTP
- A ďalšie

Protokol NetFlow verzie 9 bol navrhnutý s predpokladom, že exportér a kolektor sa nachádzajú v jednej privátnej sieti v tesnej blízkosti. Avšak, môže byť použitý na transport tokov cez verejné siete, čo ukazuje na bezpečnostné riziká. Napríklad útočník môže exportované pakety odchytiť,

modifikovať alebo uložiť. Preto je tu riziko, že pakety budú odchytené a sfalšované alebo môžu byť smerované na kolektor [1].
V protokole nebolo zavedené žiadne utajenie dát, integrita alebo autentifikačné požiadavky, pretože by to redukovalo efektívnosť implementácie a predpoklad bol kladený na nasadenie do privátnych sietí. Keďže pakety nie sú šifrované, odposluch môže dať útočníkom informácie o aktívnych tokoch v sieti, komunikačných koncových zariadení a vzorky premávky. Tieto informácie môžu byť použité na špehovanie užívateľov a naplánovanie utajených útokov v budúcnosti. Informácie, ktoré si útočník môže odvodiť z odpočúvania paketov záleží na definícii toku. Ich silná iniciatíva sfalšovať záznamy sa väčšinou môže prejaviť napríklad v bankovníctve. Sfalšované môžu byť šablóny a tak zmiasť kolektor, ktorý nebude môcť dekódovať záznamy, ktoré používajú danú šablónu.
Útok DoS (Denial of service) môže zničiť veľa zdrojov z kolektoru, ktorý nebude preto môcť zachytiť a dekódovať nejaké pakety NetFlow. Avšak známe metódy na ochranu serveru od DoS útoku, znižujú tento výskyt problému.

2.5 Záznam NetFlow verzie 9

Počas vývoja protokolu NetFlow bolo už niekoľko formátov pre záznamy. Táto najnovšia verzia NetFlow je charakteristická, že je založená na šablónach. Šablóny uskutočňujú rozšírený dizajn pre záznam. Táto črta, ktorá by mala podporiť budúce vylepšenia protokolu NetFlow bez núdze dočasných zmien základného formátu záznamu. Použitie šablón má niekoľko kľúčových výhod:

- Firmy, ktoré produkujú aplikácie a zadovažujú kolektor alebo služby pre NetFlow, nebudú potrebovať prekompilovať svoje aplikácie ak bude pridaná nová funkcia. Namiesto toho, môžu použiť externé súbory s dátami, ktoré dokumentujú známe šablóny
- Nové funkcie môžu byť pridané do NetFlow oveľa rýchlejšie a to bez porušenia súčasnej implementácie
- Formát verzie 9 môže byť adaptovaný na podporu ďalších nových alebo vyvíjajúcich protokolov

Keďže štruktúra záznamu je pomerne rozsiahla, je potrebné vysvetliť základné pojmy pre ľahšie pochopenie [1].

Exportovaný paket – je vytvorený zariadením so zapnutou NetFlow službou. Tento typ paketu je adresovaný inému zariadeniu, ktoré daný paket spracuje.

Packet header – hlavička je ako prvá časť exportovaného paketu, ktorá obsahuje základné informácie o pakete, ako napríklad NetFlow verziu, počet záznamov v pakete a číslovanie sekvencie pre odhalenie stratených paketov.

FlowSet – nasleduje za hlavičkou paketu. Exportovaný paket obsahuje informácie, ktoré musia byť rozdelené a interpretované kolektorom. FlowSet je všeobecný pojem pre kolekciu záznamov, ktoré nasledujú po hlavičke v exportovanom pakete. Poznáme dva rôzne typy záznamov FlowSet a to

šablona a data. Exportovaný paket je zložený z jedného alebo viac záznamov FlowSet a šablony aj dáta môžu byť mixované v jednom exportovanom pakete.

Šablóna FlowSet – je kolekcia jednej alebo viac šablón záznamu, ktoré boli zoskupené v jednom exportovanom pakete.

Šablóna záznamu – používa sa na definovanie formátu ďalších data záznamov, ktoré môžu byť prijaté v súčastnom alebo budúcom exportovanom pakete. Dôležité je, že šablóna záznamu v exportovanom pakete nemusí nevyhnutne indikovať formát záznamu dát v tom istom pakete. Kolektor musí uchovávať v pamäti každú šablónu záznamu, ktorá bola prijatá a potom spájať jednotlivé dátové záznamy so šablónami záznamu.

Identifikátor šablóny – je unikátne číslo, ktoré odlišuje túto šablónu záznamu od všetkých ostatných šablón záznamu vyprodukované rovnakým exportérom. Aplikácia kolektoru, ktorá príjma exportované pakety z niekoľkých zariadení by mala byť upozornená, že jedinečnosť nie je garantovaná cez exportéry. A tak by mal kolektor ukladať do pamäte adresy zariadení, ktoré exportujú pakety a produkujú identifikatory šablón v poradí na uskutočnenie jedinečnosti.

FlowSet dát – je kolekcia jedného alebo viacero data záznamov, ktoré boli zoskupené do exportovaného paketu.

Záznam dát – uchováva informácie o IP toku, ktorý existuje na zariadení, ktorý produkuje exportovaný paket. Každá skupina záznamov dát má referenciu na predchádzajúce identifikačné čísla šablóny, ktoré slúži na rozdelenie dát v zázname.

Voliteľná šablóna – je špeciálny typ šablóny záznamu použitá na komunikáciu formátu dát súvisiaci s NetFlow procesom.

Voliteľný záznam dát – je špeciálny typ záznamu dát s rezervovaným identifikačným číslom šablony, ktorý nesie svoje informácie o NetFlow procese.

2.5.1 Štruktúra paketu

Na začiatku každého záznamu je hlavička (packet header) nasledujúca minimálne jedným alebo viacerými šablónami (template) alebo dátami uložené podľa danej šablóny, čo vidíme aj v tabuľke 2.1. V exportovanom pakete môžu nastať tieto kombinácie:

- Exportovaný paket, ktorý pozostáva z prekladanej šablóny a FlowSet dát. Kolektor by nemal prijať, že identifikátory šablóny definované v tom pakete majú špecifickú príbuznosť s FlowSet dát v tom istom pakete. Kolektor musí stále mať uložené každú prijatú šablónu a priradiť správne identifikačné čísla aby mohli byť dátové záznamy interpretované.

- Exportovaný paket pozostáva z FlowSet dát. Po tom, ako boli identifikačné čísla šablóny správne definované a poslané na kolektor, väčšina paketov predpísane pozostáva z FlowSet dát.
- Exportovaný paket pozostáva zo šablón FlowSet. Tento prípad je výnimkou ale je možné prijať pakety obsahujúce iba záznamy so šablónami. Keď sa exportér reštartuje, musí sa čo najskôr zosynchronizovať s kolektorom. Exportér odošle šablóny FlowSet, či má kolektor správne informácie na interpretovanie každého FlowSet dát. Šablóny záznamov majú limitovaný čas platnosti a musia byť periodicky obnovované. Ak nastane obnovovanie šablóny a nie je žiadny dátový FlowSet, ktorý je potrebný na odoslanie na kolektor, tak je odoslaný exportovaný paket so šablónami.

Obsah	Popis
Packet header	Hlavička paketu
Template FlowSet	Šablóna FlowSet
Data FlowSet	Dáta uložené podľa šablóny
Data FlowSet	Dáta uložené podľa šablóny
...	...
Template FlowSet	Šablóna FlowSet
Data FlowSet	Dáta uložené podľa šablóny
...	...

Tabuľka 2.1 Formát štruktúry záznamu

2.5.1.1 Hlavička paketu

Formát hlaviči paketu NetFlow verzie 9 ostal relatívne nezmenený od predchádzajúcich verzií. Je založený na hlavičke paketu NetFlow verzie 5 a je zobrazený v tabuľke 2.2. Na začiatku hlavičky paketu je zapísaná informácia o verzii záznamu. Obsahuje taktiež počet šablón a dat, časové značky a ďalšie dôležité informácie [2].

Bajty	Obsah	Popis
0-1	Version	Verzia NetFlow záznamu. Pre verziu 9 je to hodnota 0x0009
2-3	Count	Počet Flowset záznamov v pakete
4-7	Sys_uptime	Čas v milisekundách odkedy je exportér zapnutý
8-11	Unix_secs	Aktuálny čas v sekundách od roku 1970
12-15	Package_sequence	Sekvenčné číslo všetkých exportovaných paketov poslané exportérom. Slúži na identifikovanie, či chýba nejaký paket
16-19	Source_id	Hodnota určujúca garanciu jedinečnosti pre každý tok exportovaný z konkrétneho zariadenia

Tabuľka 2.2 Štruktúra hlavičky paketu

2.5.1.2 Štruktúra šablóny FlowSet

Štruktúra šablóny je jedným z kľúčových elementov vo verzii 9 [2]. Šablóny urýchľujú flexibilitu formátu NetFlow záznamu lebo umožňujú kolektoru alebo zobrazovacej aplikácii spracovať dáta bez znalosti formátu dát. Šablóny slúžia na popis typu a dĺžky každého poľa v ďalšom NetFlow zázname dát, ktorý je zhodný s identifikačným číslom šablóny [1]. Formát šablóny FlowSet je popísaný v tabuľke 2.3.

