

Technická univerzita v Košiciach  
Fakulta elektrotechniky a informatiky  
Katedra počítačov a informatiky

**Analýza, návrh implementácie a vlastná  
implementácia štandardov IPFIX a PSAMP v  
meracom nástroji BasicMeter**

Diplomová práca

Študijný odbor: Informačné systémy a technológie

Vedúci diplomovej práce:

Ing. František Jakab, PhD.

Diplomant:

Miroslav Potocký

Konzultant diplomovej práce:

Ing. František Jakab, PhD.

Košice 2006

### **Čestné vyhlásenie**

Vyhlasujem, že som diplomovú prácu vypracoval(a) samostatne s využitím uvedenej odbornej literatúry.

Košice 1. 4. 2006

.....

*Vlastnoručný podpis*

Na tomto mieste bude vložené zadanie diplomovej práce

## **Podakovanie**

Chcem sa poďakovať Ing. Františekovi Jakobovi, PhD. a Ing. Jurajovi Giertlovi za odbornú pomoc, cenné rady a pripomienky pri riešení tejto diplomovej práce. Ďakujem aj mojej rodine a členom Laboratória počítačových sietí za podporu.

Názov práce: Analýza, návrh implementácie a vlastná implementácia štandardov IPFIX a PSAMP v meracom nástroji BasicMeter

Pracovisko: Katedra počítačov a informatiky, FEI TU v Košiciach

Autor: Miroslav Potocký

Vedúci DP: Ing. František Jakab, PhD.

Konzultant DP: Ing. František Jakab, PhD.

Dátum: 1. 4. 2006

Kľúčové slová: IPFIX, PSAMP, BasicMeter, QoS, meranie, IP siete, štandard

Anotácia: Pre potreby merania a vyhodnocovania parametrov počítačových sietí bol v Laboratóriu počítačových sietí vyvinutý merací nástroj BasicMeter, ktorý dokázal exportovať štatistické dáta o prevádzke v počítačovej sieti vo formáte NetFlow v5 a v9. Pre potreby novovznikajúceho štandardu IPFIX, ktorý sa má stať robustnejším nástupcom všeobecne rozšíreného štandardu NetFlow v9, má táto diplomová práca za úlohu implementovať spomínaný štandard ako exportný protokol meracieho nástroja BasicMeter. V súčinnosti s exportným protokolom, pri nasadení vo vysokorýchlostných sieťach, dochádza k využitiu vzorkovania a filtrovania prevádzky, za účelom zníženia záťaže na merací bod. Týmito otázkami sa zaoberá štandard PSAMP, z ktorého má táto práca vychádzať pri implementovaní vzorkovania a filtrovania.

Thesis title: Analysis, implementation proposal, main implementation of IPFIX and PSAMP standards in BasicMeter measurement software

Department: Department of computers and informatics, TU FEI Košice

Author: Miroslav Potocký

Supervisor: Ing. František Jakab, PhD.

Tutor: Ing. František Jakab, PhD.

Date: 1. 4. 2006

Keywords: IPFIX, PSAMP, BasicMeter, QoS, measurement, IP networks, standard

Annotation: Computer networks laboratory developed BasicMeter for evaluation and measuring of computer networks parameters. This tool can export statistical data in NetFlow v5 and v9 format. For the needs of drafted IPFIX standard, which should replace NetFlow v9 protocol, is the task of this diploma work to implement mentioned standard as an export protocol of BasicMeter measuring tool. For the use of this tool in high-speed computer networks, sampling and filtering are deployed in order to lower the overhead in measuring point. These problems are targeted by PSAMP standard, which is the base of one part of this diploma work

## **Predhovor**

Projekt QoS@Lab v rámci Laboratória počítačových sietí bol už od svojho začiatku konfrontovaný s potrebou vyvinúť nástroj, ktorý zodpovedá najnovšiemu vývoju v oblasti vyhodnocovania QoS parametrov počítačových sietí. Ďalší vývoj štandardov popisujúcich export štatistických dát o tokoch v sieti, prináša so sebou určité zmeny oproti predchádzajúcim verziám. Preto bolo nutné opätovne analyzovať požiadavky, ktoré tieto štandardy kladú na implementácie meracích nástrojov a príslušne ich inovovať. Úlohou tejto diplomovej práce je vypracovanie základnej komponenty meracieho nástroja schopného exportovať a spracovávať informácie o kvalitatívnych a kvantitatívnych parametroch počítačových sietí vo formáte IPFIX (IP Flow Information Export). Tieto informácie sú hlavnou zložkou vyhodnocovania QoS (Quality of Services) počítačových sietí. Rovnako s prechodom sieťových technológií k systémom s vysokou prenosovou rýchlosťou je nutné brať ohľad na výkonnostné charakteristiky meracieho nástroja pri jeho použití v takýchto prostrediach. Z tohoto dôvodu je súčasťou tejto diplomovej práce aj analýza a zhodnotenie konformity meracieho nástroja voči štandardu PSAMP (Packet SAMPLing). Táto diplomová práca analyzuje jednotlivé povinné aspekty týchto štandardov a porovnáva ich s reálnymi požiadavkami kladenými na vyvíjaný nástroj. Pre tento účel bolo použitých niekoľko open-source projektov, ktoré poskytujú funkcionality potrebnú pre dosiahnutie bezproblémového chodu programu pri zachovaní všetkých požiadaviek na neho kladených.

Východiskom práce je projekt QoS@Lab BasicMeter. V rámci uvedeného projektu je vyvíjaný nástroj BEEM. Tento schopný exportovať merané dáta vo všeobecne rozšírenom NetFlow formáte a spolupracuje s ďalšími dvoma vrstvami meracej platformy, a to JXColl (ako zhromažďovač) a BMAalyzer (ako analyzátor a poskytovateľ grafického výstupu a rozhrania pre celú meraciu platformu). Táto práca sa venuje len najspodnejšej vrstve meracej architektúry, ktorá obsahuje časti určené na odchyťovanie, klasifikáciu a export informácií.

# Obsah

<b>Úvod</b>	<b>1</b>
<b>1 Formulácia úlohy</b>	<b>2</b>
<b>2 Terminológia</b>	<b>3</b>
2.1 Pozorovací bod . . . . .	3
2.2 Pozorovacia doména . . . . .	3
2.3 IP tok . . . . .	3
2.4 Kľúč toku . . . . .	4
2.5 Záznam toku . . . . .	4
2.6 Merací proces . . . . .	4
2.7 Exportovací proces . . . . .	5
2.8 Exportér . . . . .	5
2.9 IPFIX zariadenie . . . . .	5
2.10 Zhromažďovací proces . . . . .	5
2.11 Zhromažďovač . . . . .	5
2.12 Šablóna . . . . .	5
2.13 Kontrolné informácie, dáta . . . . .	6
2.13.1 Kontrolné informácie . . . . .	6
2.13.2 Dáta . . . . .	6
2.14 IPFIX správa . . . . .	6
2.15 Hlavička správy . . . . .	6
2.16 Šablónový záznam . . . . .	6
2.17 Dátový záznam . . . . .	7
2.18 Šablónový záznam s nastaveniami . . . . .	7
2.19 Sada . . . . .	7
2.20 Šablónová sada . . . . .	7
2.21 Šablónová sada s nastaveniami . . . . .	7

2.22	Dátová sada . . . . .	8
2.23	Informačný element . . . . .	8
2.24	Obsah paketu . . . . .	8
2.25	Proces výberu (selekcie) . . . . .	8
2.26	Stav výberu (selekcie) . . . . .	8
2.27	Selektor . . . . .	9
2.28	Zložený selektor . . . . .	9
2.29	Primitívny selektor . . . . .	9
<b>3</b>	<b>Analýza IPFIX protokolu</b>	<b>10</b>
3.1	Bloková schéma architektúry IPFIX . . . . .	10
3.2	Merací proces . . . . .	11
3.3	Exportovací proces . . . . .	14
3.4	Zhromažďovací proces . . . . .	15
3.5	IPFIX zariadenie . . . . .	15
3.6	Informačný model . . . . .	17
3.7	IPFIX správy . . . . .	19
3.7.1	Formát špecifikátorov poľa . . . . .	21
3.7.2	Sady . . . . .	22
3.7.3	Záznamy . . . . .	24
3.7.4	Kontrolné informácie . . . . .	27
3.8	Prenos správ protokolom UDP . . . . .	30
3.8.1	Správa šablón pri použití UDP protokolu . . . . .	31
3.8.2	Zhromažďovací proces pri použití UDP protokolu . . . . .	31
3.8.3	Zlyhanie spojenia . . . . .	32
<b>4</b>	<b>Analýza PSAMP protokolu</b>	<b>33</b>
4.1	Vzorkovanie . . . . .	34
4.1.1	Systematické vzorkovanie . . . . .	35
4.1.2	Náhodné vzorkovanie . . . . .	36

4.2	Filtrovane . . . . .	37
4.2.1	Filtrovane podľa masky . . . . .	38
4.2.2	Filtrovane podľa hash funkcie . . . . .	38
4.2.3	Filtrovane podľa stavu smerovača . . . . .	39
<b>5</b>	<b>Analýza súčasného stavu nástroja Basicmeter</b>	<b>40</b>
5.1	Architektúra nástroja BasicMeter . . . . .	40
5.2	Zhodnotenie konformity častí architektúry BasicMeter so štandardami IPFIX a PSAMP . . . . .	44
5.2.1	Merací proces . . . . .	44
5.2.2	Exportovací proces . . . . .	47
5.2.3	Zhromažďovací proces . . . . .	48
<b>6</b>	<b>Zhodnotenie implementácie analyzovaných požiadaviek</b>	<b>49</b>
	<b>Zoznam použitej literatúry</b>	<b>51</b>
	<b>Zoznam príloh</b>	<b>54</b>
	<b>Zoznam obrázkov</b>	<b>55</b>
	<b>Zoznam tabuliek</b>	<b>55</b>

## Úvod

Celosvetová expanzia počítačových sietí a technológií postavených na počítačových sieťach je vo veľkom ovplyvňovaná dôrazom kladeným na jednoduchú správu a monitoring aj tých najväčších systémov. S nárastom prenášaných dát však úmerne rastie aj zložitosť takýchto operácií. Keďže znalosti o tom, čo tvorí sieťovú prevádzku v jednotlivých bodoch siete sú jednou zo základných podmienok spoľahlivo fungujúcej správy počítačových sietí, je potrebné tieto informácie vhodne získať, spracovať, zobrazit' a prípadne aj archivovať. Prvými dvoma aspektami týchto informácií, t.j. získavaním a spracovávaním, sa zaoberajú aj systémy pre export informácií. V tejto práci je detailne analyzovaný pripravovaný protokol IPFIX, ktorý má všetky predpoklady stať sa štandardom pre export informácií zo sieťových zariadení a nahradiť tak doteraz používaný proprietárny protokol firmy Cisco, NetFlow v9. IPFIX protokol, ako taký, je v štádiu vývoja a schvaľovania jednotlivých častí skupinou IETF (Internet Engineering Task Force) a jeho nasadenie sa predpokladá v najbližších mesiacoch. Podobne ako protokol IPFIX, aj protokol PSAMP je vo fáze draftu a čaká na finalizáciu a schválenie ako štandardu pre aplikáciu filtračných a/alebo vzorkovacích techník na množinu paketov a ich následný export. Pre potrebu tejto diplomovej práce bola využitá len časť tohoto štandardu. Konkrétne sa jedná o špecifikáciu vzorkovacích a filtrovacích techník, implementovateľných na vysokorýchlostných sieťach za účelom zníženia zaťaženia meracieho bodu.

V súčasnej dobe existuje niekoľko riešení pre export informácií v rôznych formátoch [15], napriek tomu len málo využíva aj aktuálnu definíciu protokolu IPFIX na export informácií (YAF [16], nProbe [10]). Z tohoto dôvodu a pre potrebu merania tokov v sieťach Laboratória počítačových sietí vznikla potreba vývoja IPFIX kompatibilného meracieho nástroja na monitorovanie parametrov počítačových sietí, špeciálne QoS parametrov. Praktickým cieľom tejto diplomovej práce je implementácia tohoto štandardu v novej verzii exportovacej časti meracieho nástroja BasicMeter.

## 1 Formulácia úlohy

Úlohou diplomovej práce bolo zhodnotiť konformitu, analyzovať nezrovnalosti a implementovať riešenie exportovacej časti, ktoré bude maximálne konformné so štandardom pre export meraných dát IPFIX a štandardom pre vzorkovanie a filtrovanie paketov PSAMP.

Na dosiahnutie tohoto cieľa je potrebné:

- Analyzovať vlastnosti štandardu IPFIX
- Analyzovať vlastnosti štandardu PSAMP
- Vyhodnotiť nezrovnalosti medzi analyzovanými štandardmi a exportovacou časťou BasicMeter-a
- Navrhnuť riešenia problémov vyplývajúcich zo zmeny exportného protokolu na IPFIX.
- Navrhnuť riešenia problémov súvisiacich s použitím exportovacej časti v nástroji vyhodnocujúcom QoS parametre počítačových sietí.
- Implementovať riešenia podporujúce konformitu exportovacej časti s protokolom IPFIX.
- Dokumentovať exportovací a merací proces podľa katedrových štandardov.

Podmienkou efektívneho využitia meracej a exportovacej časti meracieho nástroja BasicMeter konformnej so štandardom IPFIX je použitie kolektora, ktorý je schopný tieto informácie vhodne spracovať a následne uložiť, alebo odoslať na ďalšie spracovanie. V súčasnosti túto funkciu plní program JXColl, ktorý bol vyvíjaný ako súčasť meracej architektúry BasicMeter-a.

## 2 Terminológia

### 2.1 Pozorovací bod

Pozorovací bod je miesto v sieti kde sú pozorované IP pakety. Ako príklad môžeme uviesť linku, ku ktorej je pripojený merač. Alebo v prípade zdieľaného média, ako napr. Ethernet LAN, jeden port na smerovači, alebo množina rozhraní (fyzických, alebo logických) smerovača. Treba brať do úvahy, že každý pozorovací bod je asociovaný s pozorovacou doménou (definovanou nižšie), a že jeden pozorovací bod môže reprezentovať množinu ďalších individuálnych pozorovacích bodov.

