VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

ARCHITEKTURA PROGRAMOVÉHO VYBAVENÍ MONITOROVACÍ SONDY NA BÁZI TOKŮ

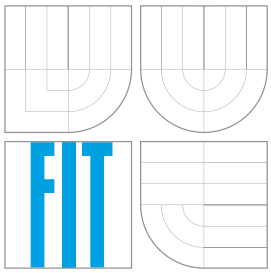
SEMESTRÁLNÍ PROJEKT
TERM PROJECT

AUTOR PRÁCE
AUTHOR

Bc. PETR ŠPRINGL

BRNO 2008

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

ARCHITEKTURA PROGRAMOVÉHO VYBAVENÍ MONITOROVACÍ SONDY NA BÁZI TOKŮ

SOFTWARE ARCHITECTURE FOR FLOW BASED MONITORING PROBE

SEMESTRÁLNÍ PROJEKT
TERM PROJECT

AUTOR PRÁCE
AUTHOR

Bc. PETR ŠPRINGL

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. TOMÁŠ MARTÍNEK

BRNO 2008

Architektura programového vybavení monitorovací sondy na bázi toků

Prohlášení

Prohlašuji, že jsem tuto práci vypracoval samostatně pod vedením pana Ing. Tomáše Martínka. Další informace mi poskytli kolegové z projektu Liberouter. Uvedl jsem všechny literární prameny, ze kterých jsem čerpal.

.....
Petr Špringl
3. ledna 2008

Poděkování

Především bych rád poděkoval vedoucímu své práce panu Ing. Tomáši Martínkovi za odborné vedení a čas věnovaný konzultacím této práce. Také bych chtěl poděkovat kolegům z projektu Liberouter za poskytnutí informací a zajištění technické podpory při návrhu a implementaci.

© Petr Špringl, 2008.
Tato práce vznikla jako školní dílo na Vysokém učení technickém v Brně, Fakultě informačních technologií. Práce je chráněna autorským zákonem a její užití bez udělení oprávnění autorem je nezákonné, s výjimkou zákonem definovaných případů.

Abstrakt

Tato práce se zabývá návrhem achitektury programového vybavení pro Flexibílní FlowMon sondu, zařízení monitorující vysokorychlostní sítě na základě datových toků, které je vyvíjeno v rámci projektu Liberouter. Je zde rozebrána problematika monitorování na základě datových toků, detailněji jsou popsány používáne exportovací formáty NetFlow verze 5 a verze 9. Práce obsahuje popis hardwarové části Flexibilní FlowMon sondy včetně jejích požadavků na programové vybavení, ze kterých vychází zde prezentovaný návrh kompletní programové architektury.

Klíčová slova

Síť, IP tok, monitorování, NetFlow, formát, kolektor, FlowMon, sonda

Abstract

This thesis deals with design of software architecture for Flexible FlowMon probe, accessories for monitoring high speed computer networks based on IP flows. The probe has been developed in project named Liberouter. There is described flow based monitoring and export formats NetFlow version 5 and version 9, which are very widely used. The thesis contains description of hardware part of Flexible FlowMon probe including its requirements for software, which are the base of the whole software architecture.

Keywords

Network, IP flow, monitoring, NetFlow, format, collector, FlowMon, probe

Citace

Petr Špringl: Architektura programového vybavení monitorovací sondy na bázi toků, semestrální projekt, Brno, FIT VUT v Brně, 2008

Obsah

Kapitola 1

Úvod

V posledních době dochází k obrovskému rozvoji informačních technologií a to především technologií, které jsou vytvořeny nad počítačovými sítěmi a Internetem. Neustále se zvyšuje počet uživatelů, jenž využívají informační prostředky pro přenos, ukládání a zpracování dat. S tímto souvisí rostoucí požadavky na přenosy většího množství dat po síti vyššími rychlostmi, přičemž se zcela automaticky předpokládá, že tyto přenosy budou probíhat spolehlivě a bezpečně. Ovšem tento samozřejmý požadavek je zcela netriviální, neboť s rostoucím počtem uživatelů Internetu také dochází ke zvyšování četnosti útoků, jejichž odhalování je stále náročnější. Současně také neustále rostou rychlosti počítačových sítí, které nyní dosahují až 10 Gb/s, přičemž v brzké budoucnosti bude pravděpodobně dosaženo ještě rychlostí vyšších, což opět správu a detekci problémů na síti ještě více zkomplikuje. Proto je nutné vyvíjet stále nová zařízení, která budou sloužit pro správu a monitorování i nejmodernějších složitých počítačových sítí.

