

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

**Implementácia exportáčného protokolu NetFlow v9  
v meracom nástroji BasicMeter**

Vedúci diplomovej práce:  
Ing. František Jakab

Diplomant:  
Martin Révés

Konzultant diplomovej práce:  
Ing. František Jakab

Košice 2005

### **Čestné prehlásenie**

Prehlasujem, že som diplomovú prácu vypracoval samostatne s využitím uvedenej odbornej literatúry.

V Košiciach dňa 02.05.2005

.....  
*vlastnoručný podpis*

Na tomto mieste bude vložené zadanie diplomovej práce

## **Pod'akovanie**

Ďakujem Ing. Františkovi Jakobovi, členom BasicMeter tímu a členom Laboratória počítačových sietí za cenné rady, pripomienky a odbornú pomoc pri tvorbe diplomovej práce.

Názov práce : Implementácia exportačného protokolu NetFlow v9  
v meracom nástroji BasicMeter

Katedra : Katedra počítačov a informatiky, TU FEI Košice  
Autor : Martin Révész  
Vedúci DP : Ing. František Jakab  
Konzultant DP : Ing. František Jakab  
Dátum : 02.05.2005  
Kľúčové slová : kvalita služieb (QoS), tok, export informácií o tokoch,  
IPFIX, pasívne merania, počítačová sieť, internet,  
monitorovanie prevádzky, NetFlow

Anotácia : Práca je venovaná problematike exportu informácií  
o tokoch za účelom merania parametrov kvality služieb.  
Pozornosť je venovaná predovšetkým protokolu NetFlow  
v9. Súčasťou práce je aj analýza ďalších protokolov  
vyhovujúcich požiadavkám IPFIX. Riešenie pozostáva  
z návrhu a implementácie modulu pre export v protokole  
NetFlow v9.

Thesis title : NetFlow v9 export Protocol Implentation in BasicMeter Environment

Department : Department of Computers and Informatics, TU FEI Košice

Author : Martin Révés

Supervisor : Ing. František Jakab

Tutor : Ing. František Jakab

Date : 05/02/2005

Keywords : Quality of Service (QoS), flow, flow information export, IPFIX, passive measurement, computer network, internet, traffic monitoring, NetFlow

Annotation : The thesis deals with flow information export in purpose of measurement quality of service parameters. The thesis focuses mainly on the NetFlow v9 protocol. The thesis also contains analysis of other export protocols conformed to IPFIX. Solution consist of design and module implementation for export in NetFlow v9 protocol.

# Obsah

1. Formulácia úlohy.....	1
1.1 Motivácia.....	1
2. Analýza podmienok prenosu informácie.....	2
2.1 Kvalita služieb.....	2
2.2 Parametre kvality služieb.....	4
2.3 Metódy merania prevádzkových parametrov.....	5
2.4 Prenos nameraných údajov.....	6
3. Požiadavky pre export informácií o tokoch.....	9
3.1 Real Time Flow Measurement, RTFM.....	9
3.2 IP Flow Information Export, IPFIX.....	9
4. Analýza existujúcich exportných protokolov.....	15
4.1 CRANE.....	15
4.2 Diameter.....	16
4.3 LFAP.....	16
4.4 NetFlow v9.....	17
4.5 Streaming IPDR.....	17
4.6 Klasifikácia exportných protokolov.....	18
4.7 Hodnotenie zhody s IPFIX.....	21
4.8 Zhrnutie.....	25
5. Analýza exportného protokolu NetFlow verzia 9.....	26
5.1 Terminológia.....	26
5.2 Úloha exportéra.....	28
5.3 Formát paketu.....	29
5.4 Správa šablón.....	36
5.5 Úloha zhromažďovača.....	37
5.6 Bezpečnostné riziká.....	37
6. Konceptia a architektúra meracieho nástroja BasicMeter.....	39
6.1 Špecifikácia požiadaviek.....	39
6.2 Konceptia meracieho nástroja.....	39
6.3 Architektúra meracieho nástroja BasicMeter.....	41
7. Návrh exportného modulu.....	44
7.1 Analýza vstupných dát.....	45
7.2 Analýza výstupných dát.....	46
8. Experimentálne overenie funkčnosti nástroja.....	47
8.1 Inštalácia.....	47
8.2 Experimentálne meranie.....	48
8.3 Meranie prenosovej rýchlosti.....	48
8.4 Zhrnutie výsledkov experimentu.....	53
9. Zhodnotenie riešenia.....	55
10. Zoznam použitej literatúry.....	56
11. Zoznam príloh.....	59
12. Zoznam obrázkov a tabuliek.....	60



# 1. Formulácia úlohy

Diplomová práca sa zaoberá analýzou exportných protokolov za účelom ich využitia pre potreby pasívnych meraní parametrov kvality služieb v počítačových sieťach založených na protokole IP. Podstatou pasívnych meraní je využitie existujúcej prevádzky na účely merania, pričom sa vyžaduje, aby merací proces neovplyvňoval sieťovú prevádzku.

Súčasťou práce je hodnotenie existujúcich exportných protokolov podľa požiadaviek vznikajúceho štandardu pre export informácií o tokoch IPFIX[5].

Cieľom diplomovej práce je navrhnúť koncepciu modulu pre export informácií o tokoch, ako súčasť meracieho nástroja BasicMeter. Implementovaný exportný modul bude vykonávať export v protokole NetFlow verzia 9[2]. Predpokladá sa použitie nástroja v segmente vysokorýchlostných sietí (napr. 1Gb/s). Túto skutočnosť je nutné pri návrhu exportného modulu zohľadniť.

Funkčnosť implementovaného modulu vrámci celého nástroja bude otestovaná experimentálnym meraním prevádzkových parametrov siete.

## 1.1 Motivácia

Nárast záujmu o export informácií o tokoch, súvisí rastúcou potrebou monitoringu charakteristík prevádzky v počítačových sieťach. Zároveň narastá aj počet sieťovo orientovaných služieb, ktoré vyžadujú zabezpečenie kvality služieb (QoS) pozdĺž celej trasy prevádzky. Požiadavka centrálného monitorovania prevádzky v každom uzle siete podnietila vznik protokolov na prenosu informácií o tokoch. Pretože neexistoval štandard pre exportný protokol, vzniklo niekoľko proprietárnych riešení. V súčasnosti sa organizácia IETF pokúša vytvoriť univerzálny štandard pre export informácií o tokoch IPFIX. Každý z existujúcich exportných protokolov má určité výhody a nevýhody, ktoré je potrebné zohľadniť pri jeho nasadení v konkrétnych podmienkach.

Exportované informácie spracuje analyzujúca aplikácia, výstupy ktorej sú použiteľné pre ďalšie optimalizácie topológie sietí, ich profylaktiku a plánovanie ďalších rozšírení.

## 2. Analýza podmienok prenosu informácie

### 2.1 Kvalita služieb

V čase vzniku internetu boli používané najmä sieťové aplikácie akými sú elektronická pošta a prenos súborov. Tomuto charakteru prevádzky úplne postačoval model najlepšej prevádzky s minimálnym úsilím (best-effort traffic model). Transportný protokol TCP, ktorý využívajú mnohé sieťové služby, tiež vychádza z tohto modelu. Požiadavky na zabezpečenie určitej úrovne kvality služieb neboli uvažované s ohľadom na charakter spomínaných sieťových služieb. Narastajúci výkon osobných počítačov umožnil spracovanie multimédií (obrazu a zvuku) v reálnom čase. Multimediálne aplikácie pre svoju správnu a spoľahlivú činnosť potrebujú sieťovú architektúru schopnú na nižšej vrstve zabezpečiť určitý stupeň kvality prenosu.

Kvalita služieb (Quality of Service, QoS) [15] je pojem, ktorý označuje zabezpečenie potrebných prenosových vlastností pre prevádzku v sieti. Parametre kvality služieb možno merať, vylepšovať a do určitej miery aj garantovať. Záujmom je definovať tieto parametre v zmluve medzi používateľom a poskytovateľom komunikačných služieb – SLA (Service Level Agreement).

Na prvý pohľad by sa mohlo zdať, že kvalitu služieb možno zvýšiť jednoducho zväčšením šírky prenosového pásma. Toto riešenie môže skutočne priniesť úspech, no nie je dostatočne efektívne. Mnohé aplikácie ako sú prenos videa na požiadanie (Video On Demand, VoD), IP telefónia, telekomunikácie a digitálna televízia s vysokou rozlišovacou schopnosťou (High Definition TV, HDTV) vyžadujú najmä garanciu časových charakteristík, nielen šírky prenosového pásma.

K rozširovaniu záujmu o kvalitu služieb v dátových sieťach prispieva tiež konvergencia, teda zlučovanie klasických telekomunikačných a dátových sietí. Telekomunikačná prevádzka sa začína prenášať na existujúce dátové siete, ale aj naopak telekomunikačné siete v čoraz väčšej miere poskytujú prostriedky pre prenos dát. Konvergencia sietí bola sa stala jedným z najsilnejších impulzov pre vývoj technológií merania a vyhodnocovania kvality služieb v počítačových sieťach.

Garantovať kvalitu služieb medzi koncovými bodmi možno, len ak je garantovaná pre každý úsek trasy prenosu. V prípade, že je možné toto zabezpečiť,

hovoríme o manažovateľnej počítačovej sieti. O manažovateľnej sieti sa hovoriť nedá, ak dochádza len k pridelovaniu priority pre určité dátové toky na strane poskytovateľa.

V súčasnosti je vyvinutých viacero mechanizmov pre vyhodnocovanie a meranie kvality služieb. Často využívanou implementáciou bola technológia ATM (Asynchronous Transfer Mode). ATM ako spojovo-orientovaná (connection-oriented) technológia umožňuje nadviazať spojenie s už definovanou kvalitou prenosu. ATM ako technológia bola vyvinutá pre potreby telekomunikačného priemyslu a k jej nasadeniu v oblasti počítačových sietí nedošlo v očakávanom rozsahu najmä kvôli rozsahu potrebných zmien. ATM technológia už v súčasnosti nie je považovaná za perspektívnu a jej ďalší rozvoj a implementácia sa nepredpokladá.

V počítačových sieťach naberajú na význame implementácie používajúce tretiu vrstvu OSI modelu – sieťový protokol IP (Internet Protocol). Pre riešenie problému zabezpečovania kvality služieb existujú dva prístupy:

***diferencované služby*** [16]

Poskytujú škálovateľné obmedzenie služieb bez potreby stavových informácií o prenose a signalizácie pri každom prenose medzi uzlami siete. Kombinácia nastavených bitov v poli určenom pre typ služby paketu špecifikuje ako má byť paket spracovaný smerovačom.

***integrované služby***

Poskytujú diferenciaciu na základe explicitného vyjadrenia požiadaviek na kvalitu služby pomocou špeciálneho protokolu RSVP (Resource Reservation Protocol).[17]

S neúspechom technológie ATM v oblasti počítačových sietí, súvisí rozšírenie technológie MPLS (Multi-protocol Label Switching)[18]. MPLS umožňuje nasadenie zabezpečenia kvality služieb pri použití IP. Táto technológia je využiteľná najmä pri zrýchlení a zjednodušení smerovania v počítačových sieťach. Každému paketu je priradené krátke návěstie s pevnou dĺžkou a jeho účelom je zastupovať informácie obsiahnuté v hlavičke IP paketu ako ich skrátená reprezentácia. Smerovanie sa potom vykonáva na základe týchto návěstí namiesto informácií z hlavičky IP paketu. MPLS tak možno použiť aj pri zabezpečení kvality služieb najmä pri klasifikácii IP paketov.

## 2.2 Parametre kvality služieb

Kvalitu služieb predstavuje množina presne špecifikovaných parametrov s definovaným významom a spôsobom merania. Špecifikácia kvality služieb je v súčasnej dobe podložená štandardmi ako od IETF [19] tak od ITU-T [20]. Zatiaľ čo RFC2330 sa zameriava skôr na procedúry merania, tak Y.1540 popisuje štatistické vyhodnocovanie parametrov kvality služieb. Prehľad najvýznamnejších parametrov kvality služieb obsahuje tabuľka 2.1.

<i>Parameter kvality služieb</i>	<i>Popis</i>
šírka pásma [22]	parameter definovaný ako efektívne množstvo dát prenesených za jednotku času
stratovosť paketov [21]	množstvo nedoručených paketov alebo množstvo doručených, ale poškodených paketov
jednosmerné oneskorenie [19]	čas potrebný na odoslanie paketu od zdroja k cieľu
kolísanie oneskorenia [23]	parameter pre dva pakety definovaný ako rozdiel medzi hodnotou jednosmerného oneskorenia prvého paketu a hodnoty jednosmerného oneskorenia druhého paketu
spiatočné oneskorenie[24]	čas potrebný na odoslanie paketu od zdroja k cieľu, jeho prijatie v cieľi, okamžité spätné odoslanie a jeho prijatie naspäť v zdroji
priepustnosť paketov	množstvo paketov prenesených za jednotku času

**Tab. 2.1: Najvýznamnejšie parametre kvality služieb**

## 2.3 Metódy merania prevádzkových parametrov

Rozdelenie metód merania a ich krátku charakteristiku obsahuje 2.2.

<i>Typ merania</i>	<i>Popis</i>
aktívne merania (intruzívne merania)	meranie charakteristík siete a prevádzkových parametrov vykonávajú pomocou generovania testovacej prevádzky
pasívne merania	meranie charakteristík siete a prevádzkových parametrov vykonávajú pomocou už existujúcej prevádzky
semi-aktívne merania	meranie charakteristík siete a prevádzkových parametrov vykonávajú pomocou existujúcej prevádzky, ale modifikujú pakety, napríklad pridávanie časových známok a identifikátorov

**Tab. 2.2: Rozdelenie a stručná charakteristika typov meraní**

### 2.3.1 Aktívne merania

Merania charakteristík počítačovej siete založené na generovaní dodatočnej meracej prevádzky, nazývame aktívne merania. Výhodou aktívnych meraní je možnosť vykonávať ich v ľubovoľnom čase a pre ľubovoľný typ prevádzky, ktorá je predmetom merania. Aktívne merania svojim charakterom kladú zvýšené nároky na priepustnosť a výkon prvkov siete. Prenos testovacej prevádzky vždy ovplyvňuje prenos užitočnej prevádzky, čo pri nevhodne zvolenom množstve testovacej prevádzky môže viesť k ovplyvňovaniu výsledkov merania. Toto je hlavná nevýhoda aktívnych meraní.

Špecifickú skupinu merní tvoria aktívne merania bez reálnej prevádzky, možno ich využiť pri testovaní sietí, ak už existujúca prevádzka nie je vyhovujúca pre meranie. V takom prípade testovacia prevádzka nahrádza reálnu, a preto by aj mala mať vlastnosti reálnej prevádzky. Ukázalo sa, že emulácia špecifických vlastností aplikácií spôsobuje značné ťažkosti.

Aktívne merania nachádzajú použitie najmä pri plánovaní sietí pre predikciu zaťaženia siete, úpravy podmienok a parametrov v sieti.

### **2.3.2 Pasívne merania**

Pre účely merania parametrov kvality služieb sú vhodnejšie pasívne merania, pretože negenerujú dodatočnú prevádzku, ale využívajú existujúcu reálnu prevádzku. Využitie reálnej prevádzky na účely merania prináša niekoľko výhod. Prvky siete sú zaťažované len reálnou prevádzkou. Neexistuje možnosť ovplyvnenia výsledkov merania samotným meraním. Výsledky pasívnych meraní sú dobre interpretovateľné a využiteľné v praxi. Nemožno tiež identifikovať testovaciu prevádzku poskytovateľom a následne ju uprednostňovať za účelom dosiahnutia lepších výsledkov.

Charakter pasívnych meraní prináša určité nevýhody ako napríklad nemožnosť riadiť testovaciu prevádzku. Aby sa vylúčilo ovplyvnenie výsledkov priebehom merania nie je možné prenášať ani riadiace dáta. Táto skutočnosť výrazne komplikuje meranie časových charakteristík, napr. jednosmerného oneskorenia. Riešením je zabezpečiť synchronizáciu hodín v jednotlivých meracích bodoch mimo meraní sietí. Ďalším významným problémom je potreba identifikovať pakety v meracích bodoch.

### **2.3.3 Semi-aktívne merania**

Pojem semi-aktívne merania zahŕňa metódy, ktoré využívajú súčasnú prevádzku, ale pridávajú ďalšie informácie – modifikujú pakety (časová značka, identifikátor paketu). Rozsah ovplyvňovania výsledkov semi-aktívnymi meraniami nemožno vylúčiť. Ako problém tu možno vidieť nutnosť vykonávať klasifikáciu a modifikáciu v reálnom čase, čo sa prejaví oneskorením paketu v meracom bode. Výkonové nároky na merací bod sú vyššie ako u predchádzajúcich typov meraní. Semi-aktívne merania možno jednoducho využiť na meranie časových charakteristík pomocou viacerých meracích bodov.

## **2.4 Prenos nameraných údajov**

Ak meranie vyžaduje použitie viacerých meracích bodov, je potrebné prenášať namerané a vygenerované údaje do zberného bodu. Zberným bodom môže byť aj jeden z meracích bodov, čím sa zredukuje množstvo prenášaných dát a spojení meracím bodom.