### 2.2 Pozorovacia doména

Pozorovacia doména je najväčšia množina pozorovacích bodov z ktorých môže merací proces agregovať informácie o tokoch. Každá pozorovacia doména je kolektoru reprezentovaná unikátnym ID kvôli identifikácii IPFIX správ, ktoré generuje. Pozorovaciú doménu môžu napríklad tvoriť všetky sieťové adaptéry v počítači, keďže merací proces je schopný získať informácie o tokoch z každej z nich naraz.

### 2.3 IP tok

Tok je definovaný ako „množina IP paketov prechádzajúcich pozorovacím bodom v počítačovej sieti počas určitého časového intervalu. Všetky pakety prislúchajúce k určitému toku majú množinu spoločných vlastností. Vlastnosti sú definované nasledovne:

1. Jeden alebo viac polí hlavičky paketu (napr. cieľová IP adresa), transportnej hlavičky (napr. číslo cieľového portu), alebo aplikačnej hlavičky (napr. polia RTP hlavičky [14] )
2. Jedna alebo viac charakteristík samotného paketu. (napr. počet MPLS značiek)
3. Jeden alebo viac charakteristík derivovaných zo spracovania paketu (napr. adresa nasledujúceho smerovača, výstupné rozhranie)

Paket prislúcha k toku, ak kompletne spĺňa všetky tokom definované požiadavky.

## 2.4 Kľúč toku

Ktorékoľvek pole, ktoré:

1. Patrí do hlavičky paketu (napr. cieľová IP adresa)
2. Je vlastnosťou samotného paketu (napr. dĺžka paketu)
3. Je derivované zo spracovania paketu (napr. číslo autonómneho systému)

a ktoré sú použité na definovanie toku, sa nazývajú Kľúče toku.

## 2.5 Záznam toku

Záznam toku obsahuje informácie o špecifickom toku, ktorý bol pozorovaný v pozorovacom bode. Záznam obsahuje merané vlastnosti (napr. celkový počet bajtov pre všetky pakety toku) a charakteristické vlastnosti (napr. zdrojová IP adresa).

## 2.6 Merací proces

Merací proces generuje záznamy tokov. Vstupom do procesu sú hlavičky paketov, ich pozorované charakteristiky ako aj spracovanie paketu v pozorovacom bode (napr. zvolené výstupné rozhranie). Všetky merania musia byť prevádzané z pohľadu pozorovacieho bodu.

Merací proces pozostáva z množiny funkcií, ktorá zahŕňa odchytyvanie hlavičiek paketov, časové značkovanie, vzorkovanie, filtrovanie, klasifikáciu a správu záznamov tokov.

Správa záznamov tokov môže zahŕňať vytváranie nových záznamov, aktualizovanie existujúcich, výpočty štatistík, odvodzovanie ďalších vlastností, detekovanie expirácie, odovzdávanie záznamov exportovaciemu procesu a odstraňovanie záznamov.

## 2.7 Exportovací proces

Exportovací proces posiela záznamy o tokoch jednému, alebo viacerým zhromažďovacím procesom. Záznamy sú generované jedným, alebo viacerými meracími procesmi.

## 2.8 Exportér

Zariadenie, ktoré obsahuje jeden, alebo viac exportovacích procesov sa nazýva exportér.

## 2.9 IPFIX zariadenie

Zariadenie, ktoré obsahuje najmenej jeden pozorovací bod, merací proces a exportovací proces, sa nazýva IPFIX zariadenie.

## 2.10 Zhromažďovací proces

Zhromažďovací proces prijíma záznamy tokov z jedného alebo viacerých exportovacích procesov. Tento proces môže ďalej spracovávať, alebo uskladňovať obdržané záznamy, ale tieto činnosti sú mimo záber tejto práce.

## 2.11 Zhromažďovač

Zariadenie, ktoré obsahuje, najmenej jeden zhromažďovací proces sa nazýva zhromažďovač.

## 2.12 Šablóna

Šablóna je usporiadaná sekvencia ;typ, dĺžka; párov, používaná na komplexnú špecifikáciu a sémantiku určitej množiny informácií, ktorá má byť prenesená z IPFIX zariadenia do zhromažďovača. Každá šablóna je unikátne identifikovaná svojím ID.

## **2.13 Kontrolné informácie, dáta**

Informácie exportované z IPFIX zariadenia sa dajú klasifikovať do nasledujúcich kategórií:

### **2.13.1 Kontrolné informácie**

Tieto zahŕňajú definíciu toku, výberové kritériá pre pakety obsiahnuté v tomto toku a šablóny popisujúce exportované dáta. Kontrolné informácie obsahujú všetky dáta pre inicializáciu IPFIX protokolu a špecificky pre zhromažďovač aj interpretáciu dát odoslaných exportérom.

### **2.13.2 Dáta**

Dáta zahŕňajú záznamy tokov, obsahujúce hodnoty polí pre rôzne pozorované toky na každom pozorovacom bode.

## **2.14 IPFIX správa**

IPFIX správa sú dáta, ktorých zdrojom je exportovací proces, ktoré prenášajú IPFIX záznamy tohoto exportovacieho procesu, a ktorých cieľ je zhromažďovací proces. IPFIX správa je zapuzdrená na transportnej vrstve.

## **2.15 Hlavička správy**

Hlavička správy je prvou časťou IPFIX správy, ktorá poskytuje základné informácie o správe, ako napr. verzia IPFIX protokolu, dĺžka správy, sekvenčné číslo, atď.

## **2.16 Šablónový záznam**

Šablónový záznam definuje štruktúry a interpretáciu polí v dátovom zázname.

## 2.17 Dátový záznam

Dátový záznam je záznam, ktorý obsahuje hodnoty parametrov korešpondujúce so Šablónovým záznamom.

## 2.18 Šablónový záznam s nastaveniami

Tento záznam definuje štruktúru a interpretáciu polí v dátovom zázname, ale na rozdiel od obyčajného šablónového záznamu obsahuje definície rozsahu a aplikovateľnosti dátového záznamu.

## 2.19 Sada

Sada je všeobecný termín pre kolekciu záznamov, ktoré majú podobnú štruktúru. V IPFIX správe nasleduje po hlavičke jedna alebo viac sád. Existujú tri rozdielne typy sád:

- Šablónová sada
- Šablónová sada s nastaveniami
- Dátová sada

## 2.20 Šablónová sada

Šablónová sada je kolekcia jedného, alebo viacerých šablónových záznamov, ktoré sú zjednotené v IPFIX správe.

## 2.21 Šablónová sada s nastaveniami

Šablónová sada s nastaveniami je kolekcia jednej, alebo viacerých týchto sád, ktoré sú zjednotené v IPFIX správe.

## 2.22 Dátová sada

Dátová sada je jeden alebo viac dátových záznamov rovnakého typu, ktoré sú zjednotené v IPFIX správe. Každý dátový záznam je predtým definovaný šablónovým záznamom alebo šablónovým záznamom s nastaveniami.

## 2.23 Informačný element

Informačný element je opis atribútu, ktorý je nezávislý od protokolu a kódovania. Informačný model IPFIX [9] opisuje základnú množinu informačných elementov pre IPFIX. Typ asociovaný s informačným elementom indikuje obmedzenia, čo môže daný typ obsahovať a takisto určuje správny typ kódovania pre použitie v IPFIX.

## 2.24 Obsah paketu

Termín obsah paketu označuje spojenie hlavičky paketu (čo zahŕňa všetky zapuzdrovacie hlavičky) a tela paketu.

## 2.25 Proces výberu (selekcie)

Proces výberu paketu je postupnosť krokov, kde vstupom je množina pozorovaných paketov a výstupom je jej podmnožina.

## 2.26 Stav výberu (selekcie)

Proces výberu môže udržiavať stavové informácie pre použitie pri výbere paketov. Príklady týchto informácií sú:

- Sekvenčné čísla paketov na vstupe do procesu výberu.
- Časová známka pozorovania paketu v pozorovacom bode
- Iterátory pre pseudonáhodné číselné generátory

- Hash hodnoty vypočítané počas výberu
- Indikátory, či paket bol konkrétnym procesom vybraný

Proces výberu môže tieto dáta meniť ako výsledok spracovania paketu. Stav výberu paketu po spracovaní paketu reflektuje jeho stav.

## **2.27 Selektor**

Selektor definuje akcie výberového procesu na jednom pakete na vstupe. Ak je výsledok selektora pozitívny, potom sa paket stáva súčasťou výstupnej množiny paketov.

Selektor môže pri rozhodovaní o výbere paketu použiť nasledujúce informácie:

- Obsah paketu
- Informácie odvodené zo spracovania paketu v pozorovacom bode
- Akúkoľvek informáciu zo stavu výberu

## **2.28 Zložený selektor**

Zložený selektor je usporiadaná kompozícia selektorov, v ktorých výstupná podmnožina paketov jedného selektora tvorí vstupnú množinu paketov nasledujúceho.

## **2.29 Primitívny selektor**

Selektor je primitívny, ak nie je zložený.

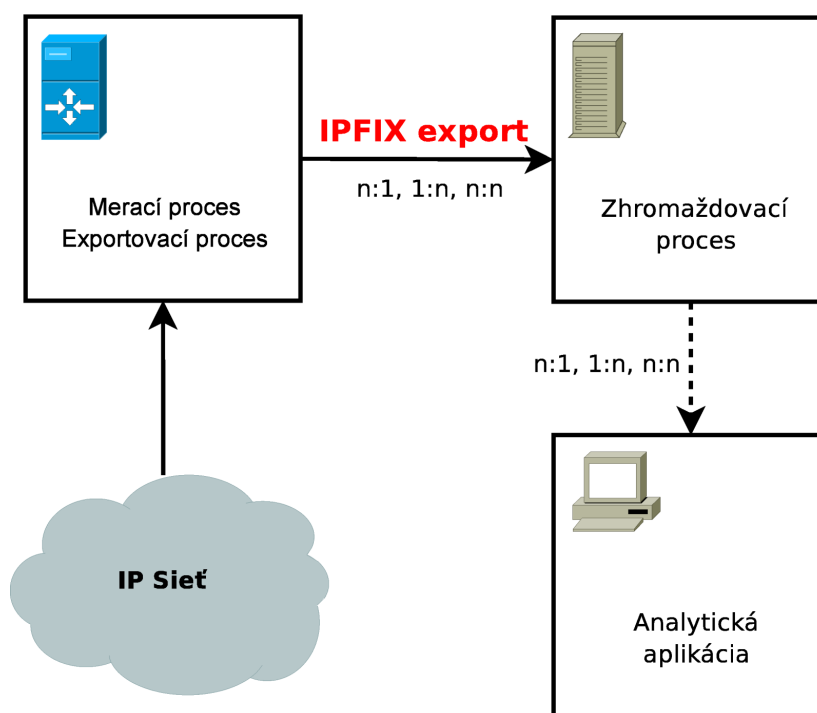
### 3 Analýza IPFIX protokolu

Exportný protokol IPFIX vyvíjaný pracovnou skupinou IETF za účelom exportu informácií o tokoch prechádzajúcich smerovačmi, ktoré sú nezávislé od platformy a výrobcu. Ako nástupca protokolu NetFlow v9 [2], ktorý sa používa v majoritnej časti sieťových zariadení od spoločnosti Cisco Systems. Oproti protokolu NetFlow prináša protokol IPFIX niekoľko vylepšení, ktoré súvisia hlavne so správou šablón a spoľahlivosťou doručovania IPFIX správ zhromažďovaču. Konceptia šablón, ktorá uľahčuje popis a interpretáciu prenášaných štruktúr a umožňuje flexibilné pridávanie a spracovávanie nových položiek do exportovaných dát má aj agregáčny charakter, ktorý spolu s implementáciou vzorkovacích a filtrovacích techník z protokolu PSAMP [18] tvorí robustný protokol, vhodný pre nasadenie vo vysokorýchlostných sieťach. Informácie derivované z týchto exportovaných dát na strane zhromažďovača, resp. analyzujúcej aplikácie môžu byť použité na účely účtovania, plánovania prenosových kapacít, bezpečnostnú analýzu, detekciu krízových stavov v sieti a v neposlednom rade aj vyhodnocovanie QoS parametrov počítačovej siete.

#### 3.1 Bloková schéma architektúry IPFIX

Na obrázku 3 – 1 vidíme blokovú schému IPFIX protokolu, ktorá pokrýva jednotlivé možnosti, ako môže IPFIX systém fungovať. Rozhranie definované plnou šípkou je časťou IPFIX architektúry. Rozhrania definované bodkovanou šípkou nie sú súčasťou architektúry. Všetky funkčné bloky môžu mať medzi sebou násobnú väzbu, teda jeden exportovací proces môže predávať IPFIX správy jednému, alebo viacerým zhromažďovacím procesom a naopak, viac zhromažďovacích procesov môže preberať informácie od jedného, alebo viacerých exportovacích procesov.

Obrázok 3 – 2 znázorňuje typické IPFIX zariadenie, kde IPFIX komponenty sú znázornené jednotlivými obdĺžnikmi. Z diagramu je viditeľný aj smer prenosu získaných dát o sieti v smere od meracieho procesu, cez exportér až po odoslanie dát na spracovanie do zhromažďovača. Je potrebné si všimnúť, že jeden exportovací proces môže spracovávať dáta z viacerých meracích procesov. Ako príklad sa dá uviesť smerovač s niekoľkými



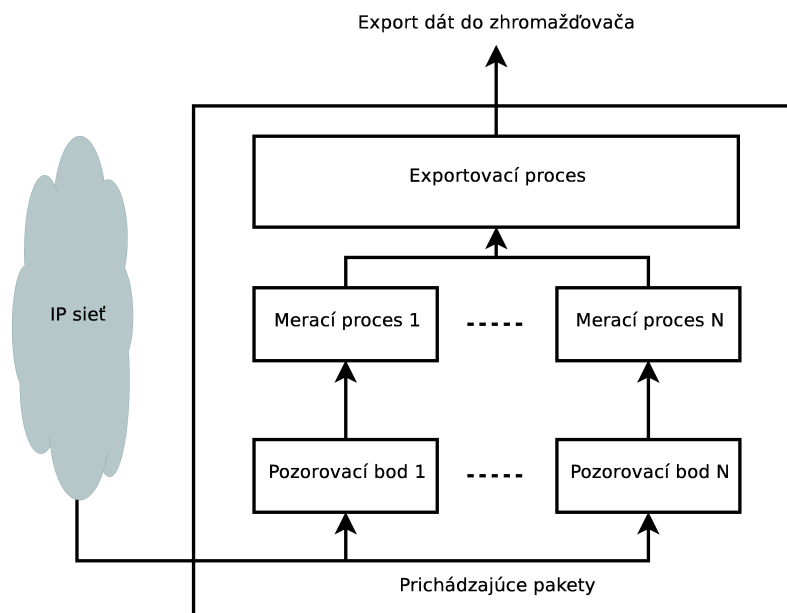
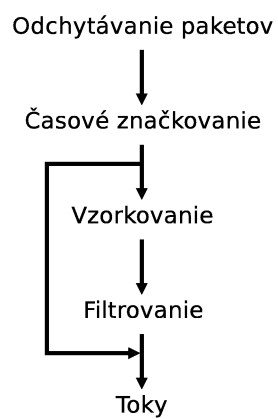
Obrázok 3–1 Referenčný model IPFIX

sietovými rozhraniami, kde merací proces funguje na každom z nich.