Flowset ID	Identifikačné číslo záznamu
Length	Veľkosť FlowSet
Template ID	Identifikačné číslo šablóny
Field_count	Počet polí
Field_type	Typ prvého poľa
Field_length	Dĺžka prvého poľa
Field_type	Typ druhého poľa
Field_length	Dĺžka druhého poľa
...	...
Field_type	Typ posledného poľa
Field_length	Dĺžka posledného poľa

Tabuľka 2.3 Štruktúra šablóny FlowSet

Identifikačné číslo záznamu slúži na rozoznanie šablóny záznamov zo záznamov dát. Šablóna záznamov má vždy identifikačné číslo v rozsahu 0-255. Celková veľkosť FlowSet je zaznamenaná lebo individuálny FlowSet šablón môže obsahovať viacero identifikačných čísel šablón. Veľkosť nám určuje pozíciu ďalšieho FlowSet záznamu, ktorý by mal byť FlowSet dát alebo šablón. Identifikačné číslo šablóny slúži na identifikovanie, ktorá šablóna sa použije na záznamy dát. FlowSet šablón môže

obsahovať viacero záznamov so šablónami, tak počet polí umožňuje určiť koniec a začiatok nového záznamu šablón. Dĺžka polí nám určuje veľkosť typov polí v bajtoch. Poznáme 87 typov polí, ktoré môžu byť zahrnuté v šablóne. Tieto typy polí môže ale nemusí podporovať exportér. To znamená, že ich nebude zaznamenávať. Jedná sa o pomerne veľké množstvo údajov, ktoré slúžia administrátorom na prehľad, čo sa na sieti deje. Tieto typy sú znázornené v prílohe 1. Ak je potrebné rozšíriť šablónu, nový typ poľa je pridaný do zoznamu. Tento typ musí byť aktualizovaný na strane exportéru a kolektora ale exportovaný NetFlow formát by mal zostať nezmenený. V niektorých prípadoch veľkosť typu poľa nemenná napríklad protokol alebo IPv4 cieľová adresa. Avšak nachádzame tu aj polia s mennou veľkosťou. To vylepšuje efektívnosť miesta na kolektory a redukuje sieťovú priepustnosť medzi kolektorom a exportérom.

Ďalšou možnosťou je nadefinovať si vlastnú šablónu. Lepšia alternatíva ako si uchovávať informácie o IP toku je použiť možnosť dodávania “meta-dat” NetFlow. Formát šablóny je znázornený v tabuľke 2.4.

Flowset_id = 1	Rozlišuje šablónu záznamu od dát. Identifikačné číslo je stále 1
Length	Určuje veľkosť daného záznamu
Template_id	Identifikačné číslo šablóny generované exportérom
Option_scope_length	Dĺžka každého poľa v tejto šablóne
Option_length	Dĺžka každého obsahu v tejto šablóne
Scope_field_N_type	Určuje významnú časť, do ktorej patrí daný záznam
Scope_field_N_length	Dĺžka oblasti poľa
Option_field_N_type	Typ poľa
Option_field_N_length	Dĺžka poľa
Padding	Slúži na zarovnanie záznamu na 32 bitov

Tabuľka 2.4 Štruktúra vlastnej šablóny

2.5.1.3 Štruktúra FlowSet dát

Štruktúra FlowSet dát je závislá na šablóne a preto je potrebné identifikačné číslo šablóny aby bolo možné určiť ako sú dáta uložené. Ak sa nenájde šablóna pre dáta, záznam by sa mal zahodiť [1]. Štruktúra FlowSet dát je znázornená v tabuľke 2.5.

FlowSet ID = Template ID	Identifikačné číslo šablóny.
Length	Dĺžka dát.
Record 1 – Field 1	Záznam 1 – pole 1
Record 1 – Field 2	Záznam 1 – pole 2
...	...
Record 1 – Field N	Záznam 1 – pole N
Record 2 – Field 1	Záznam 2– pole 1
Record 2 – Field 2	Záznam 2 – pole 2
...	...
Record 2 – Field N	Záznam 2 – pole N
...	...
Padding	Zarovnanie

Tabuľka 2.5 Štruktúra FlowSet dát

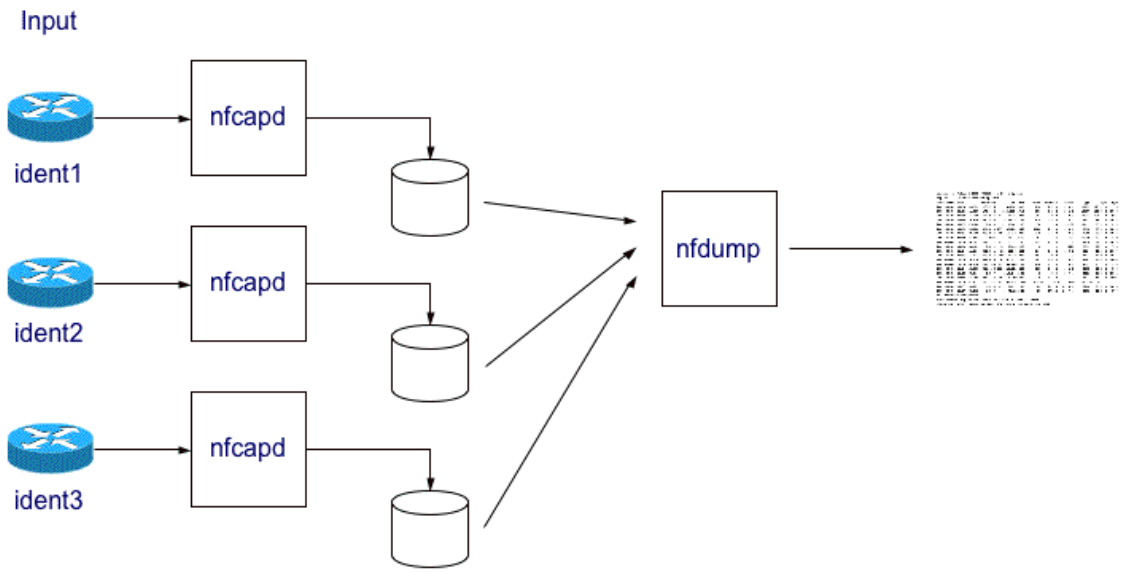
Identifikačné číslo šablóny slúži kolektoru na nájdenie korešpondujúcej šablóny a následne tak dekódovať záznam. Dĺžka dát zahrňuje veľkosť celého FlowSet dát. Záznamy obsahujú niekoľko polí. Ich typ a dĺžka bola už predtým definovaná v šablóne. Exportér na koniec FlowSet dát vloží nejaké bajty na zarovnanie, ktoré sú nulové. Hranica na zarovnanie je 32 bitov.

3 Nfdump

Táto kapitola je zameraná na popis programu nfdump a jeho nástrojov, ktorý bude používaný v tejto práci. Taktiež náčrt programu nfsen, ktorý je grafickou reprezentáciou tohto programu.

3.1 Popis programu nfdump

Nfdump (NetFlow dump) je nástroj pre prácu so záznamami NetFlow. Jeho úlohou je čítať netflow dáta zo súborov uložené nástrojom nfcapd. Užívateľ si môže zobraziť a vytvoriť mnoho štatistik, čo môže pomôcť administrátorom pri určovaní, kto najviac zaťažil sieť za určité obdobie. Je podobný nástroju tcpdump [10].
Cieľom nástroja je analyzovať dáta z minulosti a nepretržite sledovať premávku na sieti. Nfdump je limitovaný miestom na disku, ktoré je určené pre NetFlow dáta.



Obrázok 3.1: Architektúra nfdump

Všetky data sú naskôr uložené nástrojom nfcapd na disk. Pomocou nástroju nfdump môžeme tieto dáta čítať a zobraziť. Nfdump je konzolová aplikácia implementovaná v jazyku C. Z toho vyplýva, že sa jedná o pomerne rýchly nástroj.

3.2 Nástroje nfdump

Popísané nástroje umožňujú flexibilnú a uľahčenú prácu s NetFlow dátami [10]. Všetky nástroje podporujú prácu s NetFlow záznamami verzie 5, 7 a 9.

