

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

**Meranie a vyhodnocovanie  
prevádzkových parametrov v  
počítačových sieťach**

Diplomová práca

Študijný odbor: Výpočtová technika a informatika

Vedúci diplomovej práce:

Ing. František Jakab

Diplomant:

Marián André

Konzultant diplomovej práce:

Ing. František Jakab

Košice 2004

### **Čestné vyhlásenie**

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

Košice 10. 5. 2004

.....

*Vlastnoručný podpis*

Zadanie DP namiesto tohoto papiera.

## **Podakovanie**

Ďakujem Ing. Františkovi Jakobovi a Ing. Jurajovi Sučíkovi za odbornú pomoc, cenné rady a pripomienky. Ďakujem členom Laboratória počítačových sietí za podporu.

Názov práce: Meranie a vyhodnocovanie prevádzkových parametrov v počítačových sieťach

Pracovisko: Katedra počítačov a informatiky, FEI TU v Košiciach

Autor: Marián André

Vedúci DP: Ing. František Jakab

Konzultant DP: Ing. František Jakab

Dátum: 10. 5. 2004

Kľúčové slová: kvalita služieb, počítačová sieť, merania prevádzky, pasívne merania

Anotácia: Práca sa zaoberá problematikou merania prevádzkových parametrov kvality služieb v počítačových sieťach. Práca sa podrobne venuje najmä pasívnym meraniam parametrov kvality služieb v počítačových sieťach. Súčasťou práce je komparatívna analýza rôznych metód merania pasívnych parametrov. V práci je popísaný návrh, koncepcia a implementácia meracieho nástroja pre tento typ meraní.

Thesis title: Measurement and Evaluation of Operational Parameters in Computer Networks

Department: Department of Computers and Informatics, TU FEI Košice

Author: Marián André

Supervisor: Ing. František Jakab

Tutor: Ing. František Jakab

Date: 10. 5. 2004

Keywords: quality of service, computer network, traffic measurement, passive measurements

Annotation: The thesis deals with performance parameters measurement of quality of service in computer networks. The thesis focuses mainly on passive measurements of quality of services. The part of the thesis is comparative analysis of various passive measurement methods. The design, concept and implementation of basic measurement tool is introduced.

# Obsah

Úvod	1
<b>1 Formulácia úlohy</b>	<b>3</b>
<b>2 Analýza podmienok prenosu informácie</b>	<b>4</b>
2.1 Kvalita služieb . . . . .	4
2.2 Parametre kvality služieb . . . . .	6
2.3 Metódy merania prevádzkových parametrov . . . . .	6
2.3.1 Aktívne merania . . . . .	7
2.3.2 Pasívne merania . . . . .	9
2.3.3 Semi-aktívne merania . . . . .	9
<b>3 Pasívne metódy merania prenosových parametrov</b>	<b>11</b>
3.1 Metódy merania objemových charakteristík . . . . .	11
3.2 Metódy merania časových charakteristík . . . . .	12
3.3 Konceptia všeobecnej architektúry merania oneskorení . . . . .	13
3.4 Prostriedky pre synchronizáciu meracích bodov . . . . .	15
3.4.1 Sieťový časový protokol (Network Time Protocol, NTP) . . . . .	16
3.4.2 Globálny pozičný systém (Global Positioning System, GPS) . . . . .	18
3.4.3 Rádiový hodinový signál DCF77 . . . . .	20
3.5 Odchytávanie paketov . . . . .	21
3.6 Generovanie časových známkov . . . . .	21
3.7 Klasifikácia a filtrovanie . . . . .	22
3.8 Generovanie identifikátora paketu . . . . .	23
3.8.1 Výber položiek hlavičky IP paketu . . . . .	23
3.8.2 Funkcia pre generovanie identifikátora paketu . . . . .	24
3.8.3 Suma veľkostí uvažovaných položiek . . . . .	25
3.8.4 Jednosmerné slovníkové funkcie . . . . .	26
3.8.5 Kontrolné súčty . . . . .	26

3.8.6	Kompresné funkcie . . . . .	26
3.9	Prenos nameraných údajov . . . . .	27
3.9.1	Prenos údajov v pakete . . . . .	27
3.9.2	Prenos údajov v okruhu . . . . .	27
3.9.3	Prenos údajov mimo okruhu . . . . .	28
<b>4</b>	<b>Komparatívna analýza metodík merania a nástrojov</b>	<b>29</b>
4.1	Metrika výkonnosti IP (IP Performance Metric, IPPM) . . . . .	29
4.1.1	IPPM metrika pre meranie spojenia . . . . .	32
4.1.2	Metrika oneskorenia jednej cesty pre IPPM . . . . .	34
4.1.3	Metrika pre stratovosť paketov v jednej ceste pre IPPM . . . . .	35
4.1.4	Metrika pre oneskorenie uzavretej slučky pre IPPM . . . . .	35
4.2	ITU-T . . . . .	35
4.3	Real Time Flow Measurement, RTFM . . . . .	37
4.4	NetraMet . . . . .	38
4.5	IP Flow Information Export, IPFIX . . . . .	40
4.5.1	Bod merania . . . . .	42
4.5.2	Merací proces . . . . .	42
4.5.3	Exportovací proces . . . . .	44
4.5.4	Zhromažďovací proces (collecting process) . . . . .	45
4.5.5	Všeobecné požiadavky . . . . .	45
4.6	NetFlow . . . . .	46
4.6.1	NetFlow verzia 5 . . . . .	46
4.6.2	NetFlow verzia 9 . . . . .	47
4.7	NetMate . . . . .	47
4.8	Ntop . . . . .	47
<b>5</b>	<b>Návrh, koncepcia a architektúra meracieho nástroja</b>	<b>49</b>
5.1	Špecifikácia požiadaviek . . . . .	49
5.2	Koncepcia meracieho nástroja . . . . .	50

5.3	Návrh meracieho nástroja . . . . .	52
5.4	Architektúra meracieho nástroja . . . . .	53
<b>6</b>	<b>Implementácia meracieho nástroja</b>	<b>56</b>
6.1	Algoritmus spracovania paketu . . . . .	56
6.2	Knižnica libpcap . . . . .	58
6.3	Koncept verifikácie šablón . . . . .	59
<b>7</b>	<b>Experimentálne overovanie funkčnosti nástroja</b>	<b>61</b>
7.1	Inštalácia . . . . .	61
7.2	Experimentálne meranie v laboratórnom segmente . . . . .	61
7.2.1	Meranie využitia šírky pásma . . . . .	63
7.2.2	Meranie priepustnosti paketov . . . . .	64
<b>8</b>	<b>Zhodnotenie dosiahnutých výsledkov</b>	<b>66</b>
	<b>Zoznam použitej literatúry</b>	<b>68</b>
	<b>Zoznam príloh</b>	<b>73</b>
	<b>Zoznam obrázkov</b>	<b>74</b>
	<b>Zoznam tabuliek</b>	<b>74</b>

## Úvod

Diplomová práca sa zaoberá analýzou, popisom a špecifikáciou existujúcich metód pre vykonávanie meraní prevádzkových parametrov v počítačových sieťach.

Pojem kvalita služieb sa viaže na množinu parametrov definujúcich prevádzkové charakteristiky počítačovej siete. V práci budú popísané a analyzované jednotlivé parametre, rovnako ako budú analyzované charakteristiky jednotlivých metód merania.

V práci je popísaná koncepcia a návrh nástroja pre pasívne merania parametrov kvality služieb. Nástroj sa návrhom a celkovou koncepciou zameriava najmä na podporu formujúceho sa štandardu IP Flow Information Export (IPFIX). S týmto nástrojom budú realizované aj špecifikované merania prevádzkových parametrov sietí.

Práca je štruktúrovaná nasledujúcim spôsobom. Prvá kapitola podrobne formuluje úlohu a cieľ práce. Druhá kapitola sa venuje analýze podmienok prenosu informácie s požadovanými parametrami prenosu. V rámci tejto kapitoly je definovaný pojem kvalita služieb, sú definované parametre kvality služieb a druhy existujúcich metód meraní. Tretia kapitola sa podrobne venuje pasívnym metódam meraní, zaoberá sa analýzou problémov vznikajúcich pri vykonávaní pasívnych meraní a navrhuje možné riešenia. Obsahom štvrtej kapitoly je komparatívna analýza existujúcich metód a metodík, nástrojov a postupov pre vykonávanie pasívnych meraní. Ďalšie kapitoly sa zaoberajú popisom koncepcie, návrhu, implementácie nástroja a experimentov, ktoré majú za úlohu overiť funkčnosť nástroja.

Pri návrhu, plánovaní a aj zabezpečovaní služieb sa okrem základnej požiadavky spoľahlivej konektivity čoraz väčší dôraz kladie aj na zabezpečenie určitej, požadovanej úrovne kvality služieb. Úroveň kvality služieb je definovaná hodnotami prevádzkových parametrov kvality služieb, preto je potrebné vypracovať a navrhnúť metódy pre zabezpečenie kvality služieb.

Pre sledovanie a monitorovanie prevádzkových parametrov počítačovej siete existuje

tuje viacero dôvodov. Mnoho aplikácií, najmä aplikácií zaoberajúcich sa prenosom obrazových a zvukových informácií, je citlivých na dodržanie určitej úrovne parametrov prevádzky — týka sa to najmä oneskorenia, jednosmerného aj spätného.

Pojmy týkajúce sa kvality služieb sa stávajú predmetom zmluvných vzťahov medzi poskytovateľmi služieb a zákazníkmi. Zákazníkov zaujíma, či hodnoty prevádzkových parametrov, zmluvne dohodnuté v Service Level Agreement (SLA), sú aj skutočne dodržiavané.

Výstupy z meraní prevádzkových parametrov počítačových sietí sa často používajú pre ďalšie optimalizácie topológie sietí, ich profylaktiku a plánovanie ďalších rozšírení.

# 1 Formulácia úlohy

Cieľom predloženej práce je návrh a implementácia nástroja pre vykonávanie pasívnych meraní prevádzkových parametrov v počítačových sieťach. V rámci tejto úlohy je potrebné:

- analyzovať architektúry merania parametrov kvality služieb
- špecifikovať dostupné štandardy a koncepcie merania parametrov kvality služieb s dôrazom na koncepciu štandardu Internet Protocol Flow Information Export
- navrhnuť koncepciu nástroja pre vykonávanie pasívnych meraní
- implementovať merací nástroj
- overiť funkčnosť nástroja experimentálnymi meraniami
- dokumentovať navrhnutý a implementovaný nástroj

## 2 Analýza podmienok prenosu informácie s požadovanými parametrami prenosu

### 2.1 Kvalita služieb

Architektúra internetu je založená na modeli najlepšej prevádzky s minimálnym úsilím (best-effort traffic model). Tento model je dostatočne funkčný a vhodný pre tradičné sieťové aplikácie ako sú elektronická pošta a prenos súborov. Tieto aplikácie sú založené na spoľahlivom protokole prenosu dát (napr. Transmission Control Protocol, TCP) bez ďalších požiadaviek na zabezpečenie určitej úrovne kolísania oneskorenia alebo spätného oneskorenia. Na druhej strane, existuje množstvo aplikácií, ktoré od sieťovej architektúry na nižšej vrstve vyžadujú a pre svoju správnu a spoľahlivú činnosť potrebujú aj zabezpečenie takýchto parametrov. Z pohľadu počítačovej siete ide o rozšírenie spoľahlivosti a efektivity jej architektúry.

Riešením na prvý pohľad by mohlo byť zväčšenie šírky prenosového pásma — toto riešenie nie je nákladné a do istej miery môže priniesť úspech. Napriek tomu, mnoho aplikácií ako prenos videa na požiadanie (Video On Demand, VoD), IP telefónia, telekonferencie, televzdelávanie, digitálna televízia s vysokou rozlišovacou schopnosťou (High Definition TV, HDTV) a rozsiahle distribuované výpočtové systémy vyžadujú najmä garanciu časových charakteristík, nielen šírky prenosového pásma.

Kvalita komunikačných služieb (Quality of Service, QoS) (RFC2212, 1997) je daná množinou výkonových parametrov, ktoré charakterizujú prevádzku pri danom spojení. Tieto parametre môžu byť merané, vylepšované a do určitej miery aj garantované.

Požiadavky definované používateľom sa opierajú najmä o zmluvne definované podmienky v SLA (Service Level Agreement) — teda o dohodnuté parametre kvality služieb v rámci zmluvy medzi používateľom komunikačných služieb a ich poskytovateľom.

Postupom času a vývojom nových komunikačných technológií dochádza postupne ku konvergencii, teda zlučovaniu klasických telekomunikačných a dátových sietí. Telekomunikačná prevádzka sa začína prenášať na existujúce dátové siete, kde existuje multimediálna prevádzka — prenos zvuku a obrazu — vedľa klasickej dátovej prevádzky. Konvergencia sietí bola jedným z najsilnejších impulzov pre vývoj technológií merania, vyhodnocovania parametrov kvality služieb v počítačovej sieti.

Pri riešení požiadaviek na meranie a vyhodnocovanie parametrov kvality služieb je potrebné dbať aj na dosiahnutie efektivity riešenia. Efektívnosť riešenia je možné dosiahnuť len umiestnením mechanizmov zabezpečujúcich kvalitu služieb v počítačovej sieti po celej trase od zdroja až k cieľu prenosu informácie. V prípade, že je možné zabezpečiť umiestnenie a implementáciu týchto mechanizmov po celej ceste od zdroja až k cieľu, je možné hovoriť o **manažovateľnej počítačovej sieti**. V opačnom prípade nemožno hovoriť o manažovateľnej sieti, hoci aj napriek tomu sa jednotlivé mechanizmy používajú najmä u poskytovateľov služieb, ktorí pomocou týchto mechanizmov pridelujú prioritu pre určité dátové toky a takto preferujú určitých používateľov (Jakab, 2002).

Mechanizmy zabezpečujúce vyhodnocovanie a meranie parametre kvality služieb je možné implementovať za použitia rôznych technológií.

Najčastejšie používanou implementáciou a prístupom k riešeniu je implementácia pomocou technológie ATM (Asynchronous Transfer Mode). ATM ako spojovo-orientovaná (connection-oriented) technológia umožňuje nadviazať spojenie s už definovanou kvalitou prenosu.

Implementáciou na ktorú sa zameriava čoraz väčší význam je implementácia na tretej vrstve OSI modelu — pomocou použitia IP (Internet Protocol). Pri riešení problému zabezpečenia kvality služieb existujú dva prístupy:

**diferencované služby** (RFC2638, 1999) — poskytujú škálovateľné obmedzenie služieb bez potreby stavových informácií o prenose a signalizácie pri každom prenose medzi uzlami siete. Kombináciou nastavení bitov v poli určenom pre typ služby paketu je možné špecifikovať ako má s paketom pracovať smerovač

vo vnútri siete.

**integrované služby** — poskytujú diferenciáciu na základe explicitného vyjadrenia požiadaviek na kvalitu služby pomocou špeciálneho protokolu RSVP. (Resource Reservation Protocol) (Sučík, 2003)

V súvislosti s celkovým útlmom v oblasti používania ATM technológií a ústupe týchto technológií do pozadia sa čoraz väčšia pozornosť venuje zabezpečeniu kvality služieb pri použití IP a najmä v súvislosti s technológiou MPLS (Multi-protocol Label Switching).

MPLS je technológia využívaná najmä pri zrýchlení a zjednodušení smerovania v počítačových sieťach. Pre každý paket je generované krátke návěstie s pevnou dĺžkou, ktoré v ďalšom smerovacom procese vystupuje ako skrátená reprezentácia informácií obsiahnutých v hlavičke IP paketu. Nasledujúce smerovacie rozhodovania sa dejú na základe týchto návěstí namiesto informácií z hlavičky IP paketu. MPLS sa využíva aj pri zabezpečovaní kvality služieb najmä pri klasifikácii IP paketov.

## 2.2 Parametre kvality služieb

Pojem kvalita služieb je definovaný množinou parametrov. Je presne špecifikovaný počet parametrov, ich význam aj spôsob merania. Špecifikáciou kvality služieb sa zaoberajú dve organizácie IETF (Internet Engineering Task Force) a ITU-T (International Telecommunication Union — Telecom Standardization). IETF (RFC2330, 1998) sa zameriava na špecifikáciu presnej procedúry merania, zatiaľ čo ITU-T (Y.1540, 1999) popisuje skôr štatistické vyhodnocovanie parametrov kvality služieb. Najvýznamnejšie parametre kvality služieb sú opísané v tabuľke 2–1.

## 2.3 Metódy merania prevádzkových parametrov

Metódy merania je možné rozdeliť do troch kategórií. Ich rozdelenie s krátkou charakteristikou je popísané v tabuľke 2–2.

Parameter kvality služieb	Popis
šírka pásma (RFC3148, 2001)	parameter definovaný ako efektívne množstvo dát prenesených za jednotku času
stratovosť paketov (RFC2680, 1999)	množstvo nedoručených paketov alebo paketov doručených poškodených
jednosmerné oneskorenie (RFC2330, 1998)	as potrebný na odoslanie paketu od zdroja k cieľu
kolísanie oneskorenia (RFC3393, 2002)	parameter pre dva pakety definovaný ako rozdiel medzi hodnotou jednosmerného oneskorenia prvého paketu a hodnotou jednosmerného oneskorenia druhého paketu
spiatočné oneskorenie	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

**Tabulka 2 – 1** Najvýznamnejšie parametre kvality služieb

### 2.3.1 Aktívne merania

Aktívne merania využívajú pri meraní charakteristík počítačovej siete dodatočnú špeciálne vygenerovanú prevádzku. Používajú sa najmä pri plánovaní sietí pre predikciu zaťaženia siete a úpravy podmienok a parametrov v sieti (Paxson, 2000; Kalidindi, 1999; Paxson, 1998; RIPE-158, 1997). Aktívne merania sú kontrolovateľnými meraniami, ktoré môžu byť vykonané v ľubovoľnom čase a pre ľubovoľný typ prevádzky, ktorá je predmetom merania. (Seshan, 1997)

Typ merania	Popis
aktívne merania (intruzívne merania)	pre meranie charakteristík, parametrov generujú do siete ďalšiu testovaciu prevádzku
pasívne merania	pre meranie charakteristík siete a prevádzkových parametrov využívajú existujúcu prevádzku v sieti
semi-aktívne merania	pre meranie a vyhodnocovanie prevádzkových parametrov využívajú existujúcu prevádzku, ale modifikujú pakety napr. pridávaním časových známk k paketom, poprípade generovaním identifikátorov pre pakety

**Tabuľka 2–2** Rozdelenie a stručná charakteristika typov meraní

Charakter aktívnych meraní, generovanie prídavnej prevádzky kladie zvýšené nároky na priepustnosť a výkon sieťových prvkov, tak pasívnych ako aj aktívnych. Pri nedostatočných kapacitách sieťových prvkov a nevhodne zvolenom množstve generovanej testovacej prevádzky môže dochádzať k ovplyvňovaniu výsledkov merania.