### 3.2 Merací proces

Každý pozorovací bod v IPFIX zariadení musí byť asociovaný najmenej s jedným meracím procesom. Každý paket prichádzajúci do pozorovacieho bodu je prenesený do všetkých meracích procesov asociovaných s týmto bodom. Vo všeobecnosti každý merací proces skúma paket prechádzajúci pozorovacím bodom, vykonáva časové značkovanie a klasifikuje paket do toku v závislosti na výberových kritériách.

Merací proces môže definovať pravidlá tak, aby iba určité pakety prichádzajúce do pozorovacieho bodu boli zvolené pre meranie. To môže byť dosiahnuté jednou z dvoch metód, ktoré sú definované v ďalších podkapitolách, alebo ich kombináciou v ľubovoľnom poradí. Obrázok 3–3 zobrazuje operácie, ktoré môžu byť aplikované ako súčasť typického meracieho procesu.

**Obrázok 3–2** IPFIX zariadenie**Obrázok 3–3** Vzorkovanie a filtrovanie

**Vzorkovacia funkcia** určuje, ktoré pakety z prichádzajúcich sú vybrané pre meranie, t.j. pakety spĺňajúce vzorkovacie kritériá pre tento merací proces. Výber všetkých prichádzajúcich paketov je špeciálnou formou vzorkovania s pomerom 1:1.

*Príklad: vzorkuj každý stý paket, ktorý bol pozorovaný v pozorovacom bode.*

**Filtrovacia funkcia** vyberá iba také prichádzajúce pakety, ktoré spĺňajú požiadavky na polia definované v hlavičke paketu, polia získané pri spracovaní paketu, alebo vlastnosti paketu samotného.

*Príklad: Mask/match filter definovaný ako (Protokol = TCP, Cieľový port medzi 80 a 120).*

Merací proces je aj funkčný blok, ktorý spravuje všetky toky generované pozorovacou doménou. Typická funkcia meracieho procesu zahŕňa:

- Udržiavanie databázy tokov z pozorovacieho bodu.
- Udržiavanie štatistických informácií o meracom procese samotnom, ako napr.: množstvo generovaných záznamov tokov, , pozorovaných paketov, atď.

Databáza tokov obsahuje všetky toky pozorované na meracích bodoch v rámci jednej pozorovacej domény. Nachádzajú sa v nej práve prebiehajúce toky, čakajúce toky (kým im nevyprší niektorý z časovačov), ako aj expirované toky určené na export. Tok je považovaný za expirovaný za nasledujúcich podmienok:

1. Ak po určitú časový interval nebol pozorovaný žiaden paket prislúchajúci k tomuto toku. Tento časový interval by mal byť v meracom procese konfigurovateľný s minimálnou hodnotou 0 pre okamžitú expiráciu. Táto hodnota zabezpečí aby sa generovali toky o veľkosti jedného paketu.
2. Ak merací proces zistí nedostatok systémových prostriedkov, tok môže byť ukončený predčasne, aby sa tieto prostriedky uvoľnili pre uloženie nových tokov.
3. V prípade dlhotrvajúcich tokov by mal merací proces expirovať tieto toky v pravidelných intervaloch. Tento interval by mal tiež byť konfigurovateľný v meracom

proces. Pokiaľ je dlhotrvajúci tok expirovaný, merací proces si môže ponechať tento záznam pre zachytenie ďalších paketov náležiacich do tohoto toku, bez nutnosti vytváranie nového záznamu.

Pozorovacia doména je logický blok ktorý prezentuje navonok jedinečnú identitu pre skupinu pozorovacích bodov v IPFIX zariadení. Jedno IPFIX zariadenie môže mať viacero pozorovacích domén, z ktorých každá obsahuje podmnožinu celkového počtu pozorovacích bodov. Každá pozorovacia doména musí byť označená unikátnym identifikátorom v kontexte IPFIX zariadenia. V prípade výskytu viacerých pozorovacích domén v rámci jedného IPFIX zariadenia musí byť tento identifikátor prenesený ako parameter do exportovacej funkcie. Tento identifikátor je označovaný ako 'IPFIX Source ID'.

### 3.3 Exportovací proces

Exportovací proces je funkčný blok ktorý odosiela dáta do jedného, alebo viacerých IPFIX zhromažďovačov použitím IPFIX protokolu. Na jednej strane tento exportovací proces spolupracuje s meracím procesom (procesmi), aby získal záznamy tokov, pokiaľ na druhej strane odovzdáva dáta zhromažďovaciemu procesu v zhromažďovači.

Rozhodnutie o tom kedy, a ktorý tok exportovať je v kompetencii exportovacieho procesu. Tok môže byť exportovaný pretože z vyššie uvedených dôvodov expiroval. Pre dlhotrvajúce toky by mal byť export spúšťaný periodicky s konfigurovateľnou periódou.

V pozorovacej doméne môžu byť definované doplnujúce pravidlá tak, že exportované sú len niektoré záznamy tokov. To je docielené použitím jednej výberovej funkcie, alebo ich kombináciou.

Záznam toku môže byť efektívnejšie analyzovaný, pokiaľ je známy jeho pôvod. Teda, v ktorom pozorovacom bode bol tento tok zaznamenaný. Preto je odporúčané, aby IPFIX zariadenia posielali túto informáciu zhromažďovaču. V prípade, že táto informácia nie je relevantná, alebo pri použití len jedného pozorovacieho bodu je prenos tejto informácie na zhromažďovač nepovinný.

### 3.4 Zhromažďovací proces

Zhromažďovací proces používa identifikátor šablóny v zázname toku na interpretáciu informačných elementov v tomto zázname. Preto musí IPFIX zhromažďovač rozoznať identifikátor šablóny pre každý prichádzajúci záznam toku. V zhromažďovacom procese musia byť implementované nasledujúce funkcie:

- Identifikácia, prijatie a dekódovanie IPFIX správ z rôznych dvojíc (exportovacích procesov, pozorovacích domén).
- Uloženie kontrolných informácií a záznamov tokov prijatých z IPFIX zariadenia.

V širšej abstrakcii teda zhromažďovací proces:

1. Prijíma a udržiava kontrolné informácie.
2. Dekóduje a spracúva záznamy tokov pomocou kontrolných informácií.

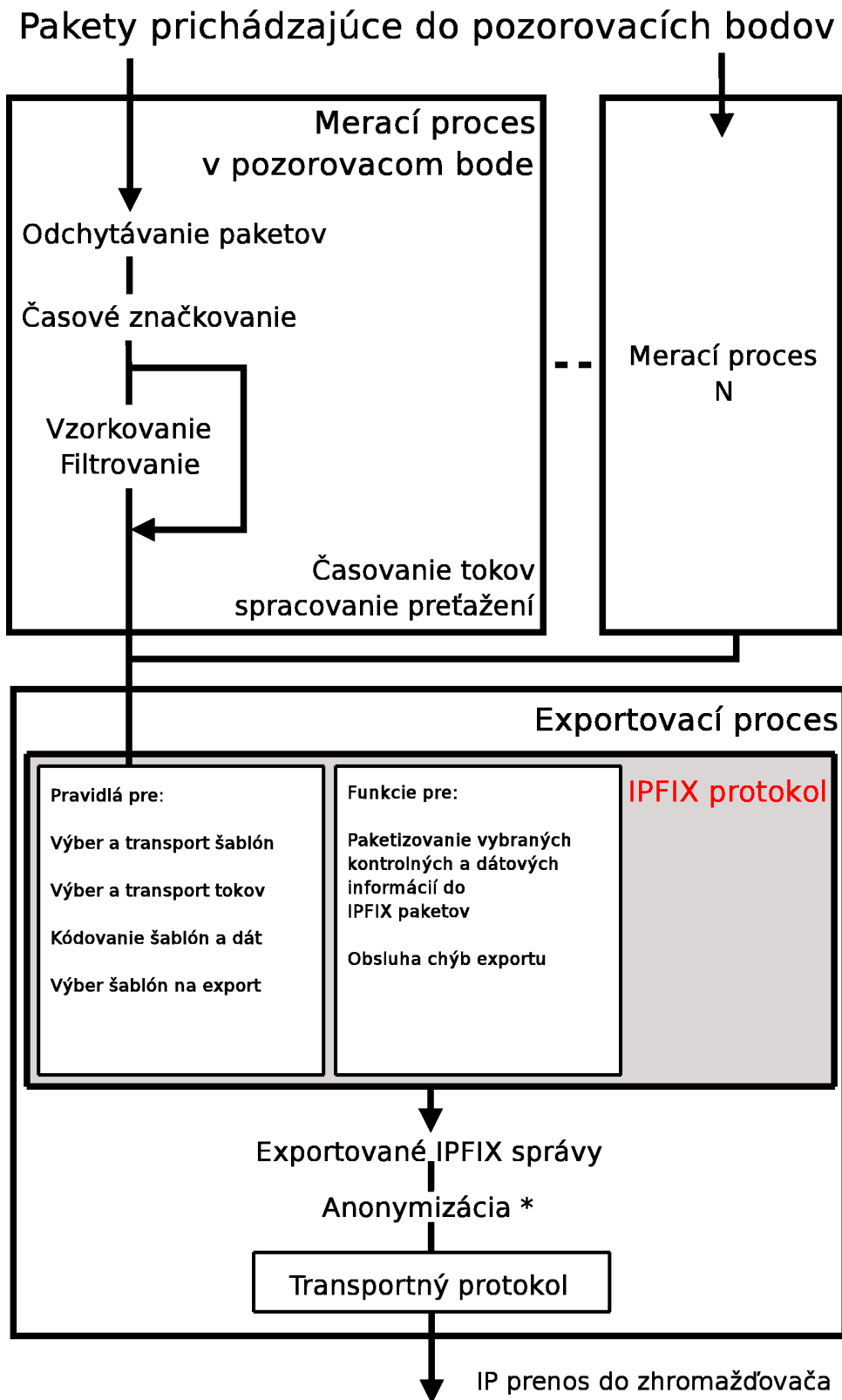
### 3.5 IPFIX zariadenie

Obrázok 3–4 znázorňuje detailný pohľad na funkčné a logické bloky IPFIX zariadenia spolu s ich funkciami.

IPFIX je tvorené množinou kooperujúcich procesov, ktoré implementujú funkčné bloky opísané v predchádzajúcej časti tejto práce. Alternatívne môže byť IPFIX zariadenie chápané ako sieťová entita, ktorá implementuje IPFIX protokol. Exportovací proces preberá záznamy tokov od meracieho procesu a posiela ich zhromažďovaču (zhromažďovačom).

IPFIX zariadenie vykonáva nasledujúce činnosti:

1. Kóduje kontrolné informácie do šablón.
2. Kóduje pozorované pakety do záznamov tokov.
3. Paketizuje zvolené šablóny a záznamy do IPFIX správ.
4. Odosiela IPFIX správy zhromažďovaču.



Obrázok 3-4 Detailný pohľad na architektúru IPFIX

IPFIX protokol komunikuje informácie z IPFIX exportéra do IPFIX zhromažďovača. Táto informácia neobsahuje len záznamy tokoch, ale aj informácie o meracom procese. Takáto informácia (označovaná ako kontrolná) obsahuje detaily dátových polí v záznamoch toku. Môže obsahovať aj štatistiku z meracieho procesu, ako napr. počet stratených paket. Detailný popis protokolu IPFIX poskytuje [3]

### 3.6 Informačný model

Informácie v správach IPFIX protokolu je modelovaná v zmysle informačných elementov IPFIX informačného modelu. Špecifikácia protokolu IPFIX definuje, ako sú prenášané informačné elementy. Špecifikuje pre nich kódovanie a základné dátové typy. Zoznam všetkých položiek definovaných pracovnou skupinou IPFIX, ktoré môžu byť protokolom prenášané je definovaný v dokumente IPFIX: Informačný model [9].

Informačný model protokolu poskytuje kompletný dátový opis vlastností každého informačného elementu. Tento opis podáva aj sémantiku elementu, t.j. ako je odvodený z toku, alebo inej informácie dostupnej v IPFIX zariadení. Všetky informačné elementy špecifikované pre IPFIX protokol v pôvodnej definícii pracovnej skupiny, alebo v budúcnosti musia mať definované nasledujúce vlastnosti.

- *name* - Unikátne a zmysluplné pomenovanie informačného elementu
- *description* - Sémantika informačného elementu. Opisuje, ako je tento informačný element získaný z toku, alebo iných informácií prístupných pozorovateľovi.
- *dataType* - Jeden z typov definovaných v [9], alebo v budúcich rozšíreniach. Typy pre atribúty sú obmedzené len implementáciou. Existujúce typy pokrývajú väčšinu základných typov používaných v moderných programovacích jazykoch, ako aj niekoľko odvodených, ktoré je vhodné v oblasti počítačových sietí rozoznávať (napr. IPv4 adresa)
- *status* - Status špecifikácie konkrétneho informačného elementu. Povolené hodnoty sú "aktuálny", "neschválený", "zrušený", resp. ich anglické verzie "current",

”deprecated”, alebo obsolete”.