- **nfcapd** (NetFlow capture deamon): Ukladá zaznamenané dáta zo siete do súborov. Pre každý NetFlow prúd je potrebný jeden nfcapd proces pre spracovanie.
- **nfprofile** (NetFlow profiler): Spracováva NetFlow dáta zo súborov, ktoré boli uložené nfcapd. Filtruje NetFlow dáta pomocou špecifikovaných filtrov a ukladá filtrované dáta do súborov pre použitie v budúcnosti.
- **nfreplay** (NetFlow replay): Číta uložené dáta a posiela cez sieť inému užívateľovi.
- **nfclean.pl** (cleanup old data): Jednoduchý skript pre vymazanie starých dát.
- **ft2nfdump** (Read and convert flow-tools data): Konvertuje dáta do nfdump formátu aby mohli byť spracované.
- **nfsen** (NetFlow sensor): Nástroj pre grafickú reprezentáciu NetFlow dát. Používa nfdump ako záložný nástroj. Jeho webové rozhranie je ľahko ovládateľné. Je implementovaný v skriptovacích jazykoch PHP a Perl. Môže byť rozšírený použitím rôznych rozšírení. Vytvára históriu, nastavuje upozornenia založené na rôznych podmienkach [11].
- **nfanon** (NetFlow anonymisation): Používa sa na anonymizovanie všetkých IP adries v zázname NetFlow použitím kryptografie.

3.3 Štruktúra súboru nfdump

V tejto podkapitole sa budeme venovať ako nástroj nfdump ukladá súbory do binárnej formy. Na obrázku 3.2 vidíme náčrt súboru. Je rozdelený na logické celky hlavička súboru (File header), štatistiky záznamov (stats of record) a jednotlivé bloky dát (data blocks). Túto štruktúru súboru som zistil z hlavičkového súboru nffile.h, ktorý sa nachádza v zdrojových súboroch nástroja nfdump.

Obrázok 3.2: Štruktúra súboru

3.3.1 Hlavička súboru (File header)

Každý súbor začína hlavičkou, ktorá nám identifikuje, že sa jedná o súbor, ktorý uložil nfdump. V tabuľke 3.1 vidíme, že na začiatku každého súboru je 16 bitové číslo, takzvané magic number 0xA50C. To nám garantuje, že poradie bajtov (endian) je správne a taktiež, že sa jedná o súbor uložený nástrojom nfdump. Nasleduje verzia štruktúry binárneho súboru. Momentálne je implementovaná iba verzia 1. Flagy nám určujú či sa jedná o komprimovaný súbor alebo nie. V hlavičke sa nachádza počet blokov dát, ktoré sú v súbore. Ako posledná položka je reťazec. Slúži nám na identifikovanie súboru. V tabuľke 3.1 je ako za príklad počet blokov 110 a identifikátor súboru CESNET.

Magické číslo	0xA50C
Verzia	1
Flagy	0 - nekomprimovaný, 1 - komprimovaný
Počet blokov	110
Identifikátor	CESNET

Tabuľka 3.1 Hlavička súboru (File header)

3.3.2 Štatistiky záznamov (Stats of records)

Po hlavičke súboru nasledujú štatistiky záznamov. Tie sú určené skôr pre informatívnu hodnotu. Pomocou nástroja nfdump si ich môžeme vypísať pomocou prepínača `-I` (`nfdump -I <file>`). Tieto štatistiky si môžme rozdeliť do šiestich skupín. Do prvej skupiny môžeme zaradiť takzvané úplné štatistiky (overall stats). Je tam celkový počet tokov, počet bajtov a počet paketov. Druhá skupina pozostáva zo štatistík tokov (flow stats) ako je počet TCP, UDP, ICMP a iných tokov. Počty bajtov (byte stats) jednotlivých TCP, UDP, ICMP a iných tokov nájdeme v tretej skupine. Štvrtá skupina obsahuje počty paketov (packet stats). Predposlednú skupinu tvoria časové značky a v poslednej nachádzame iba sekvenciu porúch. Štatistiky zaberajú v súbore 136 Bajtov.

Úplné štatistiky	**Štatistika tokov**	**Štatistika bajtov**	**Štatistika paketov**	**Štatistika sekvencie porúch**
Počtet tokov	Počet tokov TCP	Počet bajtov TCP	Počet paketov TCP	Počet sekvencií porúch
Počet bajtov	Počet tokov UDP	Počet bajtov UDP	Počet paketov UDP	
Počet paketov	Počet tokov ICMP	Počet bajtov ICMP	Počet paketov ICMP	
	Počet iných tokov	Počet iných bajtov	Počet iných paketov	

Tabuľka 3.2 Delenie štatistík záznamov (Stats of records)

3.3.3 Bloky dát (Data blocks)

Každý datablok sa skladá z hlavičky a známym počtom záznamov. Každý blok nezaberá v súbore viac ako 1MB. Je to z dôvodu nadefinovanej konštantnej hodnoty v zdrojových súboroch nástroja nfdump v nfreader.c a nf_common.h. Ak by malo dôjsť k tomu, že sa prekročí 1MB, nfdump vytvorí nový blok dát a tam začne nové prichádzajúce záznamy ukladať. Manuálnym manipulovaním a zasahovaním do súboru môže dôjsť k tomu, že bude mať súbor viac ako 1MB dát v bloku. Pri čítaní a iných operáciách nás nfdump upozorní, že došlo k chybe lebo daný súbor je poškodený.

Obrázok 3.3: Blok dát

3.3.3.1 Hlavička bloku dát (Data block header)

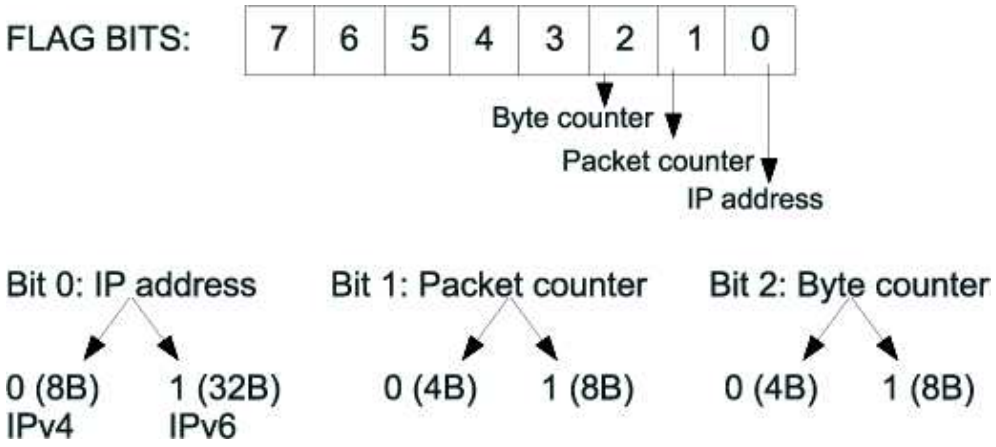
V hlavičke bloku dát je uložená informácia o počte záznamov. Počet môže byť rôzny a záleží hlavne na ich veľkosti, ktorá nesmie presiahnuť 1MB. Identifikátor bloku nám určuje akého je typu. Poznáme dva typy, ktoré budú následne stručne rozobrané. Posledná 2 bajtová položka slúži na zarovnanie a je nevyužitá.

Obsah	Popis
Number of records	Počet záznamov
Size	Veľkosť
ID	Identifikátor
Padding	Zarovnanie

Tabuľka 3.3 Hlavička bloku dát (Data block header)

3.3.3.2 Blok typu 1 (Block type 1)

Blok typu 1 obsahuje záznamy, ktoré majú iba základne informácie zo siete. Jedná sa väčšinou o záznamy NetFlow verzie 5 a 7. Záznam obsahuje napríklad položky ako časové značky, flagy a veľkosť záznamu, zdrojový a cieľový port, zdrojový a cieľový autonómny systém, ToS, protokol, TCP flagy, SNMP index vstupného a výstupného rozhrania. Flagy zaberajú 8 bitov a najmenšie tri bity nám určujú tri základné prvky. Ak nultý bit je 0 jedná sa o IP adresu verzie 4. V inom prípade sa jedná o IP adresu verzie 6, ktorá zaberá pomerne viac miesta. Je zahrnutá zdrojová a aj cieľová. Prvý bit určuje, či počet paketov je 32 (bit má hodnotu 0) alebo 64 (bit má hodnotu 1) bitové číslo. Počet bajtov taktiež môže zaberať 32 alebo 64 bitov. Položky, ktoré nám určujú flagy sú uložené na konci záznamu a pre jednoduchšie pochopenie sú znázornené na obrázku 3.4.



Obrázok 3.4 Flagy v zázname

3.3.3.3 Blok typu 2 (Block type 2)

Základné informácie zo siete nachádzame aj v záznamoch, bloku typu 2. Nástroj nfdump od svojej verzie 1.6.x začal pracovať s protokolom NetFlow verzie 9. Tym pádom sa otvorili nové možnosti ukladania dát do súboru a uchovávať viac informácii zo siete. Štruktúra NetFlow verzie 9 je daná šablónami a preto umožňuje mnoho kombinácii.
V tomto bloku rozdeľujeme záznamy na 4 typy:

- **Typ 0** je rezervovaný
- **Typ 1** je všeobecný a zahŕňa všetky rozšírenia (extensions), ktoré sú nadefinované v mape rozšírení (extension map)
- **Typ 2** označujeme za mapu rozšírení
- **Typ 3** je záznam o exportéri

O aký typ záznamu sa jedná, vieme posúdiť podľa hlavičky, ktorá nám prezrádza taktiež počet bajtov koľko zaberá daný záznam. V tejto práci podrobne rozoberiem typy 1 a 2, ktorých štruktúra bola znázornená v hlavičkovom súbore nffile.h.