Generovanie testovacej, prídavnej prevádzky by malo odrážať vlastnosti reálnej prevádzky. Generovaná prevádzka by sa mala svojou štruktúrou približovať k reálnej prevádzke, najmä emulácia špecifických vlastností aplikácií spôsobuje značné ťažkosti.

Jedným zo spôsobov vykonávania aktívnych meraní je prestavať aplikácie tak, aby mali schopnosť merať niektoré parametre kvality služieb. Iným prístupom je generovanie úplne umelej prevádzky — existujú aplikácie klient-server, ktoré vysielajú špeciálne sondovacie pakety a z týchto paketov sú vypočítavané charakteristiky a parametre siete.

### 2.3.2 Pasívne merania

Pri meraní charakteristík počítačovej siete a parametrov merania kvality služieb sa pri pasívnych meraniach negeneruje dodatočná prevádzka, meranie sa vykonáva len s existujúcou prevádzkou.

Tento prístup má viaceré výhody oproti aktívnym meraniam. Pri pasívnych meraniach nie sú prvky v sieti zaťažované dodatočnou prevádzkou. Vzhľadom na neexistenciu dodatočnej prevádzky, neexistuje ani možnosť prípadného ovplyvnenia výsledkov merania. Pri použití reálnej prevádzky nie je potrebné vyvíjať a venovať úsilie o vygenerovanie testovacej prevádzky s charakteristikami podobnými reálnej prevádzke. Keďže sa merania vykonávajú na reálnej, existujúcej prevádzke, výsledky sú dobre interpretovateľné a využiteľné v praxi — pri použití existujúcej prevádzky sa navyše stráca možnosť identifikácie testovacej prevádzky poskytovateľmi a následného uplatnenia špeciálneho spracovania kvôli dosiahnutiu lepších výsledkov.

Použitie pasívnych meraní má aj svoje nevýhody. Pasívne merania sú najmä kvôli nevytváraniu špeciálnej, testovacej prevádzky neriaditeľnými experimentami. Vzhľadom na nemožnosť ovplyvňovania prevádzky, nie je možné prenášať ani riadiace dáta, a preto je potrebné prídavné riadenie prevádzky pre prenos výsledkov merania. Pri meraní časových charakteristík, napr. jednosmerného oneskorenia, je potrebné zabezpečiť externú synchronizáciu hodín v jednotlivých meracích bodoch. Pre meranie oneskorenia je okrem toho potrebné rozlišovať pakety — vzniká potreba implementácie klasifikačných a filtračných algoritmov (Gupta, 1999).

### 2.3.3 Semi-aktívne merania

Pojem semi-aktívne merania bol zavedený najmä pre rozlíšenie pasívnych meraní, ktoré existujúcu prevádzku nemodifikujú žiadnym spôsobom, od tých, ktoré využívajú pre zisťovanie charakteristík a parametrov existujúcu prevádzku, ale pridávajú k nej aj ďalšie informácie — typickými informáciami sú časová značka paketu a jeho jednoznačný identifikátor. Modifikácia paketov je jednou z nevýhod semi-aktívnych

meraní, pretože môže ovplyvňovať výsledky meraní tým, že označené pakety môžu byť ďalej spracovávané.

Semi-aktívne merania sú náročnejšie na výkon meracieho bodu, najmä preto, že modifikované pakety sú posielané naspäť do siete a preto klasifikácia a modifikácia paketu musí byť urobená v reálnom čase priamo v meracom bode, zatiaľ čo pri pasívnych meraniach je možné klasifikáciu paketov vykonávať aj v inom mieste ako je merací bod.

Pre meranie časových charakteristík je potrebné použiť aspoň dva meracie body a je potrebné medzi nimi zabezpečiť synchronizáciu hodín. Druhou možnosťou je vzhľadom na povahu semi-aktívnych meraní pridávanie časových značiek priamo k paketom — v tomto prípade je možné urobiť vyhodnotenie oneskorenia v druhom meracom bode a nie je potrebný centrálny vyhodnocovací bod.

### 3 Pasívne metódy merania prenosových parametrov pre potreby vyhodnocovania kvality služieb

Pasívne metódy merania, nazývané aj neintruzívne, využívajú pre meranie charakteristík a parametrov kvality služieb existujúcu prevádzku v sieti, negenerujú dodatočnú testovaciu prevádzku.

Pasívne merania je možné rozdeliť do viacerých kategórií podľa počtu meracích bodov a podľa typu charakteristík, ktorých zisťovaním sa zaoberajú:

**merania objemových charakteristík** — sem sa zaraďujú merania šírky pásma a priepustnosti paketov

**merania časových charakteristík** — medzi merania časových charakteristík je možné zaradiť meranie jednosmerného oneskorenia (one-way delay), spätného oneskorenia (round trip time) a kolísania oneskorenia (jitter, variation delay)

Pre meranie jednotlivých charakteristík je potrebné definovať vstupné, počiatočné podmienky, je potrebné navrhnúť riešenie problémov vzniknutých pri meraní týchto charakteristík a napokon je potrebné navrhnúť konkrétne riešenia. V nasledujúcom texte budú rozobraté jednotlivé problémy vznikajúce pri meraní rôznych charakteristík.

#### 3.1 Metódy merania objemových charakteristík

Pre meranie intenzity prevádzky dátových tokov sa používajú najmä metódy s jedným meracím bodom. Intenzita prevádzky dátového toku je opísaná parametrami kvality služieb šírka pásma (bandwidth) a rýchlosť prenosu paketov (packet rate). Spôsob výpočtu týchto charakteristík sa odvíja od nasledujúceho schematického vzťahu:

$$rate = \frac{count}{time} \quad (3.1)$$

Význam jednotlivých členov vo vzťahu sa odvíja od meranej charakteristiky:

- **rate** — požadovaný parameter kvality služieb
- **count** — počet prenesených jednotiek údajov pre konkrétny parameter — pre šírku pásma je to počet bitov, resp. bajtov, pre rýchlosť prenosu paketov je to počet paketov
- **time** — dĺžka trvania merania

### 3.2 Metódy merania časových charakteristík

Pri meraniach parametrov kvality služieb sa pod časovými charakteristikami rozumie jednosmerné oneskorenie (one-way delay), spätné oneskorenie (round trip time) a kolísanie oneskorenia (variation, jitter). S metódami merania časových charakteristík sú späté dva základné problémy. Je to najmä problém synchronizácie hodín na jednotlivých meracích bodoch a generovania jednoznačných identifikátorov paketov.

Pre meranie časových charakteristík sa využívajú najmä merania s dvoma a viacerými meracími bodmi. Jednou z kľúčových metód pasívnych metód merania kvality služieb je metóda založená na rozpoznávaní paketov. Pasívne metódy žiadnym spôsobom neovplyvňujú pakety, preto rozpoznávanie musí byť realizované na základe charakteristík špecifikovaných v štandardných paketoch.

Časové charakteristiky je možné merať aj jedným meracím bodom. Ide najmä o merania spiatočného oneskorenia (round trip-time, RTT). Čas uzavretej slučky je čas, ktorý uplyne medzi vyslaním paketu s požiadavkou v jednom mieste a prijatím príslušného paketu s odpoveďou (napr. TCP-SYN/SYN-ACK). Tento spôsob však nie je možné použiť na odhad jednosmerného oneskorenia, pretože nie je možné zabezpečiť rovnakú cestu pre požiadavku aj odpoveď. Cesty môžu mať rôzne charakteristiky a slučka môže byť asymetrická (RFC2681, 1999).

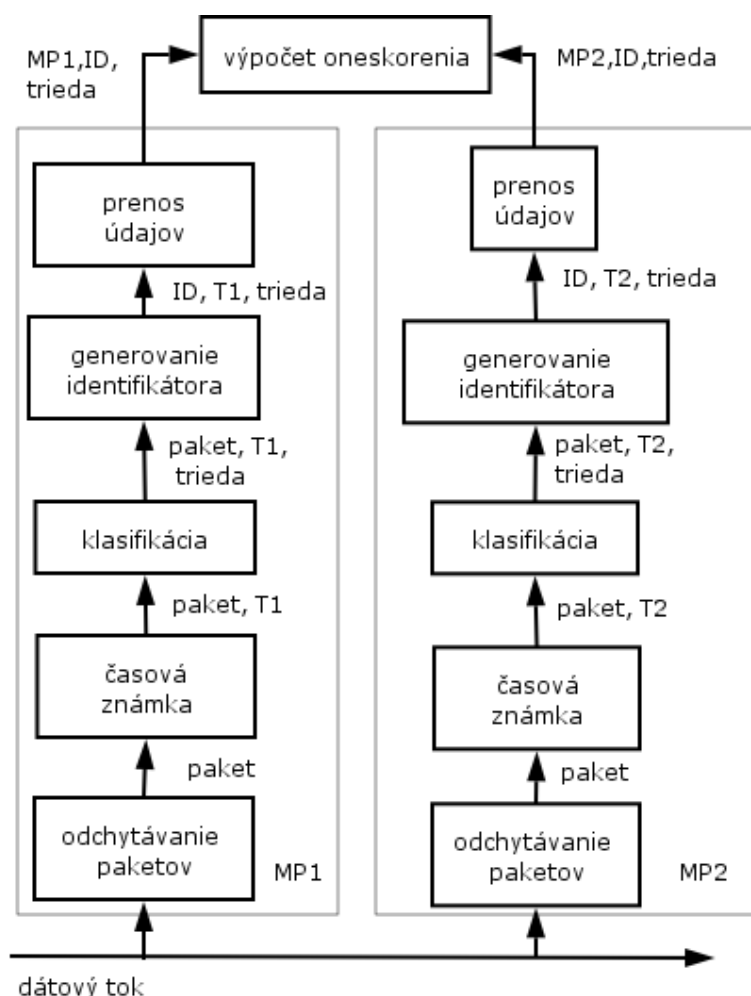
### 3.3 Konceptia všeobecnej architektúry merania oneskorení

Realizácia pasívnych metód merania časových charakteristík kvality služieb — najmä oneskorení — je založená na myšlienke odmerania času prechodu paketu medzi dvoma meracími bodmi. Pre odmeranie času prechodu paketu medzi dvoma meracími bodmi je potrebné zabezpečiť presnú synchronizáciu času na jednotlivých meracích bodoch a identifikovať paket. Vzhľadom na to, že táto metóda sa opiera o čisto pasívne merania, nie je možné modifikovať paket tak, aby obsahoval údaje o vygenerovanom identifikátore popri prípade o časovej známke k nemu prislúchajúcej. Tieto údaje je potrebné uchovávať vo vopred definovanom zbernom bode. V praxi tento bod nemusí byť nutne fyzicky odlišný od meracieho bodu, môže to byť s ním totožný proces — najmä kvôli redukcii réžie potrebnej k prenosu vygenerovaných informácií z meracích bodov na zberný bod. Všeobecná architektúra merania oneskorení je na obrázku 3–1.

Na obrázku 3–1 sú zobrazené dva meracie body  $MP_1$  a  $MP_2$ . Princíp merania oneskorenia spočíva v prechode paketu prvým meracím bodom, vygenerovania jednoznačného identifikátora paketu, vygenerovania časovej známky udávajúcej čas prechodu paketu a odoslanie získaných údajov na zberný bod. Samotné oneskorenie paketu je definované ako rozdiel príchodu paketu do meracích bodov:

$$\Delta T = T_2 - T_1 \quad (3.2)$$

Pre meraný paket je vypočítaný čas  $\Delta T$ . Vzťah časových známkov paketu medzi jednotlivými meracími bodmi je realizovaný práve prostredníctvom identifikátorov paketu. Identifikátor paketu musí byť jednoznačný a navyše, pretože nie je možné modifikovať pakety a obohatiť ich o informáciu o identifikátore, pri každom vygenerovaní musí byť tento identifikátor rovnaký. Preto je na generovanie identifikátora vyberať jednoznačné a pritom nemenné informácie. K týmto informáciám sa pridáva ešte informácia o čase  $\Delta T_1$ . Čas  $\Delta T_1$  predstavuje priemerný čas prechodu paketu do meracieho bodu  $MP_1$  k meraciemu bodu  $MP_2$ . Pokiaľ paket s daným identifikátorom odchytený v jednom meracom bode nedôjde do druhého meracieho bodu pred



Obrázok 3–1 Všeobecná architektúra merania oneskorenia

uplynutím času  $\Delta T_1$ , je tento paket považovaný za stratený. Tento spôsob výpočtu jednosmerného oneskorenia pomocou rozdielu oneskorenia medzi dvoma meracími bodmi pre špecifický paket je sémanticky zhodný so singletonovou metódou merania jednosmerného oneskorenia.

Vypočítavanie času  $\Delta T$  pre každý paket by kládlo veľké nároky na výpočtovú a pamäťovú kapacitu meracieho bodu, rovnako ako na jeho priepustnosť, preto sa pre jednotlivé meracie body definujú filtre, ktoré obmedzia množstvo dát významných pre ďalšie spracovanie meracím bodom. Pre konečné spracovanie zberným bodom a určenie jednosmerného oneskorenia na trase danej dvoma meracími bodmi má však

význam brať do úvahy aj typ zachytených a spracovaných paketov, preto sú filtre definované na jednotlivých meracích bodoch súčasťou výsledku.

Pri inštalovaní a prevádzke meracích bodov je treba riešiť niekoľko problémov s tým spojených. Umiestnenie meracích bodov je veľmi dôležité z pohľadu relevancie zistených údajov. Ak je cieľom merania získať prehľad a informácie o oneskorení medzi zdrojom a cieľom prenosu, je potrebné umiestňovať merací bod tak blízko k zdroju, resp. cieľu ako je to len možné. Pri tomto probléme je potrebné poznať fyzickú cestu, ktorou budú prechádzať analyzované dátové toky.

Pri použití viacerých meracích bodov je potrebné zabezpečiť synchronizáciu jednotlivých meracích bodov.

Problém súkromia je takisto jedným z dôležitých problémov, ktorým je potrebné sa pri inštalácii a prevádzke meracieho bodu zaoberať. Pri vykonávaní pasívneho merania oneskorenia je odchytná reálna prevádzka klientov, preto je potrebné zabezpečiť merací bod tak, aby nedošlo k úniku informácií, poprípade k ich poškodeniu.

Pri vysokorýchlostných a širokopásmových sieťach je potrebné riešiť problémy súvisiace so stratenými, poprípade duplikovanými paketmi a s celkovým množstvom odoslaných paketov.

### **3.4 Prostriedky pre synchronizáciu meracích bodov**

Synchronizácia meracích bodov je významným problémom pri meraní časových charakteristík kvality služieb. Vzhľadom na dôležitosť dát získaných meraním času na meracích bodoch — vygenerované časové známky paketov — je potrebné zabezpečiť čo možno najpresnejšiu synchronizáciu meracích bodov. Ďalším dôvodom je koordinácia meraní — pri koordinácii meraní je možné využiť systém „trojcestného podania si rúk“ (3-way handshake) známeho z inicializácie spojenia pri protokole TCP. V praxi sa pre synchronizáciu a koordináciu meracích bodov používajú najmä:

- sieťový časový protokol (Network Time Protocol, NTP)

- globálny pozičný systém (Global Positioning System, GPS)
- hodinové rádiové signály (DCF77)

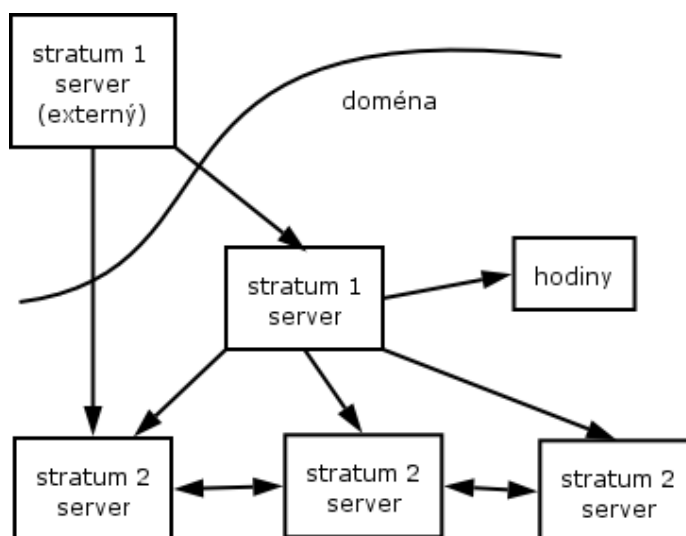
### 3.4.1 Sieťový časový protokol (Network Time Protocol, NTP)

NTP (RFC1305, 1992) je časový distribuovaný protokol založený na rozmiestnení časových serverov vo viacerých vrstvách. Každá vrstva je v terminológii NTP nazývaná *stratum*. Jednotlivé vrstvy podliehajú hierarchii protokolu. Servery umiestnené v jednej vrstve sa spájajú medzi sebou a poskytujú časové synchronizačné služby serverom na nižšej, v hierarchii NTP podradenej vrstve. Servery na najvyššej vrstve (stratum 1) sú pripojené priamo na zdroj veľmi presného časového signálu, napr. atómové hodiny alebo prijímače rádiového časového signálu. Prijímače rádiového signálu sú po pripojení sa na autoritatívny zdroj času (GPS, vysielajúce rádiového časového signálu) schopné poskytovať vysoko presné časové služby serverom na stratum 1 úrovni.

Vzhľadom na riziko zlyhania zdrojov časového signálu, sa servery na najvyššej úrovni okrem týchto zdrojov spájajú aj medzi sebou. NTP predpokladá správnu hodnotu času a neprimerané hodnoty dokáže do určitej miery napraviť, ak však hodiny divergujú o určitú hodnotu od času poskytovaného ostatnými servermi najvyššej úrovne, stratum 1 servery prestanú používať svoje vlastné hodiny.

Servery na nižších úrovniach (úroveň stratum 2, stratum 3, atď.) získavajú časové údaje od serverov na rovnakej alebo vyššej úrovni ako je ich vlastná. Každý server najvyššej úrovne špecifickej pre danú doménu by mal získavať časové údaje aspoň od dvoch serverov na vyššej úrovni a mal by sa spájať s ostatnými servermi v jeho doméne na rovnakej úrovni a aspoň s jedným serverom na rovnakej úrovni mimo domény. Servery nižšej úrovne neposkytujú svoje časové služby serverom vyššej úrovne – vystupujú v úlohe klienta. Na obrázku 3–2 je znázornená komunikácia medzi NTP servermi v špecifickej doméne.