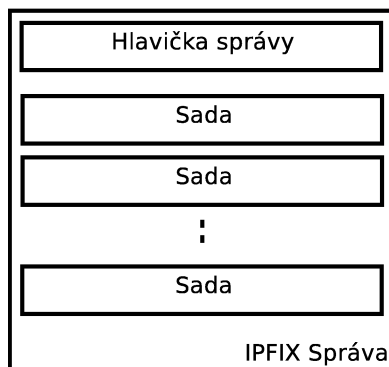
Informačné elementy, ktoré sú definované výrobcami IPFIX zariadení a nie sú schválené organizáciou IANA, sa nazývajú Enterprise informačné elementy. Pre tieto, keďže nie sú štandardizované, je povinná ešte jedna vlastnosť, a to:

- *enterpriseID* - Je identifikátor pridelený organizáciou IANA a používaný na označovanie osobitne definovaných informačných elementov, ktoré sa používajú len v rámci jedného podniku. Pokiaľ sú IPFIX správy, ktoré obsahujú takéto informačné elementy prenášané globálne, musia mať pripojený tento identifikátor kvôli zabezpečeniu unikátnosti identifikácie informačného elementu. Enterprise identifikátory vydané organizáciou IANA sú definované v [6].

IPFIX protokol definuje aj nepovinné vlastnosti pre informačné elementy, ktoré upresňujú, alebo inak objasňujú určenie, syntax a sémantiku informačného elementu. Tieto vlastnosti sú:

- *dataTypeSemantics* - Je doplňujúca informácia o sémantických detailoch. Platné hodnoty tohoto typu sú definované v [9]. alebo v budúcich rozšíreniach informačného modelu.
- *units* - Pokiaľ je informačný model v nejakom zmysle merateľný, táto položka určuje v akej jednotke je táto miera.
- *range* - Niektoré informačné elementy môžu byť kvalifikované len na obmedzenej množine hodnôt, ktorá môže byť vyjadrená ako interval. V tomto prípade je možné v tejto položke takýto interval špecifikovať.
- *reference* - Identifikuje doplňujúce špecifikácie, ktoré môžu rozširovať kontext použitia konkrétneho informačného elementu.

Štandardne majú informačné elementy platnosť špecifikovanú svojimi definíciami. IPFIX informačný model rozdeľuje túto platnosť na dva typy:



Obrázok 3–5 Formát IPFIX správy

- Informačné elementy s platnosťou vo špecifickom meracom procese, resp. špecifickom exportovacom procese.
- Informačné elementy s platnosťou v špecifickom toku.

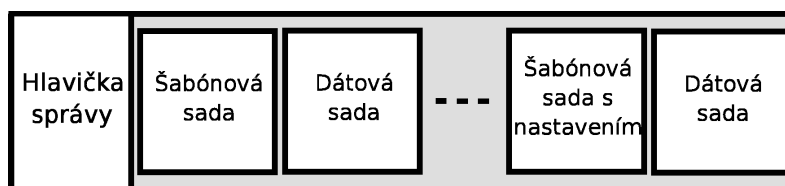
### 3.7 IPFIX správy

IPFIX správa pozostáva z hlavičky nasledovanej jednou, alebo viacerými sadami. Tieto sady, môžu byť dátové, šablónové, alebo šablónové s nastaveniami. Formát IPFIX správy je znázornený na obrázku 3–5.

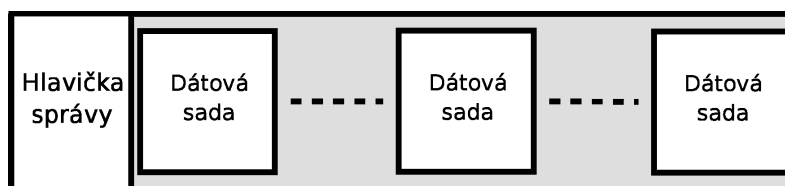
Je nutné aby exportér kódoval všetky celočíselné hodnoty hlavičky správy a všetky sady v "network byte order", ktoré je taktiež označované ako "Big-endian" kódovanie.

Nasledujúce diagramy objasňujú príklady IPFIX správ z pohľadu ich obsahu.

- IPFIX správa pozostávajúca zo striedajúcich sa šablónových sád 3–6, dátových sád a šablónových sád s nastaveniami. Novo vytvorená šablóna je exportovaná hneď ako je to možné. Preto, ak už existuje IPFIX správa s dátovou sadou, ktorá je pripravená na export, šablónová sada a šablónová sada s nastaveniami je priložená k týmto informáciám podľa toho, koľko miesta ešte v tejto správe zostáva.
- IPFIX správa pozostávajúca iba z dátových sád 3–7, po tom čo boli príslušné šablónové záznamy definované a prenesené do zhromažďovacieho procesu. Z takýchto správ pozostáva majoritná časť komunikácie v IPFIX protokole.



Obrázok 3–6 Príklad IPFIX správy 1



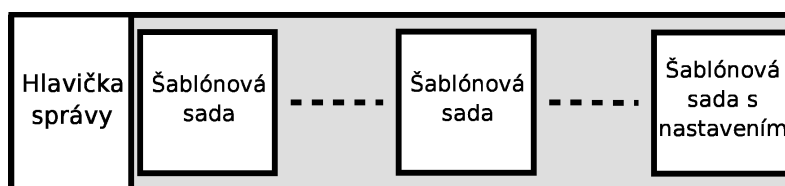
Obrázok 3–7 Príklad IPFIX správy 2

- IPFIX správa pozostávajúca výhradne z šablónových sád a šablónových sád s nastaveniami 3–8.

Formát hlavičky IPFIX správy je znázornený na obrázku 3–9

Opis jednotlivých častí znázornených na obrázku 3–9 je nasledovný:

- *verzia* - Verzia formátu záznamu toku exportovaného v tejto správe. Hodnota tohoto poľa je 0x000a pre aktuálnu verziu. Táto hodnota vznikla inkrementáciou hodnoty z protokolu NetFlow [2]
- *dĺžka správy* - Celková dĺžka IPFIX správy udávaná v oktetoch vrátane hlavičky správy a sád.
- *čas exportu* - Čas v sekundách od začiatku unix epochy (00:00 UTC 1. Január 1970), kedy IPFIX správa opustila exportér.



Obrázok 3–8 Príklad IPFIX správy 3

0				1				2				3											
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3
Verzia IPFIX								Dĺžka správy															
Čas exportu																							
Sekvenčné číslo																							
ID pozorovacej domény																							

Obrázok 3–9 Formát hlavičky IPFIX správy

- *sekvenčné číslo* - Inkrementálne sekvenčné počítadlo s rozsahom  $2^{32}$  všetkých IPFIX dátových záznamov odoslaných z tejto pozorovacej domény exportovacím procesom v jednom behu. Táto hodnota by mala byť použitá pri identifikovaní výpadkov dátových záznamov. Ostatné záznamy toto počítadlo neinkrementujú.
- *ID pozorovacej domény* - 32-bitový identifikátor pozorovacej domény, ktorý je lokálne unikátny v exportovacom procese. Exportovací proces používa tento identifikátor na označenie pozorovacej domény, ktorá dáta odovzdávané v tejto správe namerala Zhromažďovací proces by mal použiť kombináciu exportéra (jeho IP adresa, alebo iný identifikátor) a identifikátora pozorovacej domény na oddelenie rôznych exportných tokov vychádzajúcich z rovnakého exportovacieho procesu. Identifikátor pozorovacej domény by mal byť nastavený na nulu, pokiaľ je táto informácia irelevantná.

### 3.7.1 Formát špecifikátorov poľa

Informačné elementy sú jednoznačne identifikované svojimi identifikátormi. Výrobcovia IPFIX zariadení musia mať možnosť definovať proprietárne informačné elementy. Špecifikátory poľa preto obsahujú enterprise bit. 3 – 10

Obrázok 3–10 znázorňuje formát špecifikátorov poľa a postavenie enterprise bitu. Jednotlivé položky majú nasledujúci význam:

- *E* - Enterprise bit. Je to prvý bit poľa špecifikujúceho informačný element. Keď je

0	1	2	3																												
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
E	ID informačného elementu										Dĺžka poľa																				
Enterprise číslo																															

**Obrázok 3–10** Formát špecifikátora poľa

tento bit nastavený na nulu, korešpondujúci informačný element predstavuje element špecifikovaný IETF a enterprise číslo nesmie byť prítomne. Pokiaľ je „enterprise“ bit nastavený na jednotku, korešpondujúca informácia v dátovom zázname predstavuje dáta definované podnikom ktorému patrí spomínané enterprise číslo, ktoré v tomto prípade musí byť prítomné.

- *ID informačného elementu* - Numerická hodnota reprezentujúca typ informačného elementu. Tieto typy sú detailnejšie opísané v [9]
- *Dĺžka poľa* - Dĺžka korešpondujúceho kódovaného špecifikátora poľa v oktetoch [9]. Hodnota 65535 je rezervovaná pre informačné elementy s premenlivou dĺžkou.
- *Enterprise číslo* - IANA enterprise číslo [6] autority definujúcej informačný element v tomto šablónovom zázname.

### 3.7.2 Sady

Sada je všeobecný názov kolekcie záznamov ktoré majú podobnú štruktúru. Existujú tri rozličné druhy sád: šablónové sady, šablónové sady s nastavením a dátové sady. Každá z týchto sád pozostáva zo svojej hlavičky a jedného alebo viacerých záznamov. Formát sady a jej hlavička sú opísané nižšie.

Formát sady je zobrazený na obrázku 3–11. Záznamy v ňom obsiahnuté môžu byť buď šablónové, šablónové s nastavením, alebo dátové. Tieto typy sa v rámci jednej sady nesmú miešať.

Definície polí v sade sú nasledovné:

Hlavička sady
Záznam
Záznam
⋮
Záznam
Doplnenie

Obrázok 3–11 Formát sady

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			
ID sady		Dĺžka sady	

Obrázok 3–12 Hlavička sady

- *hlavička sady* - Hlavička sady 3–12
- *záznam* - Jeden alebo viac záznamov: šablónových, šablónových s nastavením, alebo dátových.
- *doplnenie* - Exportovací proces môže na koniec sady umiestniť doplňujúce oktety, aby sa nasledujúce sady začínali rovnomerne. Pre bezpečnostné dôvody musia byť tieto doplňujúce oktety zložené z nulových (0) hodnôt. Dopĺňovaná dĺžka musí byť menšia ako ktorýkoľvek povolený záznam v tejto sade.

Každá sada obsahuje vlastnú hlavičku, ktorá obsahuje nasledujúce časti:

- *ID sady* - ID hodnota identifikuje sadu. Hodnota 2 je rezervovaná pre šablónovú sadu. Hodnota 3 je rezervovaná pre šablónovú sadu s nastavením. Všetky ostatné hodnoty od 4 po 25 sú rezervované pre budúce použitie. Hodnoty nad 255 sú použité pre dátové sady. ID hodnoty 0 a 1 nie sú použité z historických dôvodov.
- *Dĺžka sady* - Celková dĺžka sady v oktetoch zahrňujúca hlavičku, záznamy a voliteľné doplnenie. Pretože niektoré sady môžu obsahovať viaceré záznamy, musí byť pre zistenie začiatku ďalšej sady použitá táto hodnota.

### 3.7.3 Záznamy

IPFIX definuje tri formáty záznamov:

- šablónový záznam
- šablónový záznam s nastavením
- dátový záznam

Jedným zo základných elementov v záznamových formátoch IPFIX je šablónový záznam. Šablóny zlepšujú flexibilitu záznamového formátu, pretože dovoľujú zhromažďovaciemu procesu spracovať IPFIX záznamy bez toho, aby vedel interpretáciu všetkých dátových záznamov. Šablónový záznam môže obsahovať akúkoľvek kombináciu identifikátorov informačných elementov pridelenú organizáciou IANA.

Formát šablónového záznamu je zobrazený na obrázku 3–13. Pozostáva z hlavičky 3–14 a jedného alebo viacerých špecifikátorov polí 3–10. Hlavička obsahuje nasledujúce polia:

- *ID šablóny* - Každému z novovytvorených šablónových záznamov je pridelené unikátne ID číslo. Unikátnosť je v rámci pozorovacej domény ktorá túto šablónu vytvorila. Identifikátory 0-255 sú vyhradené pre šablónové sady, šablónové sady s nastavením a iné rezervované sady, ktoré môžu byť v budúcnosti doplnené. Identifikátory šablón dátových sád sú číslované od 256 po 65535. Nie sú žiadne obmedzenia, ktoré by sa týkali poradia rezervácie identifikátorov šablón.
- *počet polí* - Počet polí v tomto šablónovom zázname

Obrázok 3–15 ukazuje príklad možnej prenášanej šablónovej sady so zmiešanými štandardnými a podnikovo špecifickými informačnými elementami. Pozostáva z hlavičky a špecifikátorov poľa.

Identifikátory informačných elementov 1.2 a 2.1 sú definované v IETF, keďže ich enterprise bit je nastavený na 0 a teda nepotrebujú enterprise číslo na svoju identifikáciu. S

Hlavička šablónového záznamu
Špecifikátor poľa
Špecifikátor poľa
⋮
Špecifikátor poľa

Obrázok 3–13 Formát šablónového záznamu

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			
ID šablóny (ID > 255)		Počet polí	

Obrázok 3–14 Hlavička šablónového záznamu

Vďaka použitiu poľa pôsobnosti, šablónový záznam s nastavením dáva exportéru možnosti na poskytovanie dodatočných informácií, ktoré by nebolo možné poskytovať len pomocou samotných tokov.

Pole pôsobnosti, ktoré je prístupné iba v sade šablón s nastavením, označuje kontext oznamovaných informačných elementov v dátových záznamoch. IPFIX hlavička už obsahuje jedno implicitné pole pôsobnosti, ktorým je identifikátor pozorovacej domény, ale len pokiaľ je tento identifikátor nenulový.

V šablónovom zázname s nastavením môžu byť prítomné viaceré polia pôsobnosti. V tomto prípade je celkové pole pôsobnosti ich kombináciou. Poradie týchto polí pôsobnosti v šablóne môže a nemusí byť dôležité. Pokiaľ je toto poradie nevyhnutné pre správnu aplikáciu polí pôsobnosti, potom toto poradie musí byť definované. Pole pôsobnosti je informačný element definovaný v IPFIX informačnom modeli [9]. IPFIX konformná aplikácia by mala implementovať aspoň minimálnu skupinu informačných elementov slúžiacich ako pole pôsobnosti: LineCardId, TemplateId, exporterIPv4Address, exporterIPv6Address a ingressInterface. Ostatné informačné elementy môžu byť taktiež poliami pôsobnosti. Aj keď pre niektoré elementy je takéto priradenie bezpredmetné (napr. počítadlo informačných elementov). Jednou z dôležitých podmienok je, že počet



0				1				2				3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
ID šablóny (> 255)										Dĺžka polí											
Počet polí pôsobnosti																					

**Obrázok 3–16** Hlavička šablónovej sady s nastavením

polí pôsobnosti nesmie byť nula.