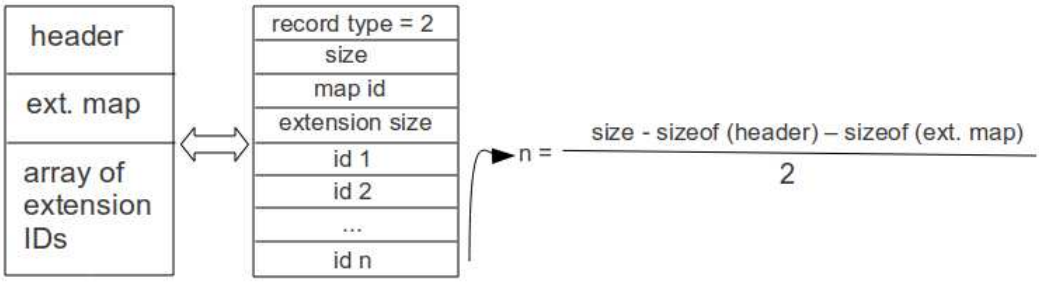
Záznam typu 1 popisuje NetFlow dátový záznam vrátane všetkých voliteľných rozšírení. Každý záznam vyžaduje minimálne prvé tri rozšírenia tj. IP adresa, počet paketov a počet bajtov. Môžeme ich vyčítať z prvých troch bitov vo flagoch. Na obrázku 3.5 vidíme základnú štruktúru. Na začiatku záznamu je typ. Prvý riadok nám určujú bajty. Keďže sa jedná o záznam typu 1 tak hodnota tohto poľa je nastavená na 1. Nasleduje veľkosť záznamu, flagy, tagy, identifikátor pre mapu rozšírení. Potom následujú časové značky, status, ktorý určuje či paket bol zahodení, prerušený alebo fragmentovaný. Následne TCP flagy, protokol, zdrojový ToS, zdrojový a cieľový port.

	0	1	2	3	4	5	6	7
0	record type = 1		size		flags	tag	ext. map	
1	msec_first		msec_last		first			
2	last				fwd status	tcp flags	protocol	src tos
3	src port		dst port/ICMP					

Obrázok 3.5: Záznam typu 1

Po tomto základe nasledujú ďalšie údaje, ktoré sú nadefinované v mape rozšírení. Pole ext. map nám určuje, ktorú šablónu použiť pre daný záznam.

Záznam typu 2 je mapa rozšírení. Vytvára sa na základe toho, aké údaje boli prijaté z exportéra. S množstvom rozšírení a kombinácií rozšírení je viac účinná a flexibilná pri čítaní a dekódovaní záznamov. V poslednej verzii nástroja nfdump je podporovaných maximálne 65535 individuálnych máp, čo je považované za postačujúce. Pre každý prístupný rozšírený záznam sú identifikátory zaznamenané v mape rozšírení v poradí v akom nasledujú.
Všetky mapy obsahujú jednoznačný identifikátor, veľkosť rozšírení koľko bajtov zaberajú v súbore a následne pole identifikátorov rozšírení, ktoré sú kľúčovým aspektom.



Obrázok 3.6: Počet rozšírení v jednom zázname

Výpočet koľko rozšírení obsahuje daná mapa je znázornený na obrázku 3.6. Od veľkosti celej mapy odčítame veľkosť hlavičky a veľkosť, ktorú zaberá identifikátor s veľkosťou rozšírení. Keďže jedna položka v poli zaberá 2 bajty, je to potrebné celé vydeliť 2, a tak získame počet rozšírení. Mapa je zarovnaná na 32 bitov, čo vidíme aj na obrázku 3.7 zobrazujúci štruktúru mapy.

	0	1	2	3	4	5	6	7
0	record type = 2		size		map id		extension size	
0	extension id 1		extension id 2		extension id 3		extension id 4	
...								
0	extension id n		extension id n+1		extension id n+2		extension id n+3	
...								
0	0		opt. 32 bit alignment					

Obrázok 3.7: Záznam typu 2

Nástroj nfdump obsahuje celkovo 25 rozšírení. Z toho prvé tri má každý záznam implicitne a medzi ne patrí IP adresa, počet paketov a počet bajtov. Tak isto ako záznamy v bloku typu 1 obsahujú tieto položky a sú identifikované podľa poľa flagy, tak aj záznamy v bloku typu 2 obsahujú pole flagy a určujú nám prvé tri rozšírenia. Pole flagy zaberá osem bitov. Ak záznam obsahuje zdrojovú aj cieľovú IP adresu verzie 4, tak nultý bit je nastavený na hodnotu 0. V opačnom prípade, ak sa jedná o IP adresu verzie 6, tak nultý bit je nastavený na hodnotu 1. Počet paketov je určený prvým bitom. Ak je hodnota prvého bitu rovná 0, tak veľkosť, ktorú zaberá toto pole je 4 bajty. Inak ak je nastavený hodnota 1, pole zaberá 8 bajtov. Tak ako aj pre počet paketov, tak aj pre počet bajtov je nastavenie bitov a zaberanie miesta v súbore rovnaké. Na obrázku 3.4 sú graficky znázornené flagy v zázname.
Ďalej nasledujú voliteľné rozšírenia definované v mapách. Pre jednoduchšie pochopenie a znázornenie ich rozdelím do niekoľkých skupín. V zátvorkách sú uvedené anglické názvy a identifikačné čísla rozšírení.

Rozšírenia zaberajúce 4 alebo 8 bajtov. Tieto rozšírenia sa vyskytujú iba zriedkavo.

- Vstupné a výstupné rozhranie (Input and output interface) (4, 5)
- Autonómny systém (Autonomous system) (6, 7)
- Odchádzajúci počet paketov (Out packets) (14, 15)
- Odchádzajúci počet bajtov (Out bytes) (16, 17)
- Agregované toky (Aggregated flows) (18, 19)

Zaberajúce 4 bajty s viacerými položkami.

- ToS, smer (direction), zdrojová a cieľová maska (source and destination mask) (8)
- Zdrojová a cieľová VLAN (Source and destination VLAN) (13)
- Typ toku zariadenia a identifikačné číslo toku zariadenia (Engine type, engine ID) iba ak sa jedná o verziu NetFlow 5 a pre verziu 9 je identifikačné číslo zdroja (Source ID) (25)

MPLS značky (labels) sú uložené ako 3 bajtové hodnoty a je ich dokopy desať. Ich uloženie a zarovnanie je znázornené v nasledujúcej tabuľke. Identifikátorom pre tieto rozšírenia je číslo 22.

0 (1 bajt)	MPLS značka 2 (3 bajty)	0 (1 bajt)	MPLS značka 1 (3 bajty)
0 (1 bajt)	MPLS značka 4 (3 bajty)	0 (1 bajt)	MPLS značka 3 (3 bajty)
0 (1 bajt)	MPLS značka 6 (3 bajty)	0 (1 bajt)	MPLS značka 5 (3 bajty)
0 (1 bajt)	MPLS značka 8 (3 bajty)	0 (1 bajt)	MPLS značka 7 (3 bajty)
0 (1 bajt)	MPLS značka 10 (3 bajty)	0 (1 bajt)	MPLS značka 9 (3 bajty)

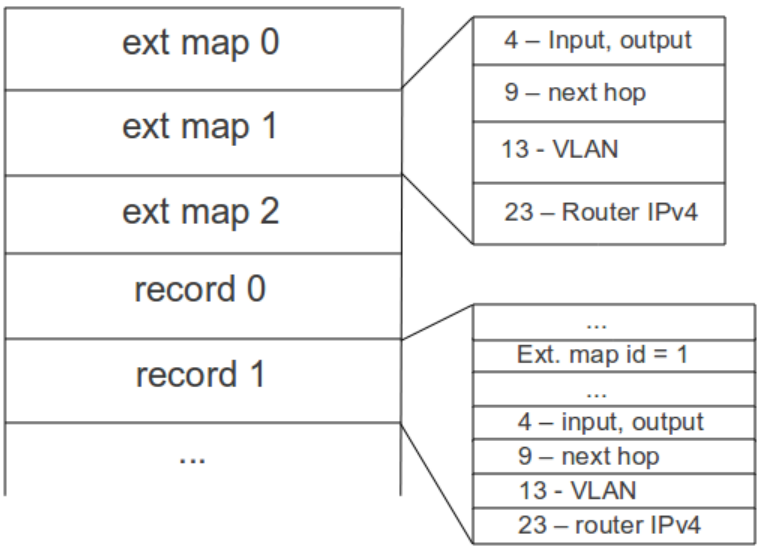
Rozšírenia obsahujúce IP adresy. Prvé číslo v zátvorke určuje rozšírenie s IP adresou verzie 4 a druhé s IP adresou verzie 6.