Ak NTP server emuluje správanie klienta a získava časové údaje od iného NTP



Obrázok 3–2 Komunikácia medzi NTP servermi v doméne

servera, tak odmeria čas potrebný na získanie odpovede. Predpokladá, že oneskorenie je  $\frac{1}{2}$  času potrebného na získanie odpovede a na základe toho vypočíta posunutie lokálnych hodín. Najmä kvôli rôznym sieťovým podmienkam, môžu byť výsledné hodnoty oneskorenia rozdielne na dvoch častiach cesty. Komunikáciou s viacerými servermi získa NTP server pomerne presnú množinu platných hodnôt časov, z ktorých potom vypočíta posunutie lokálnych hodín. Toto posunutie sa nazýva *drift*. Pri prvom spustení NTP server väčšinou potrebuje urobiť veľké zmeny v nastavení časových údajov na lokálnych hodinách. Takýto skok by však mohol spôsobiť problémy pri vykonávaní ďalších aplikácií; typickým príkladom sú časované aplikácie v dávkovom spracovaní, poprípade záznamový (logovací) subsystém operačného systému. NTP server sa preto snaží urobiť len sériu veľmi malých zmien, táto vlastnosť je priamo podporovaná operačnými systémami unixového typu, kde sa požiadavka na sériu veľmi malých zmien lokálnych hodín premieta do zmeny relatívnej dĺžky jednej sekundy — ide o zmeny v rádoch milisekúnd.

NTP server priebežne počíta drift lokálnych hodín počítača a používa ho na kontinuálnu zmenu. Výpočet driftu sa môže meniť v závislosti na presnosti lokálnych hodín. Ich rastúca presnosť je závislá na dobe ako dlho je spustený NTP server.

Cieľom NTP servera je pomocou série malých zmien v lokálnych hodinách počítača vypočítaných komunikáciou s viacerými zdrojmi priblížiť k skutočnému medzinárodnému koordinovanému času (Universal Coordinated Time, UTC). Pre NTP server je dôležitá komunikácia s viacerými zdrojmi, ktorá vylučuje pri problémoch na jednom zdroji výrazné odchýlenie sa od správneho času. Rovnako dĺžka spustenia NTP servera a presnosť driftu má vplyv na udržanie presného času aj v prípade odpojenia NTP servera od ostatných zdrojov presného času. V takom prípade je NTP server schopný udržať presný čas po dobu niekoľkých hodín.

Presnosť synchronizácie počítača pomocou NTP servera do veľkej miery závisí od výkonnosti koncového prenosu v počítačovej sieti, vrátane NTP klientov a serverov. Ak je NTP server synchronizovaný so stratum 1 servermi, je dosiahnuteľná presnosť v rádoch milisekúnd.

### **3.4.2 Globálny pozičný systém (Global Positioning System, GPS)**

GPS je pozičný a navigačný systém založený na satelitnej komunikácii. Hoci bol tento systém pôvodne vyvíjaný pre potreby armády, napokon našiel uplatnenie v širokej škále aplikácií.

Globálny pozičný systém pozostáva z troch segmentov:

- satelitný (vesmírny) segment
- riadiaci segment
- používateľský segment

Satelitný (vesmírny) segment pozostáva z konštelácie 24 satelitov s niekoľkými náhradnými satelitmi. Každý satelit obehne Zem raz za 12 hodín po niektorej zo šiestich orbitálnych hladín. Konštelácia satelitov je zostavená tak, aby z ľubovoľného miesta na Zemi bolo v každom momente viditeľných päť až osem satelitov.

Riadiaci segment je systém monitorovacích staníc, pozemných antén a hlavnej riadiacej stanice. Monitorovacie stanice merajú signál zo všetkých viditeľných satelitov. Zhromaždené údaje sú spracovávané hlavnou riadiacou stanicou. Jej úlohou je

z týchto dát vypočítavať orbity a aktualizovať navigačné údaje v satelitoch vrátane úpravy hodín. Revidované údaje sú jednak poslané späť satelitom, sú aj šírené cez rádiové signály až ku GPS prijímačom.

Prijímače GPS signálu tvoria používateľský segment. Táto časť systému má za úlohu signál z pozemných antén konvertovať do informácií o čase a polohe GPS prijímača. Na výpočet polohy a času používa GPS metódu triangulácie. Metóda triangulácie spočíva v meraní a porovnávaní doby rádiového signálu vysielaného zo štyroch viditeľných satelitov so známou pozíciou. Každý satelit vysielá unikátny pseudo-náhodný kód (pseudo-random code, PRC), čo umožňuje vysielat' na rovnakej frekvencii. Tri merania sa používajú pre určenie polohy GPS prijímača v trojrozmernom priestore, štvrté meranie sa používa pre určenie času.

Nevýhoda metódy triangulácie spočíva vo vysokých nárokoch na presnosť merania. Presnosť metódy triangulácie sa znižuje najmä kvôli používaniu GPS prijímačov s menej presnými hodinami. Systém GPS sa toto snaží odstrániť používaním ďalšieho satelitu počas procesu triangulácie. Použitie ďalšieho satelitu umožňuje do istej miery opraviť časový posun a tak udržiavať vysokú mieru presnosti. Napriek tomu metóda triangulácie vyžaduje aj precízne časovanie zo strany satelitov pri vysielaní PRC. Precízne časovanie je preto kritickým prvkom správnej implementácie GPS.

Globálny pozičný systém používa svoj vlastný systémový čas odvodený od zložených hodín pozostávajúcich zo všetkých funkčných satelitov a časového štandardu UTC. Každý GPS satelit obsahuje štyri atómové hodiny obsahujúce atómy cézia a rubídia s veľmi vysokou úrovňou presnosti. Satelity vysielajú časové informácie ako súčasť signálov pre monitorovacie pozemné stanice. Hlavná monitorovacia stanica zhromažďuje údaje a z výpočtov robí potrebné úpravy hodín. Revidovaný signál je potom späť vyslaný do satelitov.

Globálny pozičný systém poskytuje dostatočne presné riešenie pre problém synchronizácie času. Signál môže byť prijatý kdekoľvek na Zemi a samotný GPS prijímač dosahuje presnosť s maximálnou odchýlkou sto nanosekúnd.

Hlavným nedostatkom GPS je to, že GPS prijímače vyžadujú priamu viditeľnosť

na štyri alebo viac satelitov. Vzhľadom na to, že GPS prijímač by mal byť spojený s meracím bodom, môže to spôsobovať problémy, keďže meracie body sa nachádzajú v blízkosti hlavných uzlov sieťovej infraštruktúry bez okien alebo v suterénoch (serverovne, haly vo výpočtových strediskách a pod.).

### 3.4.3 Rádiový hodinový signál DCF77

Pre synchronizáciu času na meracích bodoch je možné použiť aj rádiový signál. Jednou z možností je použitie rádiového signálu DCF77, ktorý je vysielaný na dlhých vlnách na frekvencii 77,5 kHz zo stanice neďaleko Frankfurtu nad Mohanom v Nemecku. Signál môže byť prijímaný takmer v celej strednej Európe a používa sa napríklad na synchronizáciu verejných hodín na železničných stanicách.

V distribuovanom signále sa nachádzajú dve časové informácie. Prvou informáciou je časový telegram založený na 59 pulzoch za minútu. Telegram sa začína chýbajúcim 60. sekundovým pulzom. Každý začiatok sekundy je označený znížením amplitúdy nosnej frekvencie o 75 % na 0,1 až na 0,2 sekundy. Dĺžka tejto značky reprezentuje binárne kódovanú jednotku alebo nulu. Vysielaná informácia obsahuje čas, dátum, paritu a stavový bit. Kvôli filtrovaniu a signálovému spracovaniu rádiového signálu na potlačenie interferencie sa používa časový posun 10 ms v prijímači. Nevýhodou tejto metódy sú fluktuácie v signále, ktoré môžu viesť k zlému určeniu začiatku sekundy. Presnosť tejto metódy je limitovaná na 1 ms za dobrých podmienok.

Druhý spôsob distribúcie času je založený na fáze šumu v 77,5 kHz nosnom signále. Tento šum je pseudo-náhodná bitová postupnosť 512 bitov, ktorá je vysielaná medzi sekundovými časovými značkami. Koreláciou s lokálnymi sekvenciami pseudo-náhodných bitov pri širokopásmových prijímačoch je možné získať časové značky s rozptylom v rádoch mikrosekúnd — zvyčajne ide o presnosť 20 mikrosekúnd voči UTC.

Medzi hlavné výhody tohoto spôsobu synchroniácie času patrí nenáročnosť riešenia. Väčšinou ide o zákaznícky obvod s časovaním menej náročným na presnosť a

s jednoduchou inštaláciou antény, ktorá nepotrebuje priamu viditeľnosť.

Nevýhody súvisia so základným princípom tohoto spôsobu — so šírením rádiového signálu. Problémom je atmosferické rušenie rádiového signálu. Pre presnejšie určenie synchroniácie času by bolo potrebné poznať fyzickú vzdialenosť k vysielateľu. DCF77 je vysielaný iba v strednej Európe, preto môže pokrývať len merania vykonávané v strednej Európe. Rádiové signály sú však synchronizované po celom svete, preto je možné využiť rozdielne rádiové signály pre meracie body na rozdielnych kontinentoch (Zseby, 2001).

### 3.5 Odchyťovanie paketov

Pasívne merania sú uskutočňované odchyťovaním kópií paketu a získavaním informácií obsiahnutých v týchto paketoch. Pri meraní oneskorení je potrebné pre funkciu generujúcu jednoznačný identifikátor paketov okrem samotnej hlavičky odchytiť navyše určitý počet bajtov z dátovej časti paketu. Počet bajtov zachytených z dátovej časti paketu musí byť daný tak, aby sa vylúčila možnosť kolízií. Podľa Duffielda (Duffield, 2000) je uvedené, že prvých 40 bajtov z dátovej časti je postačujúcich.

Výkon odchyťovacej časti je limitovaný niekoľkými faktormi:

- počtom prerušení vyvolaných sieťovými rozhraniami
- počtom prepnutí kontextu medzi priestorom jadra operačného systému (kernel-space) a priestorom používateľských aplikácií (userspace)
- množstvom dát prenesených do používateľskej oblasti
- ďalším zaťažením systému

### 3.6 Generovanie časových známk

Časové známky (timestamp) sú generované ako absolútne hodnoty času. Pre unixové operačné systémy je absolútnym časom, čas od začiatku unixovej epochy,

1.1.1970. Počet bitov  $l_t$  použitých na reprezentáciu časovej známky je závislý na požadovanej presnosti pre danú metódu merania.

Jednou z možností redukcie počtu bitov použitých pre časové známky je použitie relatívnych hodnôt času. Je možné predpokladať maximálny čas  $t_{max}$ , ktorý paket potrebuje na presun v sieti od vstupného meracieho bodu po výstupný merací bod. Časová známka musí byť jednoznačná len v rámci tohoto limitu. Hodnota  $l_t$  nezávisí len od požadovanej presnosti reprezentácie času, ale aj na preddefinovanom limite pre maximálny čas, ktorý potrebuje paket na prechod sieťou.

Ďalšia z možností je použiť absolútnu reprezentáciu času pre prvý paket v intervale  $\langle 0, t_{int} \rangle$  a pre nasledujúce pakety v danom intervale použiť relatívne hodnoty času. Presnosť môže byť ovplyvnená, ak čas použitý procesom generujúcim časové známky nie je rovnaký pre všetky pakety.

### 3.7 Klasifikácia a filtrovanie

Klasifikácia paketov je potrebná v prípade, že merania len vybraných paketov. Hlavné výhody klasifikácie spočívajú v zmenšení množstva dát pre vyhodnotenie merania a zmenšenie času potrebného na spracovanie ďalšími časťami meracieho bodu.

Klasifikácie vyberá pakety so špecifickými charakteristikami — takýmito paketmi sú pakety patriace do špecifického toku, triedy kvality alebo triedy prevádzky.

Často je potrebné okrem identifikátora paketu uchovávať aj informáciu o triede kvality, poprípade informáciu o toku, do ktorého patrí paket. Identifikátor paketu často obsahuje dodatočnú informáciu, najmä kvôli tomu, že je vypočítaný bijektívnou funkciou, takou funkciou je napríklad bezstratová komprimačná funkcia, ktorá komprimuje hlavičku IP paketu, môže byť použitá na dekomprimáciu informácií v cieľovom meracom bode. V ostatných prípadoch je potrebné prenášať na ďalšie spracovanie okrem identifikátora paketu aj informáciu o toku, do ktorého patrí paket.

Najjednoduchším algoritmom klasifikácie je lineárne vyhľadávanie. Lineárne vy-

hľadávanie využíva na uchovávanie pravidiel spojkový zoznam. Pravidlá sú uložené v poradí podľa znižujúcej sa priority. Paket sa sekvenčne porovnáva s každým pravidlom, pokiaľ sa nenájde pravidlo vyhovujúce všetkým poliam v hlavičke IP paketu. Algoritmus lineárneho vyhľadávania je jednoduchý, pamäťovo efektívny, ale nie je dobre škálovateľný. Čas klasifikácie paketu rastie lineárne s počtom pravidiel.

### 3.8 Generovanie identifikátora paketu

Pasívne metódy merania sú založené na princípe nulovej modifikácie paketu a sledovaní reálnej prevádzky. Preto je rozpoznávanie paketov pri meraní časových charakteristík realizované generovaním jednoznačného identifikátora paketu. Identifikátor paketu je založený na existujúcich položkách v hlavičke paketu, poprípade na spojení položiek hlavičky paketu s určitou množinou bajtov z dátovej časti paketu. Základnou požiadavkou na funkciu generujúcu identifikátor paketu je jej schopnosť vygenerovať jedinečný identifikátor vo viacerých bodoch merania. Identifikátor paketu by mal byť preto založený na nemenných, invariantných položkách počas doručenia paketu, alebo na predpovedateľných položkách v IP pakete. Vysoko variabilné položky paketov sú pre jedinečnosť identifikátora paketu vhodnejšie ako položky paketov so statickými hodnotami, resp. položky paketov, kde sa strieda malá množina hodnôt, poprípade sa hodnoty v položke nemenia.

#### 3.8.1 Výber položiek hlavičky IP paketu

V tejto časti budú popísané položky, ktoré svojou povahou vyhovujú podmienkam pre výber položiek z hlavičky IP paketu. Podmienky pre vhodnosť výberu položiek pre generovanie identifikátora paketu sú nasledujúce:

- pre generovanie by mali byť vybrané položky, ktoré existujú v pakete, nie je potrebná žiadna modifikácia paketu
- položky sú invariantné, alebo ich hodnota je predpovedateľná aspoň v rámci prenosu

- položky majú vysokú variabilitu medzi jednotlivými paketmi — zaisťuje sa tak jedinečnosť identifikátorov, teda sa znižuje riziko kolízií identifikátorov

Položka hlavičky IP paketu	Nemennosť počas cesty	Variabilita medzi paketmi	Uvažované
header	áno	extrémne malá	nie
dĺžka hlavičky	áno	malá	nie
typ služby (TOS)	nie	môže byť vysoká	nie
celková dĺžka	áno	môže byť vysoká	áno
identifikátor datagramu	áno	vysoká	áno
príznamy	nie	priemerná	nie
offset fragmentu	nie	môže byť vysoká	nie
čas trvania (time to live, TTL)	nie	môže byť vysoká	nie
protokol	áno	malá	áno
kontrolný súčet hlavičky	nie	môže byť vysoká	nie
zdrojová adresa	áno	môže byť vysoká	áno
cieľová adresa	áno	môže byť vysoká	áno

Tabuľka 3 – 3 Položky hlavičky IP paketu

### 3.8.2 Funkcia pre generovanie identifikátora paketu

Funkcia generujúca identifikátor paketu musí dosiahnuť vyváženosť medzi požiadavkou na malé hodnoty identifikátora paketu a jedinečnosť identifikátora. Tieto dve požiadavky sú v rozpore, pretože čím viac bitov je použitých na identifikátor paketu, tým nižšia je pravdepodobnosť kolízie. Pravdepodobnosť kolízie v zaznamenej premávke závisí od:

- distribúcie postupnosti bitov na vstupe funkcie generujúcej identifikátor paketu

- funkcie generujúcej identifikátoru paketu
- veľkosti identifikátora paketu  $l_{id}$
- použitom operačnom systéme

Cieľom vyváženosti je dosiahnuť akceptovateľne nízku pravdepodobnosť kolízií identifikátorov paketov, ktoré neprekračuje kapacitu dostupnú pre prenos namera-  
ných údajov. Identifikátor paketu musí byť jedinečný pri určitom časovom intervale  $\langle 0, t_{max} \rangle$ . Ohraničenie na časovom intervale ohraničuje maximálny možný počet kombinácií na množstvo paketov  $n_{max}$ , ktoré môžu byť merané v tomto časovom intervale.

Pri generovaní identifikátora paketu z uvažovaných položiek hlavičky IP paketu existuje viacero možností:

- suma veľkostí uvažovaných položiek
- jednosmerné slovníkové (hashovacie) funkcie
- kontrolné súčty (checksums)
- kompresné funkcie

### 3.8.3 Suma veľkostí uvažovaných položiek

Pri mapovaní postupnosti veľkého množstva bitov do menšej postupnosti bitov vzniká veľká pravdepodobnosť výskytu kolízie. Použitie vybraných položiek hlavičky IP paketu ako identifikátora je spôsob ako takúto pravdepodobnosť významne znížiť. Tento spôsob nevyžaduje ďalšie spracovanie. V praxi sa používajú dva prístupy:

$$id = \sum_{i=0}^n p_i \quad (3.3)$$

kde  $id$  je identifikátor paketu,  $n$  je počet uvažovaných položiek IP paketu,  $p_i$  sú jednotlivé položky

Výhodnejším postupom je použitie modifikovanej funkcie pre vytvorenie jednoznačného identifikátora paketu:

$$id = \sum_{i=0}^n p_i \bmod b \quad (3.4)$$

kde  $id$  je identifikátor paketu,  $n$  je počet uvažovaných položiek IP paketu,  $p_i$  sú jednotlivé položky IP paketu,  $b$  je počet uvažovaných pravidiel pri klasifikácii a filtrovaní.

#### 3.8.4 Jednosmerné slovníkové funkcie

Najpoužívanejšou jednosmernou slovníkovou funkciou je kryptografická funkcia založená na algoritme MD5 generujúca 128 bitový odtlačok správy ľubovoľnej dĺžky. Kryptografické funkcie sú odolné voči kolíziám.

#### 3.8.5 Kontrolné súčty

Medzi najpoužívanejšie algoritmy kontrolných súčtov patrí cyklický kontrolný súčet s redundanciou (Cyclic Redundant Checksum, CRC32). Primárne sú algoritmy kontrolných súčtov používané pre detekciu chýb v dátach a ich opravu, z toho vyplýva aj ich slabá odolnosť voči kolíziám identifikátorov. Frekvencia kolízií závisí od veľkosti CRC a od veľkosti generačného polynómu.