Šablónový záznam s nastavením obsahuje akúkoľvek kombináciu informačných identifikátorov. Formát šablónového záznamu s nastavením je zobrazený na obrázku 3–16. Pozostáva z hlavičky a jedného alebo viacerých špecifikátorov polí. Definícia týchto špecifikátorov je na obrázku 3–10. Hlavička tohoto záznamu je znázornená na obrázku 3–17. Počet polí pôsobnosti tu predstavuje ich počet v šablónovom zázname s nastavením. Polia pôsobnosti sú normálne polia v zázname, s tým rozdielom, že sú v zhromažďovači interpretované ako polia pôsobnosti. Táto hodnota nesmie byť nulová.

Na obrázku 3–17 je zobrazená šablónová sada s nastavením s rôznymi IETF a podnikovými informačnými elementami. Pozostáva z hlavičky 3–12, hlavičky šablóny s nastavením 3–16 a niekoľkých špecifikátorov polí.

Dátové záznamy sú prenášané v dátových sadách. Formát dátového záznamu je uvedený na obrázku 3–18. Pozostáva z jednej alebo viacerých hodnôt polí. Identifikátor šablóny ktorá opisuje kódovanie týchto polí je určená v hlavičke sady, v položke "identifikátor sady".

Hodnoty polí nemusia mať nutne dĺžku 16 bitov. Tieto hodnoty sú kódované podľa svojich dátových typov uvedených v [9]. Interpretácia dátových záznamov je možná iba v prípade, že je v zhromažďovači prítomná šablóna korešpondujúca so šablónovým identifikátorom. Na obrázku 3–19 je znázornená dátová sada skladajúca sa z hlavičky a niekoľkých hodnôt polí.

### 3.7.4 Kontrolné informácie

Nasledujúce pravidlá sú predpísané pre kódovanie kontrolných informácií:

0										1										2										3										
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	
ID sady = 3										Dĺžka																														
ID šablóny = 258										Počet polí = N + M																														
Počet polí pôsobnosti = N										0	Pole pôsobnosti 1 (ID IE)																													
Dĺžka poľa pôsobnosti 1										0	Pole pôsobnosti 2 (ID IE)																													
Dĺžka poľa pôsobnosti 2										...																														
...										1	Pole pôsobnosti N (ID IE)																													
Dĺžka poľa pôsobnosti N										Enterprise č. poľa pôsobnosti N																														
...																																								
Enterprise č. poľa pôsobnosti N										1	Inf. element nastavenia 1																													
Dĺžka nastavenia 1										Enterprise č. nastavenia 1																														
...																																								
Enterprise č. nastavenia 1										...																														
...										0	Inf. element nastavenia M																													
Dĺžka nastavenia M										Doplnenie (voliteľné)																														

Obrázok 3–17 Príklad šablónovej sady s nastavením

Hodnota poľa
Hodnota poľa
:
Hodnota poľa

Obrázok 3–18 Formát dátového záznamu

0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
ID sady = ID šablóny										Dĺžka																													
Záznam 1 - Hodnota poľa 1										Záznam 1 - Hodnota poľa 2																													
Záznam 1 - Hodnota poľa 3										- -																													
Záznam 2 - Hodnota poľa 1										Záznam 2 - Hodnota poľa 2																													
Záznam 2 - Hodnota poľa 3										- -																													
Záznam 3 - Hodnota poľa 1										Záznam 3 - Hodnota poľa 2																													
Záznam 3 - Hodnota poľa 3										- -																													
- -										Doplnenie (voliteľné)																													

Obrázok 3–19 Príklad dátovej sady

- Kontrolné informácie tokov by mali byť kódované tak, aby zhromažďovací proces vedel zachytiť štruktúru a sémantiku korešpondujúcich dát tokov, pre každý záznam toku exportovaný IPFIX zariadením.
- Konfiguračné kontrolné informácie sú prenesené do zhromažďovača tak, aby zhromažďovací proces vedel zachytiť štruktúru s sémantikou korešpondujúcich konfiguračných dát. Konfiguračné dáta, ktoré sú aj kontrolnými informáciami by mali obsahovať dodatočnú informáciu o pozorovacej doméne, v ktorej je táto konfigurácia účinná.

Záznam toku obsahuje dostatok informácií, aby zhromažďovací proces vedel identifikovať korešpondujúce dvojice kontrolných informácií tokov a konfiguračných kontrolných informácií. Exportovací proces kóduje dané informačné elementy na základe štandardu uvedeného v [3] .

Kontrolné informácie sú v zhromažďovacom procese použité na:

- Dekódovanie a interpretovanie záznamov tokov.
- Detekciu stavu exportovacieho procesu.

Periodické a spoľahlivé odosielanie kontrolných informácií z exportovacieho procesu je kritické pre správnu funkcionálnu zhromažďovacieho procesu. Na export kontrolných informácií môžu byť použité nasledujúce prístupy:

1. Odoslanie všetkých kontrolných informácií o tokoch ešte pred samotným exportom záznamov tokov. To zahŕňa všetky inkrementálne zmeny v definícii záznamov tokov.
2. V skoro reálnom čase notifikovať zhromažďovací proces o stave IPFIX zariadenia. To zahŕňa všetky zmeny, ako napr. zmena konfigurácie, ktorá ovplyvňuje toky, zmeny exportovacieho procesu, ktoré menia rýchlosť exportu, atď., o ktorých musí zhromažďovací proces vedieť.
3. Pretože je dôležité aby mal zhromažďovací proces aktuálne informácie o stave exportéra, export kontrolných informácií musí byť vykonávaný spoľahlivo. Jednou z možností ako to dosiahnuť, je posielat' tieto informácie cez spoľahlivý transportný protokol.

### **3.8 Prenos správ protokolom UDP**

Z času na čas nebude IPFIX zariadenie schopné pozorovať všetky pakety, ktoré dosiahli jeden z jeho pozorovacích bodov. Táto situácia môže nastať v prípade, keď merací proces bude dočasne trpieť nedostatkom systémových prostriedkov. V takýchto situáciách musí IPFIX zariadenie oznámiť počet stratených paket zhromažďovaču.

UDP nemá žiadny mechanizmus kontroly zahltenia spojenia. Preto môže byť UDP nasadené len v prípade, že spojenie medzi exportérom a zhromažďovačom nemôže byť zahltené. UDP nie je ani spoľahlivý protokol a teda nemôže zaručiť doručenie správ. IPFIX správa odoslaná z exportovacieho procesu do zhromažďovača sa môžu stratiť. UDP protokol nesmie byť použitý, pokiaľ aplikácia nemôže tolerovať stratu niektorých IPFIX správ.

Zhromažďovací proces môže zistiť výpadky IPFIX správ tak, že bude sledovať v ich sekvenčných číslach. V prípade UDP, toto číslo predstavuje celkový počet IPFIX dátových záznamov pre konkrétne UDP spojenie. Nesúvislosti medzi sekvenčnými číslami IPFIX správ by mali byť zaznamenané. Maximálna dĺžka exportovaných správ musí byť konfigurovateľná alebo nastavená tak, aby nepresiahla maximálne MTU (Message Transfer Unit) sieťovej cesty po ktorej bude cestovať.

Šablóny zasielané z exportovacieho procesu do zhromažďovacieho procesu cez UDP protokol musia byť znova preposielané v pravidelnom intervale pre prípad, že sa predchádzajúce kópie stratia.

Podľa štandardu by mal zhromažďovací proces počúvať na čísle UDP portu 4739, ktorý je pridelený IANA organizáciou pre IPFIX export. Musí ale byť zabezpečená konfiguračná možnosť, pre použitie iného portu.

### **3.8.1 Správa šablón pri použití UDP protokolu**

Pokiaľ je na prenos šablón použitý UDP protokol, všetky sady šablón musia byť prenášané pravidelne s nastaviteľným intervalom. Nové šablóny by mali byť prenesené hneď po vytvorení, ešte pred tým, ako je prenesený akýkoľvek dátový záznam asociovaný z touto šablónou. V prípade zmeny konfigurácie by exportovací proces mal v zrýchlenej miere preposlať kópie nových definícií šablón. V takomto prípade môže poslať šablóny bez akýchkoľvek pridaných dát, aby mal zhromažďovač dostatok informácií o dátach ešte pred obdržaním dát z novej konfigurácie. Pri uplatňovaní konfiguračných zmien, ktoré môžu modifikovať interpretáciu dátových záznamov, musí byť použité nové číslo šablóny a staré sa nesmie použiť znovu, pokiaľ neskončí jej platnosť (vysvetlená v ďalšej kapitole).

### **3.8.2 Zhromažďovací proces pri použití UDP protokolu**

Zhromažďovací proces musí každej šablóne definovať dobu životnosti. Šablóny, ktoré nebudú exportovacím procesom obnovené počas svojej životnosti expirujú. Pokiaľ nejaká šablóna expiruje, zhromažďovací proces ju musí zrušiť a takisto musí zahodiť všetky

dáta s ňou asociované, ktoré prijme od exportéra. V takomto prípade musí byť o tom podané upozornenie. Pokiaľ je šablóna obnovená šablónou s odlišným obsahom ako pôvodná, zhromažďovací proces by mal túto skutočnosť oznámiť a nahradiť pôvodnú šablónu novou. Životnosť šablóny musí byť aspoň 3 krát dlhšia ako obnovovací interval šablón v exportovacom procese.

### **3.8.3 Zlyhanie spojenia**

Pretože UDP nie je spojoivo orientovaný protokol, exportovací proces nemôže zistiť prerušenie spojenia so zhromažďovačom. Ako protiopatrenie sa ponúka exportovanie IPFIX správ viacerým zhromažďovačom naraz.

## 4 Analýza PSAMP protokolu

Táto časť práce je zameraná na využiteľné časti PSAMP protokolu pre použitie exportovania IPFIX správ vo vysokorýchlostných sieťach. Dôležitými elementami sú preto jednotlivé definície algoritmov pre výber a filtráciu paketov z vstupnej množiny do relevantnej podmnožiny paketov, pri zachovaní čo najvyššej presnosti rekonštruovaných dát.

Techniky výberu paketov generujú podmnožinu paketov pozorovaných v pozorovacom bode. V týchto technikách rozlišujeme medzi vzorkovaním a filtrovaním. Vzorkovanie je zamerané na výber reprezentatívnej vzorky paketov. Tieto vzorky sú použité na získanie informácií o celkovej množine pozorovaných paketov, bez nutnosti ich všetky spracovať. Výber môže závisieť od pozície paketu, obsahu paketu, alebo pseudonáhodných rozhodnutí.

Filtrovanie vyberá vzorku s určitou spoločnou vlastnosťou. Je použité hlavne vtedy, ak je záujem len o určité konkrétne pakety. Spomínané vlastnosti môžu byť odvodzované priamo z obsahu paketu, alebo z jeho spracovávaní v smerovači. Filtrovanie je deterministická operácia. Nikdy nezávisí od pozície paketu, alebo pseudonáhodných rozhodnutí.

Bežnou technikou výberu paketov je výpočet hash funkcie na niektorých bitoch paketu a jeho výberu, pokiaľ výsledok tejto funkcie spadá do určitého intervalu. Keďže hashovanie je deterministická operácia na obsahu paketu, je to technika filtrovania. Napriek tomu sú hash funkcie niekedy použité na aproximáciu náhodného vzorkovania. V závislosti na vstupných bitoch, môže byť aproximovaná náhodná vzorkovacia technika s danou pravdepodobnosťou. Je to aj dôležitá technika výberu určitej podmnožiny paketov z viacerých pozorovacích bodov.

Tabuľka 4 poskytuje prehľad techník vzorkovania a filtrovania opísaných v tejto práci a ich kategorizáciu. Hviezdička pri názve indikuje techniky pre ktoré existuje aj variant závislý na obsahu paketu. Z tejto tabuľky je jasne vidno, že len techniky ktoré spĺňajú podmienku nezávislosti na obsahu a deterministického výberu sú považované za filtre.

Táto kategorizácia uvedená v tabuľke 4 je potrebná pre definíciu informačného mo-

<b>Technika výberu</b>	<b>Deterministický výber</b>	<b>Závislosť na obsahu</b>	<b>Kategorizácia</b>
Systematická podľa počtu	Áno	Nie	Vzorkovanie
Systematická podľa času	Áno	Nie	Vzorkovanie
Náhodná n z N	Nie	Nie	Vzorkovanie
Náhodná uniformná pravdepodobnosť	Nie	Nie	Vzorkovanie
Náhodná neuniformná pravdepodobnosť	Nie	Áno*	Vzorkovanie
Náhodná neuniformná podľa stavu toku	Nie	Nie*	Vzorkovanie
Zhoda poľa	Áno	Áno	Filtrovanie
Hash funkcia	Áno	Áno	Filtrovanie
Stav smerovača	Áno	Áno*	Filtrovanie

**Tabuľka 4 – 1** Prehľad techník výberu paketov

delu opisujúceho primitívne selektory. Komplexné techniky výberu môžu byť vyjadrené kompozíciou po sebe nasledujúcich vzorkovacích a filtrovacích operácií. Napríklad, výber paketu, ktorý definuje pravdepodobnosť výberu na základe dĺžky paketu, môže byť definovaný ako následnosť filtrovacej a vzorkovacej schémy.

## 4.1 Vzorkovanie

Nasadenie vzorkovacích techník sa zameriava na získanie informácií o charakteristickej vlastnosti všetkých paketov z ich podmnožiny. Pre vhodnú vzorkovaciu stratégiu je nutné určiť potrebný typ informácií a požadovanú presnosť výsledku a to už vopred.. Predovšetkým je nutné vedieť metriku, ktorá má byť preskúmaná. Táto metrika môže mať

veľkosť jednoduchého počtu paketov, až po určenie kompletnej distribučnej funkcie (napr. veľkosti paketov). Ďalej je potrebná, už spomínaná presnosť výsledku a samozrejme (pre účtovné systémy), dôvera v nasledovnom zmysle. Napríklad pre systém použíajúce spoľahlivosť na základe využitia služieb dôvera paketu môže závisieť od peňažnej hodnoty, ktorú predstavuje poplatok za službu prepočítaný na jeden paket. To znamená, že pre drahší paket bude vyžadovaná vyššia dôvera, ako pre lacnejšie. Vzorkovacie metódy a parametre musia byť zreteľne komunikované medzi komponentami systému, v ktorom sú použité, alebo v ktorých sa používajú dáta nimi získané, pretože len takto je možné zabezpečiť správnu interpretáciu týchto dát.