Spôsobov ako preniesť namerané a vygenerované dáta je viacero:

- prenos údajov v meraných paketoch
- prenos údajov v okruhu – údaje sú prenášané tou istou cestou ako prevádzka, z ktorej boli získané
- prenos údajov mimo okruh – údaje sú prenášané inou cestou ako prevádzka, z ktorej boli získané

#### **2.4.1 Prenos údajov v meraných paketoch**

Tento spôsob prenosu údajov vyžaduje modifikáciu paketov, čo je charakteristické pre semi-aktívne merania. Výhodou je možnosť umiestniť zberný bod do jedného z meracích bodov. Ostatné výhody a nevýhody vyplývajú z charakteru semi-aktívnych meraní.

#### **2.4.2 Prenos údajov v okruhu**

Ak sú namerané a vygenerované údaje prenášané tou istou cestou ako prevádzka, z ktorej sú získavané, hovoríme o prenose údajov v okruhu. To však vedie k podobným problémom aké vznikajú pri aktívnych meraniach. Merania, pri ktorých sú údaje prenášané takýmto spôsobom nemožno považovať za aktívne, pretože odosielanie výsledkov sa nedá stotožniť s generovaním testovacej prevádzky. Ovplyvňovanie nameraných hodnôt prenosom výsledkov merania však nemožno vylúčiť. Typ a časový rámec pre testovaciu prevádzku aktívnych meraní sú predpísané na základe úlohy merania, naproti tomu odosielanie výsledkov merania môže byť riadené inými prostriedkami ako testovacia prevádzka.

Nepriaznivý vplyv prenosu výsledkov je možné eliminovať priradením nižšej priority tejto prevádzke alebo prenos len cestami, ktoré nie sú zaťažené. Použitie jednej z alternatív závisí od povahy meranej charakteristiky.

#### **2.4.3 Prenos údajov mimo okruh**

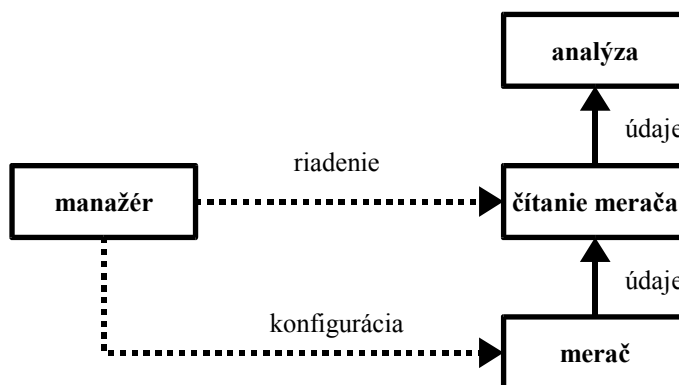
Prenos údajov mimo okruhu vyžaduje existenciu oddelenej cesty pre prenos nameraných a vygenerovaných údajov. Oddelenie ciest môže byť dosiahnuté napríklad pridaním ďalšieho sieťového rozhrania na meracie body a vytvorením oddelenej meracej siete. Tento spôsob neovplyvňuje reálnu prevádzku, ale vyžaduje prídavné

kapacity siete, s ktorými je nutné uvažovať už pri jej návrhu. Pre pasívne merania je tento spôsob prenosu odporúčaný.

### 3. Požiadavky pre export informácií o tokoch

#### 3.1 Real Time Flow Measurement, RTFM

Odporúčanie pre meranie dátových tokov v reálnom čase poskytuje všeobecný rámec pre opis a meranie toku prevádzky v sieti v reálnom čase. Architektúra merania dátových tokov je znázornená na obrázku 3.1[25]. Ako protokol na komunikáciu medzi jednotlivými komponentami slúži jednoduchý protokol pre správu siete (Simple Network Management Protocol, SNMP). Základom architektúry sú komponenty nazývané merače. Ich úlohou je odchyť a meranie objemu prevádzky. Hodnoty získané čítacími procesmi sú posielané analyzujúcej aplikácii. Manažér pravidiel udržiava pravidlá pre výber hodnôt a umožňuje definovať nové pravidlá pre meranie dátových tokov.



Obr. 3.1: Architektúra RTFM

#### 3.2 IP Flow Information Export, IPFIX

Export informácií o tokoch z internetového protokolu (IP Flow Information Export)[7] je pripravovaný štandard pre detailné meranie a získavanie informácií o tokoch v počítačových sieťach.

Základným pojmom v špecifikácii IPFIX je pojem tok (flow). Definícií toku existuje niekoľko, pre účely tohto štandardu je použitá nasledujúca definícia.

Pod pojmom tok (flow) sa rozumie množina IP paketov prechádzajúcich pozorovacím bodom v sieti počas určitého časového intervalu. Všetky pakety patriace

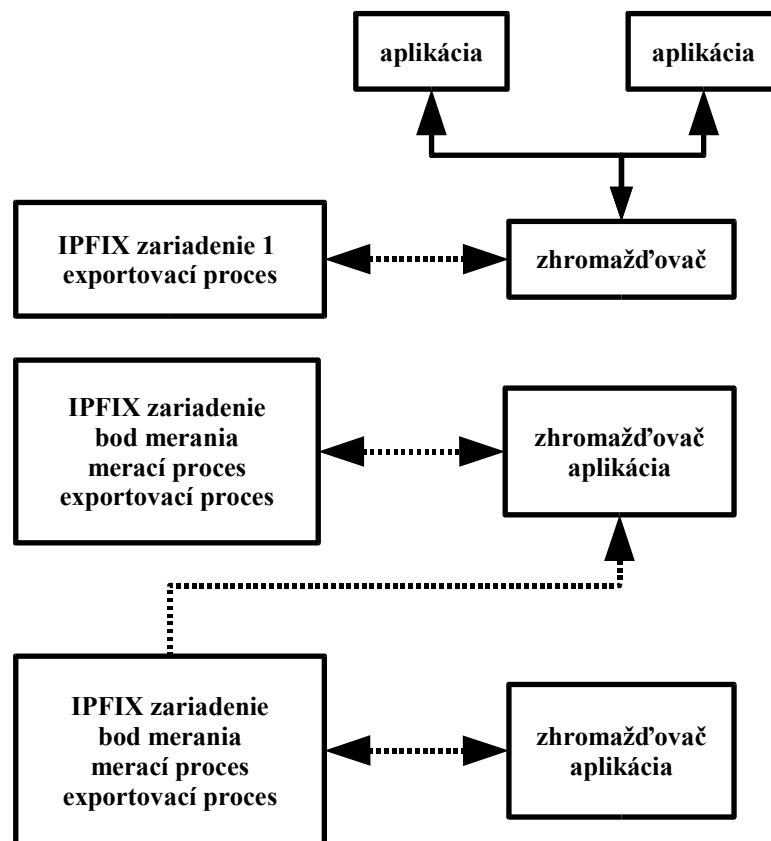
do jedného toku majú spoločnú množinu vlastností. Každá vlastnosť je definovaná ako výsledok funkcie aplikovanej na niektorú z častí paketu.

Takýmito časťami môžu byť:

- jedna alebo viac položiek hlavičky paketu (napr. cieľová IP adresa), jedna alebo viac položiek hlavičky transportného protokolu (napr. zdrojový port) alebo položky hlavičky aplikačného protokolu
- charakteristika samotného paketu (napr. počet MPLS návěstí)
- jeden alebo viac polí odvodených zo zaobchádzania s paketom (IP adresa nasledujúceho smerovača, výstupné sieťové rozhranie)

Paket patrí do toku, ak spĺňa všetky podmienky definované vlastnosťami.

Informácie o tokoch sú využiteľné pri plánovaní siete, návrhu prevádzky, plánovaní rozšírenia siete a výkonnostnom vylepšovaní jednotlivých prvkov siete. Taktiež možno tieto informácie použiť účtovaní podľa prenesených dát alebo podľa jednotlivých zákazníkov. Pre tieto aplikačné oblasti boli vypracované požiadavky návrhu architektúry IPFIX. Schéma architektúry IPFIX je na 3.2 .



Obr. 3.2: Blokovaná schéma architektúry IPFIX

### 3.2.1 Bod merania

Miesto v sieti, kde môžu byť pakety sledované sa nazýva bod merania. Môže to byť linka pripojená k IPFIX zariadeniu, zdieľané médium (Ethernet segment), port na smerovači a jedno alebo viac rozhraní smerovača.

### 3.2.2 Merací proces

Úlohou meracieho procesu je generovať záznamy tokov (flow records). Vstup do meracieho procesu tvoria hlavičky paketov získané v bode merania a hodnoty odvodené zo zaobchádzania s paketmi (výstupné rozhranie). Merací proces vykonáva niekoľko činností:

- spracovanie hlavičky
- generovanie časových známk
- vzorkovanie
- klasifikácia
- spracovanie záznamov tokov

Spracovanie záznamov tokov znamená vytváranie nových záznamov, zmenu existujúcich záznamov, detekovanie ukončenia platnosti toku, odosielanie záznamov tokov do exportovacieho procesu a odstraňovanie záznamov ukončených tokov.

Požiadavky definované na merací proces:

#### ***Spoločnosť***

Merací proces musí byť spoločnosť. To znamená, že pri danej konfigurácii bude schopný odchytiť všetky pakety prechádzajúce bodom merania. V prípade preťaženia musí byť merací bod schopný túto nespoločnosť zistiť a definovaným spôsobom aj oznámiť.

#### ***Vzorkovanie***

Vzorkovanie je všeobecne definované ako systematický alebo náhodný výber podmnožiny elementov (vzorka) z množiny všetkých elementov (rodičovská populácia). Ak je vzorkovanie podporované, potom musí byť jednoznačne definovaná vzorkovacia metóda a potrebné parametre vzorkovania. Ak nastane zmena v konfigurácii vzorkovania počas meracieho procesu, všetky zhromažďovacie procesy musia byť informované o tejto zmene. Súčasne musia byť odlišiteľné záznamy tokov vytvorené pri použití rôznych konfigurácií vzorkovania. Zmena konfigurácie vzorkovania znamená

odobratie vzorkovacej funkcie, pridanie novej vzorkovacej funkcie, zmenu parametrov a zmenu vzorkovacej metódy.

### ***Správanie sa pri preťažení***

Preťaženie môže nastať z dôvodu nedostatku pamäte alebo nedostatku výpočtovej kapacity. Merací proces by mal zareagovať na túto situáciu zavedením opatrenia pre zníženie náročnosti.

Možné reakcie na nedostatok zdrojov:

- zníženie počtu meraných tokov. Toto je možné dosiahnuť zvýšením granularity meracieho procesu alebo znížením počtu sledovaných tokov na podmnožinu z pôvodnej množiny sledovaných tokov
- nasadiť vzorkovanie skôr ako sú pakety spracovávané meracím procesom, ak sa už vzorkovanie vykonáva, tak znížiť vzorkovaciu frekvenciu
- zastaviť meranie
- znížiť zaťaženie ostatnými procesmi

Správanie sa pri preťažení nie je obmedzené len na uvedené spôsoby, no v prípade vzniku preťaženia musí byť jednoznačne definované. Podmienkou pre nasadenie, prípadne zmenu, vzorkovania je oddelenie záznamov tokov vytvorených rôznymi vzorkovacími konfiguráciami. To znamená, ukončiť všetky toky vzniknuté pred zmenou a začať vytvárať nové, čo však bude dočasne viesť naopak k zvýšeniu náročnosti na systém.

### ***Časové známky***

Časové známky musia byť generované k prvému a poslednému pozorovanému paketu toku.

### ***Synchronizácia času***

Generované časové známky musia byť synchronizované s univerzálnym koordinovaným časom (UTC).

### ***Expirácia tokov***

Merací proces musí byť schopný detekovať expiráciu tokov. Tok sa považuje za expirovaný, ak v danom časovom intervale nebol pozorovaný žiadny paket patriaci do daného toku. Merací proces môže podporovať mechanizmy pre detekciu expirácie pred vypršaním časového limitu pomocou sledovania príznakov príslušného protokolu (TCP FIN, TCP RST).

### 3.2.3 Exportovací proces

Záznamy tokov generované jedným alebo viacerými meracími procesmi odosiela exportovací proces na jeden alebo viac zhromažďovacích procesov. Pre každý meraný tok je definovaná množina atribútov, ktoré exportovací proces musí poskytovať:

- číslo verzie internetového protokolu
- zdrojová IP adresa
- cieľová IP adresa
- typ IP protokolu (TCP, UDP, ICMP,...)
- v prípade protokolu TCP alebo UDP – zdrojový port
- v prípade protokolu TCP alebo UDP – cieľový port
- počítadlo paketov
- počítadlo bajtov
- slabika typu služby (Type of Service, ToS)
- v prípade IP verzie 6 – návestie toku
- v prípade podpory špeciálnych multiprotokolových návestí (MPLS) – prvé návestie
- časová známka prvého paketu
- časová známka posledného paketu
- jednoznačný identifikátor bodu merania
- jednoznačný identifikátor exportovacieho procesu

### 3.2.4 Zhromažďovací proces

Zhromažďovací proces prijíma záznamy tokov od jedného alebo viacerých exportovacích procesov. Zhromažďovací proces môže vykonávať ďalšie spracovanie záznamov tokov ako napríklad agregáciu viacerých záznamov do jedného. Úlohou zhromažďovacieho procesu je ukladanie informácií o tokoch a poskytovanie týchto informácií aplikáciám.

### 3.2.5 Všeobecné požiadavky

Architektúra IPFIX pre svoje implementácie definuje všeobecné požiadavky, ktoré by mali byť dodržané. Prehľad všeobecných požiadaviek je v tabuľke 3.1.

---

<i>Požiadavka</i>	<i>Popis</i>
otvorenosť	implementácie špecifikácie IPFIX by mali byť otvorené voči novým technológiám. To predstavuje najmä otvorenosť v konfigurácii meracieho a exportovacieho procesu.
škálovateľnosť	musí byť podporovaná možnosť získavať toky zo stoviek rôznych exportovacích procesov
viac zhromažďovacích procesov	exportovací proces môže podporovať export na viac zhromažďovacích procesov a zároveň v prípade tejto podpory musí zaistiť jednoznačnú identifikáciu tokov, tak aby bolo možné detekovať a odstraňovať duplicitné toky

**Tab. 3.1: Všeobecné požiadavky architektúry IPFIX**

## 4. Analýza existujúcich exportných protokolov

Vzhľadom na to, že oblasť merania parametrov kvality služieb je relatívne nová, nebol doposiaľ definovaný štandard pre exportný protokol. Z tohto dôvodu budú do analýzy zahrnuté protokoly využívané v jednotlivých meracích nástrojoch ako aj návrhy štandardov a odporúčaní.

### 4.1 CRANE

Skratka CRANE[27] vznikla odvodením z anglického Common Reliable Accounting for Network Element Protocol. Tento protokol bol vyvinutý v XACCT Technologies Inc. za účelom prenosu informácií slúžiacich na účtovanie (accounting) v sieťach.

Exportná časť je označovaná ako CRANE klient, obdobne zhromažďovaciu časť tvorí CRANE server. Spojenie je inicializované serverom. Klient môže mať niekoľko spojení na rôzne servery kvôli vyššej robustnosti. Každý server má priradenú určitú prioritu. Klient vykonáva export len na dostupný server s najvyššou prioritou. Nosným protokolom prenosu informácií o tokoch je TCP, prípadne SCTP[28]. Potvrdzovanie úspešného prijatia správy sa vykonáva aj na úrovni aplikačnej vrstvy. Autentifikácia komunikujúcich strán sa môže vykonať na úrovni nižšej vrstvy, pomocou mechanizmov ako sú IPsec alebo TLS.

Protokol je obojsmerný počas celého prenosu, pričom sa rozlišuje 20 rôznych typov správ. Na potvrdzovanie a signalizáciu stavov je definovaný zvláštny protokol cez UDP.

Kódovanie prenášaných dát je založené na šablónach, ktoré sú kľúčom k reprezentácii záznamov dát. Klient posiela šablóny serveru a ten môže voliť položky, ktoré považuje za zaujímavé. Ak server položku nevybral, nebude ju klient exportovať. Dátové záznamy obsahujú odkazy na šablóny a konfigurované položky. Tiež môžu niesť sekvenčné čísla, aby sa zabezpečila detekcia duplicitných dátových záznamov v prípade poruchových stavov. Ak klient úmyselne vysiela duplikát, nastaví príslušný bit na odlišenie originálu od duplikátu. Kódovanie samotných prenášaných záznamov je veľmi kompaktné. Klient môže použiť veľký endián alebo malý endián. Celkovo je

definovaných 18 typov fixnej dĺžky, ako aj 5 typov premenlivej dĺžky (reťazcov) a čisto binárne dátové typy.

## 4.2 Diameter

Diameter je ďalším vývojovým stupňom protokolu RADIUS (Remote Authentication Dial In User Service). RADIUS sa stal rozšíreným prostriedkom na zabezpečenie autentifikácie v prostrediach voľného prístupu (dialup, wireless). Diameter je zovšeobecnený a rozšíriteľný protokol za účelom podpory autentifikácie, autorizácie a účtovania (AAA) v rôznych aplikáciách[29].