#### 3.8.6 Kompresné funkcie

Stupeň kompresie pri hlavičke IP paketu je možné ovplyvniť predpokladmi o meranej prevádzke (verzia IP protokolu je 4 alebo 6, maximálna hodnota TTL je daná). Kompresiou je možné dosiahnuť nízku pravdepodobnosť kolízie. Výhodou kompresných funkcií je ich bijektivnosť, teda z identifikátora paketu získaného kompresnou funkciou je možné spätným procesom získať ďalšie informácie o meraní.

### 3.9 Prenos nameraných údajov

Pre výpočet parametrov kvality služieb je potrebné vyhodnotiť údaje z viacerých paketov. Ak je na meranie použitých viacero meracích bodov, je potrebné preniesť namerané a vygenerované údaje do zberného bodu. Zberným bodom môže byť aj jeden z meracích bodov najmä kvôli redukcii množstva prenášaných dát.

Existuje niekoľko spôsobov prenosu nameraných a vygenerovaných údajov:

- prenos údajov v paketoch,
- prenos údajov v okruhu — namerané a vygenerované údaje sú prenášané tou istou cestou ako prevádzka, z ktorej boli získané,
- prenos údajov mimo okruhu — namerané a vygenerované údaje sú prenášané inou cestou ako prevádzka, z ktorej boli získané.

#### 3.9.1 Prenos údajov v pakete

Prenos údajov v pakete vyžaduje modifikáciu paketov, čím sa toto meranie klasifikuje ako semi-aktívne. Výhodou tohoto prístupu je to, že zberný bod môže byť umiestnený v jednom meracom bode, čím sa znižuje režia na prenos údajov od meracích bodov k zbernému bodu.

#### 3.9.2 Prenos údajov v okruhu

Prenos údajov v okruhu znamená, že všetky namerané a vygenerované údaje sú prenášané tou istou cestou ako prevádzka, z ktorej sú získané. Toto vedie k podobným problémom ako pri aktívnych meraniach, ktoré vyplývajú z použitia tej istej cesty. Odosielanie paketov s nameranými údajmi odporuje podstate pasívnych meraní, pretože do istej miery ovplyvňuje reálnu prevádzku. Odosielanie výsledkov meraní sa však nedá stotožniť s generovaním testovacej prevádzky pri aktívnych meraniach. Typ a časový rámec pre odoslanie testu prevádzky pre aktívne merania

sú predpísané na základe úlohy merania, naproti tomu odosielanie výsledkov merania môže byť riadené inými prostriedkami ako testovacia prevádzka. Odosielanie výsledkov merania môže byť vykonávané so zníženou prioritou, iba v čase nízkeho zaťaženia siete alebo cestami, ktoré nie sú zaťažené. Preferovanie niektorej alternatívy záleží od povahy meranej charakteristiky.

### **3.9.3 Prenos údajov mimo okruhu**

Prenos údajov mimo okruhu znamená prenos nameraných a vygenerovaných údajov po oddelených cestách. Oddelené cesty môžu byť dosiahnuté napríklad pridaním ďalšieho sieťového rozhrania na meracie body a vytvorením oddelenej meracej siete. Tento spôsob neovplyvňuje reálnu prevádzku, na druhej strane však vyžaduje prídavné kapacity na sieti.

## 4 Komparatívna analýza metodík merania a nástrojov

V komparatívnej analýze budú popísané jednotlivé metódy, štandardy a ich existujúce implementácie pre vykonávanie pasívnych metód merania. Vzhľadom na to, že oblasť merania parametrov kvality služieb je relatívne nová, budú do analýzy zahrnuté aj vznikajúce štandardy vo forme návrhov a odporúčaní. V rámci komparatívnej analýzy budú analyzované výhody, nevýhody a odporúčania jednotlivých metodík.

### 4.1 Metrika výkonnosti IP (IP Performance Metric, IPPM)

IPPM predstavuje všeobecný rámec pre definíciu a vývoj nových metrík pre meranie výkonnosti internetového protokolu (IP). Definuje kritériá pre vývoj nových metrík a terminológiu pre ich opis. Vývojom IPPM sa zaoberá pracovná skupina organizácie IETF (Internet Engineering Task Force) s názvom IPPM-WG (Internet Protocol Performance Metric Working Group).

Pod pojmom metrika sa rozumie veličina vzťahujúca sa k výkonnosti a spoľahlivosti internetu. Hlavným cieľom definovania metrík výkonnosti internetového protokolu je poskytnúť používateľom a poskytovateľom služieb dostatočne výstižnú a pritom všeobecnú charakteristiku výkonnosti a spoľahlivosti komponentov Internetu (sietí, podsietí, smerovačov, atď.). Pre dosiahnutie tohoto cieľa je potrebné metriky definovať. Počas vývoja boli definované všeobecné požiadavky pre každú existujúcu aj budúcu metriku:

- metrika musí byť konkrétne a jednoznačne definovaná
- metodológia používaná v implementácii metriky musí mať vlastnosť opakovateľnosti – pri viacnásobnom vykonaní postupu merania s rovnakými podmienkami musí toto dospieť stále k rovnakým výsledkom

- v prípade internetu nie je možné zabezpečiť pre každé opakovanie merania rovnaké podmienky, preto je v prípade internetových sietí stanovené pravidlo, že metóda použitá na meranie danej metriky nesmie prekročiť určitú, vopred definovanú, odchýlku
- v prípade internetových sietí implementovaných identickou technológiou musí byť pri opakovaní merania odchýlka nulová
- pre používateľov a poskytovateľov služieb má byť zmyslom definície metriky a vývoja metodológie pre jej meranie zmysluplnosť a použiteľnosť pri porozumení a pri popise výkonnostných charakteristík
- metodológia metriky sa musí dôrazne vyhýbať akýmkoľvek spôsobom merania alebo výpočtu charakteristík, ktoré by umelo zvyšovali celkové výkonnostné charakteristiky

Pri definícii metriky je potrebné klásť dôraz najmä na jej konkrétnosť a jednoznačnosť. Nemusia existovať praktické spôsoby jej merania, ale samotná definícia metriky musí byť vypracovaná jednoznačne a bez možnosti rôznych interpretácií. Jednoznačnosť definície metriky spočíva v definovaní použitia veličín pre merania, ich násobkov a kombinácií. Pri definícii časových charakteristík je potrebné použiť univerzálny koordinovaný čas (Universal Time Coordinated, UTC). Pre definíciu parametrov a charakteristík metriky sa používa medzinárodná metrická sústava s nasledujúcimi ďalšími pravidlami:

- ak je charakteristika definovaná veličinou v základných jednotkách, potom akceptovateľné príslušné násobky v tisícoch alebo v tisícinách
- ak je charakteristika definovaná v kombináciách veličín, potom sú akceptovateľné aj príslušné násobky v tisícoch alebo tisícinách, ale všetky takéto násobky musia byť uvedené na začiatku, v čitateli ( $\frac{km}{s}$  sú povolené, ale  $\frac{m}{ms}$  nie)
- jednotkou informácie je bit

- pokiaľ sú s jednotkou informácie používané metrické prefixy (kilo, mega, giga, atď.) potom majú svoj metrický význam, nie význam spojený s výpočtovou technikou, teda 1 kb je 1000 bitov, nie 1024 bitov

Pre zisťovanie, meranie a vyhodnocovanie jednotlivých metrík existujú rôzne metodológie. Môžu to byť napríklad:

- priame meranie použitím generovanej testovacej prevádzky
- zobrazenie metriky z meraní nižšej úrovne v zmysle hierarchie ISO/OSI modelu
- odhad podstatnej časti metriky z množiny viacerých súhrnných meraní
- odhad metriky v danom čase z množiny podobných meraní v inom čase

V popise rámca existujú tri prístupy k získavaniu dát potrebných pre spracovanie metriky popísané v tabuľke 4–4. Existuje veľa prístupov k vzorkovaniu. Všeobecne

Metrika	Popis
<b>singletonová metrika</b>	predstavuje atomickú metriku. Celková prenosová kapacita spojenia dvoch bodov v počítačovej sieti môže byť definovaná ako singletonová metrika
<b>vzorkovacia metrika</b>	vzniká odvodením zo singletonovej metriky procesom spojenia určitého počtu rozdielnych prípadov
<b>štatistická metrika</b>	predstavuje metriku odvodenú zo vzorkovacích metrík výpočtom štatistických hodnôt singletonových metrík prináležiacich k vzorkám

**Tabuľka 4–4** Popis metrík

rozšírený spôsob je periodický zber dát, kde sú vzorky odoberané v určitých intervaloch. Táto metóda je jednoducho implementovateľná, ale z jej podstaty vyplývajú určité nevýhody. Metóda nemusí zachytiť periodické správanie sa danej metriky,

môže byť ľahko identifikovateľná ako test prevádzky a následne môže byť na ňu uplatňované špeciálne spracovanie.

Metódou eliminujúcou tieto nevýhody je metóda náhodného adaptívneho vzorkovania. Vzorky sú oddelené nezávislými náhodne generovanými intervalmi so štatistickou distribučnou funkciou  $G(t)$  (Bilinskis, 1992).

Náhodné adaptívne vzorkovanie poskytuje nesporné výhody — eliminuje synchronizačný efekt a prináša výhodu neskresleného odhadu vzorkovanej charakteristiky. Napriek tomu adaptívne vzorkovanie má aj nevýhody. Jedna z hlavných nevýhod spočíva v jeho princípe — náhodné adaptívne vzorkovanie komplikuje analýzu na frekvenčnej základni, pretože vzorky nenasledujú za sebou v pevne stanovených intervaloch tak, ako to vyžadujú Fourierove transformácie. Pokiaľ distribučná funkcia  $G(t)$  nemá exponenciálne rozdelenie, je do istej miery predikovateľná podobne ako periodické vzorkovanie (RFC2330, 1998).

Existujú dve metódy náhodného adaptívneho vzorkovania:

- Poissonovo vzorkovanie
- geometrické vzorkovanie

Pre metriku výkonnosti internetového protokolu existujú už popísané metriky niektorých charakteristík:

- IPPM metrika pre meranie spojenia (RFC2678, 1999)
- Metrika oneskorenia jednej cesty pre IPPM (RFC2679, 1999)
- Metrika pre stratovosť paketov v jednej ceste pre IPPM (RFC2680, 1999)
- Metrika pre oneskorenie uzavretej slučky pre IPPM (RFC2681, 1999)

#### 4.1.1 IPPM metrika pre meranie spojenia

Metrika pre meranie spojenia (RFC2678, 1999) je metrika pre meranie pripojiteľnosti spojenia typu P, nazývaného aj jednosmerné pripojenie typu P (Type P Instantaneous Unidirectional Conectivity). Vstupmi pre túto metriku sú:

- zdrojová adresa (src)
- cieľová adresa (dst)
- čas merania (T)

Jednotkou a zároveň výstupnou hodnotou pre metriku je boolovská hodnota. Samotná metrika je definovaná nasledujúcim spôsobom: Zdrojová adresa má jednosmerné pripojenie typu P, ak paket typu P prenesený zo zdrojovej do cieľovej adresy prejde túto cestu za čas T.

Pre mnoho aplikácií je obojsmerná prevádzka oveľa relevantnejšia než prevádzka jednosmerná. Výnimkou môžu byť aplikácie bezpečnosti (rôzne firewally), pre ktoré je dôležitá aj jednosmerná prevádzka. Pomocou tejto singletonovej metriky je možné definovať aj obojsmernú prevádzku. Ak je k tejto metrike pridaná aj doba trvania  $dT$ , potom na uzavretom intervale  $\langle T, dT \rangle$  je definovaná nová metrika pre obojsmerné pripojenie spôsobom: Ak existujú adresy  $A_1$  a  $A_2$  pre dva rôzne body v počítačovej sieti, potom tieto body majú obojsmerné pripojenie typu P ak má adresa  $A_1$  jednosmerné pripojenie typu P na adresu  $A_2$  a adresa  $A_2$  má jednosmerné pripojenie typu P na adresu  $A_1$ .

Pre meranie spojenia je definovaná všeobecná metrika pripojiteľnosti vhodná pre spojenia s rôznymi typmi paketov. Všeobecná metrika pripojiteľnosti sa nazýva aj metrika intervalovej časovej pripojiteľnosti typu  $P_1$ - $P_2$  (Type- $P_1$ - $P_2$ -Interval-Temporal-Connectivity). Pre túto metriku je definovaná metodológia merania. Metodológia spočíva v odoslaní  $n$  paketov zo zdrojovej adresy do do cieľovej v rovnomerne rozdelenom intervale. Každý prijatý paket v cieľi je spätne odoslaný do zdroja. Ak je v zdroji paket prijatý s odpoveďou, potom je test úspešný a končí. Odporúčaná hodnota pre  $n$  je 20 paketov, ktoré majú byť odoslané v intervale 50 sekúnd. Čakací čas pre paket s odpoveďou by mal byť 10 sekúnd, teda celé meranie by malo trvať 60 sekúnd.

#### 4.1.2 Metrika oneskorenia jednej cesty pre IPPM

Metrika oneskorenia jednej cesty (RFC2679, 1999) definuje singletonovú metriku pre meranie oneskorenia. Vstupmi pre túto metriku je:

- zdrojová adresa (src)
- cieľová adresa (dst)
- čas  $T$

Výstupom je čas oneskorenia udávaný v sekundách. Meria sa čas medzi odoslaním paketu zo zdrojovej adresy a jeho prijatím v cieľovej adrese. Výsledný čas je udávaný v sekundách, alebo je to kladné nekonečno v prípade, že sa paket na ceste zo zdrojovej do cieľovej adresy stratí.

Metodológia merania pre túto metriku pozostáva zo všeobecných krokov, ktoré je potrebné vykonať pre každý typ paketu (Type-P). Pre každý typ je potrebné synchronizovať zdroj a cieľ pomocou rôznych spôsobov (NTP, GPS, DCF77) a tesne pred odoslaním paketu zo zdroja je potrebné vložiť do paketu časovú značku. Aby sa predišlo nezmyselnej kompresii údajov, je potrebné použiť náhodné údaje. V cieľi sa do paketu pridá ďalšia časová značka a na základe rozdielu týchto časových značiek je vypočítané oneskorenie.

Pre túto singletonovú metriku je definované Poissonovo rozdelenie vzorkovania. Poissonov proces pozostáva z počiatočného času  $T_0$ , konečného času  $T_f$ , a rýchlosti  $\lambda$ . Pre výpočet pseudonáhodného rozdelenia sú použité časy a rýchlosti. Výsledkom metriky je postupnosť dvojíc  $T, dT$ . Čas  $T$  je použitý pre reprezentáciu vstupného parametra do singletonovej metriky a oneskorenie je identické so singletonom.

Na základe vzorkovacej metriky je definovaných množstvo štatistických parametrov zahŕňajúcich percentily, stredné hodnoty, minimá a inverzné percentily.

### 4.1.3 Metrika pre stratovosť paketov v jednej ceste pre IPPM

Metrika pre stratovosť paketov v jednej ceste pre IPPM (RFC2680, 1999) je veľmi podobná metrike pre charakteristiku oneskorenia paketu v jednej ceste (RFC2679, 1999). Hlavný rozdiel je v definícii výstupnej hodnoty. Pre metriku stratovosti paketov v jednej ceste je výstupnou hodnotou boolovská hodnota, kde 0 znamená úspešný prenos a 1 znamená neúspešný prenos. Túto metriku je možné transformovať do tvaru, kedy každé konečné oneskorenie znamená úspešný prenos a každé nekonečné oneskorenie znamená neúspešný prenos.

Pre túto metriku je definovaná iba jedna štatistika a tou je priemer stratovosti paketov z daného počtu paketov za určitý čas.

### 4.1.4 Metrika pre oneskorenie uzavretej slučky pre IPPM

Metrika pre oneskorenie uzavretej slučky pre IPPM (RFC2681, 1999) definuje oneskorenie pre uzavretú slučku podobným spôsobom ako metriky pre oneskorenie paketu v jednej ceste (RFC2679, 1999) a metrika pre stratu paketu v jednej ceste (RFC2680, 1999). Je definovaný singleton pre meranie oneskorenia v uzavretej slučke v určitom čase. Pre kontrolu rozdelenia intervalov v rámci uzavretej slučky je definovaná metrika používajúca Poissonovo rozdelenie.

## 4.2 ITU-T

Odporúčanie (Y.1540, 1999) vydané organizáciou ITU-T (International Telecommunication Union - Telecom Standardization) sa zaoberá službou internetového protokolu údajovej komunikácie, prenosom IP paketov a definíciou vhodnej činnosti. Odporúčanie sa zaoberá len verziou 4 internetového protokolu. V odporúčaní sú definované metriky pre meranie charakteristík len na úrovni transportných protokolov (TCP, UDP).