Monitorovací zařízení slouží správcům sítí pro zjištění informací o stavu sítě či nastalých změnách v síti. Pokud tyto informace získá správce dostatečně včas, tak může na vzniklou situaci reagovat a řešit jí. Tato zařízení mohou upozorňovat na útoky, vyhodnocovat využívání jednotlivých služeb či přímo vytížení celé sítě, ale také třeba sloužit pro výpočty poplatků za služby. Existující zařízení umožňující monitorování sítě jsou dostatečně výkonnými nástroji pro použití na běžných rychlostech, ovšem při využití na vysokorychlostních sítích (>1 Gb/s) již selhávájí. To je obvykle způsobeno tím, že monitorovací činnost není jedinou činností, kterou vykonávají, nebo jsou limitovány výkonem procesoru či propustností systémové sběrnice. Síťový provoz je možné sledovat mnoha různými způsoby, přičemž každý poskytuje jiný druh informací či je prezentuje v jiné podobě. Příkladem jedné z metod je velmi využívaný SNMP (Simple Network Management Protocol), jenž slouží pro zasílání statistických dat ze síťových prvků k jejich další analýze. Poskytuje informace založené na čítačích a určených podmínkách jako jsou počet přijatých paketů, počet chybných paketů. [1]

V posledních letech získává na důležitosti především monitorování na základě datových toků, tzv. IP flows. Hlavním představitelem je v této oblasti firma CISCO [2], která v roce 1996 vyvinula metodu NetFlow. NetFlow poskytuje informace o komunikaci o IP přenosech a v jejich kontextu odpovídá na otázky: "Kdo, co, kde, kdy, kolik a jak?". [5] Neboli vystihuje komunikaci mezi dvěma IP adresami pomocí určité služby probíhající na určitých portech v určitý čas a zahrnující určité množství přenesených dat. Vytváří stručný, ale výstižný záznam o komunikaci mezi každými dvěma počítači, tedy poskytuje detailní pohled na děje probíhající v síti. Umožňuje sledování aktivity uživatelů či využívání služeb, plánování architektury sítě, napomáhat bezpečnosti sítě včasným odhalováním útoků, účtovat síťové

služby a mnohé další.

FlowMon sonda, pasivní monitorovací zařízení vznikající v rámci projektu Liberouter [9] je jedinečným nástrojem umožňující monitorovat vysokorychlostní sítě na základě datových toků. Funkčnost sondy je rozdělena mezi dvojici akcelerační karet se síťovými rozhraními a hostitelský osobní počítač, do kterého jsou karty připojeny. Zcela podle principu hardware software codesign jsou rychlostně a výpočetně náročné operace prováděny pomoci programovatelných polí (FPGA) na akceleračních kartách a méně naročné, ale o to složitější části, jsou zajišťovány programovým vybavením hostitelského počítače. Díky tomu je možné pomocí sondy monitorovat bez nutnosti vzorkování i nejmodernější sitě a to s přijatelným uživatelským rozhraním zprostředkovaným hostitelským osobním počítačem.

Tato práce se zabývá návrhem programové architektury nejnovější verze tzv. Flexibilní FlowMon sondy, jejíž hardwarová část právě vzniká. V úvodu práce je popsán princip monitorování na základě datových toků a jeho rozdělení mezi exportéry a kolektory. Detailněji je rozebrána problematika exportovacích protokolů na kolektory a jsou popsány protokoly NetFlow verze 5 a 9. Další kapitola je věnována popisu hardwarové části Flexibilní FlowMon sondy a jejích požadavcích na programové vybavení. Z této části vychází vlastní návrh programového vybavení pro ovládání a konfiguraci sondy, který bude následně implementován.

Kapitola 2

Monitorování na základě datových toků

Pro efektivní monitorování počítačové sítě je nutné zvolit takovou metodu, která bude poskytovat vhodný obraz o situaci na síti a to nejen za standardních podmínek, ale i v případě jejího vyššího zatížení či útoku. Navíc je nutné, aby byly získané informace poskytovány s co nejmenším zpožděním, neboť to ovlivňuje možnost na vzniklé situace včasně reagovat. V současné době je hlavním problémem monitorování vysokorychlostní sítích bez zkreslení, jež je způsobováno použitím vzorkování. S tímto také úzce souvisí problém s množstvím přenášených dat po síti, kdy není možné uchovávat veškeré informace o událostech v síti, ale je třeba je agregovat a vhodným způsobem prezentovat.