Vzorkovacie metódy môžu byť charakterizované vzorkovacími algoritmi, udalosťou, ktorá začína vzorkovací interval a samotnou dĺžkou vzorkovacieho intervalu. Tieto parametre sú detailne opísané v nasledujúcich kapitolách. Vzorkovací algoritmus opisuje základný proces výberu vzoriek.

#### **4.1.1 Systematické vzorkovanie**

Systematické vzorkovanie opisuje proces výberu štartovacieho bodu a trvania vzorkovacieho intervalu podľa deterministickej funkcie. To môže napríklad byť periodický výber každého  $k$ -teho elementu v poradí, alebo aj výber všetkých paketov, ktoré dorazili v určitý časový interval. Aj pokiaľ výberový proces nepodlieha periodickej funkcii, stále ho považujeme za systematické vzorkovanie, pokiaľ je výber deterministický.

Použitie systematického vzorkovania takisto prináša risk odchýlenia sa od presných výsledkov. Pokiaľ systematickosť vo vzorkovacom procese kopíruje systematickosť pozorovaného stochastického procesu (výskyt charakteristických znakov v sieti), je veľká pravdepodobnosť, že odhadované výsledky budú nepresné. Systematickosť pozorovaného procesu nemusí byť stále známa vopred.

V tejto práci sú udávané iba rovnomerne rozložené schémy, kde udalosti, ktoré spúšťajú vzorkovanie sú periodické, či už v čase, alebo v počte (paketov). Všetky pakety vyskytujúce sa v rámci výberového intervalu za spúšťajúcou udalosťou sú vybrané.

### ***Systematické vzorkovanie založené na počte***

V systematickom vzorkovaní založenom na počte je štartovacia a ukončovacia udalosť definovaná v súvislosti s pozíciou paketu v priestore (poradie).

### ***Systematické vzorkovanie založené na čase***

V systematickom vzorkovaní založenom na čase, štartovacia a ukončovacia udalosť definuje vzorkovacie intervaly. Všetky pakety, ktoré dorazia do pozorovacieho body v tomto intervale sú vybrané.

Oba schémy výberu sú nezávislé od obsahu. Obsahovo závislé deterministické selektory sú kategorizované ako filtre.

## **4.1.2 Náhodné vzorkovanie**

Náhodné vzorkovanie vyberá začiatočný bod vzorkovacieho intervalu podľa náhodného procesu. Výbery elementov sú nezávislé experimenty. S touto schémou môžu byť dosiahnuté neskreslené výsledky. V porovnaní so systematickým vzorkovaním, náhodné vzorkovanie vyžaduje generovanie vyžadujúcich čísel. Rozlišujeme dva metódy náhodného vzorkovania.

### ***n-z-N vzorkovanie***

V tomto vzorkovaní je vybraných  $n$  elementov z pôvodného počtu  $N$  paketov. Jedna z možných implementácií zahŕňa vygenerovanie  $n$  rôznych náhodných čísel v rozmedzí  $[1..N]$  a vybrať pakety, ktoré majú poradové číslo zhodné s týmito náhodnými číslami. Pre tento typ vzorkovania je veľkosť vzorky pevná, pokiaľ sa toto vzorkovanie neopakuje periodicky po vyvzorkovaní  $n$  paketov.

### ***Pravdepodobnostné vzorkovanie***

V pravdepodobnostnom vzorkovaní je rozhodnute, či daný element bude vybraný založené na preddefinovanej výberovej pravdepodobnosti. Príkladom môže byť pravdepodobnosť 0.5, teda napríklad hod mincou pre každý paket a vyvzorkovanie paketu, pokiaľ padne

dopredu určená strana. Výberová pravdepodobnosť nemusí byť rovnaká pre každý paket. Preto rozlišujeme medzi uniformným pravdepodobnostným vzorkovaním (ktoré ma rovnakú mieru pravdepodobnosti pre každý paket) a neuniformným pravdepodobnostným vzorkovaním (kde môže byť pravdepodobnosť rôzna pre rôzne pakety)

Pre uniformné pravdepodobnostné vzorkovanie sú pakety vybrané nezávisle s rovnakou pravdepodobnosťou  $p$ . Toto vzorkovanie je veľakrát označované ako geometrické náhodné vzorkovanie, pretože rozdiel poradia dvoch za sebou vybraných paketov je nezávislá náhodná premenná s geometrickou distribúciou s priemerom  $1/p$ . Rozdiel časov predstavuje exponenciálnu distribúciu. Rovnako geometrické ako aj exponenciálne náhodné vzorkovanie sú príklady aditívneho náhodného vzorkovania, definovaného ako vzorkovanie, kde intervaly, alebo počty paketov medzi nasledujúcimi vzorkami sú nezávislé identicky distribuované náhodné premenné.

Neuniformné pravdepodobnostné vzorkovanie je variant pravdepodobnostného vzorkovania, kde je vzorkovacia pravdepodobnosť závislá na vstupe výberového procesu. To môže byť použité na váženie vzorkovacej pravdepodobnosti aby sa zvýšila šanca výberu paketov označených za dôležité, ale ktoré sú zriedkavé. Neskreslené odhady pre kvantitatívnu štatistiku sú získané renormalizáciou hodnôt vzoriek.

Neuniformné pravdepodobnostné vzorkovanie závislé na stave toku je vzorkovanie, ktoré sa dá klasifikovať ako úzko späté s koncepciou tokov definovaných v protokole IPFIX [3] a je používaní iba v spojení s funkciou, ktorá ich monitoruje (merací proces IPFIX). Pakety sú vybrané v závislosti na stave toku.

Tento typ vzorkovania je závislý na obsahu paketu, pretože identifikácia toku, do ktorého paket náleží, vyžaduje analýzu časti jeho obsahu. Výber paketu v závislosti od stavu databázy tokov je užitočné pri nedostatku pamäťových zdrojov.

## 4.2 Filtrovanie

Filtrovanie je deterministický výber paketov založený na obsahu paketu, spracovania paketu v pozorovacom bode, alebo deterministickej funkcii. Paket je vybraný ak tieto

kvantily hodnoty spadajú do určitých rozsahov.

Úloha filtrovanie, ako už napovedá názov je separovať všetky pakety majúce určitú vlastnosť, od tých, ktoré túto vlastnosť nemajú. Odlišnosť od vzorkovania je v tom, že výberové rozhodnutie nie je závislé na pozícii paketu v čase, priestore, alebo od náhodného procesu. V tejto práci sú opísané nasledujúce tri filtrovacie techniky. Prvé dve (Filtrovanie podľa masky a Filtrovanie podľa hash funkcie) sú bezstavové a môžu vykonať rozhodnutie založené len na analýze samotného paketu. Posledná (Filtrovanie podľa stavu smerovača) vyžaduje aj prístup k stavovým informáciám zariadenia na ktorom sa nachádza. Preto je jej použitie komplikovanejšie a výhodné iba v určitých prípadoch.

#### 4.2.1 Filtrovanie podľa masky

Táto metóda je základná filtrovacia schéma založená na definícii IPFIX toku. Pri jej použití je paket vybraný, pokiaľ je špecifické pole paketu zhodné s preddefinovanou hodnotou. Polia filtra môžu obsahovať všetky atribúty IPFIX toku špecifikované v [9]. Ďalšie polia môžu byť špecifikované v rozšíreniach výrobcov. Masky a rozsahy zhody sú podporované len do takej miery, ako to povoľuje [9].

#### 4.2.2 Filtrovanie podľa hash funkcie

Hash funkcia  $h$  mapuje obsah paketu  $c$ , alebo jeho časti na rozsah hash funkcie  $R$ . Paket je vybraný ak  $h(c)$  spadá do  $S$ , čo predstavuje podmnožinu  $R$  nazývanú výberový rozsah hash funkcie. Aj keď je výber podľa hash funkcie určitý druh filtra, objekt je vybraný ako  $c$  je v  $inv(h(S))$ . Pre niektoré vhodné hash funkcie je inverzná funkcia k  $inv(h(S))$  extrémne zložitá a preto  $h$  nie je vyjadriteľné ako, napr. filter zhody podľa alebo jeho jednoduchá kombinácia. Filtrovanie podľa hash funkcie má väčšinou dva typy použitia. Ponúka spôsob ako aproximovať náhodné vzorkovanie použitím obsahu paketu na generovanie pseudonáhodného čísla, alebo možnosť konzistentne vybrať podmnožiny paketov, ktoré zdieľajú určitú spoločnú vlastnosť (napr. na rôznych pozorovacích bodoch).

Hash funkcie musia spĺňať nasledujúce štatistické vlastnosti, aby sa dali použiť pre

tento typ filtrovania.

- Hash funkcia  $h$  musí mať dobré zmiešavacie vlastnosti v tom zmysle, že malé zmeny na vstupe (napr. zmena jedného bitu), spôsobí veľkú zmenu na výstupe (zmena viacerých bitov).
- Druhá vlastnosť závisí bližšie na štatistike obsahu  $c$ . V aplikáciách, obsah  $c$  zahŕňa niekoľko rozličných polí  $c_1 \dots c_m$  napr. zdrojovú a cieľovú IP adresu, identifikátor IP a čísla TCP/UDP portu. S hash funkciou spĺňajúcou prvú podmienku, výberové rozhodnutia budú nekorelované s obsahom každého individuálneho poľa ak doplňujúce polia sú dostatočne variabilne menia a sú dostatočne nekorelované s  $c_j$ .

#### 4.2.3 Filtrovanie podľa stavu smerovača

Táto skupina filtrov vyberá paket na základe podmienok týkajúcich sa stavu smerovača v okamihu výberu. Nasledujúci zoznam podáva príklady takýchto podmienok. Tieto podmienky môžu byť kombinované logickou funkciou *AND*

- Vstupné rozhranie, na ktorom bol paket prijatý zodpovedá špecifikovanej hodnote.
- Výstupné rozhranie, na ktorom bol paket prijatý zodpovedá špecifikovanej hodnote.
- Paket porušil ACL (Access Control List) smerovača.
- RPF (Reverse Path Forwarding) pre tento paket zlyhalo.
- Pre tento paket zlyhalo rezervovanie systémových prostriedkov.
- Pre tento paket neexistuje trasa (route).
- Zdrojový BGP AS (Border Gateway Protocol Autonomous System) je zhodný so špecifikovanou hodnotou, alebo leží v danom rozsahu.
- Cieľový BGP AS (Border Gateway Protocol Autonomous System) je zhodný so špecifikovanou hodnotou, alebo leží v danom rozsahu.

## 5 Analýza súčasného stavu nástroja Basicmeter

Nástroj BasicMeter bol vytvorený ako základný nástroj pre pasívne merania v počítačových sieťach. Vývoj nástroja BasicMeter začal a pokračuje v Laboratóriu počítačových sietí na Technickej univerzite v Košiciach. Cieľom jeho návrhu bolo vytvorenie voľne dostupnej a použiteľnej platformy pre neintruzívne merania prevádzkových parametrov. BasicMeter nie je koncipovaný ako komplexný nástroj na meranie veľkého množstva dát, je to skôr nástroj z používateľského hľadiska relatívne jednoduchý, ale pritom s minimálnou námahou modifikovateľný, prispôsobiteľný a rozšíriteľný. To v budúcnosti umožní návrh komplexnejších meracích platforiem.

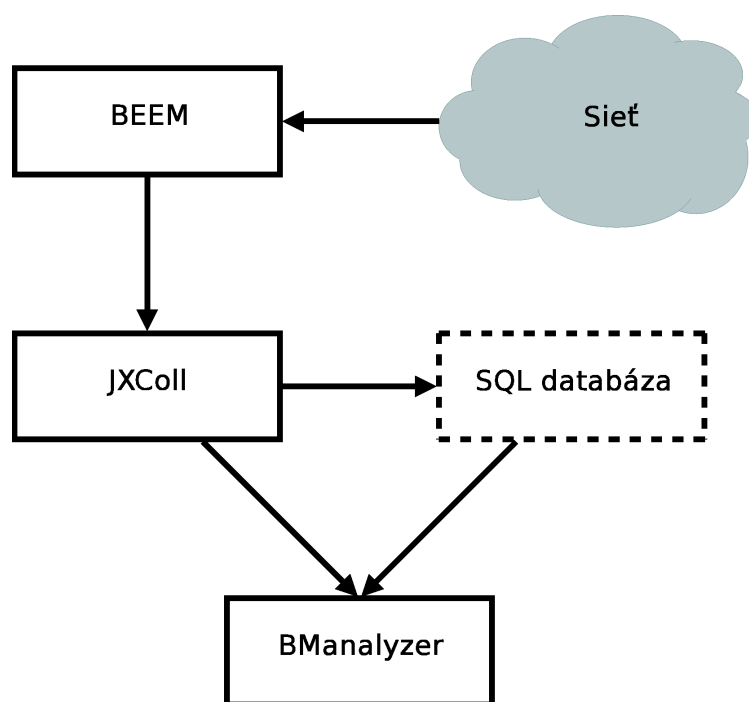
Vývoj nástroja BasicMeter začal podporou protokolu NetFlow verzie 9, ktorá umožňovala export niektorých štatistických parametrov sieťových parametrov do zhromažďovacieho procesu a následne do analyzujúcej aplikácie. Týmto nástrojom bolo uskutočnených niekoľko meraní QoS parametrov počítačových sietí.

### 5.1 Architektúra nástroja BasicMeter

Implementácia tohoto nástroja sa snaží v čo najväčšej miere priblížiť k podmienkam definovaným štandardmi IPFIX a PSAMP. To sa vo veľkej miere aj podarilo. Bez zmeny ostal iba informačný model exportu, ktorý ostal pri podpore protokolu NetFlow v9 (resp. aj NetFlow v5). To však poskytuje veľkú výhodu oproti iným riešeniam pri modifikovaní exportu v súlade so štandardom IPFIX, pretože tento protokol je definovaný ako východiskový protokol pre jeho štandardizáciu.

Priblíženie sa štandardu PSAMP bolo obmedzené na aplikáciu ním definovaných vzorkovacích a filtrovacích techník [18]. Tieto algoritmy boli implementované v skoro plnom rozsahu, okrem algoritmov vyžadujúcich externé informácie od zariadenia, na ktorom je merací bod umiestnený. Tieto boli vynechané kvôli ľahkej prenositeľnosti a širšiemu poľu nasadenia tohoto meracieho nástroja.