Pre prenos IP paketov je definovaných niekoľko parametrov. Všetky metriky definované v odporúčaní sú definované bez ohľadu na príslušný typ paketu, preto je

pri meraní dôležité brať do úvahy osobitne túto informáciu. Jednotlivé metriky sú definované v tabuľke 4–5. Odporúčanie ITU-T sa tiež zaoberá definovaním charakte-

Názov metriky	Popis
oneskorenie prenosu IP paketu (IP packet transfer delay, IPTD)	čas, ktorý potrebuje paket pre vstup do siete, prechod sieťou a na opustenie siete
stredné oneskorenie prenosu IP paketu (mean IP packet transfer delay)	aritmetický priemer množiny oneskorení IP paketov (populácia záujmu)
zmena oneskorenia prenosu IP paketov (IP packet delay variation)	metrika založená na oneskorení prenosu paketov, je definovaná ako rozdiel medzi danými oneskoreniami; popisuje zmenu oneskorení
pomer chybných IP paketov (IP packet error ratio, IPER)	pomer všetkých chybných paketov k všetkým úspešne preneseným paketom
pomer stratených IP paketov (IP packet loss ratio, IPLR)	pomer nedoručených IP paketov k celkovému počtu prenášaných IP paketov
množstvo falošných IP paketov (spurious IP packet rate)	počet nesprávnych IP paketov rozdelených podľa času merania. Metrika je definovaná ako intenzita, nie ako pomer, pretože množstvo falošných IP paketov nie je ovplyvnené množstvom prenášaných paketov. Preto je možné túto metriku definovať absolútne

**Tabuľka 4–5** Charakteristiky metrick v odporúčaní Y.1540

ristík a metrick pre popis dostupnosti služieb poskytovaných pomocou internetového protokolu. Dostupnosť služby poskytovanej internetovým protokolom je definovaná pomocou metriky pre stratovosť paketov (IPLR). Služba je nedostupná, ak straty paketov prekračujú stanovenú hranicu. Aktuálna hranica je daná hodnotou 0,75. V

odporúčaní sú definované dve metriky:

- **percento nedostupnosti IP služby (percent IP service unavailability, PIU)** — percento plánovaného času IP služby, kedy je kategorizovaná ako nedostupná
- **percento dostupnosti IP služby (percent IP service availability, PIA)** — percento plánovaného času IP služby, kedy je na základe funkcie dostupnosti kategorizovaná ako dostupná

V doplnku odporúčania Y.1540 sú definované metriky súvisiace s tokom údajov. V tejto práci sú uvádzané pre úplnosť:

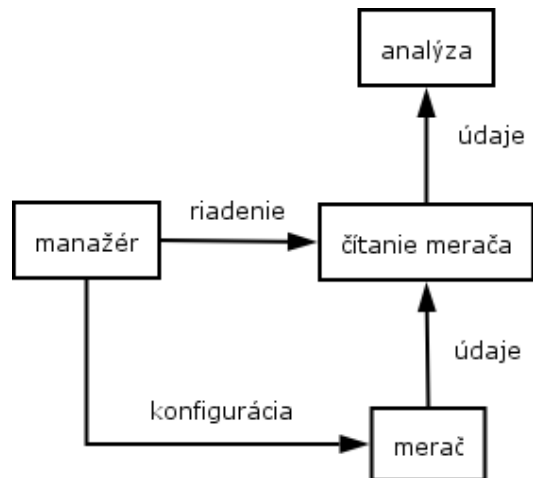
- **priepustnosť IP paketov (IP packet throughput, IPPT)** — počet paketov patriacich k meranej množine úspešne prenesených počas trvania merania
- **priepustnosť slabikovo založených IP paketov (octet based IP packet throughput, IPOT)** — pomer počtu úspešne prenesených slabík (bajtov) v IP paketoch k času trvania merania

### 4.3 Real Time Flow Measurement, RTFM

Odporúčanie pre meranie dátových tokov v reálnom čase (RFC2063, 1997) (Real Time Flow Measurement, RTFM) poskytuje všeobecný rámec pre opis a meranie toku prevádzky v sieti v reálnom čase.

Architektúra princípov merania dátových tokov je znázornená na obrázku 4–3. Jednotlivé komponenty používajú ako komunikačný protokol jednoduchý protokol pre správu siete (Simple Network Management Protocol, SNMP).

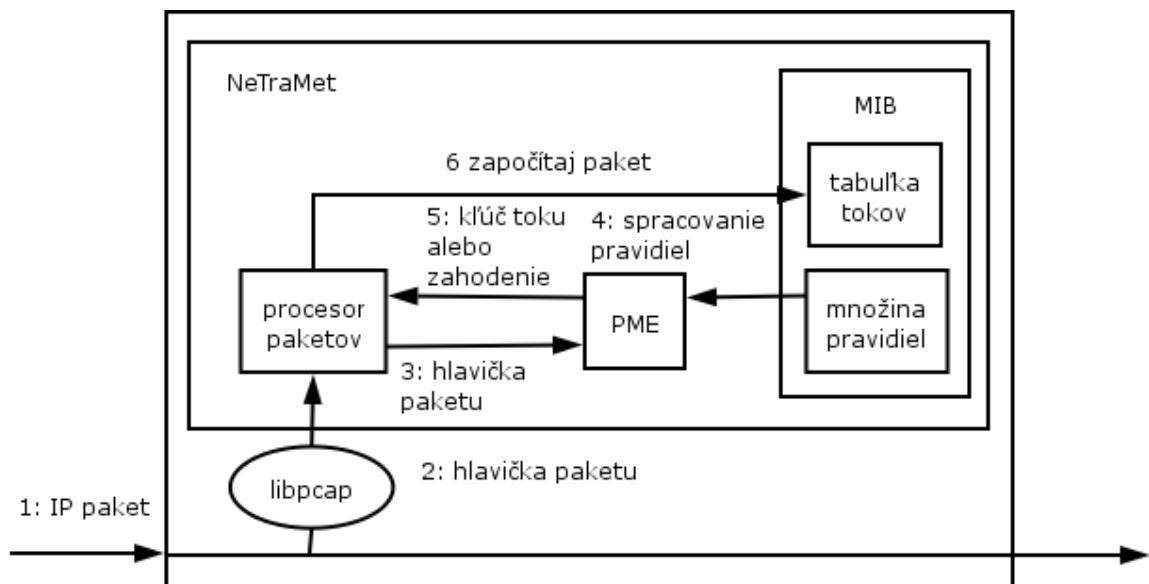
Samotná architektúra pozostáva z niekoľkých komponentov. Základom sú merače, odchyťávajú a počítajú prevádzku. Čítacie procesy na základe pravidiel čítajú hodnoty a preposielajú do analyzujúcej aplikácie. Pravidlá pre výber hodnôt sú uložené v manažéri pravidiel, kde je možné definovať nové pravidlá pre meranie dátových tokov.



Obrázok 4–3 Architektúra RTFM

#### 4.4 NetraMet

NeTraMet (Brownlee, 1997) je implementácia meracieho nástroja vyhovujúca štandardu RTFM (RFC2063, 1997). NeTraMet je softvérový balík spustiteľný pod operačným systémom DOS alebo pod rôznymi druhmi UNIXU. NeTraMet pozostáva z meracieho nástroja, analyzujúcej aplikácie a manažéra pravidiel. Bloková



Obrázok 4–4 Architektúra nástroja NeTraMet

schéma meracieho nástroja je uvedená na obrázku 4–4. NeTraMet pozostáva z pro-

cesora paketov, nástroja na porovnávanie paketov (Packet Matching Engine, PME) MIB databázy, ktorá obsahuje množinu pravidiel a udržiava tabuľku tokov. Pakety prichádzajúce do siete sú spracované na nižšej úrovni libpcap knižnicou. Hlavičky paketov sú odovzdané do procesora paketov. Procesor paketov posiela hlavičky do časti pre porovnávanie paketov (PME). PME klasifikuje pakety podľa množiny nahraných pravidiel a vracia daný kľúč toku do procesora paketov, ak má byť paket započítaný — inkrementuje sa počítadlo v zodpovedajúcej položke tabuľky tokov. V prípade, že paket nevyhovie žiadnemu pravidlu, je zahodený.

NeTraMet bol špecificky vyvinutý pre monitorovanie výstupnej prevádzky jedného zákazníka. Táto úloha vyžaduje menej činnosti a má menšie nároky na výpočtovú kapacitu meracieho bodu, na ktorom je NeTraMet prevádzkovaný. Pri prevádzkovaní v sieti poskytovateľa, kde prevádzku ovplyvňujú viacerí zákazníci, môže NeTraMet nepostačovať výkonom. NeTraMet je navrhnutý pre beh v priestore používateľa a v unixových operačných systémoch (rôzne varianty BSD, Linux), kde je v jadre dostupný jednoduchý filter paketov, je možné klasifikáciu vykonávať iba v priestore používateľa, čo vedie k nadmernému prepínaniu kontextov — pre prenos paketu z priestoru jadra do priestoru používateľa je potrebné vykonať operáciu nazvanú prepnutie kontextu — a tým aj k zníženiu výkonu.

NeTraMet podporuje aj veľmi jednoduchý algoritmus vzorkovania paketov, kedy sa meria iba každý n-tý paket. Toto môže viesť k zníženiu zaťaženia meracieho bodu pri vyčerpaní ďalších systémových kapacít a meranie môže s hrubšou granularitou pokračovať ďalej.

Zdrojové kódy meracieho nástroja NeTraMet sú voľne dostupné, na jeho vývoji sa podieľa veľké množstvo programátorov. NeTraMet podporuje zachytávanie informácií, ktorými sú špecifikované diferenciovane služby. K posledným verziám NeTraMetu bola pridaná podpora internetového protokolu verzie 6, špeciálnych multicastových atribútov a v návrhu je aj podpora pre zacytávanie informácií rezervačného protokolu (Resource Reservation Protocol, RSVP).

Do podpory pre NeTraMet je zahrnutá aj podpora pre jednobodové meranie

spätného oneskorenia (Round-Trip Time, RTT), ktoré je založené na pozorovaní párových paketov existujúcich v prevádzke. Meranie RTT je založené na nasledujúcich pároch:

- ICMP požiadavka, odpoveď
- DNS požiadavka, odpoveď
- SNMP požiadavka, odpoveď
- TCP SYN/SYN-ACK
- TCP data/ACK

## 4.5 IP Flow Information Export, IPFIX

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

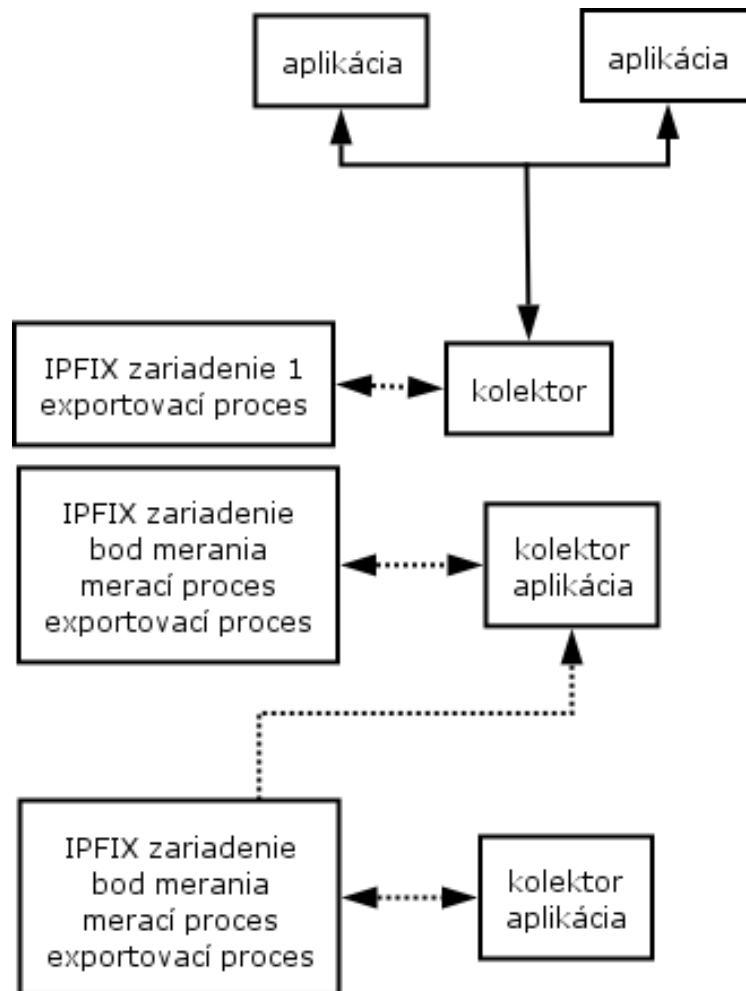
Pre ďalší popis je potrebné definovať základný pojem v špecifikácii IPFIX — **tok (flow)**. Existuje mnoho definícií toku, pre účely bližšieho popisu bude použitá definícia uvedená v (Quittek, 2004).

Pod pojmom **tok (flow)** sa rozumie množina IP paketov prechádzajúcich pozorovacím bodom v sieti počas určitého časového intervalu. Všetky pakety patriace do daného toku majú spoločné vlastnosti. 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), hlavičky transportného protokolu (napr. cieľový port) alebo položky hlavičky aplikačného protokolu (napr. RTP (RFC1889, 1996))
- charakteristika samotného paketu (napr. počet MPLS návěstí (kapitola 2.1))
- 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.

Využitie informácií o tokoch je dôležité pri plánovaní siete, inžnieringu prevádzky, plánovaní rozšírení siete a výkonnostnom vylepšovaní jednotlivých komponentov siete. Takisto je tieto dáta možné použiť pri účtovaní podľa prenesených dát alebo podľa jednotlivých zákazníkov. Podľa týchto aplikačných oblastí boli vypracované požiadavky (Quittek, 2004) pre jednotlivé časti návrhu architektúry IPFIX. Architektúra IPFIX je schematicky uvedená na obrázku 4–5.



Obrázok 4–5 Bloková schéma architektúry IPFIX

#### 4.5.1 Bod merania

Bod merania je také miesto v sieti, kde môžu byť IP pakety výhodne sledované. Môže to byť linka pripojená k IPFIX zariadeniu, zdieľané médium (napr. LAN založená na Ethernete), port na smerovači alebo jedno alebo viac rozhraní na smerovači.

#### 4.5.2 Merací proces

Merací proces generuje záznamy tokov (flow records). Vstupom do meracieho procesu sú hlavičky paketov z bodu merania a hodnoty odvodené zo zaobchádzania s paketmi. Merací proces pozostáva z viacerých podprocesov, ako je spracovanie hlavičky, generovanie časových známok, vzorkovania, klasifikovania a spracovania záznamov tokov.

Spracovanie záznamov tokov spočíva vo vytváraní nových záznamov, zmene existujúcich záznamov, počítania štatistík záznamov, odvodenia ďalších vlastností tokov, detekovania ukončenia platnosti záznamov tokov, odosielanie záznamov tokov do exportovacieho procesu a z odstraňovania záznamov tokov.

Merací proces musí spĺňať niektoré požiadavky:

- **spoľahlivosť** — merací proces musí byť spoľahlivý. Spoľahlivosť znamená, že merací proces musí byť pri danej konfigurácii schopný odchytiť všetky pakety prechádzajúce bodom merania. Pri preťažení meracieho bodu a neschopnosti zachytiť všetky pakety musí byť merací bod schopný túto nespoľahlivosť zistiť a definovaným spôsobom oznámiť.
- **vzorkovanie** — vzorkovanie popisuje systematický alebo náhodný výber podmnožiny elementov (vzorka) z množiny všetkých elementov (rodičovská populácia). Merací proces môže podporovať vzorkovanie. Ak merací proces podporuje vzorkovanie, potom musí byť jednoznačne definované v konfigurácii meracieho procesu. Konfigurácia vzorkovania zahŕňa metódu vzorkovania a všetky potrebné parametre. Ak je konfigurácia vzorkovania zmenená počas meracieho procesu, všetky zhromažďovacie procesy musia byť informované o

zmenách v konfigurácii. Zmena vzorkovania v meracom procese znamená odobratie vzorkovacej funkcie, prídanie novej vzorkovacej funkcie, zmenu parametrov a zmenu vzorkovacej metódy.

- **správanie sa pri preťažení** — v prípade preťaženia z nedostatku pamäte alebo nedostatku výpočtovej kapacity merací proces môže zmeniť svoje správanie tak, aby reagoval na nedostatok zdrojov. Možné reakcie zahŕňajú:
  - znížiť počet meraných tokov. Toto môže byť dosiahnuté jednak zvýšením granularity meracieho procesu, alebo znížením počtu sledovaných tokov na podmnožinu z pôvodnej množiny sledovaných tokov
  - začať vzorkovanie predtým ako sú pakety spracované meracím procesom, alebo, ak sa vzorkovanie už vykonáva, znížiť vzorkovaciu frekvenciu
  - zastaviť meranie
  - znížiť zaťaženie ostatnými procesmi

Správanie sa pri preťažení nie je obmedzené na vyššie popísané štyri spôsoby, ale v prípade vzniku preťaženia musí byť jednoznačne definované. Toky vytvorené jednou vzorkovacou metódou, alebo jednou vzorkovacou frekvenciou nesmú byť spojené s tokmi vytvorenými po zmene vzorkovacej metódy, alebo vzorkovacej frekvencie. Zhromažďovací proces musí byť schopný odlíšiť toky vytvorené pred a po zmene vzorkovacej metódy, alebo frekvencie.

- **časové známky** — merací proces musí byť schopný generovať časové známky pre prvé a posledné pozorovanie paketu v toku
- **synchronizácia času** — merací proces musí umožňovať synchronizáciu vygenerovaných časových známk s univerzálnym koordinovaným časom (UTC)
- **expirácia tokov** — merací proces musí byť schopný detekovať expiráciu tokov. Tok sa pokladá za expirovaný ak v danom časovom intervale nebol pozorovaný žiadny paket patriaci do daného toku. Merací proces môže podporovať

mechanizmy expirácie pred vypršaním časového limitu pomocou sledovania príznakov TCP protokolu FIN (ukončenie spojenia), RST (zrušenie spojenia)

#### 4.5.3 Exportovací proces

Exportovací proces odosiela toky záznamov na jeden alebo viac zhromažďovacích procesov. Záznamy tokov sú generované jedným alebo viacerými meracími procesmi.

Exportovací proces musí byť schopný poskytovať informácie o nasledujúcich atribútoch pre každý meraný tok:

- číslo verzie internetového protokolu
- zdrojová IP adresa
- cieľová IP adresa
- typ IP protokolu (TCP,UDP,ICMP,...)
- v prípade typu protokolu TCP alebo UDP — zdrojový port
- v prípade typu 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

#### 4.5.4 Zhromažďovací proces (collecting process)

Zhromažďovací proces prijíma záznamy tokov z jedného alebo viacerých exportovacích procesov. Exportovací proces môže vykonávať ďalšie spracovanie záznamov tokov.

#### 4.5.5 Všeobecné požiadavky

Pre implementácie podľa IPFIX architektúry existujú všeobecné požiadavky, ktoré by mala dodržiavať každá implementácia. Prehľad všeobecných požiadaviek je uvedený v tabuľke 4–6.

Požiadavka	Popis
otvorenosť	implementácie špecifikácie IPFIX by mali byť otvorené voči novým technológiám. Pod otvorenosťou voči novým technológiám sa rozumie najmä otvorenosť v konfigurácii meracieho a exportovacieho procesu
škálovateľnosť	musí byť podporovaná možnosť získania získavania tokov 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 sa zabránilo dvojitému počítaniu tokov

Tabuľka 4–6 Všeobecné požiadavky architektúry IPFIX

## 4.6 NetFlow

NetFlow je čiastočná implementácia špecifikácie IPFIX firmy Cisco Systems. NetFlow je primárne implementovaný v hardvérových zariadeniach firmy Cisco – najmä v smerovačoch. V súčasnosti sú implementované najmä verzie NetFlow 5 a NetFlow 9. V NetFlow-e sú kľúče tokov generované ako zjednodušenie a urýchlenie procesu prepínania paketov. V NetFlow-e sú toky uvažované ako jednosmerné.

### 4.6.1 NetFlow verzia 5

Toky sú vo verzii 5 vždy identifikované tou istou množinou pevných atribútov. Agregácia tokov je podporovaná iba pre pevnú množinu agregáčnych schém. Filtrovanie toku údajov môže byť vykonaná na vyššej úrovni, tak ako je dané v špecifikácii IPFIX.