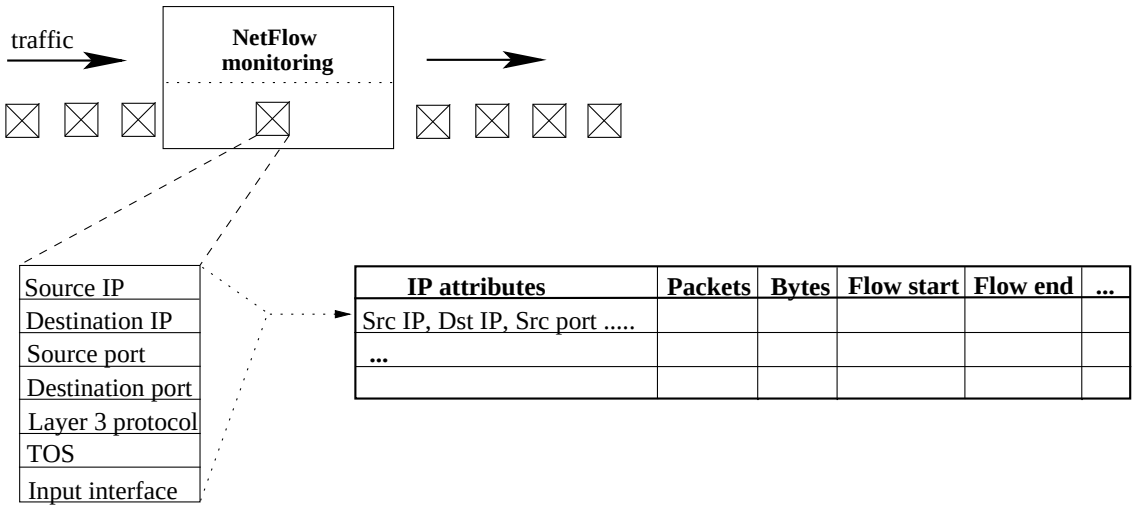
Komunikace mezi prvky na síti probíhá prostřednictvím zasílání paketů. Zařízení nejprve svá odesílaná data rozdělí na části (segmenty). Dále segmenty podle typu komunikačního protokolu zabalí do paketů, které již obsahují informace o cílovém prvku. Pakety jsou postupně odesílány do sítě. Vzhledem k obrovskému množství paketů v síti není vhodné založit monitorování na základě sledování jednotlivých paketů, ale je třeba monitorovat na vyšší úrovni abstrakce. Jako vhodná metoda se jeví monitorování na základě datových toků. [10]

2.1 NetFlow

Pojmem NetFlow se označuje metoda monitorování sítě na základě datových toků (tzv. IP flows), jenž reprezentují komunikaci mezi dvěma IP zařízeními v síti. U každého paketu, který prochází přes monitorovací zařízení, je zkoumána množina jeho IP atributů. Pomocí těchto atributů se rozlišuje, ke kterému toku daný paket náleží. Datový tok je tvořen pakety mající shodné všechny zkoumané IP atributy (viz Obrázek 2.1). Každý datový tok reprezentuje komunikaci na síti, a neboť se většina komunikace skládá z mnoha paketů, tak je současně dosahováno i výrazné agregace dat. Obvykle jsou datové toky založeny nad množinou pěti až sedmi IP atributů [5, 10], jsou to:

- zdrojová IP adresa
- cílová IP adresa
- zdrojový port
- cílový port

- typ protokolu
- druh služby (TOS)
- rozhraní monitorovacího zařízení



Obrázek 2.1: NetFlow monitoring

Teoreticky by mohly být datové toky nekonečné, ale toto v praxi není možné a musí být určitým mechanismem zajištěno, aby v určitém časovém intervalu každý tok skončil. Toky jsou totiž vyhodnocovány až v okamžiku jejich ukončení (expirace), tedy by dlouhotrvající komunikace byla vyhodnocena až s velkým zpožděním, což by výrazně snížovalo vypovídací hodnotu monitorování.

Datový tok může expirovat obvykle vlivem dvou nastavitelných vlastností - aktivní a neaktivní timeout. Datový tok je ukončen, pokud časová délka jeho neaktivity přesáhne neaktivní timeout, neboli pokud po dobu neaktivního timeoutu nepřišel žádny paket patřící do daného toku. Tímto způsobem je vlastně detekováno ukončení dané komunikace. Naproti tomu aktivní timeout slouží pro rozdělení dlouhotrvajících toků do několika různých toků, aby nedocházelo k tak velkému zpoždění v získávání informací při monitorování. Každý tok je ukončen, pokud je doba jeho trvání delší než hodnota aktivního timeoutu.

2.2 Systém monitorování

Existují dvě základní možnosti, jak získávat informace o datových tocích. Prvním je obvyklý monitorovací systém, kdy monitorování a agregaci dat na základě datových toků provádí přímo směrovače. V tomto případě jsou ovšem omezení v rychlostí i spolehlivostí monitorování, neboť primárním účelem směrovačů je směrování paketů, což je pro ně často samo o sobě dosti náročné. Monitorování proto obvykle probíhá za pomoci vzorkování, kdy jsou zpracovávány pouze pakety vybrané určitou heuristikou, což samozřejmě zkresluje naměřené výsledky.

Druhou možností je samostatný pasivní prvek sítě, který slouží jen pro monitorování a již nevykonává žádné další operace. Prochází skrze něj pakety, které si pouze zkopíruje

a následně zpracuje. Díky tomu je docíleno vyšší rychlosti zpracování, vyšší propustnosti i vyšší bezpečnosti.