Komunikácia prebieha v režime peer-to-peer. Riadenie sa vykonáva pomocou štrnástich príkazov, organizovaných ako sedem párových príkazov požiadavka/odpoveď. Zahrnutá je aj podpora potvrdzovania a oznamovania chýb. Preferovaným nosným protokolom je SCTP, ale je možné využiť aj TCP. Autentifikácia a kryptovanie zabezpečuje IPsec alebo TLS. Tento protokol bol navrhnutý s ohľadom na potrebu zvýšenia bezpečnosti (end-to-end security).

Dáta sú prenášané vo forme párov atribút/hodnota. Každý pár pozostáva z osem bajtovej hlavičky a priestoru pre dáta rôznych typov. Okrem veľkého množstva preddefinovaných typov, možno definovať ďalšie nové typy na reprezentáciu informácií o toku.

## 4.3 LFAP

Pôvodný názov LFAP znamenal odľahčený protokol pre prijímanie tokov (Lightweight Flow Admission Protocol). Bol používaný na flow-based routeroch a tiež za účelom poskytovania štatistík o tokoch. Neskoršie verzie opustili prijímaciu funkciu, čo sa prejavilo aj v názve protokolu: Lightweight Flow Accounting Protocol[30].

Úlohu exportéra plní CCE (Connection Control Entity), kolektor je označovaný ako FAS (Flow Accounting Server). Komunikácia prebieha pomocou protokolu TCP s použitím trinástich typov správ slúžiacich na správu spojenia, potvrdzovanie verzií, prenos informácií o tokoch a administratívnych požiadaviek. Autentifikáciu a kryptovanie zabezpečujú nižšie vrstvy použitím IPsec alebo TLS. Navyše samotný LFAP podporuje štyri úrovne bezpečnosti využitím HMAC-MD5 autentifikácie a DES-CBC kryptovania.

Pre LFAP sú charakteristické dva typy správ informácií o tokoch. Správa typu FAR (Flow Accounting Request) sa pošle, akonáhle je identifikovaný nový tok. Informácie súvisiace s účtovaním prenášajú správy typu FUN (Flow Update Notification). Väzbu medzi týmito typmi správ zabezpečuje Flow ID.

Informácie o tokoch sú prenášané vo formáte typ/dĺžka/hodnota, kde veľkosť každého z políček typ a dĺžka je dva bajty.

#### **4.4 NetFlow v9**

Spoločnosť Cisco vytvorila protokol NetFlow v9 pre účely exportu informácií o tokoch zo svojich smerovačov. NetFlow v9 je nástupcom protokolu NetFlow v5[2].

NetFlow používa veľmi jednoduchý protokol, kde exportér posiela „FlowSety“ šablón, volieb a dát zhromažďovaču (collector). FlowSet je definovaný ako postupnosť údajových záznamov podobného formátu. Prenos medzi exportérom a zhromažďovačom sa realizuje protokolom UDP, čo je výhodné vďaka jednoduchej jednosmernej komunikácii. Ak sa vyžaduje spoľahlivosť prenosu, je možné UDP[26] pakety zapuzdriť do protokolu SCTP[28] alebo TCP. Výhodou zapuzdrenia je schopnosť prenášať jedným SCTP spojením viacero UDP spojení. Inicializáciu spojenia vykonáva exportér.

Formát prenášaných dát je definovaný šablónou, ktorá určuje typ a veľkosť každej položky.

#### **4.5 Streaming IPDR**

Internet Protocol Detail Record Organization vytvorila Streaming IPDR[31] ako aplikáciu pre Network Data Management-Usage (NDM-U). Používaná terminológia je podobná protokolu CRANE, prvky systému sú Service Elements (SEs), Mediation systems a Business Support Systems (BSS).

Komunikácia prebieha jednosmerne pomocou protokolu TCP, pričom sa rozlišuje mód Trivial TCP Delivery a mód Acknowledged TCP Delivery (tiež Reliable Streaming). Mód Reliable Streaming zvyšuje spoľahlivosť použitím dodatočného potvrdzovania na úrovni aplikačnej vrstvy. Spojenie inicializuje exportér, vyslaním hlavičky nasledovanej popisom záznamov. Neskôr sú vysielané záznamy Usage Event

korešpondujúce s predchádzajúcim popisom až do ukončenia spojenia. Kedykoľvek môže byť vyslaný nový popis záznamov. Každá správa nesie poradové číslo, aby bolo možné odstrániť prípadné duplikáty.

Štruktúra prenášaných dát je založená na modelovacej technike vychádzajúcej z XML[1]. Okrem reprezentácie dát pomocou XML, využíva ešte externú dátovú reprezentáciu (XDR). XDR je vytvárané z Sun's Remote Procedure Call a Network File System protokolov. Výhodou je priestorová efektivita ako aj efektivita spracovania.

## **4.6 Klasifikácia exportných protokolov**

Každý z vymenovaných exportných protokolov má svoje špecifické vlastnosti, ktoré ho odlišujú od ostatných a umožňujú mu lepšie zvládať niektoré situácie. Preto je pre klasifikáciu výhodné zlúčiť protokoly do skupín na základe podobných vlastností pri sledovaní určitej charakteristiky.

### **4.6.1 Návrhové ciele**

Na základe tejto charakteristiky nemožno vytvoriť hodnotenie exportných protokolov, no je možné ich rozdeliť do skupín na základe cieľov, ktoré boli sledované pri ich návrhu. To umožní poukázať na výhody jednotlivých dizajnov.

#### ***Výkonné merania tokov***

Do tejto skupiny patria: NetFlow v9 a LFAP. NetFlow v9 protokol je príkladom úzkej špecializácie za účelom vykonávania meraní vysokorýchlostných tokov priamo na smerovačoch. Zatiaľ čo NetFlow v9 slúži na export informácií zo smerovačov nezávislých na tokoch, LFAP je určený práve pre smerovače závislé na tokoch. Ďalej LFAP zaručuje vysokú spoľahlivosť a relatívne nízke nároky na pamäť exportéra. V prípade veľkého počtu krátkotrvajúcich tokov, môže byť počet exportovaných správ značne vyšší ako pri NetFlow v9.

#### ***Viac účelové účtovanie***

Do tejto skupiny patria: Streaming IPDR a CRANE. Tieto protokoly sa vyznačujú spoľahlivým prenosom účtovacích informácií medzi sieťovými prvkami a sprostredkovacím systémom alebo BSS. Boli vytvorené ako reakcia na problematiku účtovania v tradičných vertikálne integrovaných telekomunikáciách. Obidva protokoly disponujú rozšíriteľnosťou pre rôzne úlohy v účtovaní. IPDR je založené na NDM-U,

ktoré využíva XML schému pre špecifikáciu dátových štruktúr pre potreby účtovania, kým samotný prenos dát je efektívne kódovaný pomocou XDR. CRANE prenášané dáta popisuje pomocou šablón, ktoré si exportér a zhromažďovač vymieňajú v priebehu samotného prenosu.

#### ***Pre všeobecné použitie so zameraním na AAA***

Diameter je jediným predstaviteľom tejto skupiny. Tento protokol má možnosť širokého uplatnenia, pričom poskytuje autentifikáciu, autorizáciu a účtovanie (AAA). Čo vedie k jeho silnej bezpečnosti a spoľahlivosti.

#### **4.6.2 Reprezentácia dát**

Špecifikácia IPFIX uvažuje export detailných údajov o vysokorýchlostných tokoch s uplatnením na vysokorýchlostných smerovačoch. Z tohto dôvodu je užitočné preskúmať výhody a efektívnosť dátovej reprezentácie jednotlivých protokolov. Rovnako je dôležitá aj možnosť rozšíriteľnosti dátového modelu. Cieľom efektivity je minimalizácia exportného dátového toku, a tiež minimalizácia potrebnej rézie na kódovanie informácií na strane exportéra. Réžia potrebná na dekódovanie správy na strane zhromažďovača sa považuje za menej kritickú. To podporuje aj predpoklad: všeobecne, ak je zakódovanie jednoduché, tak pravdepodobne bude jednoduché aj dekódovanie.

#### ***Externe definované kódovanie dát***

Túto skupinu tvoria protokoly CRANE, IPDR a NetFlow v9. Mechanizmy, ktoré definujú formát kódovaných dát sú definované externe. Narozdiel od CRANE a NetFlow v9, kde je týmto mechanizmom šablóna, IPDR používa XML alebo XDR. Plne externý popis formátu dát umožňuje veľmi kompaktné kódovanie, kde dátová položka zaberá len priestor odpovedajúci jej informačnej hodnote. Formát XDR, ktorý používa IPDR požaduje, aby väčšie položky boli zaokrúhlené na 32 bitov, čo umožňuje znížiť náročnosť spracovania, ako na strane exportéra, tak aj na strane zhromažďovača. Väčšina protokolov pracuje s dátami v sieťovom formáte (big-endian). CRANE je jediný protokol, ktorý umožňuje voliť formát prenášaných dát v závislosti na architektúre exportéra.

#### ***Čiastočne vnútorne definované kódovanie dát***

Do tejto skupiny patrí Diameter a LFAP, pretože používajú kódovanie vo formáte typ/dĺžka/hodnota. Takáto organizácia umožňuje dekódovať jednotlivé položky

správy, ale nedekóduje ich kontext (informáciu). Výhodou je ľahšie ladenie, avšak na úkor potreby väčšej kapacity prenosovej cesty. LFAP použitím multi-záznamového kódovania dosahuje efektívnosť blízku externe definovanému kódovaniu dát, pri zachovaní podpory diagnostických nástrojov.

#### **4.6.3 Charakter komunikácie**

Charakter komunikácie je kritériom na hodnotenie protokolov podľa povahy výmeny správ medzi exportérom a zhromažďovačom.

##### ***Prevažne jednosmerné protokoly***

Patria sem protokoly IPDR a NetFlow v9, pretože tok dát prebieha od exportéra k zhromažďovaču. Smerom od zhromažďovača k exportéru sa prenášajú iba potvrdenia. Po vytvorení spojenia sú prenesené popisy dát (šablóny), potom sa prenášajú samotné dáta založené na predchádzajúcich popisoch. Okrem toho NetFlow v9 prenáša meta-dáta o stave meraciaho a exportného procesu. Na popis meta-dát slúži šablóna volieb (option template). IPDR prenos meta-dát osobitne nedefinuje, ak je potrebné ich prenášať môžu byť dodefinované.

##### ***Obojsmerné protokoly***

Túto skupinu protokolov tvoria CRANE a LFAP. Správy posielané smerom od exportéra k zhromažďovaču prenášajú prevažne informácie o tokoch. Opačný smer slúži protokolu CRANE na prenos exportérom vyžiadaných šablón ako aj neskorších zmien v šablónach. Protokol LFAP v počiatočnej fáze vykonáva overovanie verzie a ďalších dát oboch strán. Následne exportér posiela správy FAR a FUN. Zhromažďovač posiela administratívne správy AR, na ktoré exportér odpovedá správami ARA. Administratívne správy AR slúžia na získanie informácií o konkrétnom aktívnom toku, prípadne na vyžiadanie ďalších informačných elementov od exportéra.

##### ***Jednosmerné po overení***

Do tejto skupiny sa svojou povahou radí protokol Diameter. Obojsmerná prevádzka slúži na overenie autenticity komunikujúcich strán. Po overení je už prevádzka prevažne jednosmerná. Exportér posiela požiadavky na zaúčtovanie toku (ACR) a následne dostáva odpovede (ACA) od zhromažďovača.

## 4.7 Hodnotenie zhody s IPFIX

Požiadavky pre IPFIX, tak ako sú definované v RFC3917[2], sa netýkajú len samotného exportného protokolu, ale kladú podmienky aj pre merací mechanizmus, ktorý predáva dáta exportéru. Dôvodom sú informácie o stave meracieho procesu potrebné pre zhromažďovací proces. Aj tieto informácie musia byť prenášané exportným protokolom.

### 4.7.1 Spôľahlivosť merania

Protokoly CRANE, Diameter, IPDR uvažujú merací proces ako spoľahlivý, a preto neriešia prípadnú nespoľahlivosť. Obdobne aj NetFlow v9 predpokladá merací proces so zaručenou spoľahlivosťou. Jedine LFAP uvažuje možnosť straty dát v priebehu merania. Exportér vytvára štatistiky a poskytuje ich zhromažďovačom, ktoré tak môžu odhadnúť nie len množstvo stratených dát, ale aj množstvo nezaúčtovaných dát. Vo všeobecnosti je nereálne uvažovať totálnu spoľahlivosť. Problematické sú najmä prípady, kedy aj malý paket vytvorí nový tok. Vtedy môže agresívny port scan spôsobiť pretečenie tabuliek alebo vyčerpaniu dostupnej pamäte. V niektorých situáciách môžu byť dáta strácané aj samotným exportérom, kolektorom alebo pri prenose medzi nimi. Stratu dát tiež vyvolá aktivácia vzorkovania, prípadne zväčšenie vzorkovacieho intervalu, to sa však považuje za príliš malú chybu na konečných hodnotách. Jedine LFAP uvažuje takéto poruchy.

### 4.7.2 Vzorkovanie

Vzorkovanie neuvažujú protokoly CRANE a IPDR, pretože sú zamerané na účtovanie, kde je vzorkovanie uvažované ako nezmyselné. Neschopnosť vzorkovať, obmedzuje pôsobnosť týchto protokolov v aplikáciách s vysokou agregáciou, kde sa nevyžaduje absolútna presnosť. To zahŕňa aplikácie, ako sú profilácia prevádzky, návrh prevádzky a detekcia útokov v širokom rozsahu.

Diameter vzorkovanie podporuje, chýbajú mu však mechanizmy ako oznamovať aktuálne parametre vzorkovania zhromažďovaču.

LFAP momentálne nepodporuje vzorkovanie, ale uvažuje sa s pridaním jeho podpory.

NetFlow v9 vzorkovanie podporuje a bolo implementované už v predchádzajúcej verzii. Na prenos parametrov vzorkovania slúžia voľby.

#### **4.7.3 Správanie sa pri preťažení**

Požaduje sa, aby merací proces bol schopný zareagovať na stav preťaženia, napríklad nasadením vzorkovania alebo znížením vzorkovacej frekvencie, prípadne zmenou definície toku, tak aby sa znížilo zaťaženie spôsobené spracovaním paketov.

LFAP a NetFlow v9 riešia preťaženie zavedením jednoduchých odľahčujúcich metód, ktoré nespôsobia ukončenie všetkých tokov. NetFlow v9 umožňuje vykonať expiráciu tokov so starými šablónami a zavádzanie nových tokov pre nové šablóny. Toto však môže spôsobiť špičkový nárast zaťaženia, čo je v stave preťaženia nevhodné.

Protokoly CRANE, Diameter a IPDR neumožňujú zavedenie mechanizmov pre odľahčenie meracieho systému.

#### **4.7.4 Časové známky**

Všetky protokoly podporujú časové známky s definovanou (1 centisekunda) alebo vyššou presnosťou.

#### **4.7.5 Synchronizácia času**

Časové známky v protokole NetFlow v9 sú relatívne, základ tvorí doba behu exportéra (sysUpTime). Pre aplikácie, ktoré vyžadujú absolútne časy, sa musí základ relatívneho času synchronizovať s absolútnym časom. V hlavičke každého NetFlow v9 exportného paketu je položka obsahujúca čas od začiatku Unixovej epochy (1.1.1970 00:00:00), táto sa však nedá použiť na synchronizáciu s UTC, pretože má nedostatočné 1-sekundové rozlíšenie.

Ostatné protokoly používajú relatívne časové známky odvodené od daného referenčného času.

#### **4.7.6 Expirácia toku**

Podľa súčasných špecifikácií protokolov, žiadny neexportuje informáciu o dôvode ukončenia toku, ale každý umožňuje rozšírenie o túto položku.

#### **4.7.7 Informačný model**

Všetky exportné protokoly majú informačné modely, umožňujúce reprezentovať každý z atribútov požadovaných IPFIX. Diameter presne nedefinuje mapovanie IPFIX atribútov.

#### **4.7.8 Dátový model**

Každý z uvedených protokolov definuje dátový model umožňujúci určitý stupeň rozšíriteľnosti.

CRANE používa kľúče (keys), ako špecifikáciu položiek šablóny. Špecifikácia kľúča pozostáva z jeho popisu a typu. Rozšíriteľnosť je umožnená definovaním kľúča odvodeného zo základného typu. Každý kľúč ma priradený 32 bitový identifikátor.

Diameter definuje 32 bitový identifikátor (AVP kód) pre každý pár atribút/hodnota. Pomocou špeciálneho kódu identifikujúceho výrobcu môžu byť definované ďalšie AVP kódy, spracovávané len zariadeniami od rovnakého výrobcu.

IPDR vďaka reprezentácii dát odvodenej z XML schémy, disponuje vysokým stupňom rozšíriteľnosti.

V protokole LFAP je tok atribútov definovaný ako informačné elementy. Informačným elementom je priradený 16 bitový kód typu. Jeden kód je rezervovaný pre rozšírenia definované výrobcom, pričom každé je identifikované prídavným podtypom.

NetFlow v9 určuje typ dátového záznamu pomocou 16 bitového kódu zapísaného v príslušnej šablóne. Okrem typu je možné definovať aj veľkosť záznamu s rozlíšením 1 byte.