Zhromaždené údaje sú asynchrónne exportované a potom odstránené z pamäti tokov (flow cache). Údaje sú exportované cez NetFlow Export UDP datagramy, ktoré pozostávajú maximálne z 30 záznamov tokov (flow records). Tieto datagramy sú exportované aspoň raz za sekundu alebo ihneď keď je k dispozícii UDP datagram ukončeného toku. Položky pamäte môžu expirovať kvôli jednej z nasledujúcich príčin:

- uplynul limit doby existencie toku (interval 1 až 60 minút, štandardne 30 minút)
- uplynul čas nečinnosti toku – pozorovacím miestom neprešiel žiaden paket patriaci do toku (interval 10 až 600 sekúnd)
- pamäť tokov je plná a potrebuje byť zaznamenaný nový tok
- bol signalizovaný koniec toku (TCP FIN príznak)

### 4.6.2 NetFlow verzia 9

NetFlow verzia 9 je na rozdiel od verzie 5 pri definícii toku založená na šablónach. Šablóny predstavujú rozšíriteľný návrh pre paket exportu. Táto vlastnosť umožňuje budúce rozšírenia bez potreby zmeny základných vlastností formátu záznamu tokov. Použitie šablón má niekoľko výhod:

- NetFlow je odolný voči zmenám nových alebo vyvíjajúcich sa protokolov, pretože je možné jednoducho dodať podporu pre tieto protokoly
- nové vlastnosti môžu byť k NetFlow protokolu pridané jednoducho bez znefunkčnenia existujúcich implementácií
- aplikácie pre zhromažďovanie alebo analýzu dát môžu byť jednoduchým spôsobom (zmenou šablóny) obohatené o tieto nové vlastnosti

Exportný paket sa v protokole NetFlow verzia 9 skladá z dátových položiek, položiek definujúcich šablóny a z položiek nastavujúcich parametre pre zhromažďovací proces.

## 4.7 NetMate

NetMate (Network Measurement And Accounting System) (Zander, 2004) je flexibilný a rozšíriteľný nástroj pre meranie parametrov kvality služieb v počítačovej sieti. NetMate je čiastočná implementácia protokolu NetFlow. NetMate môže byť použitý pre účtovanie, meranie oneskorenia alebo straty paketov.

NetMate je nástroj pre prevádzku pod unixovými operačnými systémami (Linux, \*BSD).

## 4.8 Ntop

Ntop (Deri, 2004) je nástroj pre meranie prevádzky v počítačovej sieti. Ntop je úplnejšou implementáciou špecifikácie IPFIX a protokolu NetFlow. Súčasná imple-

mentácia programu Ntop podporuje NetFlow verzie 5 aj verzie 9. Súčasťou programového balíka je meracia aplikácia (nProbe), analytická aplikácia (nTop) — dostupná z príkazovej riadky aj cez webové rozhranie a zhromažďovacia aplikácia (súčasť programu nTop).

Programový balík Ntop je multiplatformový umožňujúci beh na rôznych unixových platformách rovnako ako na platforme Win32.

## 5 Návrh, koncepcia a architektúra meracieho nástroja

Praktickým cieľom diplomovej práce je vytvoriť základný nástroj pre pasívne merania v počítačových sieťach. Cieľom je vytvoriť voľne dostupnú a použiteľnú platformu pre neintruzívne merania prevádzkových parametrov. Úloha sa primárne nezameriava na vytvorenie komplexného nástroja na meranie veľkého množstva, cieľom je skôr vyvinúť z používateľského hľadiska relatívne jednoduchý, ale pritom s minimálnou námahou jednoducho modifikovateľný, prispôsobiteľný a rozšíriteľný nástroj na základoch ktorého by už bolo možné navrhovať komplexnejšie meracie platformy.

### 5.1 Špecifikácia požiadaviek

Hlavné požiadavky na implementáciu meracieho nástroja boli špecifikované v nasledujúcich bodoch:

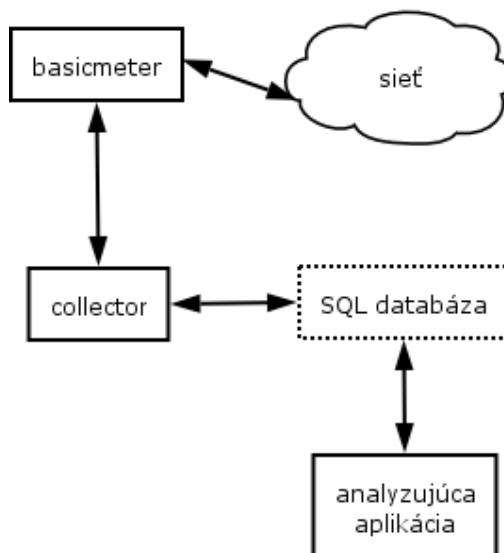
- vytvorenie jednoduchého nástroja pre ovládanie z príkazového riadku, nevytvárať komplexnú meraciu platformu
- navrhnuť modulárny dizajn, ktorý by zaručoval rozšíriteľnosť jednoduchým spôsobom
- možnosť špecifikovať súčasné meranie rôznych dátových tokov
- možnosť jednoduchého vzdialeného ovládania meracieho nástroja
- podpora protokolu NetFlow verzie 9
- podpora šablón, podpora verifikovateľnosti zadaných šablón
- možnosť konfigurácie jednoduchým textovým konfiguračným súborom
- implementácia čo najviac portabilným spôsobom

- implementácia by mala byť východiskovým bodom pre podporu meraní podľa štandardu IPFIX
- maximálnym možným využitím dostupných prostriedkov operačného systému zefektívniť činnosť programu
- navrhnuť podporu pre implementáciu vzorkovacích funkcií

V ďalšom popise bude navrhnutý a implementovaný nástroj označovaný názvom „basicmeter<sup>1</sup>“.

## 5.2 Konceptia meracieho nástroja

Koncepciou meracieho nástroja je podpora štandardu IPFIX v čo najlepšej možnej miere. Navrhovaný merací nástroj sa snaží svojou koncepciou priblížiť návrhu architektúry štandardu IPFIX (Sadasivan, 2003). Navrhovaný a implementovaný merací nástroj je súčasťou tejto koncepcie znázornenej na obrázku 5–6.



Obrázok 5–6 Architektúra meracej platformy

<sup>1</sup>Skrátene „bm“; v preklade „základný merač“

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 5–7.

Časť architektúry	Popis
basicmeter (merací proces)	popisovaná aplikácia slúžiaca ako merací proces, zachytávanie paketov a vytváranie dát pre zhromažďovací proces
collector (zhromažďovací proces)	zhromažďovací proces, spracováva exportované pakety z exportovacieho procesu, nie je súčasťou popisovaného riešenia
analyzujúca aplikácia	aplikácia, ktorá pristupuje k exportovaným dátam a vykonáva analýzu (grafickú, štatistickú) na požiadanie používateľa

**Tabuľka 5–7** Popis jednotlivých častí architektúry

SQL databáza nie je súčasťou špecifikácie IPFIX ani protokolu NetFlow — v schéme je to naznačené bodkovaním. Všeobecne sa na uloženie exportovaných paketov predpokladá akýkoľvek dátový sklad (súbor, odľahčená databáza pracujúca so súborovým systémom, vyhradená partícia disku pre uloženie neformátovaných dát, atď.) — kvôli jednoduchému použitiu, dobrým možnostiam ďalšieho spracovania uložených dát, dobrým možnostiam získavania uložených dát bola ako dátový sklad zvolená práve SQL databáza.

### 5.3 Návrh meracieho nástroja

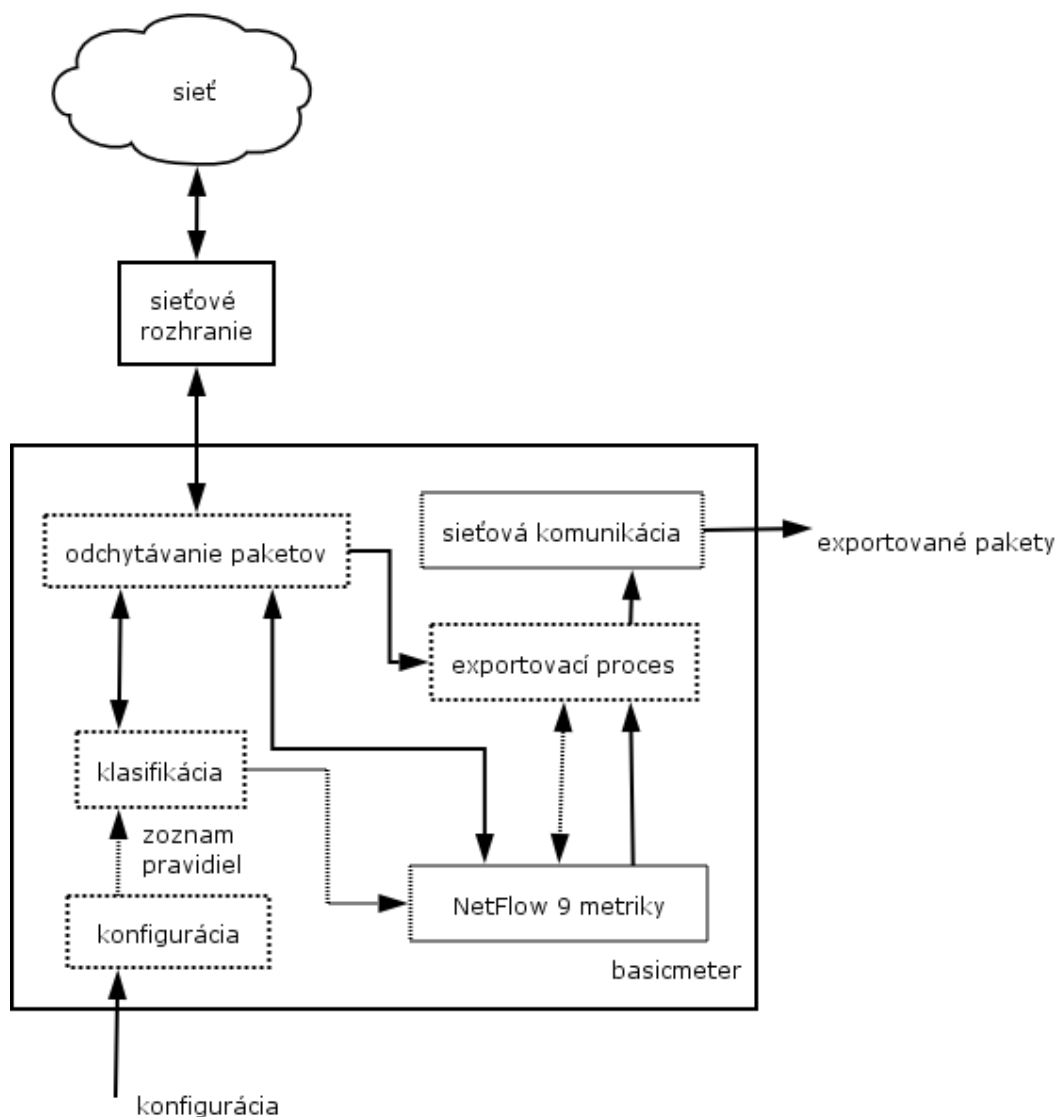
Aplikácia je koncipovaná ako samostatný spustiteľný program z príkazového riadku. Ako hlavný implementačný jazyk bol zvolený jazyk C, vzhľadom na svoju nezávislosť na platforme a širokú podporu na UNIX-ových operačných systémoch. S ohľadom na maximálnu možnú prenositeľnosť programu nebudú využívané neštandardné funkcie jadra operačného systému. Pre vývoj bola zvolená platforma operačného systému Linux kvôli jeho dostupnosti, stabilite, flexibilita a možnostiam vývoja. Bloková schéma aplikácie je na obrázku 5–7. Aplikácia je logicky rozdelená do dvoch častí:

- časť odchyťovania a sledovania paketov
- exportovacia časť (exportovací proces)

Tieto logické časti spolu komunikujú pomocou štandardných prostriedkov poskytovaných operačným systémom.

Časť sledovania a odchyťovania paketov používa k vykonávaniu týchto úloh knižnicu libpcap (McCanne, 2004). Knižnica libpcap bola zvolená kvôli svojej podpore na rôznych unixových operačných systémoch a dokonca v obmedzenej verzii na platforme Win32. Knižnica libpcap spolupracuje s jednoduchým paketovým filtrom obsiahnutým v jadrách väčšiny unixových operačných systémov a tým umožňuje významne zjednodušiť proces filtrovania paketov.

Exportovacia časť (exportovací proces) je samostatná časť programu, ktorá spracúvava dáta získané odchyťovacou časťou sledovaním procesu. Exportovacia časť bola navrhnutá tak, aby podporovala protokol NetFlow verzie 9 aj s možnosťami vytvárania šablón. Šablóny sú uložené v textových súboroch ako XML (Extensible Markup Language) (Bray, 2004) dokumenty. Pre validáciu týchto dokumentov je použitý zjednodušený jazyk pre popis štruktúry XML dokumentov — jazyk pre popis schémy XML dokumentov s názvom RelaxNG (Clark, 2001). Pre všetky činnosti súvisiace so spracovaním XML dokumentov bude použitá knižnica libxml2 (Veillard, 2004). Prenos exportovaných paketov bude prebiehať prostredníctvom UDP.



Obrázok 5–7 Architektúra meracieho nástroja

## 5.4 Architektúra meracieho nástroja

Architektúra nástroja je navrhovaná tak, aby vyhovela všetkým špecifikovaným požiadavkám. Bloková schéma nástroja je znázornená na obrázku 5–7.

Nástroj je rozdelený do dvoch hlavných častí, do časti odchyťavajúcej pakety a do exportovacej časti (exportovací proces). Ďalšími časťami podieľajúcimi sa na činnosti programu je klasifikačná časť a časť spracúvajúca konfiguráciu programu — z príkazového riadku a z textového konfiguračného súboru.

Časť *konfigurácia* má za úlohu načítať a spracovať konfiguračné parametre z príkazovej riadky a z textového konfiguračného súboru. Pre tieto činnosti sú použité knižnice *libconfuse* (Hedenfalk, 2004) — knižnica pre spracovanie textových konfiguračných súborov a knižnicu *libpopt* (Troan, 2002). Súčasťou konfiguračného modulu je aj inicializácia ostatných častí.

Odchytávacía a sledovacia časť (*capture*) má na starosti sledovanie a odchytávanie paketov na základe parametrov spracovaných konfiguračnou časťou a odovzdaných odchytávacej časti v procese inicializácie. Táto časť využíva funkcie knižnice *libpcap* (McCanne, 2004), ktorá realizuje samotné odchytenie paketov a ich prenos z priestoru jadra (*kernelpspace*) do priestoru používateľa (*userspace*). Na túto operáciu je potrebné mať v subsystéme pridelovania práv operačného systému najvyššie práva, teda práva administrátora systému, aplikáciu je potrebné spúšťať s efektívnym používateľským identifikátorom (*user identifier*, *UID*) 0 — v unixových operačných systémoch označuje používateľa s najvyššími právami v subsystéme pridelovania práv. Samotný výber paketov na sledovanie a odchytenie je realizovaný pomocou vysokoúrovňového abstraktného popisného jazyka podobného tomu, ktorý je použitý v nástroji na sledovanie sieťovej prevádzky s názvom *tcpdump* (McCanne, 2004). Odchytávajú sa všetky pakety patriace aspoň do jedného toku. Samotné odchytenie paketov je realizované pomocou berkeleyského paketového filtra (*Berkeley Packet Filter*, *BPF*) prítomného v jadrách väčšiny unixových operačných systémov. Filter je implementovaný tak, že je možné vyberať pakety na základe ďalších polí v hlavičke okrem štandardných (zdrojová a cieľová adresa, zdrojové a cieľové porty), teda je možné vyhovieť špecifikácii *IPFIX*. Použitie filtra znižuje počet prepnutí kontextu — prenosov medzi priestorom jadra a používateľským priestorom — pretože sa prenášajú len pakety so žiadanou informáciou a týmto prispieva k zvýšeniu výkonnosti meracieho nástroja.

Klasifikátor má za úlohu nájsť dátový tok, do ktorého patrí práve spracovávaný paket a odovzdať informáciu o identifikátore toku do časti vytvárania tokov (*NetFlow 9* metriky). Jednoduchý klasifikátor s algoritmom lineárneho vyhľadávania bol

realizovaný za pomoci knižnice libpcap a funkcií pre prístup k BPF.

Komponent NetFlow 9 metriky slúži na napĺňanie dátových tokov získaných z pozorovaných informácií na základe spracovania položiek v jednotlivých šablónach.

Toky sú vytvárané a spravované v časti exportovací proces, kde sú vytvárané, spravované a odosielané toky do časti sieťovej komunikácie. V časti exportovacieho procesu sú načítavané a verifikované (validované) šablóny pre správnosť zadania. Šablóny sú definované v textových súboroch ako dokumenty XML (Extensible Markup Language) (Bray, 2004). Pre verifikáciu šablón sa používa jazyk pre popis štruktúry XML s názvom RelaxNG (?)

Časť sieťovej komunikácie je použitá ako abstrakčná vrstva medzi exportovacou časťou a transportnými protokolmi. V súčasnosti program používa ako transportný protokol UDP (User Datagram Protocol).