Monitorování samo o sobě, ať již prováděné směrovači nebo speciálními zařízeními, není dostatečnou činností, neboť je nutné také získaná data zpracovávat, analyzovat, vyhodnocovat, ukládat atp. Proto metoda NetFlow využívá celý monitorovací systém složený z několika různých prvků - exportéry a kolektory. Exportéry jsou umístěny na důležitých místech sítě jako jsou směrovače a brány a zajišťují vlastní monitorování na základě datových toků. V okamžiku, kdy datový tok skončí, ať již na základě aktivního, neaktivního timeoutu či jiné situace, tak je odeslán (exportován) na vzdálené kolektory k dalšímu zpracování.[7]

Kolektory přijímají a zpracovávají příchozí toky od exportérů. Data ukládají do své databáze, vytvářejí různé statistiky, mohou zobrazovat grafy a statistická schémata. Dělají vše, aby bylo možné na základě jejich výstupů sledovat situace na síti a vytvářet dlouhodobé analýzy síťového provozu. [7]

2.3 Protokoly pro export dat

Po ukončení datového toku na straně exportéru je nutné, aby byl co nejdříve odeslán na vzdálený kolektor. Toto odesílání může být prováděno různými způsoby pomocí různých protokolů určených pro export dat. Nejčastěji používanými jsou exportovací formáty firmy CISCO zvané Cisco NetFlow Export Format a protokoly z nich odvozené (např. IPFIX). Exportovací formát NetFlow má za sebou již víceletý vývoj. Byla vytvořena jeho již devátá verze, přičemž pouze některé verze byly a jsou skutečně využívány. V současné době je především využívána verze 5 a také se začíná prosazovat nejnovější verze, verze 9. Všechny verze jsou postaveny nad protokolem UDP a verze 9 oproti ostatním verzím vyniká především svými možnostmi rozšiřitelnsoti a značnou flexibilitou. Stručné charakteristiky používaných verzí Cisco NetFlow Export Format jsou uvedeny v Tabulce 2.1). [3]

NetFlow Export Format	Charakteristika
verze 1	první verze, nejjednodušší, používán jen výjimečně
verze 5	rozšířený formát, přidává podporu o BGP autonomních systémech a podporuje sekvenční číslování toků
verze 7	přidána podpora pro některé přepínače firmy CISCO
verze 8	nově podpora pro export agregačních dat z mezipamětí směrovačů
verze 9	nejnovější formát, dosti flexibilní a rozšiřitelný, založen na principu zasílání šablon pro popis formátu přenášených dat, na jeho bázi založen i další formát - IPFIX

Tabulka 2.1: Vývoj exportovacího formátu NetFlow

2.4 NetFlow verze 5

Jedná se o základní verzi formátu, která vychází z původní verze 1. Hlavní rozdíly jsou v přidání informací o monitorovacích systémech a sekvenční číslování toků. Číslování toků je důležitou změnou, neboť je pro zasílání datagramů výhradně používán protokol UDP,

který nezajišťuje jistotu doručení. Kolektor při příjmu datagramu odečte nejvyšší sekvenční číslo přijatého toku (sekvenční číslo + počet toků v datagramu) v předchozích datagramech od sekvenčního čísla právě přijatého datagramu a tím zjistí počet ztracených toků. [3]

Tento formát má pevně danou strukturu. Skládá se z hlavičky ihned následované jedním až třiceti vlastních záznamů obsahující informace o jednotlivých tocích. Velikost hlavičky je 24 bajtů a má následující podobu:

Pozice	Obsah	Popis
0-1	Verze	NetFlow verze záznamů v paketu
2-3	Počet	Počet toků v paketu (1-30)
4-7	Čas chodu systému	Počet milisekund od spustění exportéru
8-11	UNIX čas	Čas odeslání paketu zaznamenán v sekundách od UTC (Coordinated Universal Time), tedy od 1.1. 1970.
12-15	UNIX čas	Část UNIX času v nanosekundách
16-19	Sekvenční číslo	Sekvenční číslo prvního toku v datagrmu
20	Typ zařízení	Typ monitorovacího zařízení
21	Port zařízení	Port monitorovacího zařízení
22-23	Rezervováno	Nepoužité

Tabulka 2.2: Hlavička NFv5 [3]

Záznam popisující jeden tok má velikost 48 bajtů a má také přesně danou strukturu:

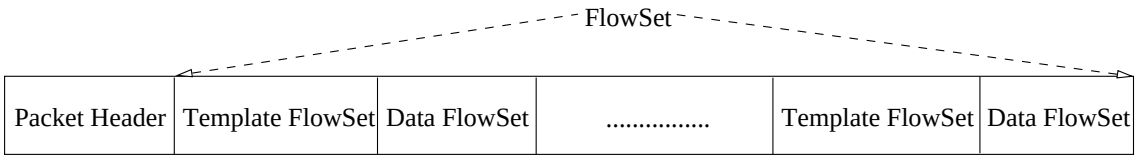
Pozice	Obsah	Popis
0-4	Zdrojová adresa	IP adresa zdrojového zařízení
4-7	Cílová adresa	IP adresa cílového zařízení
8-11	Next hop	IP adresa následujícího směrovače
12-13	Vstup	SNMP index vstupního rozhraní
14-15	Výstup	SNMP index výstupního rozhraní
16-19	Pakety	Počet paketů tvořící tok
20-23	Počet oktetů	Celkový počet bajtů v paketech (L3 vrstva)
24-27	Začátek	Systémový čas zařízení při zahájení toku
28-31	Konec	Systémový čas při přijetí posledního paketu toku
32-33	Zdrojový port	Použitý port na zdrojovém zařízení
34-35	Cílový port	Použitý port na cílovém zařízení
36	Zarovnání	Nepoužité
37	TCP flagy	Kumulativní OR TCP flagů
38	Protokol	Použitý protokol
39	TOS	Typ služby
40-41	Zdrojový AS	Autonomní systémové číslo zdrojového zařízení
42-43	Cílový AS	Autonomní systémové číslo cilového zařízení
44	Zdrojová maska	Bitová maska prefixu adresy zdrojového zařízení
45	Cílová maska	Bitová maska prefixu adresy cílového zařízení
46-47	Zarovnání	Nepoužité

Tabulka 2.3: Záznam o toku NFv5 [3]

2.5 NetFlow verze 9

Je to nejnovější verze NetFlow formátu, který byl vytvořen pro snadný export informací o datových tocích z exportérů na kolektory. Jeho hlavními výhodami oproti ostatním formátům jsou možnosti jeho rozšířitelnosti a jeho značná flexibilita. Tyto vlastnostni jsou způsobeny tím, že je založen na systému zasílání šablon (templates), které popisují strukturu odesílaných dat. Šablony poskytují rozšiřitelnou podobu formátu s tím, že až v budoucnu dojde k vzniku nové vlastnosti NetFlow služby, kterou bude třeba také exportovat, tak se daná vlastnost přidá a popíše pouze v šabloně. A od tohoto okamžiku budou obě strany, přijímací (kolektor) i vysílací (exportér), snadno přijímat či vysílat informace o této nové vlastnosti. Je zcela patrné, že nebude nutné s novými vlastnostmi vytvářet stále nové verze formátu, ale bude zcela stačit přidání dané vlastnosti do stávajícího formátu. [4, 6]

Exportéry vytváří exportované pakety (export packets), které jsou odesílány na vzdálené kolektory, kde dochází k jejich zpracování [7]. Tyto pakety se skládají z hlavičky (packet header) a z části nazývané FlowSet (viz Obrázek 2.2). Hlavička je první částí exportovaného paketu, která poskytuje základní informace o paketu jako jsou NetFlow verze, počet záznamů obsažených v paketu a číslování, pomocí kterého lze snadno zjistit ztrátu některého z paketů. FlowSet je druhou částí paketu a je to obecný pojem pro kolekci záznamů následujících za hlavičkou v exportovaném paketu. [4, 6]



Obrázek 2.2: Paket NetFlow verze 9

Existují dva druhy FlowSetů, jeden druh obsahuje šablony (templates) a druhý data. Paket může obsahovat jeden nebo více FlowSetů a oba jejich typy se mohou v jednom paketu kombinovat (viz Obrázek 2.2).

Kolekce jedné nebo více šablon (template record), které byly seskupeny v jednom paketu, se říká Flowset šablon (template FlowSet). Šablona slouží k popisu sekvenčních dat, která mohou být v současném čí v některém z budoucích exportovaných paketů odeslány na kolektor. Je důležité také poznamenat, že šablona nemusí nezbytně popisovat data v exportovaném paketu, ve kterém se vyskytuje. Naopak šablony jsou číslovány unikatním identifikačním číslem (template ID), které je později uvedeno u každého datového záznamu, aby bylo zřejmé podle které z šablon byl vytvořen a musí být interpretován. Neboť šablony se nemusí posílat v každém paketu, ale stačí je v určitých intervalech obnovovat. Je nezbytné, aby měly kolektory určitou vyrovnávací paměť pro ukládání příchozích šablon. [4, 6]

Stejně jako FlowSet šablon je kolekcí jedné či více seskupených šablon v paketu, tak FlowSet dat (data FlowSet) je kolekcí seskupených datový záznamů (data record), které jsou zásadní informační složkou NetFlow formátu. Datové záznamy poskytují informace o datových tocích, které byly expirovány na exportéru.