- IP adresa ďalšieho smerovača (IP next hop) (9, 10)
- IP adresa v doméne BGP ďalšieho smerovača (BGP next hop) (11, 12)
- IP adresa posielajúceho smerovača dané záznamy (Router IP) (23, 24)

Do ďalšej skupiny patria **MAC adresy**. Keďže veľkosť MAC adresy je 6 bajtov bola táto položka zarovnaná na 8 pre ľahšiu manipuláciu s dátami. Prvé dva bajty sú nulové. Rozšírenie 20 pozostáva zo vstupnej zdrojovej MAC adresy a výstupnej cieľovej. V rozšírení 21 môžeme nájsť vstupnú cieľovú a výstupnú zdrojovú MAC adresu. MAC adresa môže byť viac špecifická použitím viacero kombinácií smeru (direction) ako je definované v CISCO v9 [5]. Nasledujúca tabuľka zobrazuje ako sú adresy zarovnané.

0 (2 bajty)	MAC (6 bajtov)
0 (2 bajty)	MAC (6 bajtov)

Na obrázku 3.8 je znázornené ako môže vyzerať blok typu 2. Spočiatku sú nadefinované mapy a následne záznamy a pomocou identifikačného čísla mapy vieme zistiť aké ďalšie rozšírené položky obsahuje daný záznam.



Obrázok 3.8: Blok typu 2 a použie máp

Z implementačného hľadiska nástroj nfdump podporuje iba tieto rozšírenia. Vo verzii NetFlow 9 je možné zachytiť aj ďalšie ako sú napríklad minimálne a maximálne TTL (Time to live) prichádzajúcich paketov v toku, skrátený a celý názov rozhrania odkiaľ daný tok je, alebo názov vzorkovača tokov. Vývojom sa možno tieto ďalšie položky doplnia, a tak bude protokol plne využitý týmto nástrojom.

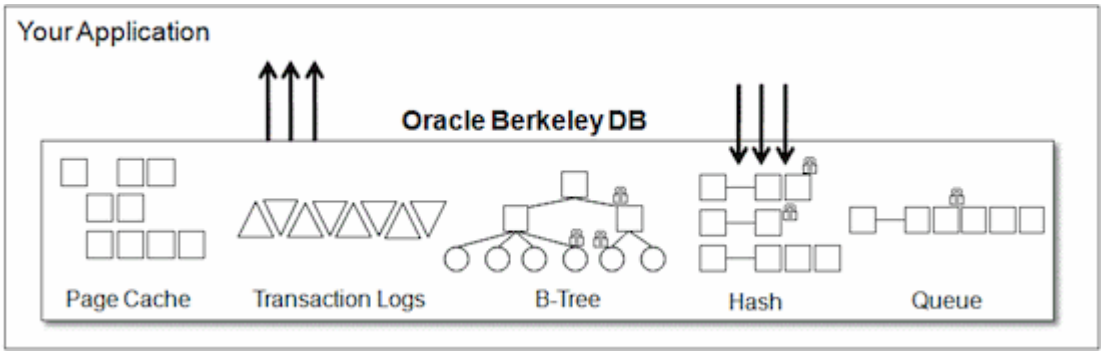
4 Oracle Berkeley databáza

Oracle je americká firma, ktorá sa špecializuje v oblasti relačnej databázovej technológie a aplikačných riešení. Táto spoločnosť vyvinula open source, vstavanú Berkeley databázu. Ponúka nám rýchle, spoľahlivé knižnice s nulovou administráciou. Je často rozvinutá okrajovo a ponúka veľmi vysoký výkon, spoľahlivosť, rozšíriteľnosť a dostupnosť pre aplikácie, ktoré nepotrebujú využívať jazyk SQL.

Berkeleyho databáza ukladá ľubovoľné páry kľúč/hodnota ako pole bajtov (nie databázová schéma), a ponúka viacero data položiek pre jeden kľúč [9]. Kľúč a dáta sú špecifikované iba ako počet bajtov a žiadna iná štruktúra nie je definovaná. Databázu je možné využívať v programovacích jazykoch ako C, C++, Java, Perl, Python, Ruby, Tcl, Smalltalk a iných.

Aj napriek jednoduchému návrhu, Berkeleyho databáza je univerzálna vstavaná databáza, ktorá umožňuje ukladať dáta dokonca až v terabajtoch. Má veľmi rýchle indexovanie a sekvenciu prístupov. To umožňuje nejaké pokročilé funkcie ako zamykanie, zdieľanie pamäte, prihlasovanie, zálohu a replikáciu. Transakcie sú vykonané spoľahlivo, čo je garanciou ACID (atomičnosť, konzistencia, samostatnosť, trvanlivosť).

Berkeleyho databáza bola použitá v programe, kde kľúčom bola IP adresa a hodnotou MAC adresa. Viac informácii je dostupných na [9].



Obrázok 4.1: Použitie Berkeley databázy [9]

5 Návrh a Implementácia

Za cieľovú platformu, na ktorej bol nástroj pre prácu s dátami NetFlow implementovaný, je operačný systém Linux. Súbory s dátami, s ktorými sa pracuje, dosahujú veľkosť až niekoľko stoviek MB. Počas vývoja aplikácie a pri testovaní mi boli poskytnuté súbory zaznamenávajúce 5 minutovú premávku na sieti, ktoré v priemere zaberali 100 MB. Z dôvodu potrebného rýchleho spracovania týchto dát a efektívneho nízkoúrovňového prístupu do pamäte, bol zvolený za programovací jazyk, jazyk C.

Implementovať danú aplikáciu bolo možné do nástroja nfdump. Keďže tento nástroj je veľmi rozsiahli a práca s ním by nebola veľmi jednoduchá, tak aplikácia bola implementovaná samostatne. Tak nie je závislá na nástroji nfdump, a práca s ňou je veľmi jednoduchá.

Nástroj pracuje s dátami NetFlow, ktoré uložil nástroj nfdump do binárneho súboru. V prvom rade bolo potrebné rozhodnúť ako sa budú dané dáta spracovávať. Boli uvažované dva spôsoby a to

- Načítanie celého súboru do pamäte a tak následná manipulácia iba s pamäťou alebo
- Postupné načítavanie zo súboru do pamäte a spracovávanie iba určitej časti súboru

Hoci práca s celým súborom v pamäti je rýchlejšia ako postupné načítavanie, bol vybraný druhý spôsob manipulácie kvôli veľkosti súboru, ktorý by zaberal v pamäti veľa miesta. Keďže štruktúra súboru nebola vopred známa a žiaden internetový zdroj neposkytoval túto štruktúru, tak ju bolo potrebné zistiť zo zdrojových súborov nástroja nfdump 1.6.1, ktorý je pod licenciou BSD. Je to pomerne rozsiahla aplikácia, na ktorej sa už dlhší čas pracuje a stále prichádzajú nové vylepšenia. K zisteniu danej štruktúry, ktorá je popísaná v kapitole 3.3 mi pomohol hlavičkový súbor nffile.h, v ktorom sú uložené štruktúry. Tieto štruktúry sú logicky rozdelené a sú akýmsi náčrtom pre binárny súbor. Takisto pomerne dostatok komentárov v tomto hlavičkovom súbore mi dopomohlo k tomuto zisteniu.

Na začiatku každého súboru je hlavička, z ktorej si zistime koľko blokov obsahuje. Nasledujú štatistiky a jednotlivé bloky, ktoré sa skladajú z hlavičky a záznamov. Z hlavičky bloku dát zistíme typ a počet záznamov v danom bloku. Ak typ bloku je 1, tak sa v ňom nachádzajú iba záznamy, ktoré obsahujú základne údaje. V blok typu 2 sa vyskytujú šablóny a záznamy, ktoré okrem základných údajov obsahujú aj ďalšie. Tie sú nadefinované v mapách a každý záznam využíva práve jednu. Ak exportér nie je schopný zachytiť údaje, ktoré sú nadefinované v mapách, tak ani nástroj nfdump nemá v binárnych súboroch miesto pre tieto dáta. Ako sa záznamy môžu vyskytovať v tomto bloku je znázornene na obrázku 3.9 v kapitole 3.3.3.3. Identifikačné čísla v šablone nám určujú aké rozšírenia sa nachádzajú v zázname.