## 6 Implementácia meracieho nástroja

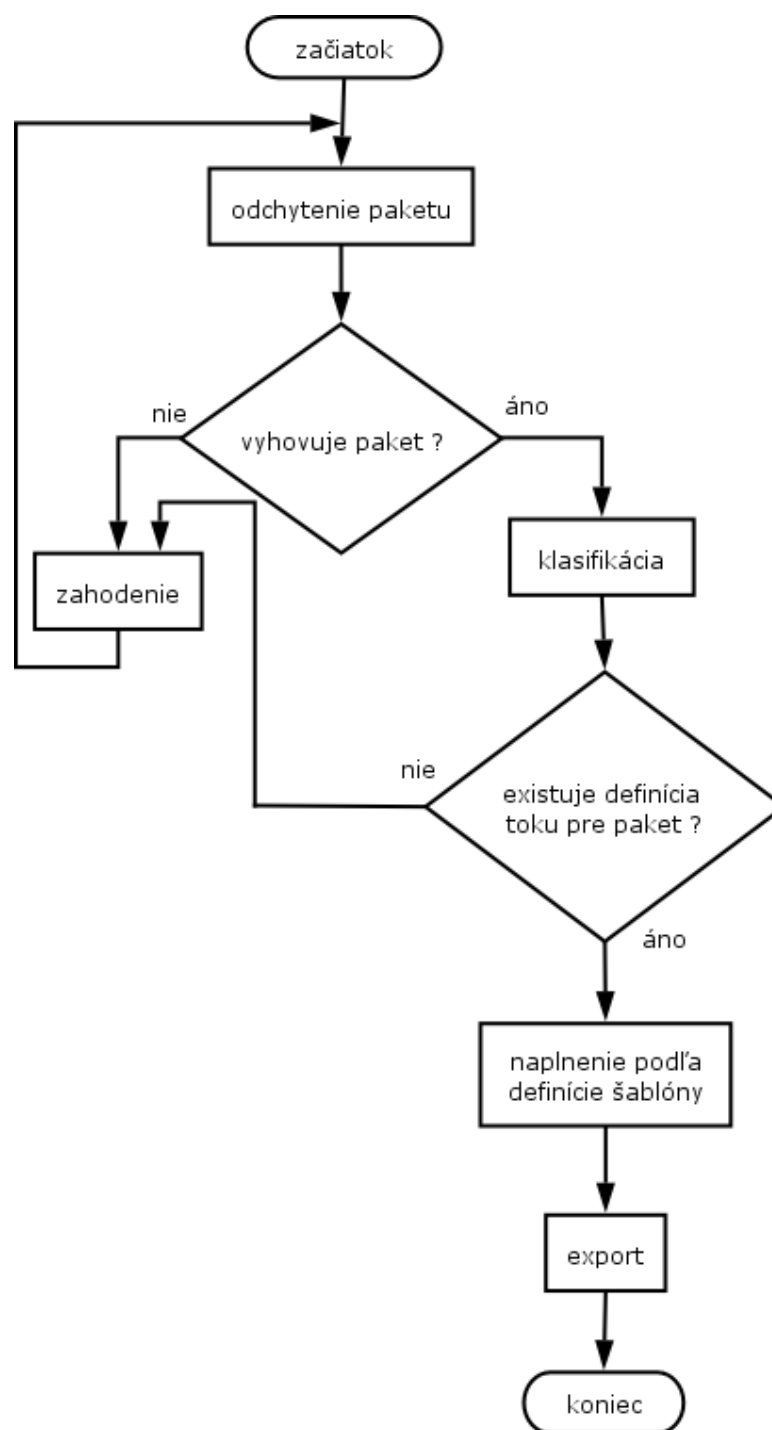
Pre implementáciu bol zvolený programovací jazyk C, najmä z dôvodu prenositeľnosti medzi jednotlivými typmi unixového operačného systému. Pri implementácii boli použité štandardné funkcie operačného systému a voľne šíriteľné knižnice dostupné vo forme zdrojových kódov.

### 6.1 Algoritmus spracovania paketu

Algoritmom spracovania paketu je konceptuálne popísaná činnosť meracieho nástroja. V tomto algoritme nie je popísaná inicializačná časť, kde prebieha inicializácia jednotlivých modulov architektúry meracieho nástroja, teda nastavenie príslušného rozhrania, načítanie a verifikovanie šablón a nadviazanie spojenia na zhromažďovací proces (collector). Samotný algoritmus spracovania paketu v schematickom vyjadrení značiek vývojového diagramu je znázornený na obrázku 6–8.

Algoritmus spracovania paketu znázorňuje cestu paketu od jeho odchytenia až po prípadné zaradenie do toku alebo odmietnutie. Paket je po odchytení skontrolovaný voči nadefinovaným pravidlám pre odchytyvanie (filtrovanie prevádzky pri odchytyvaní paketov). V prípade, že vyhoví, je potom klasifikovaný. Klasifikácia spočíva v porovnaní položiek paketu s filtrovacími výrazmi pre jednotlivé toky s využitím funkcií BPF, ktoré ponúka knižnica libpcap. V kladnom prípade je pre paket vypočítaný identifikátor v rámci daného toku a informácie z paketu sú extrahované do položiek v toku, tak ako sú zadané načítanou a inicializovanou šablónou. V súčasnosti je v nástroji implementovaná len jedna podmienka vyprázdňovania zásobníka tokov — pri jeho naplnení. Pri plnom zásobníku tokov sú pakety vo význame protokolu NetFlow verzia 9 exportované na zhromažďovací proces.

Tento proces sa opakuje dovtedy, pokiaľ nie je činnosť meracieho nástroja ukončená používateľom.



Obrázok 6 – 8 Algoritmus spracovania paketu

## 6.2 Knižnica libpcap

V dôsledku zvyšovania požiadaviek na tvorbu aplikácií monitorujúcich sieťovú prevádzku vznikla knižnica libpcap (McCanne, 2004) ako portovateľné, systémovo nezávislé rozhranie pre odchyťovanie paketov na používateľskej úrovni. Knižnica libpcap poskytuje vysokoúrovňové rozhranie pre odchyťovanie paketov. Všetky pakety v sieti sú pre aplikáciu prístupné pomocou tohoto mechanizmu.

K paketom je možné pristupovať dvoma spôsobmi:

- čítaním zo súboru
- čítaním zo sieťového rozhrania

Zápis paketov do súboru je realizovaný funkciami knižnice libpcap. Pri čítaní paketov zo sieťového rozhrania je možné pomocou knižnice nastaviť sieťové rozhranie do tzv. promiskuitného režimu práce, kedy spracováva všetky pakety, nielen tie, ktoré sú určené pre hostiteľa daného sieťového rozhrania.

Pre výber odchyťovaných paketov je možné špecifikovať filtrovací výraz, ktorý sa použije na odchytenie paketov vyhovujúcich filtrovaciemu výrazu. Filtrovanie je realizované pomocou berkeleyského paketového filtra (Berkeley Packet Filter, BPF) (McCanne, 1992).

BPF je založený na abstraktnom modeli orientovaného acyklického CFG (Control Flow Graph) grafu, ktorý je použitý na vytvorenie abstraktného stroja s registrovaným pseudo-jazykom. Program v tomto jazyku sa používa na zistenie, či je paket akceptovaný filtrom. Knižnica libpcap obsahuje kompilátor a optimalizátor, prekladajúci a optimalizujúci kód v používateľskom popisnom jazyku na program intepretovaný BPF. Preklad je voči používateľovi transparentný, ide o spôsob JIT (just-in-time) kompilátora.

### 6.3 Koncept verifikácie šablón

Protokol NetFlow verzie 9 vo svojom návrhu umožňuje pomerne flexibilnú definíciu obsahu tokov pomocou návrhu šablón. V súvislosti s týmto návrhom sa do popredia dostáva otázka jednoduchého a pritom robustného spôsobu definovania šablón.

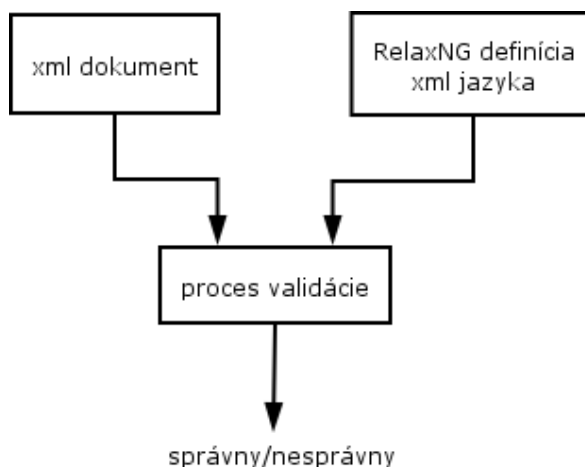
Existuje niekoľko spôsobov definície šablón. V procese analýzy požiadaviek a návrhu riešenia prichádzali do úvahy nasledujúce tri spôsoby:

- textové konfiguračné súbory
- XML dokumenty
- binárne definície šablón

Binárne definície šablón nie sú jednoduchým spôsobom modifikovateľné a vyžadujú ďalšie spracovanie — preklad do binárneho tvaru. Textové konfiguračné súbory neposkytujú dostatočnú štruktúru potrebnú pre jednoznačnú verifikovateľnosť a popis štruktúry dokumentov.

Jednoznačnú verifikovateľnosť a rozširovateľnosť do budúcnosti predstavujú XML dokumenty. Pre verifikáciu štruktúry XML dokumentov bol použitý jazyk pre popis štruktúry s názvom RelaxNG (Clark, 2001). RelaxNG je jazyk vychádzajúci z odporúčania W3 konzorcia popisujúceho jazyk XSD (XML Schema Definition) (Thompson, 2001; Biron, 2001) — definičný jazyk pre XML dokumenty. V XML dokumente sú uvedené jednotlivé elementy názvami zodpovedajúce možným položkám šablóny definovanej v špecifikácii protokolu NetFlow verzia 9. Pomocou štruktúry XML dokumentu popísanej pomocou RelaxNG je možné verifikovať syntaktickú správnosť XML dokumentu. Schematicky je tento proces znázornený na obrázku 6–9.

V meracom nástroji je spracovávanie XML dokumentov a ich následná verifikácia implementovaná za pomoci knižnice libxml2 (Veillard, 2004). Deje sa to v procese inicializácie nástroja — aktuálna programová logika je postavená na podmienke správnosti všetkých XML dokumentov popisujúcich šablóny definovaných v



Obrázok 6–9 Proces validácie XML dokumentu

textovom konfiguračnom súbore. Ak je niektorá zo šablón nesprávne definovaná, či už syntakticky alebo lexikálne, nástroj skončí s chybovým hlásením.

Náhľad na definíciu šablón ako XML dokumentov ponúka veľa ďalších myšlienok do budúcnosti, najmä pokiaľ ide o manipuláciu so šablónami a spravovanie väčšieho množstva meracích bodov. Odporúčaním do budúcnosti môže byť jednak použitie natívnej XML databázy pre uchovávanie veľkého množstva šablón, poprípade použitie šablón zo vzdialeného servera ako spôsob centralizovanej správy a uchovávanie šablón. Iným spôsobom môže byť vytvorenie popisného XML dokumentu pre šablóny a jeho uchovávanie na centrálnom serveri spolu so šablónami prístupnými pomocou štandardných prenosových protokolov (http, ftp) alebo v kombinácii s natívnou XML databázou, čo by výrazne zjednodušovalo administráciu väčšieho množstva meracích bodov a väčšieho množstva šablón pre jednotlivé meracie body. Rovnako je možné použiť všeobecnú (generickú) šablónu a za pomoci mechanizmu transformácií XML dokumentov je možné generovať šablóny s rôznymi podmienkami. Jedným z najprepracovanejších mechanizmov transformácií v súčasnosti sú XSL (Clark, 1999) transformácie.

## 7 Experimentálne overovanie funkčnosti nástroja

Experimentálnym overovaním funkčnosti sa rozumie inštalácia merača do infraštruktúry laboratórneho segmentu a jeho používanie a získavanie dát pre ďalšie vyhodnocovanie.

### 7.1 Inštalácia

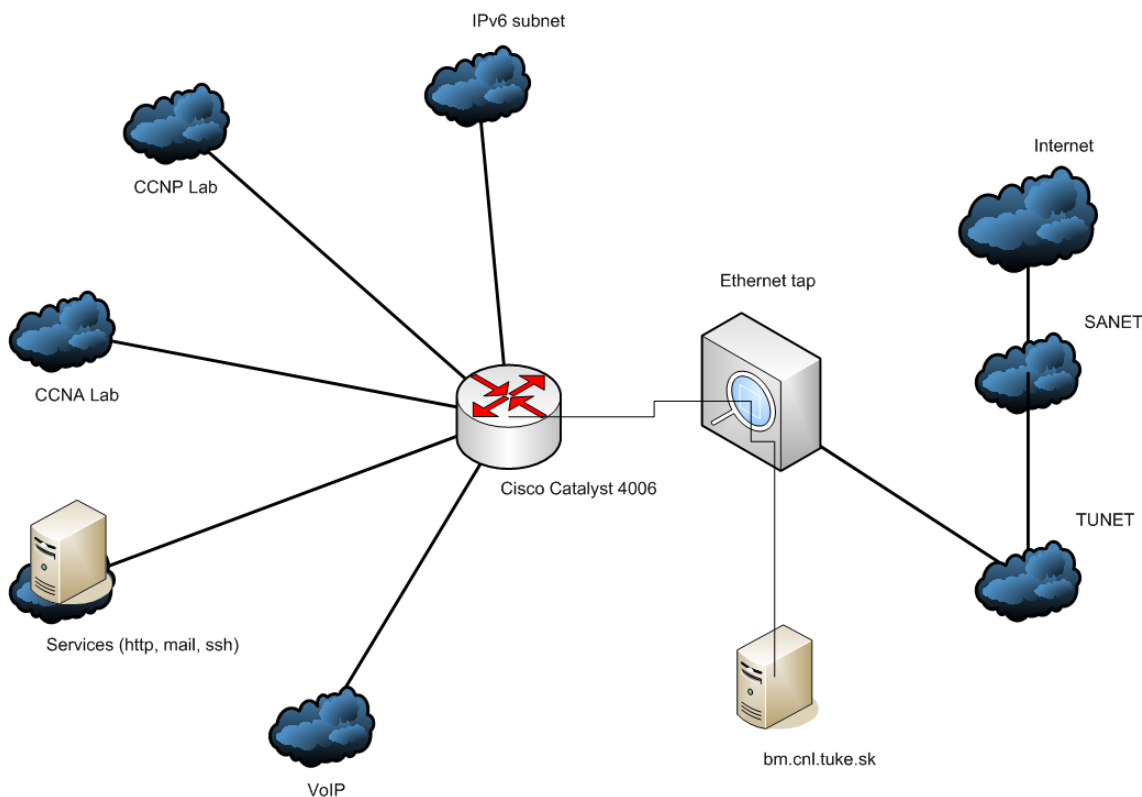
Pre testovacie účely bol merač nainštalovaný na počítač umiestnený v Laboratóriu počítačových sietí na Katedre počítačov a informatiky Fakulty elektrotechniky a informatiky Technickej univerzity v Košiciach.

Počítač bol do infraštruktúry laboratórneho segmentu pripojený cez zariadenie nazývané ethernet tap. Ethernet tap je aktívne zariadenie pracujúce na prvej vrstve ISO/OSI (International Standardization Organisation/Open Systems Interconnection) modelu. Toto zariadenie je možné transparentne pripojiť na linku bod-bod (point-to-point). Všetky prechádzajúce signály sú zachytávané a preposielané na odbočku.

V Laboratóriu počítačových sietí bol inštalovaný PC s operačným systémom Linux (procesor AMD Duron 700 MHz, sieťové rozhrania Fast Ethernet Realtek 8139, Linux kernel 2.4.24, distribúcia Linuxu Debian GNU/Linux Sid). V laboratóriu sa nachádza niekoľko lokálnych počítačových sietí na báze Ethernetu prepojených smerovačom Cisco Catalyst 4006. Pripojenie do verejnej siete je realizované pripojením do lokálnej siete Katedry počítačov a informatiky, ktorá je súčasťou univerzitnej siete TUNET. TUNET je pripojený na gigabitovú infraštruktúru akademickej siete SANET. Bloková schéma zapojenia je znázornená na obrázku 7–10.

### 7.2 Experimentálne meranie v laboratórnom segmente

Experimentálne meranie, odlaďovanie a testovanie funkčnosti prebiehalo v naznačenom zapojení. Vzhľadom na to, že nástroj bol navrhovaný ako súčasť komplexnej meracej platformy s ohľadom na IPFIX špecifikáciu, samotný nástroj neposkytuje



**Obrázok 7–10** Zapojenie v infraštruktúre Laboratória počítačových sietí

žiadne možnosti analýzy prevádzky. Preto ako zhromažďovací proces bol použitý programový balík Ntop (Deri, 2004). Zhromažďované dáta boli ukladané do dátového skladu. Dátovým skladom pre experimentálne merania bol voľne dostupný databázový server, najprv bol používaný databázový server PostgreSQL. Ukázalo sa, že pri veľkom množstve dát vznikajú problémy s výkonnosťou a odozvou databázového servera pri výbere a indexovaní dát, preto druhá časť meraní bola prenesená na databázový server MySQL, ktorý sa spočiatku, pri malom množstve dát, ukazoval ako dostatočne výkonný, ale s pribúdajúcim množstvom dát strácal najmä na rýchlosti výberu dát. Výkon pri výbere dát a indexovaní je dôležitý, ak existuje potreba analýzy získaných dát priebežne v reálnom, alebo takmer reálnom, čase. Existuje niekoľko návrhov možných riešení. Jedným z nich je zmena štruktúry dátového skladu — väčšie členenie tabuliek s dátami. Iným návrhom riešenia je zmena databázového servera, do popredia sa dostávajú databázy, ktoré svoju dátovú časť

udržiavajú v hlavnej pamäti (main memory databases, MMDB). Ďalším možným návrhom riešenia je zmena filozofie dátového skladu a upustenie od uskladňovania zhromaždených dát v SQL databáze.

Detailné preskúmanie, otestovanie a vypracovanie riešenia tohoto problému môže byť predmetom ďalšej práce na projekte.

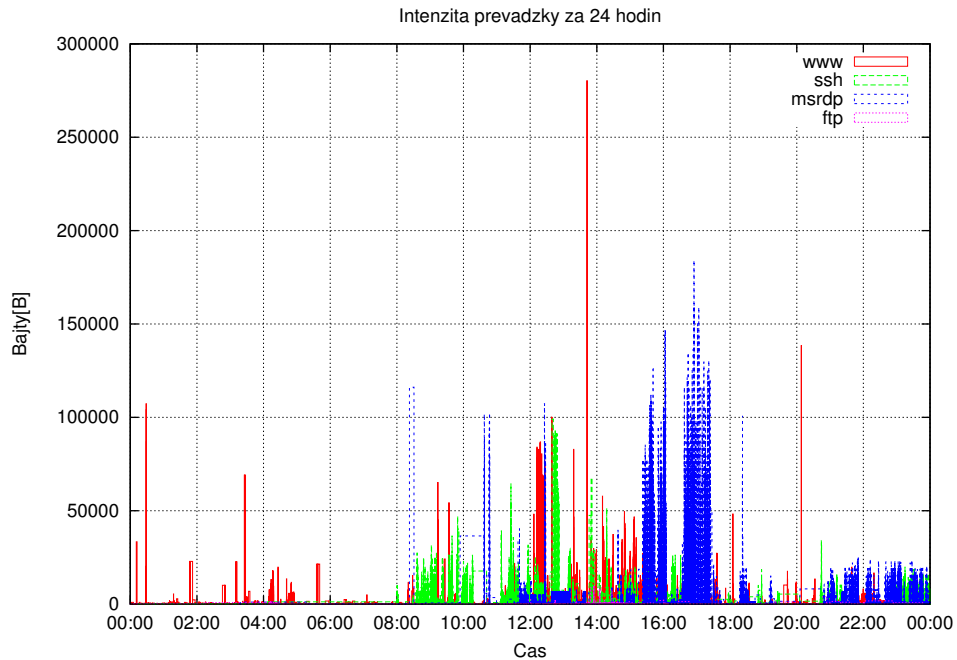
Pri experimentálnych meraniach bola pozornosť sústredená na meranie intenzity prevádzky. Pri meraní boli identifikované toky s najväčšou intenzitou prevádzky. Meranie intenzity prevádzky pozostávalo zo sledovania jednotlivých služieb prevádzkovaných nad transportnými protokolmi. Išlo o nasledujúce služby:

- www — služba prenosu hypertextu
- msrdp — vzdialený prístup na grafické pracovné stanice s OS Microsoft Windows
- ssh — služba interaktívneho prístupu na unixové pracovné stanice
- ftp — služba prenosu súborov

Na zobrazenie dát bol použitý softvérový balík Gnuplot (Bröker, 2004).