#### **4.7.9 Prenos dát**

##### ***Odolnosť voči zahĺteniu***

Všetky protokoly s výnimkou NetFlow v9 využívajú jedno TCP alebo SCTP spojenie a tak získavajú ich vlastnú odolnosť voči zahĺteniu. NetFlow v9 používa transportný protokol UDP, ale takým spôsobom, aby ostal nezávislý od implementácie transportnej vrstvy. To umožňuje jednoducho pretransformovať správy z UDP na SCTP.

##### ***Spôľahlivosť***

Podmienkou pre spoľahlivosť je schopnosť indikovať stratu správy na strane zhromažďovača. Ak došlo k strate viacerých správ musí byť známy ich počet. Vyžaduje sa, aby protokol bol rozšíriteľný z hľadiska spoľahlivosti.

Spôľahlivosť protokolov CRANE, Diameter a IPDR je veľmi vysoká, až takmer absolútna. Potreba tak vysokého stupňa spoľahlivosti je daná ich použitím v účtovaní. Všetky tri protokoly vykonávajú potvrdzovanie na úrovni aplikačnej vrstvy. Strata exportovaných dát je neprirodzeným javom, pretože sa vynakladá veľké úsilie, aby nikdy nebola stratená ani jedna správa.

LFAP taktiež využíva potvrdzovanie na úrovni aplikačnej vrstvy, naviac vysieľa rozsiahle štatistiky o stratených tokoch a množstve dát, ktoré nemôžu byť zaúčtované. Takáto koncepcia predstavuje strednú cestu medzi spoľahlivosťou a výkonom ostatných úloh (smerovanie paketov). Tento protokol sa najlepšie vysporiadava so stratou paketov.

NetFlow v9 je jediný protokol, ktorý spoľahlivosť prenosu rieši dodatočne zapuzdrením správ do protokolu SCTP a ako jediný nepoužíva potvrdzovanie na úrovni aplikačnej vrstvy. Na druhej strane NetFlow v9 ponúka veľmi jednoduchý a efektívny protokol, čím môže dosiahnuť vyššiu spoľahlivosť, ako iné protokoly pri rovnakom množstve výpočtových a prenosových zdrojov.

### ***Bezpečnosť***

Všetky protokoly podporujú použitie bezpečnostných mechanizmov nižších vrstiev akými sú IPsec a TLS. Jediné NetFlow v9 cez UDP neumožňuje použiť TLS. V aplikáciách uvažovaných odporúčaním IPFIX poskytuje IPsec aj TLS dostatočné zabezpečenie pred odcudzením dát alebo podvrhnutím falošných dát. Protokol Diameter ako jediný protokol neprístupuje k mechanizmom v TLS a IPsec s absolútnou dôverou. Uvažuje použitie len IPsec alebo len TLS, pričom zavádza zabezpečenie na úrovni aplikačnej vrstvy. LFAP tiež umožňuje zabezpečenie na úrovni vyšších vrstiev. Poskytuje štyri stupne zabezpečenia s využitím autentifikácie komunikačných koncov, autentifikácie dát a ich kryptovanie pomocou HMAC-MD5-96 a DES-CBC. Tieto vlastné bezpečnostné mechanizmy protokolu LFAP, však neposkytujú vyššiu bezpečnosť v porovnaní s TLS alebo IPsec. Môžu byť výhodné v situáciách, kde nie je možné TLS alebo IPsec použiť.

### ***Oznamovanie špecifických udalostí***

Špecifickou udalosťou je napríklad prijatie prvého paketu nového toku alebo ukončenie toku vypršaním časového intervalu. Jediné protokoly LFAP definujú správu oznamujúcu vznik nového toku. NetFlow v9 vždy exportuje informácie o toku okamžite po jeho ukončení. Ostatné protokoly nedefinujú export špecifických udalostí, ale umožňujú definovať nové záznamy v správach za týmto účelom.

### *Niekoľko zhromažďovacích procesov*

CRANE, Diameter a IPDR podporujú viaceré zhromažďovače, pričom export prebieha len na jeden a ostatné slúžia ako záložné pre prípad zlyhania. NetFlow v9 vykonáva export na všetky zhromažďovače súčasne.

## **4.8 Zhrnutie**

Každý exportný protokol má svoje silné aj slabé stránky. Pre účely účtovania s prenosom informácií o IP tokoch sú vhodné predovšetkým CRANE, Diameter a Streaming IPDR. Cieľom tejto práce je však vytvoriť nástroj pre účely merania v existujúcich IP sieťach. Zanedbať nemožno ani silnú pozíciu spoločnosti CISCO v tomto segmente a tiež s ohľadom na závery IPFIX working group[33], vychádza NetFlow v9 ako najvhodnejší aj napriek jeho niekoľkým nevýhodám. Medzi výhody patrí dobrá implementácia súčasných schopností, ale aj jednoduchosť spracovania na strane kolektora. Hlavné nedostatky sú v oblasti spoľahlivosti, čo však možno jednoducho odstrániť zmenou transportného protokolu na SCTP a zavedením potvrdzovania na úrovni aplikačnej vrstvy.

Protokol LFAP nemožno odporúčať z dôvodu veľkej zložitosti, veľkého počtu správ a nízkej efektivity reprezentácie informácií v správach. To sa prejaví aj v celkovej výkonnosti pri meraní na vysokorýchlostných linkách. LFAP má však najlepšie spracovanú indikáciu stratených dát a výhodou tiež môže byť podpora SNMP pre účely konfigurácie.

## 5. Analýza exportného protokolu NetFlow verzia 9

Exportný protokol NetFlow verzia 9[2] bol vyvinutý v Cisco Systems, za účelom exportu informácií o tokoch prechádzajúcich smerovačmi, ktoré spoločnosť Cisco Systems vyrába. Verzia 9 oproti predchádzajúcej verzii 5 prináša niekoľko vylepšení, za najvýznamnejšie možno považovať zavedenie šablón popisujúcich dátové záznamy. Implementácia šablón zefektívňuje prenos zaujímavých informácií o tokoch. Táto koncepcia predurčuje protokol NetFlow pre účely monitoringu tokov vo vysokorychlostných sieťach. Exportované informácie o tokoch sú na strane zhromažďovača spracovávané, aby mohli byť použité na účtovanie, plánovanie prenosových kapacít, bezpečnostnú analýzu, detekciu krízových stavov v sieti.

Výhody použitia šablón:

- možnosť definovať nové položky v záznamoch bez nutnosti meniť ich štruktúru,
- aj zhromažďovač, ktorý nepozná význam pridanej položky dokáže interpretovať zvyšok záznamu,
- vysoká flexibilita a efektivita zaručená možnosťou exportovať len položky potrebné pre zhromažďovač

### 5.1 Terminológia

#### *Merací bod (observation point)*

Merací bod je miesto v sieti, kde je možné zachytávať IP pakety. Napríklad jedno alebo skupina rozhraní sieťového zariadenia. Každý merací bod je súčasťou určitej meracej oblasti.

#### *Meracia oblasť (observation domain)*

Skupina meracích bodov s najväčšou zlučiteľnou množinou informácií o tokoch na sieťovom zariadení sa nazýva meracia oblasť. Napríklad karta smerovača s niekoľkými rozhraniami.

#### *Tok (flow)*

Tok je definovaný, ako jednosmerná postupnosť paketov prechádzajúcich meracím bodom siete, počas daného časového intervalu. Všetky pakety patriace

do jedného toku majú rovnaké určité vlastnosti odvodené z dát obsiahnutých v pakete a tiež vlastnosti odvodené zo spracovania paketu v meracom bode.

***Záznam toku (flow record)***

Záznam toku poskytuje informácie o toku získané v meracom bode.

***Exportér (exporter)***

Exportér je zariadenie, ktoré monitoruje pakety prechádzajúce meracím bodom, rozlišuje jednotlivé toky a posiela informácie o týchto tokoch v podobe záznamov tokov zhromažďovaču.

***Zhromažďovač (collector)***

Zhromažďovač prijíma záznamy tokov z jedného alebo viacerých exportérov. Spracováva prijaté exportné pakety a získava z nich informácie o tokoch.

***Exportný paket (export packet)***

Paket pochádzajúci z exportéra, nesúci záznamy tokov vytvorené týmto exportérom a určený pre zhromažďovač sa nazýva exportný paket.

***Záznam šablóny (template record)***

Záznam šablóny definuje štruktúru a implementáciu položiek v zázname dát.

***Záznam dát (flow data record)***

Záznam dát obsahuje hodnoty parametrov tokov definovaných záznamom šablóny.

***Záznam šablóny volieb (options template recor)***

Záznam šablóny volieb definuje štruktúru a implementáciu položiek v zázname dát volieb. Definuje tiež rozsah, v ktorom je záznam dát volieb platný.

***Záznam dát volieb (options data record)***

Záznam dát, ktorý obsahuje hodnoty parametrov merania definovaných záznamom šablóny.

***Flowset***

je všeobecný pojem pre skupinu záznamov toku, ktoré majú podobnú štruktúru. V exportnom pakete nasleduje jeden alebo viac flowsetov za hlavičkou paketu. Rozlišujú sa tri typy flowsetov: flowsety šablón, flowsety šablón volieb a flowsety dát.

## 5.2 Úloha exportéra

Exportér v priebehu meracieho procesu vykonáva niekoľko funkcií, výsledkom ktorých je exportný paket nesúci informácie o tokoch. Vykonávané funkcie sú: odchyťovanie paketov, zatriedenie odchytených paketov do tokov (klasifikácia), výpočet parametrov tokov a odosielanie parametrov expirovaných tokov.

### 5.2.1 Expirácia toku

Tok možno považovať za neaktívny (ukončený, expirovaný), ak meracím bodom v stanovenom časovom limite neprešiel ani jeden paket patriaci do tohto toku. Tok môže byť exportovaný, ak je splnená niektorá z podmienok:

1. Exportér detekoval ukončenie toku pomocou paketu oznamujúceho jeho ukončenie. Napríklad nastavený FIN alebo RST bit v pakete TCP protokolu.
2. Tok bol neaktívny počas stanoveného časového limitu. Tento čas by mal byť konfigurovateľný, s minimálnou hodnotou 0 pre okamžité ukončenie.
3. Nastala niektorá z vnútorných podmienok exportéra (nedostatok pamäte pre nové toky).

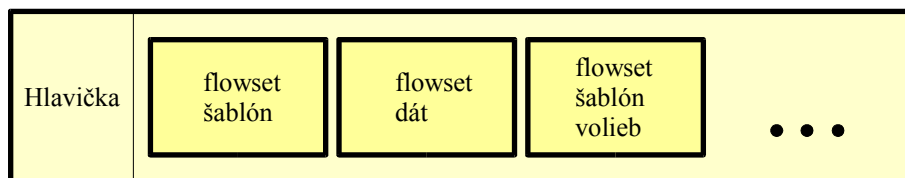
### 5.2.2 Transportný protokol

NetFlow bol navrhnutý ako nezávislý od transportného protokolu. Pre zabezpečenie efektivity aj pri veľkom množstve exportných paketov, vykonáva transport prostredníctvom protokolu UDP. Ak je potrebná vyššia spoľahlivosť prenosu, je možné zapuzdriť NetFlow pakety do protokolu SCTP. Export môže byť vykonávaný aj na niekoľko zhromažďovačov súčasne.

Pri voľbe transportného protokolu je potrebné uvažovať aj možnosť zahľadzenia linky prenášajúcej exportné pakety. Protokol UDP nie je odolný voči zahľadzeniu, a preto je vhodné spojenie medzi exportérom a zhromažďovačom vytvoriť osobitnou linkou. Ak nie je možné, aby exportér a zhromažďovač boli priamo spojené, musí byť priepustnosť spojenia vyššia ako maximálny špičkový tok exportných paketov.

### 5.3 Formát paketu

Exportný paket pozostáva z hlavičky nasledovanej jedným alebo viacerými flowsetmi. Paket môže obsahovať flowsety rôznych typov.



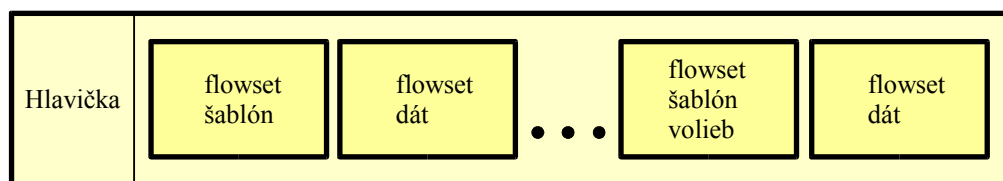
Obr. 5.1: NetFlow paket

Každý flowset má definovanú položku flowset ID, ktorá slúži na rozlíšenie typov flowsetov. Flowset ID nižší ako 256 je vyhradený pre špeciálne flowsety, akými sú flowset šablóny (ID = 0) a flowset šablóny volieb (ID = 1). Pre flowsety dát sú určené identifikátory väčšie ako 255.

Exportér musí všetky hodnoty kódovať do sieťového formátu (network byte order), tiež nazývaného veľký endián.

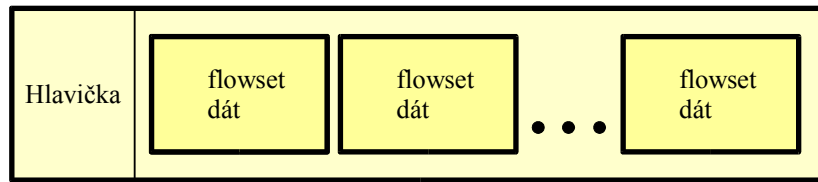
Príklady exportných paketov:

1. Paket obsahuje flowsety všetkých typov v poradí v akom boli vytvorené exportérom. Takáto situácia nastane, ak je potrebné exportovať novú šablónu pre už pripravené dáta a rovnako sú pripravené aj dáta volieb.



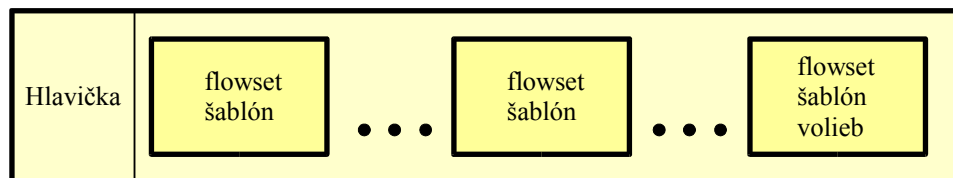
Obr. 5.2: Zmiešaný NetFlow paket

2. Exportovaný paket pozostáva výlučne z dátových flowsetov. Tento charakter má veľká väčšina exportovaných paketov.



Obr. 5.3: Dátový NetFlow paket

3. Paket tvoria len flowsety šablón dát aj volieb. Zvyčajne exportér periodicky posiela takéto pakety zhromažďovaču, aby zaistil aktuálnosť a správnosť šablón zhromažďovača.



Obr. 5.4: Šablónový NetFlow paket

### 5.3.1 Formát hlavičky

0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
Číslo verzie								Počet																							
sysUpTime																															
UNIX sekundy																															
Poradové číslo paketu																															
Identifikátor zdroja																															

Obr. 5.5: Formát hlavičky

#### *Číslo verzie*

Označuje verziu protokolu NetFlow a tým definuje vnútornú štruktúru paketu. Súčasná verzia má v tomto políčku hodnotu 9.

#### *Počet*

Obsahuje celkový počet záznamov v pakete. Vypočíta sa ako suma záznamov v jednotlivých flowsetoch.

#### *sysUpTime*

Čas v milisekundách od štartu exportéra.

***UNIX sekundy***

Čas od začiatku UNIXovej epochy. Je to počet sekúnd od 0000 UTC 1970 do súčasnosti.

***Poradové číslo***

Hodnota inkrementačného postupného počítadla paketov vyslaných exportérom z danej meracej oblasti. Táto hodnota slúži zhromažďovaču na detekciu stratených a duplicitných paketov.

***Identifikátor zdroja***

32-bitový identifikátor meracej oblasti exportéra. Zhromažďovač používa toto políčko na rozlíšenie rôznych exportných tokov vychádzajúcich z jedného exportéra.

**5.3.2 Formát flowsetu šablón**

Jedným z pokročilých elementov vo formáte NetFlow paketu je flowset šablón. Šablóny zvyšujú flexibilitu formátu záznamu daného toku tým, že umožňujú zhromažďovaču spracovanie záznamu aj bez znalosti interpretácie všetkých jeho položiek.

0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Flowset ID = 0		Dĺžka	
ID šablóny = 256		Počet položiek = N	
Typ položky 1		Dĺžka položky 1	
Typ položky 2		Dĺžka položky 2	
...		...	
Typ položky N		Dĺžka položky N	
ID šablóny = 257		Počet položiek = M	
Typ položky 1		Dĺžka položky 1	
Typ položky 2		Dĺžka položky 2	
...		...	
Typ položky M		Dĺžka položky M	
...		...	
ID šablóny = K		Počet položiek	
...		...	

**Obr. 5.6: Formát flowsetu šablón**

***Flowset ID***

Definuje typ flowsetu. Pre flowset šablóny vždy toto políčko nadobúda hodnotu 0.