Koncepcia meracieho nástroja BasicMeter bola od začiatku vývoja dizajnovaná do troch vrstiev deklarovaných štandardom IPFIX. Tieto tri vrstvy obsahujú funkcie na



Obrázok 5 – 1 Architektúra nástroja BasicMeter

odchytenie, výber paketov, ich klasifikáciu, export, zhromaždenie ,následnú analýzu 5 – 1 a prípadnú archiváciu. Takto môže používateľ jednoducho nasadiť túto architektúru do prevádzky. Jednotlivé časti nástroja sú na sebe viacmenej nezávislé, preto je ich možné použiť aj jednotlivo, pokiaľ sa dodrží určitý formát komunikácie. Predovšetkým sú ale určené pre spoločnú prevádzku a v takejto konfigurácii poskytujú aj najväčšie množstvo svojich funkcií. SQL databáza nie je súčasťou špecifikácie IPFIX, preto je v schéme naznačená bodkovanou. Všeobecne sa na uloženie exportovaných informácií o tokoch predpokladá akýkoľvek dátový sklad (súbor, databáza, vyhradená partícia disku). Kvôli jednoduchému použitiu a dobrým možnostiam ďalšieho spracovania uložených dát bola ako dátový sklad zvolená práve SQL databáza.

Podrobnejší popis znázornených častí architektúry meracieho nástroja BasicMeter 5 – 1:

- *BEEM* - (BasicMeter Exporting and Measuring process) Merací a exportovací proces vykonávajúci zachytávanie paketov, ich výber, klasifikáciu do tokov a export

informácií o tokoch pomocou protokolu IPFIX.

- *JXColl* - (Java XML Collector) Zhromažďovač pre spracovanie prijatých exportných paketov a informácií, ktoré obsahujú.
- *BAnalyzer* - (BasicMeter analyzer) Analyzujúca aplikácia, ktorá na základe dát zo zhromažďovača vykonáva grafickú a štatistickú analýzu tokov, podľa potrieb používateľa

Architektúru popisovaného nástroja možno rozdeliť do troch hlavných častí:

- odchyťovanie paketov
- klasifikácia
- export

Ďalšou časťou programu je spracovanie konfiguračného súboru programu vo formáte XML. Časť spracovania konfigurácie má za úlohu načítať a spracovať parametre z konfiguračného súboru. Pre tieto činnosti je použitá knižnica libXML [5] určená na spracovanie súborov vo formáte XML.

Odchyťovacia časť má za úlohu sledovanie, odchyťovanie paketov a ich výber na základe parametrov poskytovaných konfiguračnou časťou, odovzdaných odchyťovacej časti v procese inicializácie. Táto časť využíva funkcie knižnice libpcap [8], ktorá realizuje samotné odchytenie paketov a ich prenos z priestoru jadra (kernel space) do priestoru používateľa (user space). Na túto operáciu sú potrebné práva administrátora systému (root), teda aplikáciu je potrebné spúšťať s efektívnym používateľským identifikátorom (user identifier, UID) 0 Tento identifikátor v unixových operačných systémoch označuje používateľa s najvyššími právami v subsystéme pridelovania práv. Samotný filter pre výber paketov na sledovanie a odchytenie je realizovaný pomocou vysokoúrovňového abstraktného popisného jazyka implementovaného v knižnici na sledovanie sieťovej prevádzky s názvom libpcap [8]. Odchyťávajú sa všetky pakety patriace aspoň do jedného toku.

Samotné odchyťovanie paketov je realizované pomocou berkeleyského paketového filtra (Berkeley Packet Filter, BPF) prítomného v jadrách väčšiny unixových operačných systémov. Filter je implementovaný tak, že je možné vyberať pakety na základe ďalších polí v hlavičke okrem štandardných (zdrojová a cieľová adresa, zdrojové a cieľové porty), teda je možné vyhovieť špecifikácii IPFIX. Výhodou použitia filtra je zníženie počtu prepnutí kontextu (prenosov medzi priestorom jadra a priestorom používateľa). Prenášané sú len pakety so žiadanou informáciou, čo prispieva k zvýšeniu výkonnosti meracieho nástroja. Na pakety, ktoré prešli filtrom je aplikované vzorkovanie, teda mechanizmus výberu, ktorý sa od filtrovania odlišuje rozdielmi opísanými v kapitole č.3.

Klasifikácia určuje tok, do ktorého zachytený paket patrí a odovzdá informácie získané z paketu spolu s identifikátorom toku do časti vytvárania záznamov tokov (je súčasťou exportovacieho procesu). Časť vytvárania záznamov tokov obsahuje zásobník pre uloženie záznamov aktívnych tokov, tzv. pamäť tokov (Flow Cache). Záznamy tokov sú po ukončení toku, konfrontované s informačným modelom protokolu IPFIX..Podľa tohoto modelu sa na základe definovaných šablón napĺňajú jednotlivé položky v záznamoch dát daného toku. Hodnota príslušnej položky je určená typom zadaným v šablóne a informáciami v zázname konkrétneho toku.

Exportný proces má za úlohu vytvárať IPFIX správy na prenos získaných dát do zhromažďovača. Získané dátové záznamy s rovnakou šablónou sú vkladané do jednej sady toku, pričom je podmienkou, aby šablóna bola zhromažďovaču doručená skôr ako samotné záznamy. Nemusí však byť prenášaná v tom istom pakete ako záznamy, ak už raz bola do zhromažďovaču doručená. Šablóny sú v exportnom pakete zoskupené do sád šablón. Zoskupovanie objektov s rovnakou povahou do sád prináša jednoduchšie spracovanie paketu na oboch stranách. časť pre sieťovú komunikáciu umožňuje exportnému procesu zachovať si nezávislosť od transportného protokolu. V súčasnej implementácii exportovacieho procesu je na prenos dátových, ako aj šablónových záznamov použitý UDP protokol. Je to vyžadované kvôli kompatibilite so zhromažďovačom, ako aj inými nástrojmi analyzujúcimi dáta exportované vo formáte NetFlow.

Keďže sa štandardy IPFIX a PSAMP vyjadrujú najmä k problematike meracieho a

exportovacieho procesu a ku komunikácii medzi exportným procesom a zhromažďovačom, aj táto práca sa zameria hlavne na úpravy tejto časti architektúry nástroja BasicMeter. Koncepcia programu BEEM, ktorý implementuje merací a exportovací proces ja naznačená na obrázku 5 – 2

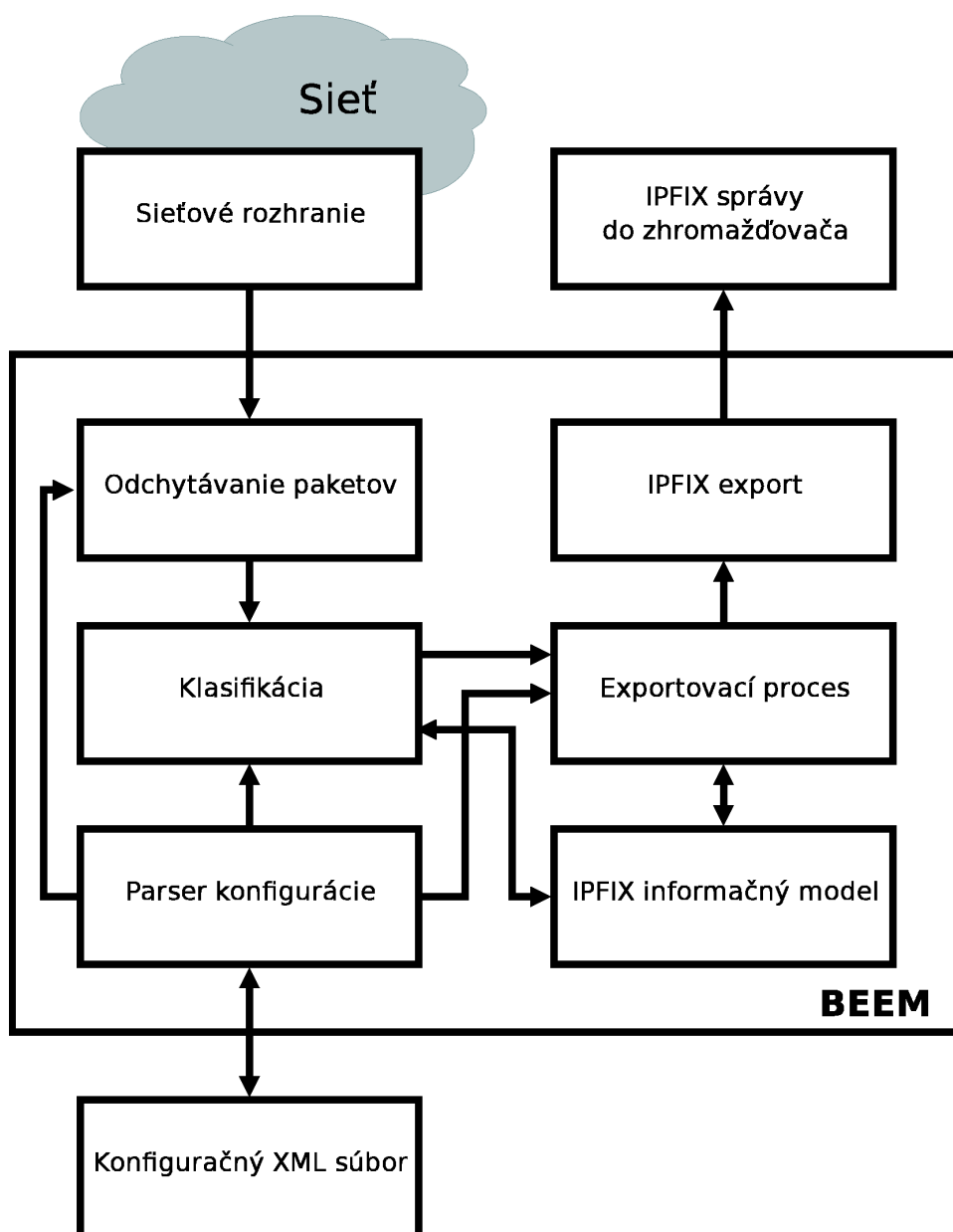
## **5.2 Zhodnotenie konformity častí architektúry BasicMeter so štandardami IPFIX a PSAMP**

Zhodnotenie konformity meracieho nástroja BasicMeter sa skladá z postupnej evaluácie požiadaviek kladených na jednotlivé časti architektúry v spomínaných štandardoch. Tieto štandardy udávajú tri stupne povinnosti označované anglickými slovami:

- *MUST* - Táto požiadavka je explicitne vyžadovaná pre použitie IPFIX protokolu na export nameraných dát. Všetky takto označené požiadavky musia byť v programových implementáciách splnené. Tieto požiadavky tvoria nosnú časť definície IPFIX protokolu. Zhodnotenie konformity meracieho nástroja BasicMeter so štandardmi IPFIX a PSAMP sa z veľkej časti skladá z vyhodnocovania týchto požiadaviek.
- *SHOULD* - Požiadavka, ktorá je síce vyžadovaná, ale nie je povinná pre základnú funkciu IPFIX protokolu. Pracovná skupina vyvíjajúca protokol IPFIX odporúča implementáciu takto označených podmienok pre lepšiu funkčnosť a použiteľnosť štandardného exportu.
- *MAY* - Časti štandardu označované týmto slovom sú pri implementácii plne voliteľné a ich vynechanie nemá vplyv na funkciu protokolu.

### **5.2.1 Merací proces**

V súčasnej implementácii meracieho procesu je dodržaná skoro kompletná definícia IPFIX štandardu. V rámci analýzy konformity boli pre merací proces programu BEEM zistené tieto nezhody so štandardom v prípadoch kde boli tieto vlastnosti povinné, alebo nepovinné, ale dôležité pre aktuálnu implementáciu:



Obrázok 5–2 Architektúra časti BEEM nástroja BasicMeter

- Štandard IPFIX definuje merací proces ako množinu funkcií ktorej vstupom sú hlavičky a telá paketov spolu s ich charakteristikami pozorovanými v pozorovacom bode. Do tejto množiny funkcií by (podľa IPFIX) mali patriť funkcie pre: odchyťovanie paketov, časové značkovanie, vzorkovanie/filtrovanie, klasifikáciu a správu tokov. V súčasnej implementácii meracieho procesu v rámci BEEM je správa tokov delegovaná priamo do exportovacieho procesu pre jednoduchosť prístupu k pamäti tokov. Štandard ale trvá na oddelení tejto pamäte a jej správe práve meracím procesom z dôvodu jednoduchšej aktualizácie exportovacieho procesu ako samostatného modulu. Zároveň definuje pojem "lokálny export", ktorý označuje prenos dát v rámci BEEM medzi meracím a exportovacím procesom. Tento lokálny export nie je bližšie definovaný a je závislý od implementácie.
- Merací proces musí byť, podľa IPFIX štandardu, schopný manipulovať s viacerými pozorovacími bodmi (tvoriacimi pozorovacie domény). V prípade aktuálnej implementácie je táto možnosť síce prístupná, ale len v podobe odchyťovania paketov zo všetkých dostupných rozhraní naraz. Nie je možné špecifikovať jednotlivé podmnožiny rozhraní, ktoré by sa dali rozdeliť do pozorovacích domén.
- Požiadavka na spoľahlivosť meracieho procesu je v IPFIX štandarde nepovinná, ale v prípade jej nesplnenie je nutné o tom používateľa informovať. Spoľahlivosť je definovaná ako schopnosť s určitou (vopred definovanou) úspešnosťou odchytiť všetky pakety prechádzajúce pozorovacím bodom a v prípade zlyhania túto skutočnosť zistiť a oznámiť. V aktuálnej implementácii táto spoľahlivosť nie je zaručená ani oznamovaná.
- Správanie sa meracieho procesu pri preťažení musí byť podľa štandardu IPFIX jasne definované. BEEM toto správanie vo svojej konfigurácii, alebo dokumentácii nedefinuje.
- Synchronizácia vnútorného času programu s UTC (Universal Time Co-ordinated) je z hľadiska spolupráce jednotlivých častí architektúry situovaných na rozličných

miestach nevyhnutná. Merací proces preto v súlade so štandardom musí poskytovať možnosť synchronizovať svoj čas, pred začiatkom odchyťovania paketov. Súčasná implementácia sa spolieha na synchronizáciu času v operačnom systéme a explicitne ju nezabezpečuje.