### 7.2.1 Meranie využitia šírky pásma

Pri meraní využitia šírky pásma sa pozornosť sústredila na využitie šírky pásma popísanými službami v časovom intervale 24 hodín. Výsledky merania sú naznačené v grafe 7–11. Z grafu vidno priebeh prevádzky, pričom najväčšiu šírku pásma zaberala prevádzka vzdialeného prístupu na pracovné stanice s operačným systémom Microsoft Windows (služba msrdp), služba vzdialeného prístupu na servery s operačným systémom Linux (služba ssh) a služba prístupu na webové stránky laboratória (služba www). Vzhľadom na zloženie serverov a pracovných staníc v Laboratóriu počítačových sietí je možné konštatovať, že zaznamenaná prevádzka zodpovedá bežnému pracovnému dňu v laboratóriu.



Obrázok 7–11 Časový priebeh využitia šírky pásma za 24 hodín

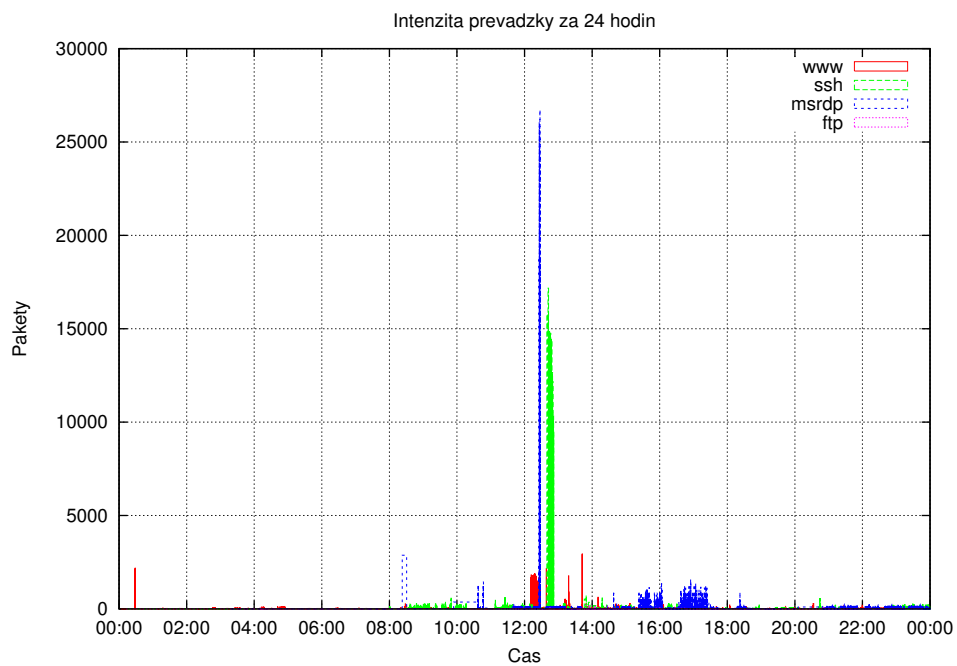
## 7.2.2 Meranie priepustnosti paketov

Pri meraní priepustnosti paketov sa zisťovala priepustnosť paketov pre vyššie popísané služby v časovom intervale 24 hodín. Výsledky merania sú zaznačené v grafe 7–12. Rovnako ako pri meraní priebehu intenzity prevádzky v bajtoch je možné obdobné výsledky konštatovať aj pri meraní charakteristiky priepustnosti paketov (packet rate).

Najväčší počet prenesených paketov patrí službe prístupu na pracovné stanice s operačným systémom Microsoft Windows (služba msrdp), službe vzdialeného prístupu na servery s operačným systémom Linux (služba ssh) a službe prístupu na webové stránky laboratória (služba www). Posledné menované služby je z grafu možné charakterizovať obtiažnejšie, čo je spôsobené najmä vysokým počtom paketov služby msrdp. Toto je spôsobené podstatou služby — ide o grafický prenos, teda relatívne veľké množstvo dát oproti terminálovému prístupu pomocou služby ssh, čo je napokon očividné aj z grafu 7–11. Preto pri tejto službe dochádza k väč-

šej fragmentácii dát a tým aj k zvýšeniu počtu paketov potrebných na prenesenie dát vygenerovaných službou msrdp. Úsporu je možné v prípade potreby dosiahnuť na klientskych stanicach znížením množstva prenášaných dát pomocou kompresie, prípadne znížením bitovej hĺbky.

Terminálový prístup zahŕňa oproti službe msrdp prístup na alfanumerický terminál, čím je spôsobené aj nižšie množstvo paketov. Pri terminálovom prístupe nie je požiadavka na prenos grafických informácií a tým klesá aj množstvo prenášaných dát.



Obrázok 7–12 Časový priebeh priepustnosti paketov za 24 hodín

## 8 Zhodnotenie dosiahnutých výsledkov

Predložená práca je venovaná analýze, popisu a špecifikácii metód, netodík a štandardov pre meranie prevádzkových parametrov v počítačových sieťach. Pozornosť je venovaná analýze pasívnych metód meraní prevádzkových parametrov, kde v rámci analýzy boli analyzované požiadavky a nutné podmienky pre umiestnenie bodov merania, synchronizácie meracích bodov, problematike odchyťovania paketov, generovania identifikátora paketu a prenos údajov.

Praktickým výsledkom práce je návrh modulárnej architektúry základného nástroja pre vykonávanie pasívnych meraní nazvaného basicmeter. Basicmeter v súčasnosti umožňuje realizovať merania objemových (šírka pásma, priepustnosť paketov) prevádzkových parametrov. Pri návrhu a implementácii basicmetra bola do úvahy braná špecifikácia vznikajúceho štandardu IPFIX. Vzhľadom na rozsiahlosť a komplexnosť štandardu IPFIX nie je basicmeter úplnou implementáciou tohoto štandardu, rovnako ako si táto práca nekladie za cieľ vyčerpávajúco obsiahnuť problematiku implementácie tohoto štandardu a navrhnúť komplexnú meraciu platformu. Hlavným cieľom tejto práce je poskytnúť základnú platformu, ktorú je možné ďalej vyvíjať a tak dosiahnuť úplnú implementáciu a zhodu so štandardom IPFIX.

S meracím nástrojom boli realizované experimenty merania prevádzkových parametrov v podmienkach Laboratória počítačových sietí, pri experimentoch sa používala reálna prevádzka laboratória za štandardných podmienok, bez vytvárania špeciálnych okruhov, alebo sietí. Merací nástroj bol zaradený do laboratórnej sieťovej infraštruktúry a poskytoval reálne informácie o dátových tokoch v laboratóriu. Pri experimentoch sa ukázalo, že je potrebné sa zamýšľať nad optimalizáciou meracej platformy najmä na strane dátového skladu, pokiaľ sa od dátového skladu a následne od analyzujúcej aplikácie, častí v zhode so štandardom IPFIX, žiadajú výsledky v reálnom čase. Rovnako do budúcnosti v prípade nasadenia meracieho nástroja v širokopásmových a vysokorýchlostných sieťach je potrebné sa zaoberať implementáciou a podporou vzorkovania a rôznych vzorkovacích algoritmov.

Počas realizácie diplomovej práce bola vďaka tomuto projektu nadviazaná užšia spolupráca s univerzitou v Jyväskylä vo Fínsku pri výmene skúseností a vedomostí v oblasti merania prevádzkových parametrov kvality služieb v počítačových sieťach.

## Zoznam použitej literatúry

- ALMES, G. — KALIDINDI, S. — ZEKAUSKAS, M.: *A One-Way Delay Metric for IPPM* [online] Publikované v septembri 1999. [citované 28.4.2004]. URL <http://www.rfc-editor.org/rfc/rfc2679.txt>
- ALMES, G. et al.: *A One-Way Packet Loss Metric for IPPM* [online] Publikované v septembri 1999. [citované 26.4.2004]. URL <http://www.rfc-editor.org/rfc/rfc2680.txt>
- ALMES, G. — KALIDINDI, S. — ZEKAUSKAS, M.: *A Round-Trip Delay Metric for IPPM* [online] Publikované v septembri 1999. [citované 26.4.2004]. URL <http://www.rfc-editor.org/rfc/rfc2681.txt>
- ANDRÉ, M. et al.: *Measurement of QoS parameters in IP networks* In Proceedings of 6<sup>th</sup> International Conference on Electronic Computers and Informatics, Košice, Herľany, Slovakia
- BILINSKIS, I. — MIKELSONS, A.: *Randomized Signal Processing*, Prentice Hall International, 1992
- BIRON, P. — MALHOTRA, A.: *XML Schema Part 2: Datatypes* [online] Publikované v máji 2001. [citované 5.5.2004] URL <http://www.w3.org/TR/xmlschema-2/>
- BRAY, T. et al.: *Extensible Markup Language (XML) 1.0 (Third Edition)* [online] Publikované vo februári 2004. [citované 4.5.2004] URL <http://www.xml.org/TR/REC-xml>
- BRÖKER, H. — GAYLORD, C. — HECKING, L.: *Gnuplot* [počítačový program] Ver. 4.0, [citované 7.5.2004] URL <http://www.gnuplot.info>
- BROWNLEE, N. — MILLS, C. — RUTH, G.: *Traffic Flow Measurement: Architecture* [online] Publikované v januári 1997. [citované 29.4.2004]. URL <http://www.rfc-editor.org/rfc/rfc2063.txt>

- BROWNLEE, N.: *Reference Manual NeTraMet & NeMaC Version 4.1* Information Technology Systems & Services, The University of Auckland, New Zealand, november 1997
- CLARK, J. — MURATA, M.: *RELAX NG Specification* [online] Publikované v decembri 2001. [citované 4.5.2004]. URL <http://www.relaxng.org/spec-20011203.html>
- CLARK, J.: *XSL Transformations* [online] Publikované v novembri 1999. [citované 5.5.2004]. URL <http://www.w3.org/TR/xslt/>
- DERI, L.: *Ntop* [počítačový program] Ver. 3.0, Pisa, Taliansko, [citované 3.5.2004] URL <http://www.ntop.org/> Merací nástroj pre Linux, FreeBSD
- DEMICHELIS, C. — CHIMENTO, P.: *IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)* [online] Publikované v novembri 2002. [citované 26.4.2004]. URL <http://www.rfc-editor.org/rfc/rfc3393.txt>
- DUFFIELD, N. — GROSSGLAUSER, M.: *Trajectory Sampling for Direct Traffic Observation*. In: Proceedings of ACM SIGCOMM 2000, Stockholm, Sweden, august 2000
- GUPTA, P. — McKEOW, N.: *Packet Classification on Multiple Fields*. In: Proc. Sigcomm, Computer Communication Review, vol. 29, no. 4, pp. 147-160, Harvard University, september 1999
- HEDENFALK, M.: *Confuse - simple configuration file parser library* [online] Publikované 25.9.2003. [citované 3.5.2004] URL <http://www.nongnu.org/confuse>
- ITU-T Recommendation Y.1540. *Internet protocol data communication service - IP packet transfer and availability performance parameters* [online] Publikované v decembri 2002. [citované 25.4.2004]. URL <http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-Y.1540>

- JAKAB, František: *Tvorba sieťových prostredí pre televzdelávanie, technická správa* č. INT 07/2002, Košice, október 2002
- KALIDINDI, S. — ZEKAUSKAS, M.: *Surveyor: An Infrastructure for Internet Performance Measurements* Proceedings of INET '99, San Jose, California, USA, jún 1999
- MAHDAVI, J. — PAXSON, V.: *IPPM Metrics for Measuring Conectivity* [online] Publikované v septembri 1999. [citované 29.4.2004]. URL <http://www.rfc-editor.org/rfc/rfc2678.txt>
- MATHIS, M. — ALLMAN, M.: *A Framework for Defining Empirical Bulk Transfer Capacity Metrics* [online] Publikované v júli 2001. [citované 26.4.2004]. URL <http://www.rfc-editor.org/rfc/rfc3148.txt>
- McCANNE, S. et al.: *Libpcap — library for capturing packets* [knížnica] Ver 0.7.2 URL: <http://www.tcpdump.org/release/libpcap-0.7.2.tar.gz>
- McCANNE, S. — JACOBSON, V.: *The BSD Packet Filter: A New Architecture for User-Level Packet Capture* Lawrence Berkeley Laboratory, Berkeley, december 1992
- McCANNE, S. et al.: *Tcpdump* [počítačový program] Ver 3.8.3 URL: <http://www.tcpdump.org/release/tcpdump-3.8.3.tar.gz>
- MILLS, D.: *Network Time Protocol (Version 3), Specification, Implementation and Analysis* [online] Publikované v marci 1992. [citované 26.4.2004]. URL <http://www.rfc-editor.org/rfc/rfc1305.txt>
- NICHOLS, K. et al.: *A Two-bit Diferentiated Services Architecture for the Internet* [online] Publikované v júli 1999. [citované 26.4.2004]. URL <http://www.rfc-editor.org/rfc/rfc2638.txt>

- PAXSON, V., et al.: *Framework for IP Performance Metrics* [online] Publikované v máji 1998. [citované 26.4.2004]. URL <http://www.rfc-editor.org/rfc/rfc2330.txt>
- PAXSON, V. — ADAMS, A. — MATHIS, M.: *Experiences with NIMI*, The First Passive and Active Measurement Workshop, Hamilton, New Zealand, apríl 2000
- PAXSON, V. et al.: *An Architecture for Large-Scale Internet Measurement*, In: IEEE Communications, vol. 36, no. 8, pp. 48-54
- QUITTEK, J. et al.: *Requirements for IP Flow Information Export* [online] Publikované v januári 2004. [citované 1.5.2004] URL <http://www.ietf.org/internet-drafts/draft-ietf-ipfix-reqs-15.txt>
- SADASIVAN, G. — BROWNLEE, N.: *Architecture Model for IP Flow Information Export* [online] Publikované v októbri 2003. [citované 1.5.2004] URL <http://www.ietf.org/internet-drafts/draft-ietf-ipfix-arch-03.txt>
- SCHULZRINNE, H. et al.: *RTP: A Transport Protocol for Real-Time Applications*, [online] Publikované v januári 1996. [citované 2.5.2004]. URL <http://www.rfc-editor.org/rfc/rfc1889.txt>
- SESHAN, S. et al.: *SPAND: Shared Passive Network Performance Discovery*, In: Proceedings 1<sup>st</sup> Usenix Symposium on Internet Technologies and Systems (USITS '97), Monterrey California, december 1997. URL: <http://daedalus.cs.berkeley.edu/>
- SHENKER, S., et al.: *Specification of Guaranteed Quality of Service* [online] Publikované v septembri 1997. [citované 26.4.2004]. URL <http://www.rfc-editor.org/rfc/rfc2212.txt>
- SUČÍK, JuraJ: *Príspevok k problematike merania a vyhodnocovania parametrov kvality služieb (QoS) v počítačových sieťach*. Košice: Technická univerzita. Fakulta elektrotechniky a informatiky. Katedra počítačov a informatiky, 2003. 66 s. Vedúci diplomovej práce: Ing. František Jakab

THOMPSON, H. et al.: *XML Schema Part 1: Structures* [online] Publikované v máji 2001. [citované 5.5.2004] URL <http://www.w3.org/TR/xmlschema-1/>

TROAN, E.: *Popt — library for parsing command line options* [knižnica] Ver 1.7 [citované 5.5.2004]. URL <ftp://ftp.rpm.org/pub/rpm/dist/rpm-4.1.x/popt-1.7.tar.gz>

VEILLARD, D.: *The XML C parser and toolkit of Gnome — libxml* [knižnica] Ver 2.6.9 [citované 29.4.2004]. URL <http://xmlsoft.org/sources/libxml2-2.6.9.tar.gz>

UJITERWAAL, H. — KOLKMAN, O.: *Internet Delay Measurements using Test Traffic* [online] Publikované v máji 1997. [citované 26.4.2004]. URL <ftp://ftp.ripe.net/ripe/docs/ripe-158.txt>

ZANDER, S. — SCHMOLL, C.: *NetMate* [počítačový program] Ver. 0.8, Berlín, Nemecko, [citované 3.5.2004] URL <http://www.fokus.fraunhofer.de/research/cc/meteor/projects/ip-qos/netmate/>  
Merací nástroj pre Linux, FreeBSD

ZSEBY, T. — ZANDER, S. — CARLE, G.: *Evaluation of Building Blocks for Passive One-Way Delay Measurements*. In: Proceedings of Workshop On Passive and Active Measurements, Amsterdam, Netherlands, apríl 2001

## Zoznam príloh

- používateľská príručka
- systémová príručka
- CD médium obsahujúce:
  - diplomovú prácu s prílohami v elektronickej podobe vo formáte PDF
  - funkčný program s dokumentáciou

## Zoznam obrázkov

3-1	Všeobecná architektúra merania oneskorení . . . . .	14
3-2	Komunikácia medzi NTP servermi v doméne . . . . .	17
4-3	Architektúra RTFM . . . . .	38
4-4	Architektúra nástroja NeTraMet . . . . .	38
4-5	Bloková schéma architektúry IPFIX . . . . .	41
5-6	Architektúra meracej platformy . . . . .	50
5-7	Architektúra meracieho nástroja . . . . .	53
6-8	Algoritmus spracovania paketu . . . . .	57
6-9	Proces validácie XML dokumentu . . . . .	60
7-10	Zapojenie v infraštruktúre Laboratória počítačových sietí . . . . .	62
7-11	Časový priebeh využitia šírky pásma za 24 hodín . . . . .	64
7-12	Časový priebeh priepustnosti paketov za 24 hodín . . . . .	65

## Zoznam tabuliek

2-1	Najvýznamnejšie parametre kvality služieb . . . . .	7
2-2	Rozdelenie a stručná charakteristika typov meraní . . . . .	8
3-3	Položky hlavičky IP paketu . . . . .	24
4-4	Popis metrík . . . . .	31
4-5	Charakteristiky metrík v odporúčaní Y.1540 . . . . .	36
4-6	Všeobecné požiadavky architektúry IPFIX . . . . .	45
5-7	Popis jednotlivých častí architektúry . . . . .	51