***Dĺžka***

Obsahuje celkovú dĺžku tohto flowsetu v bajtoch. Úlohou dĺžky je určenie polohy ďalšieho flowsetu. Vypočíta sa ako suma dĺžok flowset ID, dĺžky samotnej a všetkých záznamov v danom flowsete.

***ID šablóny***

Každá šablóna dostáva pri vytvorení jedinečný identifikátor. Jedinečnosť je vyžadovaná iba v rámci jednej meracej oblasti. Identifikátor šablóny pre dáta môže nadobúdať hodnoty od 256 do 65535.

***Počet položiek***

Obsahuje počet položiek daného záznamu šablóny. Pretože flowset šablóny obyčajne zahŕňa niekoľko záznamov, slúži toto políčko na identifikáciu začiatku nasledujúceho záznamu.

***Typ položky***

Číselná hodnota reprezentujúca typ položky v zázname dát. Definícia typov pre protokol NetFlow verzia 9 sa nachádza v [RFC3954].

***Dĺžka položky***

Dĺžka políčka obsahujúceho hodnotu položky v zázname dát. Definícia dĺžok pre protokol NetFlow verzia 9 sa nachádza v [RFC3954].

**5.3.3 Formát flowsetu dát**

0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
Flowset ID = ID šablóny								Dĺžka																							
Záznam 1 – položka 1								Záznam 1 – položka 2																							
								Záznam 1 – položka 3																							
...								Záznam 2 – položka 1																							
Záznam 2 – položka 2								Záznam 2 – položka 3																							
Záznam 2 – položka 3								...																							
Záznam 3 – položka 1								Záznam 3 – položka 2																							
								Záznam 3 – položka 3																							
...								32-bitové vyrovnanie																							

**Obr. 5.7: Formát flowsetu dát**

***Flowset ID***

Každý dátový flowset má štruktúru záznamov definovanú príslušnou šablónou. Políčko Flowset ID obsahuje práve číslo tejto šablóny. Zhromažďovač na základe šablóny s rovnakým číslom ako je v políčku Flowset ID interpretuje položky záznamov.

***Dĺžka***

Obsahuje celkovú dĺžku tohto flowsetu v bajtoch. Úlohou dĺžky je určenie polohy ďalšieho flowsetu. Vypočíta sa ako suma dĺžok flowset ID, dĺžky samotnej a všetkých záznamov v danom flowsete.

***Záznam N – položka M***

Podstatnú časť flowsetu tvoria hodnoty položiek jednotlivých záznamov. Každá položka má svoj typ a dĺžku definovanú v príslušnej šablóne.

***32-bitové vyrovnanie***

Odporúča sa, aby flowset bol zarovnaný na 32-bitov, za týmto účelom sa dopĺňajú vyrovnávacie bajty. Na ich hodnote nezáleží, odporúčaná je však 0.

Dátový flowset možno interpretovať, len ak na strane zhromažďovača existuje šablóna s rovnakým ID šablóny.

**5.3.4 Formát flowsetu šablón volieb**

Flowsety šablón volieb a ich odpovedajúce záznamy dát volieb slúžia ako zdroj informácií o nastaveniach exportéra. Napríklad takto môže exportér oznamovať aktuálnu vzorkovaciu rýchlosť pre vybrané rozhranie.

0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
Flowset ID = 1								Dĺžka																							
ID šablóny								Dĺžka rozsahu (scope) volieb																							
Dĺžka volieb								Typ položky rozsahu 1																							
Dĺžka položky rozsahu 1								...																							
Dĺžka položky rozsahu N								Typ položky volieb 1																							
Dĺžka položky volieb 1								...																							
Dĺžka položky volieb M								32-bitové vyrovnanie																							

**Obr. 5.8: Formát flowsetu šablón volieb*****Flowset ID***

Definuje typ flowsetu. Pre flowset šablóny volieb vždy toto políčko nadobúda hodnotu 1.

***Dĺžka***

Obsahuje celkovú dĺžku tohto flowsetu v bajtoch. Úlohou dĺžky je určenie polohy ďalšieho flowsetu. Vypočíta sa, ako suma dĺžok flowset ID, dĺžky samotnej a všetkých záznamov v danom flowsete.

***ID šablóny***

Každá šablóna dostáva pri vytvorení jedinečný identifikátor s hodnotou od 256 do 65535.

***Dĺžka rozsahu volieb***

Určuje dĺžku v bajtoch každého rozsahového políčka v tejto šablóne.

***Dĺžka volieb***

Určuje dĺžku v bajtoch každého políčka volieb v tejto šablóne.

***Typ položky rozsahu N***

Definuje typ položky rozsahu, v ktorom sú dáta volieb platné. Toto políčko môže nadobúdať nasledujúce hodnoty:

1 = systém

2 = rozhranie

3 = karta

4 = cache

5 = šablóna

Napríklad pre Netflow proces pracujúci nad rozhraním, bude typ položky rozsahu príslušnej voľby rovný hodnote 2. V zázname dát volieb bude odpovedajúca položka rozsahu obsahovať identifikátor rozhrania.

***Dĺžka položky rozsahu N***

Dĺžka políčka obsahujúceho hodnotu položky rozsahu v zázname dát volieb.

***Typ položky volieb M***

Číselná hodnota reprezentujúca typ položky v zázname dát volieb. Definícia typov pre protokol NetFlow verzia 9 sa nachádza v [RFC3954].

***Dĺžka položky volieb M***

Dĺžka políčka obsahujúceho hodnotu položky volieb v zázname dát volieb.

***32-bitové vyrovnanie***

Odporúča sa, aby flowset bol zarovnaný na 32-bitov, za týmto účelom sa dopĺňajú vyrovnávacie bajty. Na ich hodnote nezáleží, odporúčaná je však 0.

### 5.3.5 Formát záznamu dát volieb

Dátové záznamy volieb sú posielané vo flowsetoch dát ako bežné dátové záznamy. Vysielajú sa v konfigurovateľných časových intervaloch.

0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
Flowset ID = ID šablóny								Dĺžka																							
Záznam 1 – položka rozsahu 1								Záznam 1 – položka volieb 1																							
Záznam 1 – položka volieb 2								...																							
Záznam 2 – položka rozsahu 1								Záznam 2 – položka volieb 1																							
Záznam 2 – položka volieb 2								...																							
Záznam 3 – položka rozsahu 1								Záznam 3 – položka volieb 1																							
Záznam 3 – položka volieb 2								...																							
...								32-bitové vyrovnanie																							

Obr. 5.9: Formát flowsetu dát volieb

#### *Flowset ID*

Každý dátový flowset má štruktúru záznamov definovanú príslušnou šablónou. Políčko Flowset ID obsahuje práve číslo tejto šablóny. Zhromažďovač na základe šablóny s rovnakým číslom, ako je v políčku Flowset ID interpretuje položky záznamov.

#### *Dĺžka*

Obsahuje celkovú dĺžku tohto flowsetu v bajtoch. Úlohou dĺžky je určenie polohy ďalšieho flowsetu. Vypočíta sa ako suma dĺžok flowset ID, dĺžky samotnej a všetkých záznamov v danom flowsete.

#### *Záznam N – položka rozsahu*

Položka rozsahu, predchádza položkám volieb a svojou hodnotou identifikuje rozsah ich platnosti. Týchto položiek môže byť niekoľko, v takom prípade upresňujú definíciu rozsahu.

#### *Záznam N – položka volieb*

Položky volieb obsahujú hodnoty parametrov nastavenia exportéra. Zhromažďovač ich interpretuje na základe príslušnej šablóny.

#### *32-bitové vyrovnanie*

Odporúča sa, aby flowset bol zarovnaný na 32-bitov, za týmto účelom sa dopĺňajú vyrovnávacie bajty. Na ich hodnote nezáleží, odporúčaná je však 0.

Dátový flowset možno interpretovať, len ak na strane zhromažďovača existuje šablóna s rovnakým ID šablóny.

## 5.4 Správa šablón

Dátové záznamy tokov, ktoré odpovedajú šablónovému záznamu majú byť prenášané v tom istom alebo v nasledujúcich paketoch. Nevyžaduje sa, aby bola šablóna prenášaná v každom exportnom pakete. Z tohoto dôvodu si musí zhromažďovač ukladať záznamy šablón, pre ich neskoršie použitie pri interpretácii prijatých dátových záznamov.

Zhromažďovač, ktorý dostáva exportné pakety z niekoľkých meracích oblastí, ale od toho istého exportéra, musí byť schopný rozlíšiť šablóny s rovnakým identifikátorom, pochádzajúce s rôznych meracích oblastí.

Identifikátory šablón musia zostať konštantné počas celej doby života exportného procesu. Ak z nejakých dôvodov prebehne reštart exportéra, všetky informácie o šablónach sa stratia a musia byť vygenerované nové identifikátory. Po reštarte exportéra by mal zhromažďovač obdržať definície šablón aj pre predtým používané identifikátory a následne musí staré definície nahradiť novými.

Novej šablóne sa priraduje ešte nepoužitý identifikátor. Ak došlo k zmene v zázname šablóny, súčasný identifikátor sa neuvolňuje a nemal byť viac použitý, kým exportér neskončí.

Podmienky pre vyslanie flowsetu šablón a flowsetu šablón volieb sú nasledovné:

1. Po reštarte exportéra nesmú byť vyslané žiadne dáta, ak nebola vyslaná príslušná šablóna. Najneskôr sa môže šablóna vyslať v jednom pakete spolu s príslušnými dátami, ale aj vtedy im musí predchádzať.
2. Po vykonaní konfiguračných zmien. Šablóny by mali byť vysielané v samostatnom pakete, aby bol zhromažďovač upozornený na zmenu.
3. Exportér musí pravidelne posilať záznamy šablón zhromažďovaču. Dôvodom je obmedzená doba života identifikátora šablóny na strane zhromažďovača.

Pre určenie intervalu obnovovania existujú dva prístupy:

- po každých N paketoch
- každých N minút

Obidva spôsoby musia byť konfigurovateľné používateľom na strane exportéra.

4. Ak nastala zmena nastavenia vnútorných hodín exportéra.

Keď nastane aspoň jedna z týchto podmienok, musia byť vyslané záznamy šablón.

## 5.5 Úloha zhromažďovača

Zhromažďovač prijíma záznamy šablón pred prijatím záznamov dát alebo volieb. Dáta potom môžu byť dekodované a uložené. Ak nebola prijatá šablóna umožňujúca dekodovanie záznamov, zhromažďovač by mal záznamy odkladať a dekodovať ich neskôr, keď dostane príslušnú šablónu. Zhromažďovač nesmie požadovať prijatie dát a ich šablóny v jednom pakete. Tiež nesmie očakávať, že paket obsahuje len jeden flowset šablón. Záznamy šablón majú obmedzenú životnosť, a preto musia byť pravidelne obnovované. Šablóna s vypršanou platnosťou nesmie byť používaná na dekodovanie záznamov dát. Ak exportér oznámi zmenu nastavenia hodín, zhromažďovač musí zrušiť všetky šablóny od daného exportéra. Identifikátory šablón musia byť jedinečné len v rámci exportéra a meracej oblasti.

## 5.6 Bezpečnostné riziká

Exportný protokol NetFlow verzia 9 bol navrhnutý s predpokladom, že exportér a zhromažďovač komunikujú v rámci jednej privátnej siete, určenej výlučne na prenos exportných paketov. Konkrétna aplikácia však môže vyžadovať prenos paketov protokolu cez internet, kde sú vystavené bezpečnostným rizikám. Napríklad útočník odchyťí, zmodifikuje alebo podstrčí falošné pakety. Riziká vyplývajú zo úniku informácií, znehodnotenia vierohodnosti informácií a zo znefunkčnenia zhromažďovača.

Návrhári protokolu NetFlow verzia 9 neuvažovali zahrnutie mechanizmov na redukciiu týchto rizík, pretože by sa tak znížila efektívnosť implementácie, a tiež neuvažovali nasadenie protokolu mimo privátnej siete.

### 5.6.1 Riziká z odchytenia dát

Pretože kryptovanie nebolo implementované, útočník môže ľahko získať prehľad o aktívnych tokoch v sieti, adresách klientov a zariadení. Tieto informácie umožnia sledovanie používateľov a plánovanie ďalších útokov. Rizikovosť prenášaných dát tiež závisí od definície záznamov tokov. Čím menej dát sa prenáša a čím viac sú tieto dáta všeobecného charakteru, tým je riziko menšie. Tento poznatok treba brať do úvahy pri návrhu šablón.

### **5.6.2 Riziká z modifikácie záznamov**

Využitie protokolu NetFlow na účtovanie a bezpečnostné aplikácie prináša ďalšie riziká, vyplývajúce z citlivosti na falošné údaje. Útočník napríklad môže oklamať poskytovateľa služieb alebo zabrániť detekcii útoku. Ak zhromažďovač obdrží falošnú šablónu, nebude správne interpretovať dátové záznamy a tak dôjde k strate nameraných dát.

### **5.6.3 Útoky na zhromažďovač**

Útoky za účelom vyradenia z činnosti môžu spotrebovať toľko systémových prostriedkov, že nebude možné prijímať pakety alebo dekodovať záznamy. Toto riziko však nemá na svedomí exportný protokol, ale príslušné metódy spracovania údajov.

## 6. Koncepcia a architektúra meracieho nástroja BasicMeter

BasicMeter je vytvorený ako základný nástroj pre pasívne merania v počítačových sieťach. Vývoj BasicMetra 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, 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.

### 6.1 Špecifikácia požiadaviek

Hlavné požiadavky na implementáciu meracieho nástroja možno zhrnúť do nasledujúcich bodov:

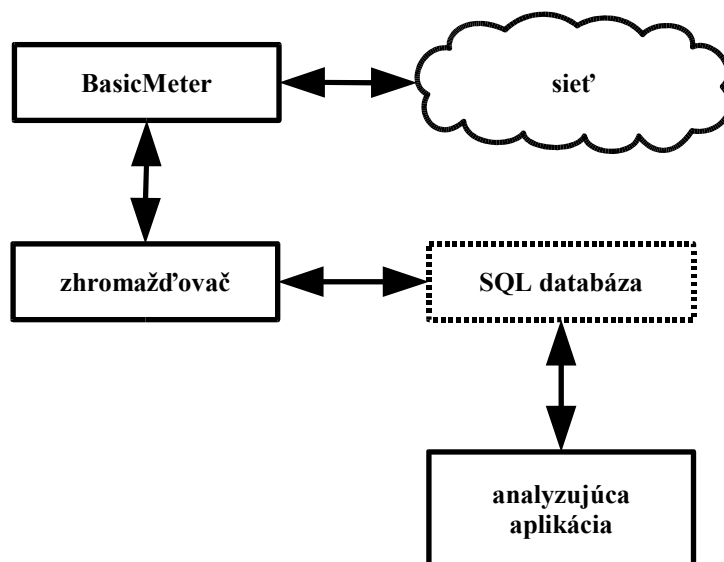
- vytvorenie jednoduchého nástroja pre ovládanie z konfiguračného súboru
- navrhnuť modulárny dizajn, ktorý by zaručoval rozšíriteľnosť jednoduchým spôsobom
- možnosť jednoduchého vzdialeného ovládania meracieho prístroja
- podpora protokolu NetFlow verzia 9
- podpora vznikajúceho štandardu vzorkovania PSAMP[14]
- podpora šablón a možnosť verifikácie zadaných šablón
- možnosť konfigurácie jednoduchým textovým konfiguračným súborom
- implementácia portabilným spôsobom
- implementácia by mala byť východiskovým bodom pre podporu meraní podľa štandardu IPFIX
- navrhnuť podporu pre implementáciu vzorkovacích funkcií

### 6.2 Koncepcia meracieho nástroja

Koncepciu meracieho nástroja ovplyvňuje najmä snaha o podporu štandardov PSAMP a IPFIX v čo najlepšej možnej miere. Navrhovaný merací nástroj

sa snaží svojou koncepciou priblížiť návrhu architektúry štandardu IPFIX. Navrhovaný a implementovaný merací nástroj je súčasťou tejto koncepcie znázornenej na obrázku 6.1 .

SQL databáza nie je súčasťou špecifikácie IPFIX a ani protokolu NetFlow, preto je v schéme naznačená bodkovane. 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.