Nástroj pre prácu s dátami NetFlow je rozdelený do modulov nffile.h, nftool.c, nfWork.c a nfWork.h. Hlavičkový súbor nffile.h je pozmenený a prebraný z nástroja nfdump. Súbor nftool.c nám slúži na spracovanie a zistenie validity parametrov. Postupné načítavanie a spracovanie dát je implementované v súbore nfWork.c. Na obrázku 5.1 je znázornený hlavný postup pri načítavaní súboru.

```
Načítaj hlavičku a zisti počet blokov
Načítaj štatistiky

Načítaj bloky
    Prečítaj hlavičku bloku a zisti počet záznamov v danom bloku
    Čítaj záznamy v danom bloku
        Ak typ bloku je 1
            Čítaj záznamy z bloku typu 1
        Ak typ bloku je 2
            Ak záznam je typu 1
                Čítaj záznamy a ich rozšírenia
            Ak záznam je typu 2
                Čítaj mapu rozšírení
            Inak
                Chyba
```

Obrázok 5.1: Pseudokód načítavania súboru

5.1 Práca s datami

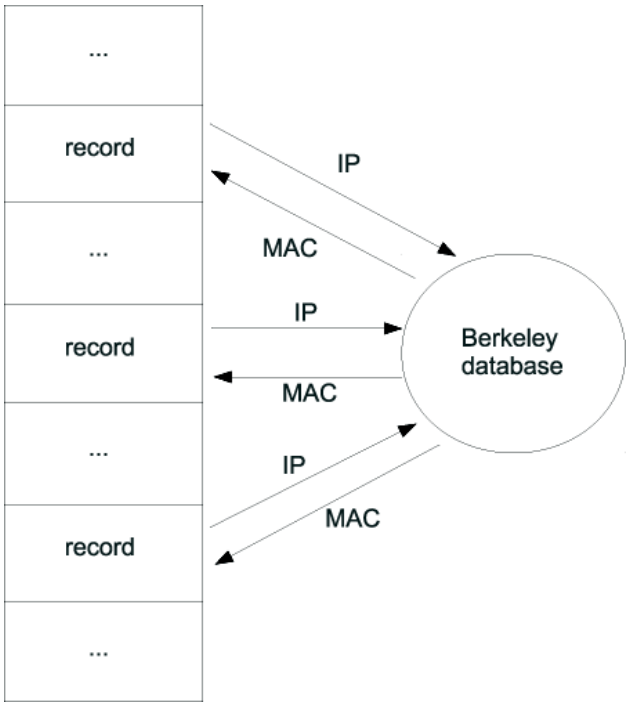
Hlavnou úlohou je manipulácia s dátami, ich zmena, aktualizácia či doplnenie. V nástroji boli implementované tri možnosti.

- Aktualizácia položky záznamov na základe jedného kľúča
- Aktualizácia položky MAC adresy na základe viac kľúčov (IP adresa)
- Doplnenie rozšírení

Kľúčom je väčšinou IP adresa, ktorá jednoznačne identifikuje o ktorý záznam sa jedná. Položka, ktorá má byť zmenená nie je v základných údajoch ale je nadefinovaná v mape rozšírení. V prvom prípade bola aktualizácia položky v zázname vykonaná, ak záznam vyhovoval danému kľúču a aktualizovaná položka bola prístupná v zázname. Ak záznam vyhovoval danému kľúču ale položka nebola v danom zázname, tak sa nebral do úvahy a program pokračoval na ďalší záznam. Nevýhoda tohto spôsobu je taká, že poznáme iba jeden pár kľúč/hodnota. Preto bolo do aplikácie implementovaná ďalšia možnosť a to viac párov kľúč/hodnota uložené buď v súbore alebo v berkeleyho databáze. Využitie tejto aplikácie je zamerané hlavne na doplňovanie a aktualizovanie MAC adresy pre danú IP adresu. Položku IP adresy nájdeme v základných údajoch. Ak chceme aby daný záznam mal položku pre MAC adresy, musíme mať v mape identifikátor rozšírenia. Ten doplníme zavolaním programu s jednotným rozšírením aby pridal do každého záznamu nulovú položku a následne zavolame program na aktualizovanie MAC adries. To by bolo z časového dôvodu náročné a preto bolo implementované doplňovanie rozšírenia a aktualizácia položky naraz. Tak nebude potrebné spustiť program dvakrát.

Vstupom programu pre viacero kľúčov bol v prvých fázach vývoja súbor, v ktorom na každom riadku bola IP a MAC adresa. Tento spôsob nebol efektívny. Preto v konečnej fáze bol implementovaný vstup s berkeleyho databázou, kde kľúčom je IP adresa a hodnotou je MAC adresa. Vyhľadávanie v tejto databázy je veľmi rýchle. Knižnica pre berkeleyho databázu bola využitá iba na vytvorenie handleru databázy a jej otvorenie, vyhľadanie a jej uzatvorenie (uvoľnenie pamäte). Ako pracuje program s databázou je znázornené na obrázku 5.2. Pri každom zázname zistíme zdrojovú a aj

cieľovú IP adresu. Následne pošleme dotaz s IP adresami a ak Berkelyho databáza obsahuje takéto kľúče s IP adresami, odošle spätne MAC adresy. V opačnom prípade sa nič neodošle a polia s MAC adresami ostanu nulové.



Obrázok 5.2 Komunikácia s Berkeleyho databázou

Keďže nfdump z dôvodu šetrenia miesta neukladá voľné polia pre ostatne rozšírenia, je potrebné pridať tieto polia. Doplnenie rozšírení spočíva v tom, že do každej šablóny sa pridá identifikátor pre zadané rozšírenie a zároveň sa v každom zázname vytvorí nulová položka pre toto rozšírenie. Táto možnosť bola implementovaná pre budúce účely, na prípravu súboru nastavením nulových hodnôt.

Po zavolaní programu sa vytvorí nový súbor a všetko čo sa postupne načítava zo vstupného súboru, ukladá do výstupného. Názov nového súboru vzniká doplnením reťazca –changed za jeho názov. Pri vývoji boli použité anonymizované dáta, no po dokončení aplikácie a následnom testovaní mi boli poskytnuté dáta z chrbticovej siete VUT.

6 Testovanie

Tvorba programu nespočíva iba z jeho vytvorenia, ale je rozdelená do viac častí a jednou z nich je testovanie. Počas vytvárania aplikácie bolo v prvom rade testované či daný súbor sa prečíta celý a správne. Takto sa zistilo validné načítavanie a daná štruktúra súboru. Následne prebiehal test po pridávaní a aktualizovaní položiek a po vytváraní nových blokov v súbore. Po každej zmene bol novo vytvorený súbor testovaný nástrojom nfdump prepínačmi [7]:

- -v slúži na overenie súboru. Vypíše verziu dát, počet blokov a status kompresie
- -x slúži na výpis máp rozšírení v danom súbore
- -r slúži na základný výpis položiek v záznamoch
- -o slúži na výpis nadefinovaných položiek

Z dôvodu pomerne rýchleho vyvíjania a vylepšovania nástroja nfdump bolo použitých viacero verzií na testovanie. Boli použité neanonymizované dáta zo siete VUT. Aplikácia bola zostrojená a testovaná na systéme s nasledujúcou konfiguráciou:

- Procesor: Intel Core 2 Duo CPU 2,20 GHz 2,20 GHz
- Pamäť: 3GB DDR2 667MHz
- Operačný systém: Linux s verziou jadra 2.6.35-28

Na testovanie boli použité dva súbory rôznej veľkosti s parametrami zobrazenými v tabuľke 6.1.

Veľkosť súboru [MB]	41,2	133
Počet blokov	42	134
Počet záznamov	635 287	2 051 036

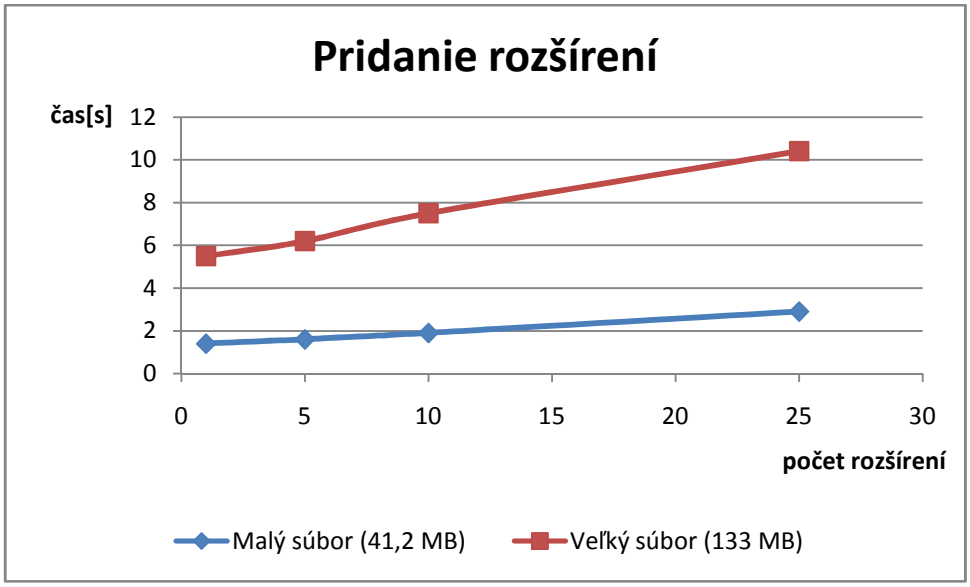
Tabuľka 6.1 Parametre súborov

V kapitole 5.1 sme sa už dozvedeli, že nástroj s dátami NetFlow môže prechádzať binárny súbor a meniť jednu hodnotu podľa zadaného kľúča. Potrebný čas na zmenenie danej položky záznamu je na to znázornený v tabuľke 6.2.