Pomocí NetFlow formátu verze 9 je možné také zasílat informace o vlastnostech celého NetFlow monitorovacího procesu, kterými například jsou vzorkování dat či identifikace rozhraní, ze kterého data přichází atp. K tomuto slouží volitelné datové záznamy (options data record), které jsou v duchu celého formátu popsány volitelnými šablonami (options template). [4, 6]

2.5.1 Formát paketu Netflow verze 9

Paket formátu NetFlow verze 9 se skládá vždy z hlavičky následované alespoň jedním FlowSetem obsahující data nebo šablony. FlowSet šablon poskytuje popis jednotlivých polí, která budou využita v budoucích datových FlowSetech, které se ale mohou vyskytnout již v daném paketu. [4, 6]

Existují tři možnosti přípustných kombinací FlowSetů v paketu:

1. Paket obsahuje různě prokládaně FlowSety se šablonami i s daty. Kolektor by v tomto případě neměl předpokládat, že šablony vložené v paketu mají nějaký zvláštní vztah k datovým FlowSetům v daném paketu. Kolektor si musí ukládat všechny přijaté šablony a k interpretaci datového FlowSetu použije šablonu, jejíž ID je shodné s identifikátorem uvedeným v datovém FlowSetu.

2. Paket obsahuje pouze datové FlowSety. Toto je nejčastější případ. Již byly odeslány veškeré šablony na kolektor, jsou dostatečně aktuální a nyní se zasílají pouze nasbíraná data.

3. Paket obsahuje pouze FlowSety se šablonami. Toto je nejméně častá situace, většinou se informace o šablonách zasílají spolu s nasbíranými daty. Používá se v situacích, kdy je třeba synchronizovat exportér s kolektorem jak nejrychleji to je možné, např. po restartu exportéru. Také je důležité, že šablony mají určitou dobu platnosti. Tedy je třeba šablony v určitých časových intervalu obnovovat a znovu zasílat na kolektor. A pokud právě nejsou žádná jiná data k odeslání, tak se může odeslat paket obsahující pouze šablony.

2.5.2 Hlavička formátu NetFlow verze 9

Formát hlavičky NetFlow verze 9 zůstává ve srovnání s dřívějšími verzemi v podstatě nezměněn, je postaven nad formátem hlavičky z NetFlow verze 5. Je pevně daná struktura jednotlivých polí i jejich pořadí. Skládá se ze těchto šesti polí: [4, 6]

Verze (version)	Vyjadřuje verzi NetFlow záznamů v paketu, pro verzi 9 se jedná o hodnotu 0x0009.
Počet (count)	Sděluje kolik FlowSetů (jak datových tak se šablonami) je obsaženo v paketu.
Čas chodu systému (system uptime)	Počet milisekund které uběhly od spuštění exportéru.
UNIX čas (UNIX seconds)	Datum a čas odeslání paketu, který je zaznamenán v sekundách od UTC (Coordinated Universal Time), tedy od 1.1. 1970.
Pořadové číslo (sequence number)	Pořadové číslo paketu odesílaného exportérem, které slouží k detekci případných nedoručených paketů s daty.

ID zdroje (source ID)	32bitová unikátní hodnota, která specifikuje zařízení, ze kterého byly pakety odeslány. Toto číslo je závislé na konkrétním výrobci.

2.5.3 NetFlow verze 9 formát FlowSetu šablon

Jedním z klíčových prvků formátu NetFlow verze 9 je FlowSet obsahující šablony. Šablony zajišťují výraznou flexibilitu formátu, neboť umožňují kolektorům správně interpretovat příchozí data bez předešlé znalosti formátu daných dat. Šablony jsou použity k popisu typu a délky jednotlivých polí uvnitř datových záznamů. Každý datový záznam NetFlow formátu obsahuje pole s jedinečným identifikátorem šablony, podle které byl záznam vytvořen a tedy má být i interpretován na straně kolektoru. FlowSet šablon se skládá z těchto polí: [4, 6]

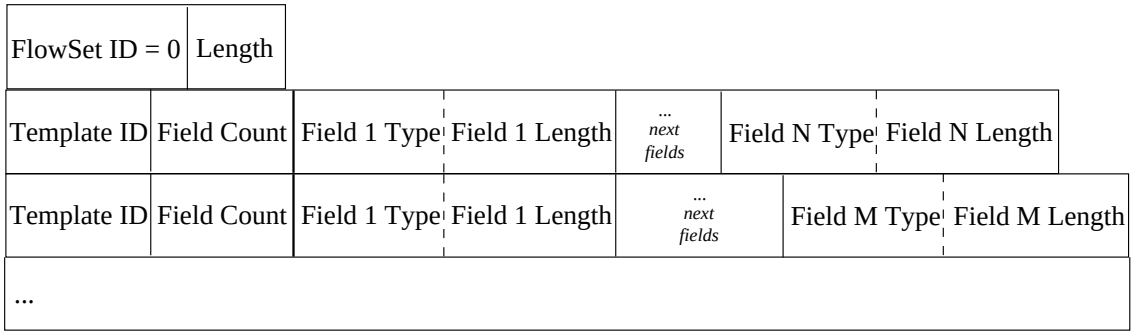
Identifikátor FlowSetu (FlowSet ID)	Tento identifikátor slouží k rozlišení záznamů šablon od dat. Má vždy hodnotu 0.
Délka (length)	Vyjadřuje celkovou délku daného FlowSetu. Neboť mohou být šablony a tedy i FlowSety různě dlouhé, tak je nutné udávat tuto hodnotu, aby byl zřejmý začátek dalšího FlowSetu. Délka je vyjádřena v TLV (type/length/value) formátu, což znamená, že obsahuje v bajtech vyjádřenou délku FlowSetu včetně polí Identifikátor FlowSetu a Délka.
Identifikátor šablony (template ID)	Každá šablona má unikátní identifikační číslo, které slouží k jednoznačnému určení šablony.
Počet polí (field count)	Určuje počet polí v dané šabloně. Je nezbytné neboť jeden FlowSet může obsahovat více šablon, tedy slouží k určení konce dané šablony.
Typ pole (field type)	Toto číslo vyjadřuje typ pole, tedy jakou informaci dané pole bude obsahovat v datovém záznamu. Definice hodnot vyjadřující určitý typ pole jsou zcela závislé na výrobci zařízení, ale obvykle se používají definice od firmy CISCO.
Délka pole (field length)	V bytech vyjádřená délka předcházejícího pole.