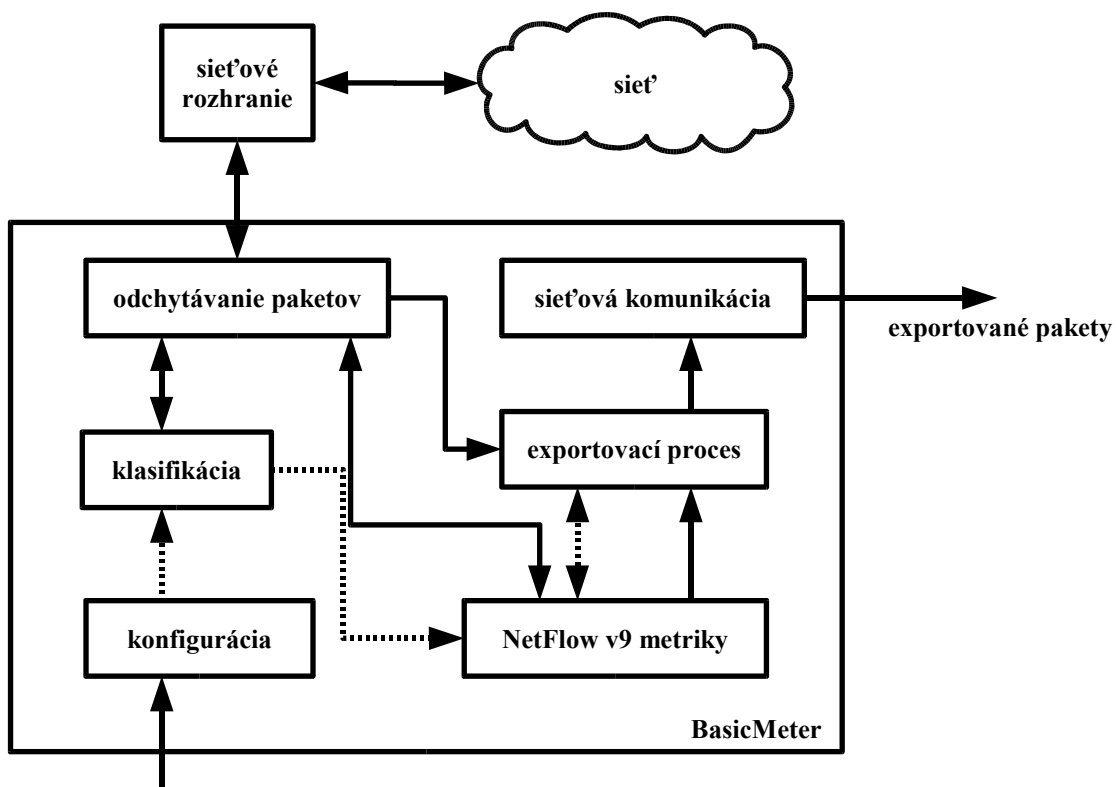
**Obr. 6.1: Architektúra meracej platformy**

Merací nástroj je súčasťou projektu vývoja kompletnej meracej platformy pre pasívne merania kvality služieb v počítačových sieťach. Časti tejto kompletnej meracej platformy sú naznačené v tabuľke 6.1 .

<i>Časť architektúry</i>	<i>Popis</i>
BasicMeter (merací proces)	aplikácia vykonávajúca zachytávanie paketov, rozlišovanie tokov a export informácií o tokoch definovaným protokolom
zhromažďovač	spracovanie prijatých exportných paketov a informácií, ktoré obsahujú; nie je súčasťou popisovaného riešenia
analyzujúca aplikácia	aplikácia, ktorá na základe dát zo zhromažďovača vykonáva grafickú a štatistickú analýzu podľa potrieb používateľa

**Tab. 6.1: Popis jednotlivých častí architektúry**

### 6.3 Architektúra meracieho nástroja BasicMeter



**Obr. 6.2: Architektúra meracieho nástroja**

Architektúra nástroja je navrhnutá tak, aby vyhovela všetkým špecifikovaným požiadavkám. Nástroj možno rozdeliť do troch hlavných častí: časť odchyťovania paketov, časť klasifikácie a exportovacia časť (exportovací proces). Ďalšou časťou programu je spracovanie textového konfiguračného súboru programu. Časť spracovania konfigurácie má za úlohu načítať a spracovať parametre z konfiguračného súboru. Pre tieto činnosti je použitá knižnica libconfuse [10] — knižnica určená na spracovanie textových konfiguračných súborov. Odchyťovacia časť (capture) má za úlohu sledovanie a odchyťovanie paketov na základe parametrov poskytovaných konfiguračnou časťou a odovzdaných odchyťovacej časti v procese inicializácie. Táto časť využíva funkcie knižnice libpcap [6], 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 subsysteme pridelovania práv. Samotný výber paketov na sledovanie a odchytenie je realizovaný pomocou vysokoúrovňového abstraktného popisného jazyka podobného tomu, aký je použitý v nástroji na sledovanie sieťovej prevádzky s názvom tcpdump [8]. Odchyťávajú sa všetky pakety patriace aspoň do jedného toku. Samotné odchyťovanie paketov je realizované pomocou berkeleyjského 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 odlišný od filtrovania.

Klasifikátor určuje tok, do ktorého odchytený paket patrí a odovzdá informácie získané z paketu spolu s identifikátorom toku do časti vytvárania záznamov tokov. Časť vytvárania záznamov tokov obsahuje zásobník pre uloženie záznamov aktívnych tokov. Záznamy tokov sú po ukončení toku, poskytované komponentu s názvom NetFlow v9 metriky.

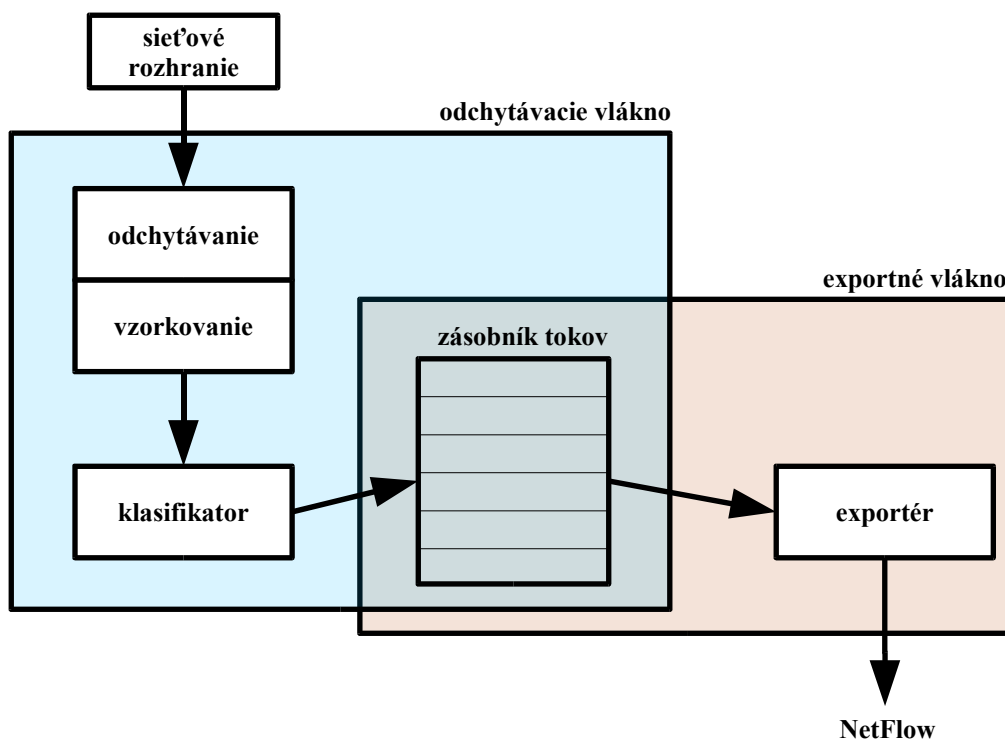
Komponent NetFlow v9 metriky na základe definovaných šablón naplňa jednotlivé položky v záznamoch dát daného toku. Hodnota príslušnej položky je určená typom zadaným v šablóne a informáciami v zázname konkrétneho toku.

Exportný proces má za úlohu vytvárať pakety protokolu NetFlow v9. Získané dátové záznamy s rovnakou šablónou sú vkladané do jedného flowsetu, 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 zhromažďovaču doručená. Šablóny sú v exportnom pakete zoskupené do flowsetu šablón. Zoskupovanie objektov s rovnakou povahou do flowsetov prináša jednoduchšie spracovanie paketu na oboch stranách.

Časť pre sieťovú komunikáciu umožňuje exportnému procesu zachovať si nezávislosť od transportného protokolu. Pôvodný transportný protokol je UDP, čo môže byť v niektorých situáciách nevyhovujúce (najmä ak je vyžadovaná spoľahlivosť a bezpečnosť). Zmenou sieťového komunikačného modulu, tak jednoducho zmeníme spôsob prenosu exportných paketov podľa požiadaviek meracej architektúry.

## 7. Návrh exportného modulu

V exportnom module bolo realizované vytváranie paketov protokolu NetFlow verzia 9, na základe informácií o tokoch získaných so zachytených paketov. Pozícia exportného modulu v architektúre meracieho nástroja BasicMeter je znázornená na obrázku 7.1. Exportný modul bol zaradený do exportného vlákna, aby spracovávať záznamy tokov paralelne so spracovaním paketov v odchyťavacom vlákne. Vlákňová architektúra tak umožňuje zvýšenie výkonu celého meracieho nástroja. Na implementáciu vlákien bola použitá knižnica pthreads[34], ktorá je súčasťou jadra operačného systému Linux. Tak ako celý merací nástroj, tak aj exportný modul bol implementovaný v programovacom jazyku C++. Použitie tohto programovacieho jazyka zabezpečuje prenositeľnosť meracieho nástroja aj na iné platformy. Na vytváranie a úpravy zdrojových textov bolo použité vývojové prostredie Eclipse[35]. Tento nástroj tiež slúžil ako klientská aplikácia systému na správu verzií CVS[36]. Požitie systému CVS umožnilo efektívne zdieľať a dopĺňať zdrojové texty celého meracieho nástroja členmi vývojového tímu. Na preklad zdrojových textov bol použitý prekladač g++, ktorý je súčasťou operačného systému Linux.



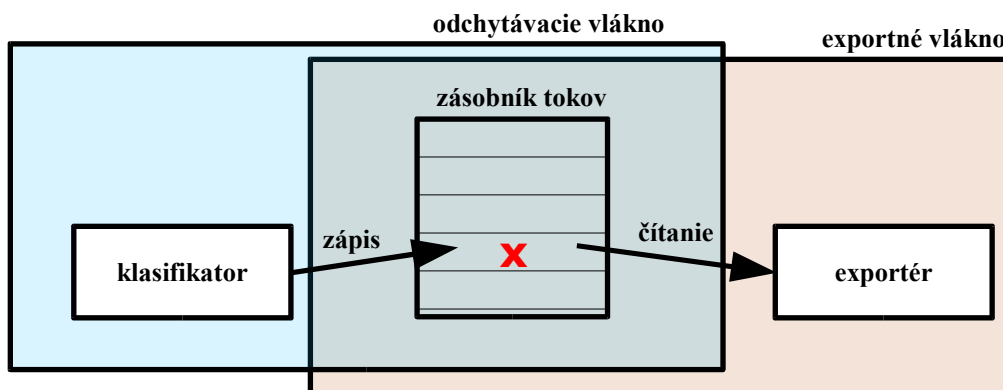
Obr. 7.1: Bloková schéma meracieho nástroja BasicMeter

Merací nástroj BasicMeter je vytvorený ako aplikácia spustiteľná z príkazového riadku. Výpisy sú minimalizované len na nevyhnutné chybové hlásenia, pretože sa predpokladá používanie nástroja na pozadí.

## 7.1 Analýza vstupných dát

Vstupné dáta pre exportný proces tvoria záznamy ukončených tokov. Záznamy tokov sa nachádzajú v zásobníku, pričom pojem zásobník v tomto prípade označuje pamäťový priestor vyhradený pre ukladanie záznamov tokov. Organizácia vkladania a výberu záznamov však neprebíha ako pri klasickom zásobníku. Okrem exportného modulu má prístup do zásobníka tokov aj klasifikátor, ktorý vykonáva operácie vytvárania, aktualizácie a ukončovania nad záznamami tokov. Exportný modul aj klasifikátor súčasne pristupujú k záznamom zásobníka a môže nastať situácia kedy obaja naraz pristúpia na ten istý záznam. V prípade jednovláknovej implementácie meracieho nástroja nehrozí žiadne riziko z tejto situácie, ale vzhľadom na to, že exportér a klasifikátor bežia v osobitných vláknach môže vzniknúť kolízia, ako je naznačené na obrázku 7.2. Nutnou podmienkou pre vznik kolízie je odchytenie paketu patriaceho do toku, ktorý už bol ukončený. To nastáva najmä ak dôvodom ukončenia toku bola expirácia časového intervalu pre životnosť dlhotrvajúcich tokov, pretože tok reálne neskončil, ale je považovaný za skončený. Pravdepodobnosť výskytu kolízie sa zvyšuje s rastúcim počtom krátkych opakovaných tokov.

Vzniku kolízie by bolo možné zabrániť, ak by sa zamedzila činnosť oboch vlákien nad jednou položkou naraz. Klasifikátor však nemá vlastné vlákno, ale je spúšťaný vo vlákne odchyťavania paketov. Akékoľvek pozastavenie vykonávania odchyťavacieho vlákna by bolo na úkor výkonnosti a spoľahlivosti meracieho nástroja. Na vyriešenie tohto problému možno využiť skutočnosť, že exportér nad zásobníkom tokov vykonáva len operáciu čítania. Ak exportér dokáže detekovať kolíziu, môže prečítané hodnoty považovať za neplatné a pokúsiť sa o čítanie záznamu znova. Detekcia realizovaná príznakom prístupu do záznamu je jednoduchá a spoľahlivá. Nevýhodou môže byť mierny pokles efektivity, no aktivita exportného vlákna je vždy nižšia ako aktivita odchyťavacieho vlákna a teda nebude brzdiť celý merací proces.



Obr. 7.2: Vznik kolízie pri súčasnom prístupe do zásobníka tokov.

## 7.2 Analýza výstupných dát

Výstupné dáta exportného procesu predstavujú pakety protokolu NetFlow v 9. Tieto pakety prenášajú informácie o skončených tokoch. Dátové záznamy jednotlivých tokov majú svoju štruktúru definovanú pomocou príslušnej šablóny. Záznamy šablón môžu byť prenášané v paketoch spolu s dátovými záznamami, ich štruktúra je definovaná v špecifikácii protokolu NetFlow verzia 9. Efektívna a flexibilná organizácia dát v paketoch protokolu NetFlow v9 bola hlavnou motiváciou k jeho implementácii v meracom nástroji BasicMeter.

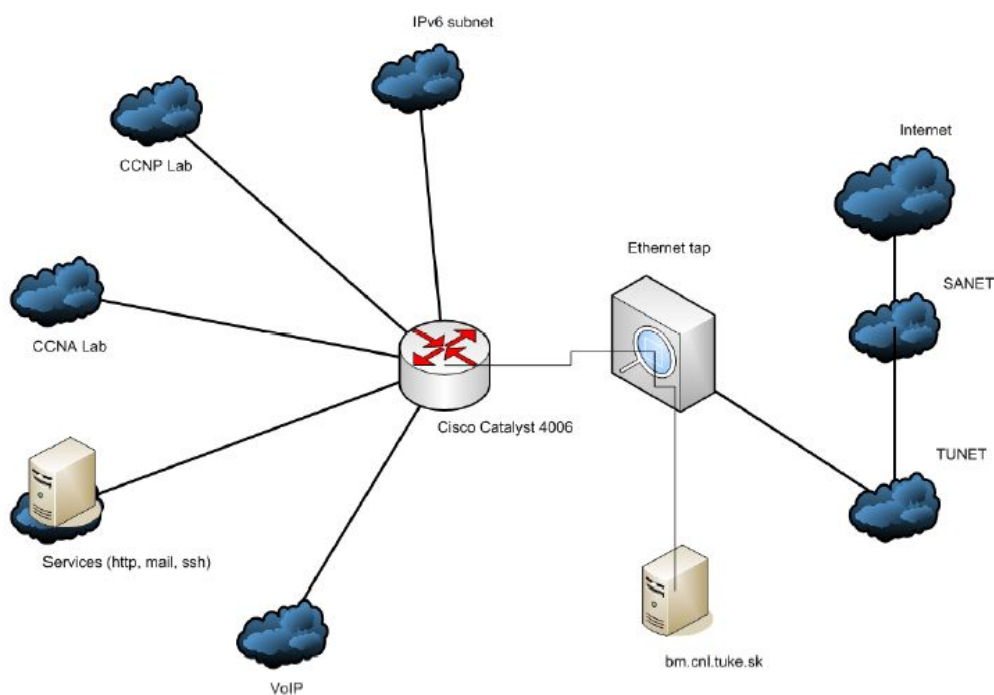
Meracia platforma, v ktorej BasicMeter pôsobí neuvažuje využitie všetkých špecifik spomínaného exportného protokolu. S ohľadom na efektivitu nástroja budú implementované len požadované prvky, ale zjednodušenie oproti špecifikácii nesmie ohroziť kompatibilitu nástroja s inými nástrojmi pracujúcimi tiež na báze protokola NetFlow v9.

## 8. Experimentálne overenie funkčnosti nástroja

Účelom experimentálneho overenia funkčnosti je inštalácia implementovaného meracieho nástroja do prostredia s reálnou alebo simulovanou prevádzkou a vyhodnotenie nameraných hodnôt.

### 8.1 Inštalácia

Merací nástroj bol nainštalovaný v Laboratóriu počítačových sietí na Katedre počítačov a informatiky Technickej univerzity v Košiciach, podľa schémy znázornenej na obrázku 8.1 .



**Obr. 8.1:** Schéma zapojenia experimentu v Laboratóriu počítačových sietí.

Na počítači `bm.cnl.tuke.sk` (alias pre `sis2.cnl.tuke.sk`) bola spustená inštancia nástroja BasicMeter. Pripojenie do sieťového segmentu laboratória bolo realizované zariadením ethernet tap, ktoré pracuje na fyzickej vrstve ISO/OSI modelu. Ethernet tap sa zapája do už existujúcej linky a umožňuje odosielať celú prevádzku na tejto linke na odbočku. Na odbočku bol pripojený počítač so spusteným nástrojom BasicMeter.