Veľkosť súboru [MB]	41,2	133
Čas [s]	1,3	4,7

Tabuľka 6.2 Čas na zmenenie jednej položky

Druhý test spočíva v pridaní rozšírení do máp a voľného miesta do záznamov s nulovými hodnotami. Na obrázku 6.1 vidíme ako postupne rastie časová zložitosť pri pridaní 1, 5, 10 a všetkých 25 rozšírení.



Obrázok 6.1 Časová zložitosť pri pridávaní rozšírení

Po pridávaní rozšírení sa zväčšovala aj veľkosť súboru, čo je znázornené v tabuľke 6.3.

Veľkosť súboru [MB]	41,2	133
Po pridaní 1 rozšírenia [MB]	46	148,7
Po pridaní 5 rozšírení [MB]	65,4	211,3
Po pridaní 10 rozšírení [MB]	94,5	305,1
Po pridaní 25 rozšírení [MB]	152,7	492,9

Tabuľka 6.3 Zväčšenie súborov po pridaní rozšírení

Posledný test je zameraný na aktualizáciu položky MAC na základe viacero kľúčov (IP adries). Porovnáva spôsob kde vstupom je súbor s IP a MAC adresami alebo vstupom je Berkeleyho databáza.

	Berkeley databáza		Súbor	
Veľkosť súboru [MB]	41,2	133	41,2	133
Čas [s]	18,6	103,1	387,4	4698,5
Nová veľkosť súboru [MB]	60,6	195,6	60,6	195,6

Tabuľka 6.4 Čas na zmenenie viac položiek

V tabuľke 6.4 je zaznamenaný čas na zmenenie viac položiek v súbore a zmena jeho veľkosti. Z dosiahnutých výsledkov vidíme, že práca s Berkeleyho databázou je oveľa rýchlejšia a preto nahradila prácu so súborom.

7 Možnosti rozšírení

V tejto kapitole sa budem venovať možnými rozšíreniami, ktoré by mohli pomôcť k rýchlosti alebo viacerými možnosťami manipulácie s dátami.

- *Implementácia do nástroja nfdump* – Keďže vytvorená aplikácia môže byť využiteľná aj pre viacero užívateľov, tak implementovanie tejto aplikácie do nástroja nfdump by im uľahčilo prácu a nemuseli by mať dve aplikácie.
- *Optimalizácia rýchlosti* – Z hľadiska rýchlosti by načítanie celého súboru do pamäte dopomohlo k zníženiu časovej náročnosti. Ďalšou možnosťou by bola implementácia dátovej štruktúry trie namiesto databázy.
- *Viac možnosti manipulácie s dátami* – Zmena MAC adresy na základe danej IP adresy je len jednou s možností manipulácie s dátami. Dali by sa implementovať aj ďalšie možnosti, ktoré by administrátorom pomohli aktualizovať poprípade pridať informácie.
- *Vytvorenie štatistik* – Po ukončení aplikácie by bola informačná hodnota koľko záznamov bolo zmenených, koľko ostáva nezmenených celkom užitočná. Poprípade vytvoriť nový súbor, kde budú záznamy, ktoré neboli zmenené.
- *Zmena platnosti MAC pre danú IP* – Po určitom časovom intervale môže dôjsť k tomu, že k danej IP adrese bude priradená v databáze iná MAC adresa. Dalo by sa to ošetriť pridaním časovej značky do databázy. Ak daný záznam bude z iného časového intervalu ako platnosť danej MAC adresy, tak hodnota MAC adresy v zázname ostane nepozmenená.

8 Záver

V tejto bakalárskej práci bolo spočiatku potrebné naštudovať teóriu k problematike a to protokol NetFlow, za ktorý môžeme ďakovať spoločnosti Cisco systems. Bol naštudovaný jeho popis, význam a architektúra, ktorá sa skladá z exportéru a kolektoru. Ďalej som sa zoznámil so záznamom NetFlow verzie 9. Bol som zameraný na jeho štruktúru, ktorá je pomerne rozsiahla ale práca s nimi je veľmi efektívna, flexibilná a má veľký prínos nielen pre administrátorov.

Aby bolo možné manipulovať s dátami, ktoré ukladá nástroj nfdump, musela byť známa štruktúra tohto súboru. Vďaka zdrojovým súborom som pomaly zisťoval ako sú dané dáta uložené. Spočiatku som sa snažil pochopiť funkcie, ktoré ukladali dané dáta. Nakoniec som natrafil na hlavičkový súbor „nffile.h”, ktorý mi prezradil väčšiu časť štruktúry. Pomocou nástroja nfdump som sa uisťoval, či daný súbor čítam správne. Pomohli mi k tomu výpisy základných údajov, výpis máp rozšírení, či overenie platnosti súboru.

Po zistení celej štruktúry som mohol začať navrhovať nástroj, ktorý by manipuloval s danými dátami. Mojou hlavnou úlohou bolo aktualizovať a doplniť adresy MAC na základe kľúča IP adresy. Spočiatku bola implementovaná jedná možnosť, no bolo to neefektívne čo sa týka počtu zmenených MAC adries. Preto mi bol poskytnutý súbor s IP a MAC adresami a hoci už program menil viac MAC adries, no nastal časový problém. Bolo potrebné eliminovať túto časovú náročnosť a preto mi bola poskytnutá Berkeleyho databáza. Práca s databázou je výrazne rýchlejšia a preto ostala aj finálnou verziou pre komunikáciu s mnoho IP a MAC adresami. Ďalej bola implementovaná možnosť pridávania máp rozšírení pre budúce účely.

Po implementovaní aplikácie som robil testy, ktoré boli zamerané na čas. Testovanie prebiehalo medzi súborom a databázou s IP a MAC adresami. Na testovanie mi už boli poskytnuté neanonymizované dáta z chrbticovej siete VUT. Daná aplikácia je prínosom pre siete, kde exportér alebo sonda nedokáže zachytiť niektoré informácie NetFlow zo siete. Preto nasadenie tejto aplikácie do praxe by mohlo pomôcť administrátorom k väčšej priehľadnosti o sieti.

Literatúra

[1] B. Claise, Ed. Cisco systems NetFlow Services Export V9. RFC 3954, Internet Engineering Task Force, Október 2004.

[2] Caligare s.r.o. NETFLOW PACKET VERSION 9 (V9) Dostupná online na <http://netflow.caligare.com/netflow_v9.htm> (február 2011)

[3] Caligare s.r.o. WHAT IS NETFLOW? Dostupná online na <http://netflow.caligare.com/index.htm> (február 2011)

[4] Cisco systems. Corporate overview. Dostupná online na <http://newsroom.cisco.com/dlls/corpinfo/corporate_overview.html> (apríl 2011)

[5] Cisco systems. Netflow. Dostupná online na <www.cisco.com/web/go/netflow> (február 2011)

[6] Cisco systems. Configuring SPAN. Dostupná online na <http://www.cisco.com/en/US/docs/switches/lan/catalyst2940/software/release/12.1_19_ea1/configuration/guide/swspan.html>

[7] Linuxcertif. Nfdump. Dostupná online na <http://www.linuxcertif.com/man/1/nfdump> (február 2011)

[8] Nextcom. Flowmon – Vaša sieť pod kontrolou. Dostupná online na <http://www.nextcom.sk/flowmon_monitorovanie_siete_uchovavanie_dat.xhtml> (apríl 2011)

[9] Oracle. Oracle Berkeley database. Dostupná online na <http://www.oracle.com/technetwork/database/berkeleydb/overview/index-085366.html> (apríl 2011)

[10] Sourceforge. NFDUMP. Dostupná online na <http://nfdump.sourceforge.net> (apríl 2011)

[11] Sourceforge. NfSen – NetFlow Sensor. Dostupná online na <http://nfsen.sourceforge.net> (apríl 2011)

[12] Wikipedia. Netflow. Dostupná online na <http://en.wikipedia.org/wiki/Netflow> (apríl 2011)

[13] Wikipedia. Network tap. Dostupná online na <http://en.wikipedia.org/wiki/Network_tap> (apríl 2011)

Zoznam príloh

Príloha 1

Táto príloha popisuje typy polí aké sa môžu vyskytovať v záznamoch NetFlow v9.