Výše uvedená pole se mohou ve FlowSetu šablon opakovat takovým způsobem, aby bylo možné dostatečným způsobem šablonou popsat datový formát(viz Obrázek 2.3).

Šablony musí být na kolektory v určitých intervalech znovu posílány a tím obnovovány, v jiném případě by došlo k jejich vypršení a zneplatnění na straně kolektoru. Existují dvě možnosti, jak šablony obnovovat. Posílat šablony vždy po uplynutí určitého časového intervalu nebo znovu zasílat šablony v každém N-tém paketu. [4, 6]

2.5.4 NetFlow verze 9 formát datového FlowSetu

V datových FlowSetech se posílají informace o tocích. Každy FlowSet odpovídá některé z dříve zaslaných šablon a podle ní je také interpretován. Jeden FlowSet může obsahovat

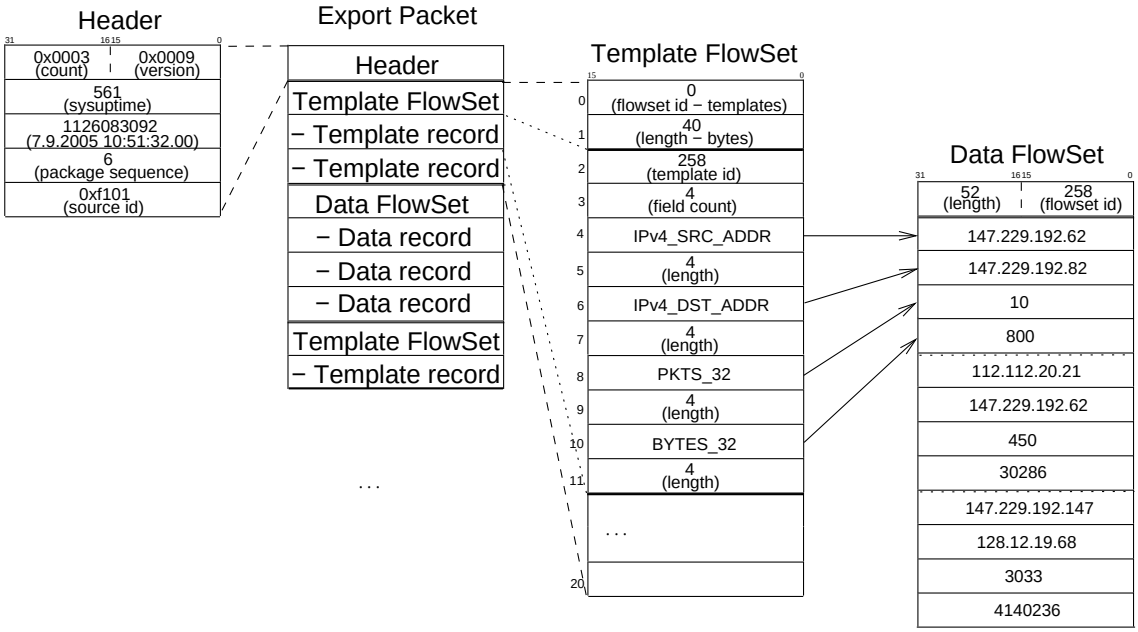


Obrázek 2.3: FlowSet šablon

data o více tocích. Pokud k danému datovému FlowSetu není nalezena šablona, tak dochází k jeho zahození. Datový FlowSet se skládá z těchto polí: [4, 6]

Identifikátor FlowSetu (FlowSet ID)	Obsahuje číslo šablony, podle které má být tento FlowSet interpretován.
Délka (length)	Vyjadřuje celkovou délku daného FlowSet v TLV (type/length/value) formátu.
Hodnoty toků (record N - field N)	Hodnoty jednotlivých polí definované v odpovídající šabloně.
Zarovnání (padding)	Zarovnání na 32bitovou hodnotu. I zarovnání se počítá do celkové délky(length).