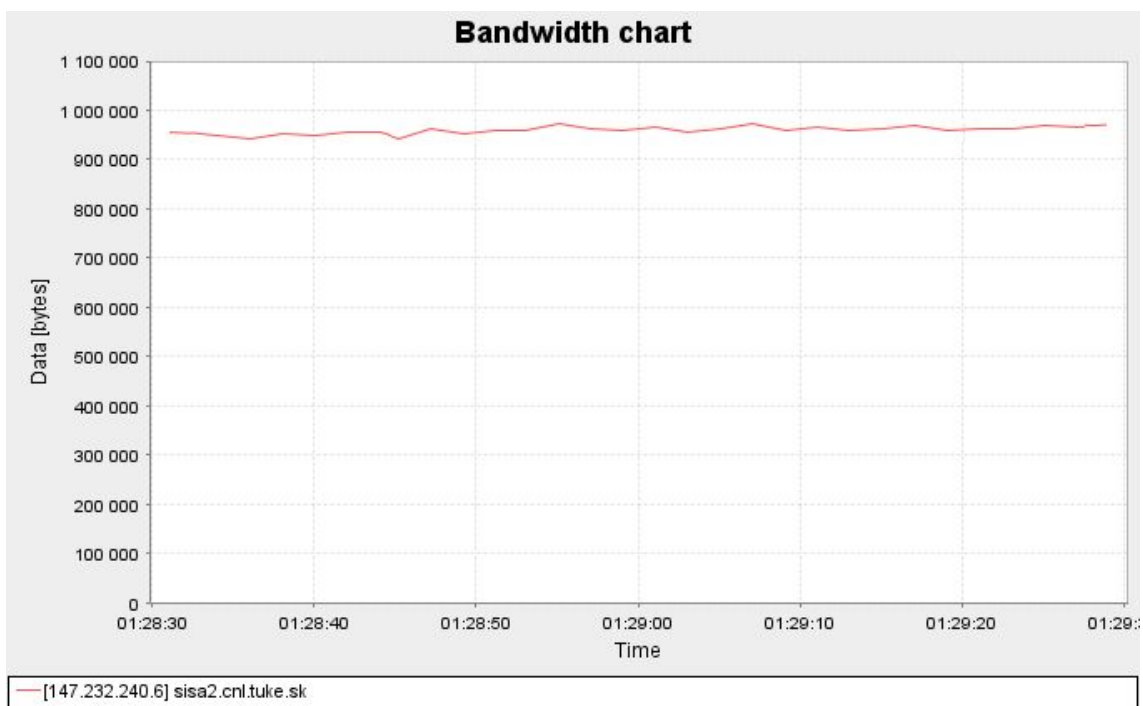
Požiadavkou na počítač bol nainštalovaný operačný systém Linux (kernel 2.6.7). Hardvérové vybavenie predstavuje procesor Intel Celeron 400MHz a sieťové rozhrania typu 3Com 3c905C-TX. Počítačové siete v laboratóriu sú prepojené switchom Cisco Catalyst 4006 a prostredníctvom univerzitnej siete TUNET je realizované pripojenie na internet.

## 8.2 Experimentálne meranie

Merací nástroj BasicMeter bol navrhnutý ako súčasť komplexnej meracej platformy s ohľadom na špecifikáciu PSAMP a IPFIX[14]. Z tohto dôvodu samotný nástroj neposkytuje žiadne možnosti analýzy prevádzky. Overenie správnej funkcie vyžaduje prepojenie so zhromažďovačom a analyzujúcou aplikáciou. Ako zhromažďovač bol použitý programový balík Jxcoll. Analyzujúca aplikácia umožnila sledovanie aktuálnej prevádzky v sieti v reálnom čase. V prípade použitia vzorkovania nebola aplikácia schopná interpretovať vzorkovanie, a preto namerané hodnoty nezodpovedali skutočnému toku prevádzky, ale len toku vzorkovaných paketov. Pozitívne možno hodnotiť nízke zaťaženie procesora BasicMetrom, ktoré sa v špičkách pohybovalo pod hranicou 5%. Na meranie zaťaženia procesora bol použitý nástroj time, ktorý je bežnou súčasťou distribúcií operačného systému Linux.

## 8.3 Meranie prenosovej rýchlosti

Meraním prenosovej rýchlosti možno jednoducho overiť správnu funkciu navrhnutého nástroja. Meranie prebiehalo na regulovanej testovacej prevádzke založenej na protokole FTP s prenosovou rýchlosťou 1024kB/s. Bola otestovaná aj činnosť meracieho nástroja pre každý typ podporovaného vzorkovania. Vzorkovanie bolo nastavené tak, aby vzorka tvorila 20% z celkovej populácie. Parametre exportu BasicMetera boli zvolené tak, aby analyzujúca aplikácia mohla zobrazovať priebehy v reálnom čase a s čo možno najväčšou presnosťou. Interval maximálnej aktivity toku bol nastavený na 1s a tak sa dosiahlo odosielanie informácií o aktuálnych tokoch každú sekundu. Na obrázku 8.2 je priebeh prenosovej rýchlosti zobrazený analyzujúcou aplikáciou.



**Obr. 8.2: Zaznamenaný priebeh prenosovej rýchlosti**

### 8.3.1 Vplyv vzorkovania na namerané hodnoty

Vzorkovanie umožňuje vykonávať merania aj na vysokorýchlostných sieťach, kde by už veľké množstvo paketov nebolo spracovateľné na bežných hardvérových prostriedkoch. Nevýhodou je vnášanie určitej nepresnosti do merania, pretože charakteristiky vzorkovaných paketov nemusia byť zhodné s charakteristikami celkovej prevádzky. Výberom vhodného vzorkovacieho algoritmu možno túto nepresnosť eliminovať na únosnú mieru.

Prehľad nameraných priebehov s nasadením jednotlivých vzorkovacích algoritmov:

#### *Systematické vzorkovanie založené na počte*

Systematické vzorkovanie založené na počte deterministicky určuje začiatok a koniec vzorkovacieho intervalu v závislosti na počte paketov prevádzky. Príkladom tohto vzorkovania môže byť selekcia každého  $n$ -tého paketu. Priebeh prevádzky zaznamenaný s použitím tohto vzorkovania je na obrázku 8.3. Porovnaním priebehu s

použitým vzorkovaním a bez neho sa zistilo, že objem meranej prevádzky je nižší, ale tvar charakteristiky je veľmi podobný.

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

Systematické vzorkovanie založené na čase deterministicky určuje začiatok a koniec vzorkovacieho intervalu v závislosti na čase. Príkladom môže byť vzorkovanie paketov prichádzajúcich každých 20 sekúnd. Priebeh prevádzky zaznamenaný s použitím tohto vzorkovania je na obrázku 8.4 . Porovnaním priebehu s použitým vzorkovaním a bez neho sa zistilo, že objem meranej prevádzky je nižší, ale tvar charakteristiky je odlišný. Túto odlišnosť je možné eliminovať, ak sa interval aktualizácie grafu predĺži, tak aby z dvoch bodov vznikol jeden.

#### ***Vzorkovanie $n$ -z- $N$***

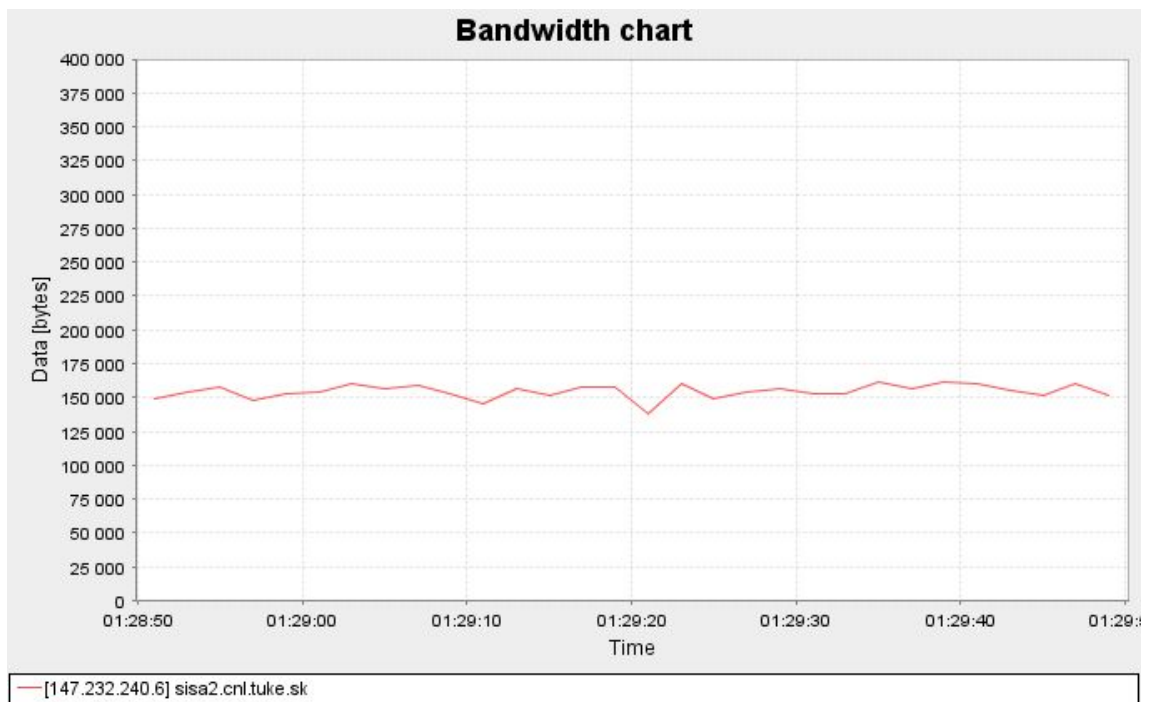
Vzorkovanie  $n$ -z- $N$  je predstaviteľom skupiny náhodných vzorkovaní. Jeho princíp spočíva vo výbere  $n$  paketov z celkovej populácie, ktorá pozostáva z  $N$  paketov. Priebeh prevádzky zaznamenaný s použitím tohto vzorkovania je na obrázku 8.5 . Porovnaním priebehu s použitým vzorkovaním a bez neho sa zistilo, že objem meranej prevádzky je nižší, ale tvar charakteristiky je čiastočne odlišný.

#### ***Uniformné náhodné pravdepodobnostné vzorkovanie***

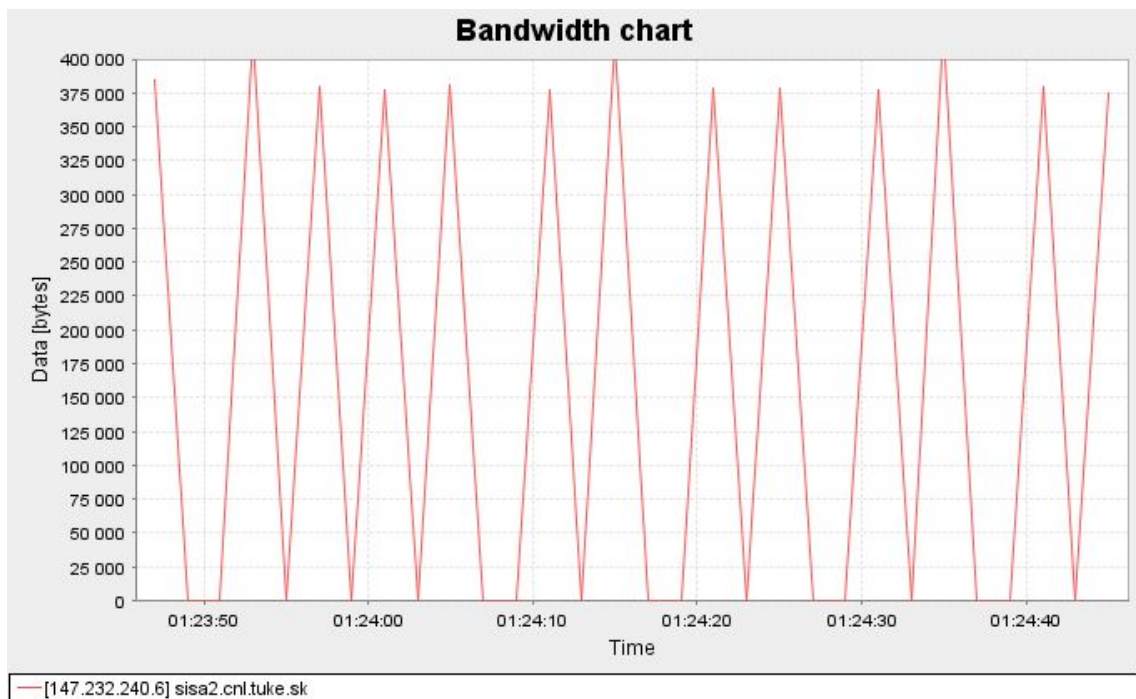
Uniformné náhodné pravdepodobnostné vzorkovanie vyberá pakety s definovanou pravdepodobnosťou. Pre každý paket je pravdepodobnosť výberu rovnaká. Priebeh prevádzky zaznamenaný s použitím tohto vzorkovania je na obrázku 8.6 . Porovnaním priebehu s použitým vzorkovaním a bez neho sa zistilo, že objem meranej prevádzky je nižší, ale tvar charakteristiky je podobný.

#### ***Neuniformné náhodné pravdepodobnostné vzorkovanie založené na počte***

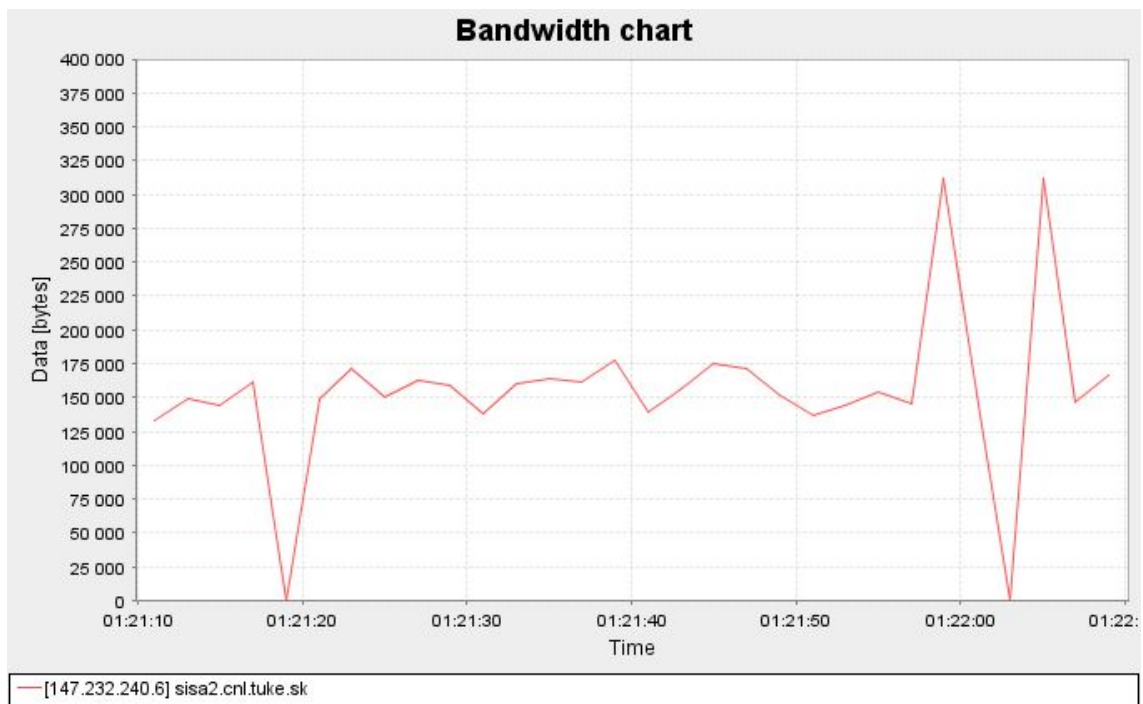
Neuniformné náhodné pravdepodobnostné vzorkovanie založené na počte vyberá pakety s definovanou pravdepodobnosťou, pričom pravdepodobnosť výberu paketu sa mení v závislosti na určitej vlastnosti paketu. Priebeh prevádzky zaznamenaný s použitím tohto vzorkovania je na obrázku 8.7 . Porovnaním priebehu s použitým vzorkovaním a bez neho sa zistilo, že objem meranej prevádzky je nižší, ale tvar charakteristiky je podobný.