Typ poľa	Hodnota	Bajty	Popis
IN_BYTES	1	N (predvolené sú 4)	Príchodzí počet bajtov v IP toku
IN_PKTS	2	N (predvolené sú 4)	Príchodzí počet paketov v IP toku
FLOWS	3	N (predvolené sú 4)	Počet agregovaných tokov
PROTOCOL	4	1	Protokol
SRC_TOS	5	1	ToS bajt vstupného prichádzajúceho rozhrania
TCP_FLAGS	6	1	TCP flagy v danom toku
L4_SRC_PORT	7	2	TCP/UDP zdrojový port
IPV4_SRC_ADDR	8	4	IPv4 zdrojová adresa
SRC_MASK	9	1	Maska zdrojovej adresy
INPUT_SNMP	10	N (predvolené sú 2)	Vstupne rozhranie indexu
L4_DST_PORT	11	2	TCP/UDP cieľový port
IPV4_DST_ADDR	12	4	IPv4 cieľová adresa
DST_MASK	13	1	Maska cieľovej adresy
OUTPUT_SNMP	14	N (predvolené sú 2)	Výstupné rozhranie indexu
IPV4_NEXT_HOP	15	4	IPv4 adresa ďalšieho smerovača
SRC_AS	16	N (predvolené sú 2)	Zdrojový BGP autonómny systém
DST_AS	17	N (predvolené sú 2)	Cieľový BGP autonómny systém
BGP_IPV4_NEXT_HOP	18	4	IPv4 adresa ďalšieho routra v BGP doméne
MUL_DST_PKTS	19	N (predvolené sú 4)	Počet IP multicast odchádzajúcich paketov
MUL_DST_BYTES	20	N (predvolené sú	Počet IP muticast odchádzajúcich

		4)	bajtov
LAST_SWITCHED	21	4	Uptime posledného paketu v toku
FIRST_SWITCHED	22	4	Uptime prvého paketu v toku
OUT_BYTES	23	N (predvolené sú 4)	Počet odchádzajúcich bajtov
OUT_PKTS	24	N (predvolené sú 4)	Počet odchádzajúcich paketov
MIN_PKT_LNGTH	25	2	Minimálna dĺžka prichádzajúcich paketov
MAX_PKT_LNGTH	26	2	Maximálna dĺžka prichádzajúcich paketov
IPV6_SRC_ADDR	27	16	IPv6 zdrojová adresa
IPV6_DST_ADDR	28	16	IPv6 cieľová adresa
IPV6_SRC_MASK	29	1	Maska zdrojovej adresy
IPV6_DST_MASK	30	1	Maska cieľovej adresy
IPV6_FLOW_LABEL	31	3	Značka IPv6 toku
ICMP_TYPE	32	2	Typ ICMP paketu
MUL_IGMP_TYPE	33	1	Typ IGMP paketu
SAMPLING_INTERVAL	34	4	Množstvo vzorkovaných paketov
SAMPLING_ALGORITHM	35	1	Vzorkovací algoritmus: 0x01 – deterministický, 0x02 - náhodný
FLOW_ACTIVE_TIMEOUT	36	2	Čas pre aktívne toky
FLOW_INACTIVE_TIMEOUT	37	2	Čas pre neaktívne toky
ENGINE_TYPE	38	1	Typ zariadenia
ENGINE_ID	39	1	ID zariadenia
TOTAL_BYTES_EXP	40	N (predvolené sú 4)	Počet exportovaných bajtov
TOTAL_PKTS_EXP	41	N (predvolené sú 4)	Počet exportovaných paketov
TOTAL_FLOWS_EXP	42	N (predvolené sú 4)	Počet exportovaných tokov
IPV4_SRC_PREFIX	44	4	IPv4 prefix zdrojovej adresy
IPV4_DST_PREFIX	45	4	IPv4 prefix cieľovej adresy
MPLS_TOP_LABEL_TYPE	46	1	Top typ pre MPLS
FLOW_SAMPLER_ID	48	1	ID “show flow sampler”

FLOW_SAMPLER_MODE	49	1	Typ algoritmu pre vzorkované dáta
FLOW_SAMPLER_RANDOM_INTERVAL	50	4	Inteval vzorkovania
MIN_TTL	52	1	Minimálne TTL v prichádzajúcich paketoch toku
MAX_TTL	53	1	Maximálne TTL v prichádzajúcich paketoch toku
IPV4_IDENT	54	2	IPv4 identifikátor
DST_TOS	55	1	ToS vychádzajúceho rozhrania
SRC_MAC	56	6	Zdrojová MAC adresa
DST_MAC	57	6	Cieľová MAC adresa
SRC_VLAN	58	2	Zdrojová VLAN
DST_VLAN	59	2	Cieľová VLAN
IP_PROTOCOL_VERSION	60	1	IP verzia: 4 – IPv4, 6 – IPv6
DIRECTION	61	1	Smer toku: 0 – vstup, 1 - výstup
IPV6_NEXT_HOP	62	16	IPv6 adresa ďalšieho routra
BPG_IPV6_NEXT_HOP	63	16	IPv6 adresa ďalšieho routra v BGP doméne
IPV6_OPTION_HEADERS	64	4	Identifikuje IPv6 hlavičku v toku
MPLS_LABEL_1	70	3	MPLS na pozícii 1 na halde
MPLS_LABEL_2	71	3	MPLS na pozícii 2 na halde
MPLS_LABEL_3	72	3	MPLS na pozícii 3 na halde
MPLS_LABEL_4	73	3	MPLS na pozícii 4 na halde
MPLS_LABEL_5	74	3	MPLS na pozícii 5 na halde
MPLS_LABEL_6	75	3	MPLS na pozícii 6 na halde
MPLS_LABEL_7	76	3	MPLS na pozícii 7 na halde
MPLS_LABEL_8	77	3	MPLS na pozícii 8 na halde
MPLS_LABEL_9	78	3	MPLS na pozícii 9 na halde
MPLS_LABEL_10	79	3	MPLS na pozícii 10 na halde

Príloha 2. Užívateľská príručka

Preložiť aplikáciu je možné pomocou príkazu **`make`** z hlavného adresára. K úspešnemu prekladu je potrebné mať nainštalovaný prekladač GCC a knižnice Berkeley databázy. Knižnice Berkeley databázy je možné stiahnuť na stránkach spoločnosti Oracle na adrese:

http://www.oracle.com/technetwork/database/berkeleydb/downloads/index.html

Medzi možnosti spustenia aplikácie patrí:

`-h`

Tento argument slúži na výpis možností spustenia aplikácie.

`-r <súbor>`

Tento argument nám určuje súbor, ktorý má byť aktualizovaný/zmenený. Je potrebný pri každom spustení okrem argumentu –h.

`-mac <bdb>`

Tento argument nám určuje Berkeleyho databázu, v ktorej sú uložené MAC a IP adresy.

`-k <kľúč> <hodnota>`

Tento argument nám určuje kľúč, v ktorom zázname má prebehnúť zmena. Vyžaduje prítomnosť argumentu –ch.

`-ch <položka> <hodnota>`

Tento argument nám určuje hodnotu, ktorá má byť pridaná alebo zmenená. Vyžaduje prítomnosť argumentu –k.

`-e <ID of extensions>`

Tento argument slúži na pridávanie rozšírení do súboru.

Identifikačné čísla rozšírení:

4 - Input & Output (size: 2 bytes)
5 - Input & Output (size: 4 bytes)
6 - AS (size: 2 bytes)
7 - AS (size: 4 bytes)
8 - Dst tos, Dir, Src & Dst mask
9 - IP next hop ipv4
10 - IP next hop ipv6
11 - BGP next hop ipv4
12 - BGP next hop ipv6
13 - VLAN
14 - Out packet counter size (2 byte)

15 - Out packet counter size (4 byte)
16 - Out byte counter size (4 byte)
17 - Out byte counter size (8 byte)
18 - Aggr flows (4 byte)
19 - Aggr flows (8 byte)
20 - In src & Out dst MAC
21 - Out src & In dst MAC
22 - MPLS label
23 - Router IPv4
24 - Router IPv6
25 - fill, NetFlow v5: engine type & id, Netflow v9: source id

Príklady spustenia

`-r file -mac database.db`

Zmena položky MAC adresy v záznamoch v súbore file. Berkeleyho databáza (database.db) obsahuje IP adresy, ktorým sú priradené MAC adresy.

`-r file -e 13,23`

Pridanie rozšírení 13 (VLAN) a 23 (Router IPv4) do každého záznamu do súboru file. Dané položky budú obsahovať nulové hodnoty. Identifikačné čísla rozšírení musia byť oddelené čiarkou.

`-r file –k sa 147.229.1.1 –ch sm AA:BB:CC:11:22:33`

Zmena položky zdrojovej MAC adresy (sm) na AA:BB:CC:11:22:33 v záznamoch, kde zdrojová adresa (sa) je zhodná s 147.229.1.1

Príloha 3

- Písomná správa vo formáte pdf
- Zdrojový kód písomnej správy
- Zdrojové kódy programu
- Manuál