- Podľa štandardu IPFIX musí byť možné si v konfigurácii zvoliť šablónu, podľa ktorej budú exportované nazbierané dáta. V súčasnej implementácii je šablóna pevne zadaná a nie je možné ju zmeniť.

### 5.2.2 Exportovací proces

Implementácia exportovacieho procesu prešla od začiatku projektu asi najväčšími zmenami v architektúre nástroja BasicMeter. Preto je aj jeho konformita s protokolmi IPFIX a PSAMP najťažšie definovateľná. Vo všeobecnosti však exportovací proces nespĺňa tieto predpoklady uvedené v štandardoch:

- Použitie spoľahlivého protokolu na prenos IPFIX správ. Exportovací proces, implementovaný v BEEM programe architektúry BasicMeter využíva, z dôvodu kompatibility s ostatnými časťami architektúry, na prenos exportovaných dát, ako aj šablón, UDP protokol. IPFIX štandard však vyžaduje, kde je to možné, aby bol na prenos dát (hlavne šablón) použitý spoľahlivý protokol s ochranou proti zahlteniu. Ďalej určuje, že UDP protokol môže byť použitý na prenos IPFIX správ, len v prípade, pokiaľ sú tieto linky vyhradené a nepodliehajú zahlteniu.
- V prípade nesplnenia predchádzajúcej podmienky je možné protokol IPFIX na UDP transporte nasadiť iba v aplikáciách tolerujúcich stratu určitého percenta prenosených dát. Z rovnakého dôvodu musia byť šablóny odoslané po nespoľahlivom transporte preposielané znovu po uplynutí určitého časového intervalu, pre prípad, že predchádzajúce kópie nedorazili do zhromažďovača.
- Rovnako je nutné, pri použití nespoľahlivého protokolu, zabezpečiť túto vlastnosť na aplikačnej vrstve architektúry.

### 5.2.3 Zhromažďovací proces

V architektúre nástroja BasicMeter je zhromažďovací proces programovo aj platformovo nezávislý od meracieho a exportovacieho procesu zjednoteného v programe BEEM. Štandard IPFIX však kladie povinné podmienky aj na túto časť meracej architektúry. Nasledujúce výhrady vznikli po vyhodnotení analýzy IPFIX protokolu vzhľadom k programu JXColl:

- Zhromažďovací proces musí s každou šablónou prijatou cez nespoľahlivý transport (UDP) asociovať nejakú dobu životnosti. Šablóny, ktoré nebudú počas svojej doby životnosti obnovené musia byť zrušené a v tomto prípade musí byť vygenerované varovné hlásenie o tomto kroku. Zhromažďovací proces nesmie ďalej dekodovať žiadne dáta asociované s touto expirovanou šablónou. Životnosť šablóny v zhromažďovači musí byť aspoň trojnásobne dlhšia, ako je interval obnovovania šablón v exportovacom protokole.
- V prípade použitia nespoľahlivého transportného protokolu, musí byť zhromažďovač schopný zabezpečiť spoľahlivosť na aplikačnej vrstve.

## 6 Zhodnotenie implementácie analyzovaných požiadaviek

Pri implementácii štandardov IPFIX a PSAMP do meracieho nástroja BasicMeter, resp. do jeho meracej a exportovacej časti (BEEM) bola splnená väčšina analyzovaných požiadaviek.

Použitím XML (eXtensible Markup Language) jazyka ako nástroja na konfiguráciu parametrov meracieho a exportovacieho procesu bola dosiahnutá jednoduchá rozšíriteľnosť, čitateľnosť a kompatibilitnosť konfiguračného súboru. V rámci jednoduchosti výmeny konfiguračných parametrov by bolo vhodné spracovávať konfiguračné nastavenia v jazyku XML aj v ostatných častiach architektúry BasicMeter. Ďalším krokom pri implementácii tohoto jazyka ako konfiguračného nástroja pre časti architektúry by mala byť validácia konfiguračných súborov podľa definovanej schémy.

Rozdelenie modulu BEEM na viacero vlákien bolo dosiahnuté zvýšením výpočtového výkonu oproti sekvenčnému spracovaniu. V rámci rozdelení funkcií meracieho, exportovacieho procesu, ako aj pamäte tokov do vlákien bola splnená požiadavka na oddelenie exportovacieho procesu od ostatných komponentov IPFIX zariadenia. Takto bude v budúcnosti možná jednoduchá výmena a nahradenie exportovacieho procesu.

V súvislosti so správou šablón, ktorá bola v doterajšej implementácii exportovacieho procesu vyhodnotená ako nedostatočná, bola implementovaná podpora pre konfiguráciu šablón cez konfiguračný súbor. Táto konfigurácia využíva jazyk XML na popis jednotlivých atribútov a polí šablóny, ako ju definuje štandard IPFIX. Analýza tohoto protokolu preukázala, že momentálne nie je jasne definovaný spôsob priradzovania šablón exportovaným dátam. Preto je podpora pre viac šablón počas jedného behu programu momentálne implementovaná, ale používateľsky nedostupná. V budúcnosti bude potrebné jasne definovať vzťah medzi šablónami a exportovanými dátami, aby mohol používateľ architektúry BasicMeter v priebehu merania meniť šablóny pre exportované dáta podľa potreby.

Požiadavka protokolu IPFIX na manipuláciu meracieho procesu s viacerými meracími bodmi sa v praxi ukázala ako nesplniteľná. Merací proces IPFIX zariadenia v architektúre BasicMeter je postavený na knižnici libpcap [8], ktorá neumožňuje simultánne spracová-

vane paketov z viacerých sieťových rozhraní. Jedinou výnimkou z tohoto obmedzenia je odchyťvanie paketov zo všetkých rozhraní naraz.

Spoľahlivosť meracieho a exportovacieho procesu bola po analýze upravená nasledujúcimi spôsobmi:

- Implementáciou spoľahlivého transportného protokolu TCP. Pretože protokol TCP zabezpečuje spoľahlivé doručenie exportovaných dát, je spoľahlivosť oproti použitiu nespojovaného protokolu UDP, výrazne vyššia.
- Zaručením preposielania šablón pri použití nespoľahlivého transportného protokolu znižuje riziko chybnnej, alebo nemožnej interpretácie exportovaných dát v zhromažďovači.
- Detekciou a znovunadviazaním prerušeného spojenia pri použití transportného protokolu TCP je zaručený bezproblémový export dát aj v sieti s vysokou mierou zlyhávania.
- Notifikáciou používateľa o činnostiach meracieho a exportovacieho procesu, ktoré by mohli viesť k poklesu spoľahlivosti nástroja.
- Jasná definícia postupu pri vyčerpaní systémových prostriedkov (preplnenie pamäte tokov, atď.) bola pevne zapracovaná do zdrojového kódu.

Synchronizácia vnútorného času meracieho a exportovacieho procesu s presným časom bola zabezpečená pomocou volaní operačného systému. V podstate v tomto smere nedošlo po implementačnej stránke k výraznému posunu. Bola však upravená presnosť odčítavania systémového času, keďže IPFIX štandard vyžaduje odčítavanie časových značiek s presnosťou na nanosekundy. Táto požiadavka bola novou implementáciou splnená.

Zhromažďovací proces, ako časť architektúry BasicMeter je úzko spojený s exportovacím procesom na strane IPFIX zariadenia. Preto je pre spoľahlivú funkčnosť všetkých implementovaných zmien v meracom a exportovacom procese potrebná podobná analýza konformity so spomínanými štandardami. Ako najakútnejšia požiadavka sa javí implementácia spoľahlivého protokolu na prenos exportovaných dát v IPFIX správach.

Pri implementácii analyzovaných požiadaviek do modulu BEEM meracej architektúry BasicMeter boli použité nasledujúce nové vývojové prostriedky:

- Vývojové prostredie, ladiaci nástroj a CVS (Concurrent Version System) klient pre jazyk C, Eclipse IDE (Integrated Developing Enviroment) [4]
- C knižnica pre spracovávanie XML súborov, libXML2 [5]

Pri ďalšom vývoji architektúry BasicMeter, resp. meracieho a exportovacieho procesu v rámci IPFIX zariadenia by bolo vhodné rozšíriť spoluprácu medzi jednotlivými blokmi architektúry. Takto by sa docielila jednoduchosť používania všetkých častí bez doplňujúcich znalostí, ktoré momentálne obsluha týchto komponentov vyžaduje. V ďalšom pokračovaní zlepšovania komunikácie jednotlivých modulov je potrebné brať do úvahy primárne určenie tohoto meracieho nástroja, ktorým je vyhodnocovanie QoS parametrov počítačových sietí. V mnohých najčastejšie používaných aplikáciach takýchto meraní je tento nástroj vyhovujúci už v doterajšej implementácii. Ide predovšetkým o merania objemových parametrov. V budúcnosti by sa malo zlepšiť najmä meranie a vyhodnocovanie časových vlastností sieťovej prevádzky.

## Zoznam použitej literatúry

- [1] CAHN R., S.: *Wide Area Network Design. Concepts and Tools for Optimization* S. Francisco, California: Morgan Kaufmann Publishers Ins, 2003, 430pp.
- [2] CISCO SYSTEMS: *Cisco IOS NetFlow Overview* White Paper [online] Publikované vo februári 2006, URL: [http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/honf\\_c/ov\\_nf\\_ov.pdf](http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/honf_c/ov_nf_ov.pdf)
- [3] CLAISE, B. et al: *IPFIX: Protocol* Internet Draft [online] Publikované v apríli 2006, URL: <http://www.ietf.org/internet-drafts/draft-ietf-ipfix-protocol-21.txt>
- [4] ECLIPSE FOUNDATION: *Eclipse IDE* [online] Publikovaná v máji 2006, URL: <http://www.eclipse.org/>
- [5] GNOME PROJECT: *The XML C parser and toolkit of Gnome* [online] Publikované v marci 2005, URL: <http://xmlsoft.org/index.html>
- [6] IANA: *SMI Network Management Private Enterprise Codes* [online] Publikované 2006, URL: <http://www.iana.org/assignments/enterprise-numbers>
- [7] LEINEN, S. *IPFIX: Evaluation of Candidate Protocols for IP Flow Information Export* RFC 3955 [online] Publikované v októbri 2004, URL: <http://www.ietf.org/rfc/rfc3955.txt>
- [8] McCANNE, S. et al.: *Libpcap: library for packet capturing, v0.9.4* [online] Publikované v októbri 2005 URL: <http://www.tcpdump.org/>
- [9] MEYER, J., QUITTEK, J., BRYANT, S.: *IPFIX: Information Model* Internet Draft [online] Publikované v septembri 2005, URL: <http://www.ietf.org/internet-drafts/draft-ietf-ipfix-info-11.txt>
- [10] NTOP.ORG: *nProbe: An Extensible NetFlow v5/v9/IPFIX GPL Probe for IPv4/v6* [online] Publikované 1998-2006, URL: <http://www.ntop.org/nProbe.html>

- [11] QUITTEK, J. et al. *IPFIX: Requirements for IP Flow Information Export* RFC 3917 [online] Publikované v októbri 2004, URL: <http://www.ietf.org/rfc/rfc3917.txt>
- [12] RÉVEŠ, M.: *Implementácia exportáčného protokolu NetFlow v9 v meracom nástroji BasicMeter* Diplomová práca, Košice: KPI FEI TUKE, 2005
- [13] SADASIVAN, G. - BROWNLEE, N.: *Architecture for IP Flow Information Export* [online] Publikované v apríli 2006, URL: <http://www.ietf.org/internet-drafts/draft-ietf-ipfix-architecture-10.txt>
- [14] SCHULZRINNE, H. et al. *RTP: A Transport Protocol for Real-Time Applications* RFC 1889 [online] Publikované v januári 1996, URL: <http://www.ietf.org/rfc/rfc1889.txt>
- [15] THE SWISS EDUCATION AND RESEARCH NETWORK: *FloMA: Pointers and Software* [online] Publikované v máji 2006, URL: <http://www.switch.ch/tf-tant/floma/software.html>
- [16] TRAMMEL, B.: *YAF: Yet Another Flow sensor* [online] Publikované v marci 2006, URL: <http://aircert.sourceforge.net/yaf/>
- [17] ZSEBY, T. et al. *IPFIX: Applicability* Internet Draft [online] Publikované v máji 2006, URL: <http://www.ietf.org/internet-drafts/draft-ietf-ipfix-as-07.txt>
- [18] ZSEBY, T. et al. *PSAMP: Sampling and Filtering Techniques for IP Packet Selection* Internet Draft [online] Publikované v júli 2005, URL: <http://www.ietf.org/internet-drafts/draft-ietf-psamp-sample-tech-07.txt>

## **Zoznam príloh**

1. CD médium - diplomová práca v elektronickej podobe, prílohy v elektronickej podobe, funkčný program s dokumentáciou
2. Používateľská príručka
3. Systémová príručka
4. Zoznam obrázkov a tabuliek

## Zoznam obrázkov

3–1 Referenčný model IPFIX . . . . .	11
3–2 IPFIX zariadenie . . . . .	12
3–3 Vzorkovanie a filtrovanie . . . . .	12
3–4 Detailný pohľad na architektúru IPFIX . . . . .	16
3–5 Formát IPFIX správy . . . . .	19
3–6 Príklad IPFIX správy 1 . . . . .	20
3–7 Príklad IPFIX správy 2 . . . . .	20
3–8 Príklad IPFIX správy 3 . . . . .	20
3–9 Formát hlavičky IPFIX správy . . . . .	21
3–10Formát špecifikátora poľa . . . . .	22
3–11Formát sady . . . . .	23
3–12Hlavička sady . . . . .	23
3–13Formát šablónového záznamu . . . . .	25
3–14Hlavička šablónového záznamu . . . . .	25
3–15Príklad šablónovej sady . . . . .	26
3–16Hlavička šablónovej sady s nastavením . . . . .	27
3–17Príklad šablónovej sady s nastavením . . . . .	28
3–18Formát dátového záznamu . . . . .	28
3–19Príklad dátovej sady . . . . .	29
5–1 Architektúra nástroja BasicMeter . . . . .	41
5–2 Architektúra časti BEEM nástroja BasicMeter . . . . .	45

## Zoznam tabuliek

4–1 Prehľad techník výberu paketov . . . . .	34
--	----