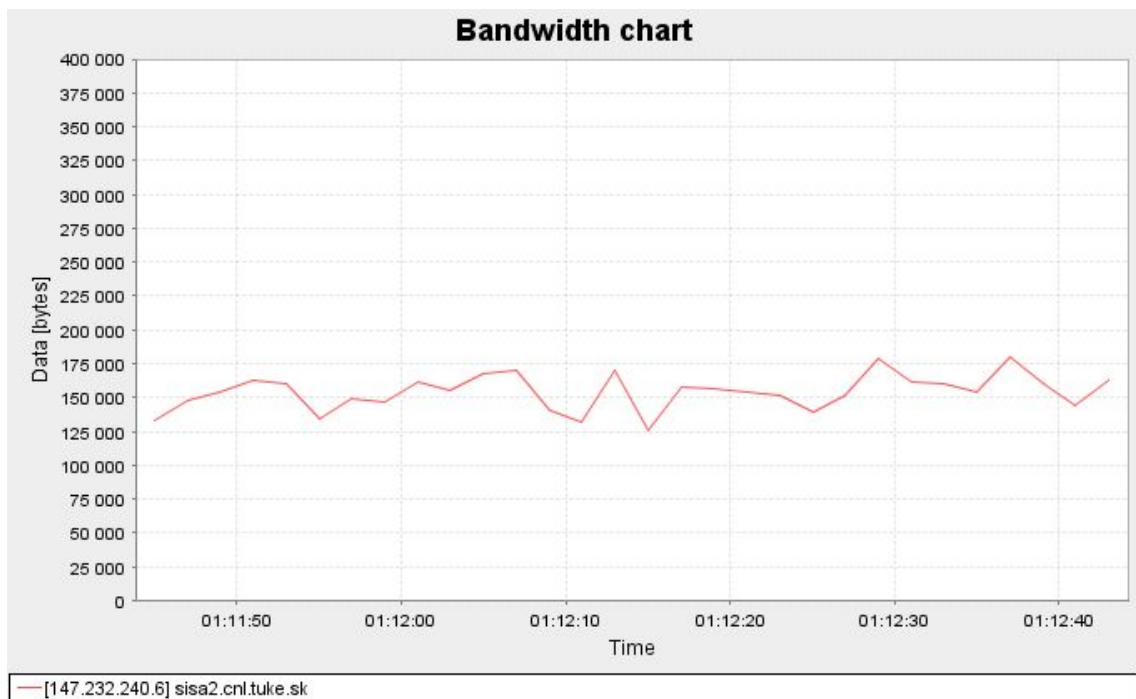
**Obr. 8.3: Systematické vzorkovanie založené na počte**



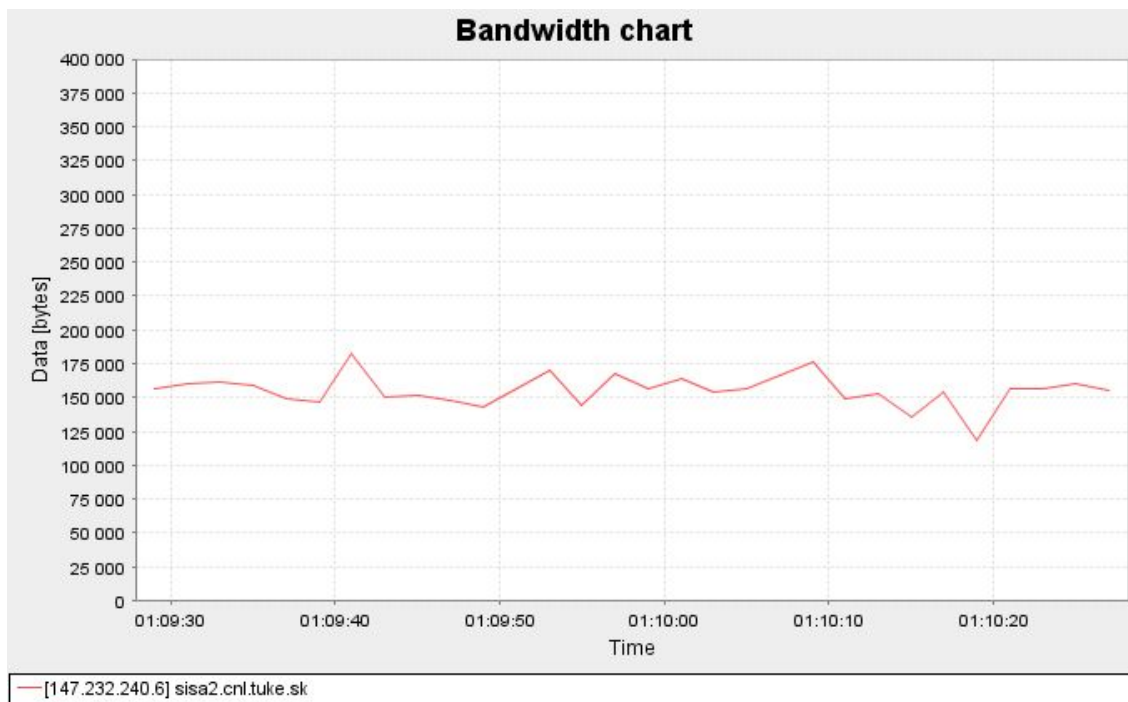
**Obr. 8.4: Systematické vzorkovanie založené na čase**



Obr. 8.5: Vzorkovanie n-z-N



Obr. 8.6: Uniformné náhodné pravdepodobnostné vzorkovanie



**Obr. 8.7: Neuniformné náhodné pravdepodobnostné vzorkovanie založené na počte**

## 8.4 Zhrnutie výsledkov experimentu

Experimentom sa podarilo overiť funkčnosť meracieho nástroja s implementovanou podporou exportu v protokole NetFlow verzia 9. Systém merania charakteristík sieťovej prevádzky založený na exporte informácií o tokoch, radikálne znižuje objem prenášaných dát v porovnaní s prenosom hlavičiek všetkých paketov prevádzky. Pre názornosť možno uviesť výsledok experimentu, kde na export informácií o toku prevádzky FTP s prenosovou rýchlosťou 40Mb/s, by postačovala linka s priepustnosťou 1,5kb/s (pričom zaťaženie procesora neprekročilo 30%). Je nutné poznamenať, že pre iné protokoly môže byť táto hodnota odlišná, najmä ak je potrebná iná šablóna. Maximálny tok paketov vychádzajúcich z exportéra v konfigurácii použitej pri experimente bol menší ako 5kB/s. Výhodou je aj nezávislosť množstva exportných paketov od množstva prenesených dát na meranej linke za jednotku času.

Vzorkovanie sa ukázalo ako výhodné za účelom zníženia spotreby systémových zdrojov meracím nástrojom, pretože klesol počet paketov, ktoré boli spracovávané. Vzhľadom na nezávislosť od typu prevádzky a pomerne dobré výsledky je zaujímavé neuniformné náhodné pravdepodobnostné vzorkovanie založené na počte paketov

a uniformné náhodné pravdepodobnostné vzorkovanie. Bez nutnosti použitia vzorkovania, je možné vykonávať merania na linkách o rýchlosti 100Mb/s. Pre merania na linkách o rýchlosti 1Gb/s a vyšších, je už nevyhnutné nasadiť vzorkovanie alebo zvýšiť výpočtový výkon počítača, na ktorom je merací nástroj spustený..

## 9. Zhodnotenie riešenia

Predložená práca je zameraná na analýzu a popis existujúcich exportných protokolov vhodných na implementáciu v meracích architektúrach, ktoré spĺňajú požiadavky vznikajúceho štandardu IPFIX. Zvláštna pozornosť sa venuje výberu protokolu vhodného pre potreby pasívnych meraní objemových a aj časových charakteristík prevádzky v počítačových sieťach. Vďaka vysokej flexibilitě, jednoduchosti a efektívnosti bol zvolený, ako najvhodnejší, protokol NetFlow verzia 9.

V rámci riešenia diplomovej práce bol navrhnutý exportný modul meracieho nástroja BasicMeter, pridávajúci podporu protokolu NetFlow verzia 9. Export informácií o tokoch v tomto protokole, umožňuje na jednom zhromažďovači prijímať informácie od BasicMetra aj smerovačov Cisco súčasne. Prínosom je aj možnosť spolupráce BasicMetra s inými aplikáciami podporujúcimi spomínaný exportný protokol.

Vzhľadom na požiadavku pasívnych meraní QoS parametrov v segmente vysokorýchlostných sietí, nebola cieľom komplexná, ale efektívna implementácia štandardov pre export informácií o tokoch. Súčasťou implementácie exportného protokolu NetFlow verzia 9 bolo aj vytvorenie novej štruktúry, pre uchovávanie záznamov o aktívnych tokoch. Touto zmenou bolo sledované rovnomernejšie rozloženie výkonu medzi jednotlivé vlákna programu.

Funkčnosť modulu bola overená, meraním objemových charakteristík prevádzky. Overená bola aj funkcia vzorkovania pri odchyťovaní paketov zo siete. Pre účely týchto experimentov bola použitá simulovaná prevádzka protokolu FTP v rámci Laboratória počítačových sietí. Merací nástroj umožnil získať reálne hodnoty dátových tokov v sieti laboratória. Efektívnu architektúru BasicMetra potvrdila nízka spotreba systémových zdrojov aj pri relatívne vysokých prietokoch meranou sieťou. Meranie QoS parametrov na vysokorýchlostných sieťach typu 1 Gb/s až 10 Gb/s môže byť realizované, ak sa použije vzorkovanie.

## 10. Zoznam použitej literatúry

- [1] BRAY, T. et al.: Extensible Markup Language (XML) 1.1 [online] Publikované vo apríli 2004. [citované 7.4.2004] URL <http://www.w3.org/TR/xml11/>
- [2] NetFlow Services and Applications, White Paper, Cisco Systems, 1999, URL [http://www.cisco.com/warp/public/cc/pd/iosw/ioft/neflct/tech/napps\\_wp.htm](http://www.cisco.com/warp/public/cc/pd/iosw/ioft/neflct/tech/napps_wp.htm)
- [3] Clark, J., Murata, M.: RELAX NG Specification [online] Publikované v decembri 2001. [citované 4.2.2004]. URL <http://www.relaxng.org/spec-20011203.html>
- [4] Duffield, N., Grossglauser, M.: Trajectory Sampling for Direct Traffic Observation. In: Proceedings of ACM SIGCOMM 2000, Stockholm, Sweden, august 2000
- [5] J. Quittek, J., Briant, S., Molina, Information Model for IP Flow Information Export [online] Publikované vo februári 2005. [citované 9.4.2005] URL <http://www.ietf.org/internet-drafts/draft-ietf-ipfix-info-06.txt>
- [6] McCANNE, S. et al.: Libpcap — library for capturing packets [knihnica] Ver 0.8.3 URL: <http://www.tcpdump.org/release/libpcap-0.8.3.tar.gz>
- [7] SADASIVAN, G. — BROWNLEE, N.: Architecture for IP Flow Information Export [online] Publikované v marcii 2005. [citované 7.4.2005] URL <http://www.ietf.org/internet-drafts/draft-ietf-ipfix-architecture-07.txt>
- [8] <http://www.tcpdump.org/daily/tcpdump-current.tar.gz>
- [9] VEILLARD, D.: The XML C parser and toolkit of Gnome — libxml [knihnica] Ver2.6.19 [citované 9.4.2004]. URL <http://xmlsoft.org/sources/libxml2-2.6.19.tar.gz>
- [10] HEDENFALK, M.: Confuse - simple configuration file parser library [online] Publikované 17.10.2004. [citované 3.2.2004] URL <http://www.nongnu.org/confuse/>
- [11] Duffield N., A Framework for Passive Packet Measurement [online] Publikované vo februári 2002. [citované 14.4.2005] URL <http://psamp.ccrle.nec.de/drafts/draft-duffield-framework-papame-01.txt>
- [12] <http://www.tcpdump.org/release/libpcap-0.8.3.tar.gz>

- [13] Zseby, T., Molina, M., Sampling and Filtering Techniques for IP Packet Selection [online] Publikované vo februári 2005. [citované 9.4.2005] URL <http://www.ietf.org/internet-drafts/draft-ietf-psamp-sample-tech-06.txt>
- [14] J. Quittek, On the Relationship between PSAMP and IPFIX [online] Publikované vo októbri 2002. [citované 14.4.2005] URL <http://psamp.ccrle.nec.de/drafts/draft-quittek-psamp-ipfix-00.txt>
- [15] Shenker, S., Partridge, C., Guerin, R.: Specification of Guaranteed Quality of Service, RFC2212, September 1997
- [16] Nichols, K., Jacobson, V., Zhang, L.: A Two-bit Differentiated Services Architecture for the Internet, RFC2638, July 1999
- [17] Braden, R., Zhang, L., Berson, S., a i.: Resource ReSerVation Protocol (RSVP), RFC 2205, September 1997
- [18] Rosen, E., Viswanathan, A., Callon, R.: Multiprotocol Label Switching Architecture, RFC 3031, January 2001
- [19] Paxson, V., Almes, G., Mahadavi, J., a i.: Framework for IP Performance Metrics, RFC 2330, May 1998
- [20] ITU-T Recommendation Y.1540 [online] URL <http://www.itu.int/itudoc/itu-t/aap/sg13aap/history/y1540/>
- [21] Almes, G., Kalidindi, S., Zekauskas, M.: A One-way Packet Loss Metric for IPPM, RFC 2680, September 1999
- [22] Mathis, M., Allman, M.: A Framework for Defining Empirical Bulk Transfer Capacity Metrics, RFC 3148, July 2001
- [23] Demichelis, C., Chimento, P.: IP Packet Delay Variation Metric for IP Performance Metrics (IPPM), RFC 3393, November 2002
- [24] Almes, G., Kalidindi, S., Zekauskas, M.: A Round-trip Delay Metric for IPPM, RFC 2681, September 1999
- [25] Brownlee, N., Mills, C., Ruth, G.: Traffic Flow Measurement: Architecture, RFC2063, January 1997
- [26] Postel, J.: User Datagram Protocol, RFC 768, 28 August 1980
- [27] Zhang, K., Elkin, E.: XACCT's Common Reliable Accounting for Network Element (CRANE), RFC3423, November 2002
- [28] Setwart, R., Xie, Q., Morneault, K., a i.: Stream Control Transmission Protocol, RFC 2960, October 2000

- [29] Calhoun, P., Loughney, J., Guttman, E.: Diameter Base Protocol, RFC 3588, September 2003
- [30] Calato, P., MacFaden, M.: Lightweight Flow Accounting Protocol (LFAP) [online] URL [www.ietf.org/proceedings/01aug/slides/ipfx-6/](http://www.ietf.org/proceedings/01aug/slides/ipfx-6/)
- [31] Meyer, J., Reliable Streaming Internet Protocol Detail Records, August 2002.
- [32] Quittek, J., Zseby, T., Claise, B., a i.: Requirements for IP Flow Information Export, RFC 3917, October 2004
- [33] Leinen, S.: Evaluation of Candidate Protocols for IP Flow Information Export (IPFIX), RFC3955, October 2004
- [34] Walton, S.: Linux Threads Frequently Asked Questions,[online] URL <http://linas.org/linux/threads-faq.html>
- [35] Eclipse Foundation, [online] URL <http://www.eclipse.org/>
- [36] CVS - Concurrent Versions System, [online] URL <https://www.cvshome.org/>

## 11. Zoznam príloh

Súčasťou diplomovej práce sú nasledujúce prílohy:

1. Používateľská príručka
2. Systémová príručka
3. Zdrojové texty exportného modulu
4. CD médium
  - diplomová práca s prílohami v elektronickej podobe (pdf, sxw, rtf, doc)
  - merací nástroj BasicMeter so zdrojovými textami

## 12. Zoznam obrázkov a tabuliek

### Zoznam obrázkov

Obr. 3.1: Architektúra RTFM.....	9
Obr. 3.2: Bloková schéma architektúry IPFIX.....	10
Obr. 5.1: NetFlow paket.....	29
Obr. 5.2: Zmiešaný NetFlow paket.....	29
Obr. 5.3: Dátový NetFlow paket.....	30
Obr. 5.4: Šablónový NetFlow paket.....	30
Obr. 5.5: Formát hlavičky.....	30
Obr. 5.6: Formát flowsetu šablón.....	31
Obr. 5.7: Formát flowsetu dát.....	32
Obr. 5.8: Formát flowsetu šablón volieb.....	33
Obr. 5.9: Formát flowsetu dát volieb.....	35
Obr. 6.1: Architektúra meracej platformy.....	40
Obr. 6.2: Architektúra meracieho nástroja.....	41
Obr. 7.1: Bloková schéma meracieho nástroja BasicMeter.....	44
Obr. 7.2: Vznik kolízie pri súčasnom prístupe do zásobníka tokov.....	46
Obr. 8.1: Schéma zapojenia experimentu v Laboratóriu počítačových sietí.....	47
Obr. 8.2: Zaznamenaný priebeh prenosovej rýchlosti.....	49
Obr. 8.3: Systematické vzorkovanie založené na počte.....	51
Obr. 8.4: Systematické vzorkovanie založené na čase.....	51
Obr. 8.5: Vzorkovanie n-z-N.....	52
Obr. 8.6: Uniformné náhodné pravdepodobnostné vzorkovanie.....	52
Obr. 8.7: Neuniformné náhodné pravdepodobnostné vzorkovanie založené na počte.....	53

### Zoznam tabuliek

Tab. 2.1: Najvýznamnejšie parametre kvality služieb.....	4
Tab. 2.2: Rozdelenie a stručná charakteristika typov meraní.....	5
Tab. 3.1: Všeobecné požiadavky architektúry IPFIX.....	14
Tab. 6.1: Popis jednotlivých častí architektúry.....	41