Na Obrázku 2.4 je vyobrazen vzorový příklad činnosti formátu NetFlow verze 9. Exportovaný paket obsahuje určitou hlavičku následovanou FlowSetem šablon, kde jsou popsány použité šablony, přičemž jedna je detailně rozepsána. Paket obsahuje i datový FlowSet s několika záznamy a jeden z nich je schématicky vztažen k příslušné šabloně.



Obrázek 2.4: Schéma formátu NetFlow verze 9

Kapitola 3

FlowMon sonda

FlowMon sonda je zařízení vyvíjené v rámci projektu Liberouter sloužící pro monitorování vysokorychlostních sítí na základě datových toků. Prvotní verze sondy byla navržena pro 1 Gb/s sítě, na kterých probíhalo monitorování bez ztráty paketu. Ovšem při použití na 10 Gb/s sítích již nebylo možné monitorovat bez použití vzorkování nebo dokonce ztráty výrazné části paketů vlivem přijímání velkého množství paketů vysokými rychlostmi. Proto bylo nutné vytvořit zcela novou architekturu firmwaru sondy nazvanou Flexibilní FlowMon sonda, pro kterou je nezbytné navrhnout a vytvořit novou architekturu navazujícího programového vybavení. [9]

3.1 Flexibilní FlowMon sonda

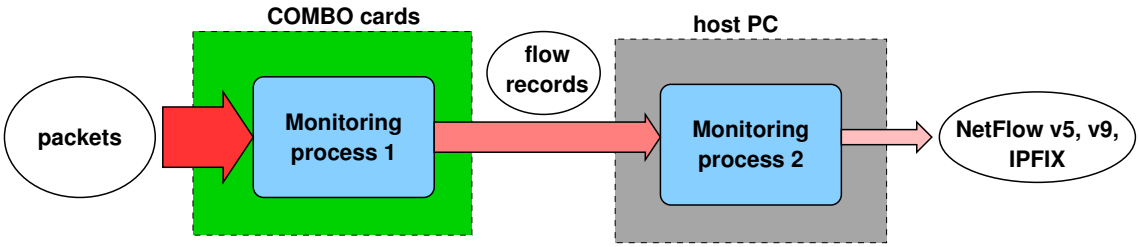
FlowMon sonda je založena na bežném osobním počítači s operačním systémem Linux obsahující dvojici akceleračních karet, které jsou vyvíjeny v rámci projektu Liberouter. Jedná se o hlavní kartu zapojenou do PCI sběrnice základní desky, k níž je připojena druhá z karet mající 2 až 4 síťová rozhraní. Na obou kartách jsou mimo jiné programovatelné čipy (FPGA), jenž umožňují zpracovávat velká množství dat vysokými rychlostmi. Karty poskytují jednotné rozhraní použitím platformy NetCOPE [9] pro přístup k periferním rozhraním (síťová rozhraní, paměti, PCI sběrnice), které umožňuje rychlou implementaci celé architektury firmwaru a odstíňuje konkrétní použitou dvojici akceleračních karet (např. různá síťová rozhraní atp.). [11, 12]

Při návrhu Flexibilní FlowMon sondy byly brány v podtaz zkušenosti zjištěné používáním předchozích verzí a bylo rozhodnuto o rozdělení monitorovacího procesu mezi akcelerační kartu a osobní počítač. Toto je výrazná změna v přístupu k implementaci celé sondy oproti předchozím verzím, kde byl monitorovací proces implementován zcela na kartě a osobní počítač zajišťoval pouze konfiguraci sondy a export přijatých toků na kolektory. V tomto případě byla akcelerační karta plně vytížena, zatímco procesor počítače byl využit přibližně z 5 procent. Proto bylo rozhodnuto o zjednodušení a tím i zrychlení části firmwaru a o vyšším využití zdrojů osobního počítače.

3.2 Monitorovací proces

Monitorovací proces je rodělen do dvou částí mezi akcelerační karty (COMBO cards) a osobní počítač (host PC). Prostřednictvím rozhraní na akcelerační kartě jsou přijímány pakety a zpracovávány na základě datových toků. Toky, které jsou uvolněny z pamětí ak-

celeračních karet, jsou přenášeny do hostitelského osobního počítače, kde je rozhodnuto o jejich dalším zpracování na základě datových toků nebo o jejich exportu na kolektory s využitím exportovacích formátů NetFlow verze 5 či 9 nebo IPFIX (viz Obrázek 3.1). [11, 12]



Obrázek 3.1: Koncept Flexibilní FlowMon sondy [12]

Dva stupně monitorovacího procesu pracují následovně - na akcelerační kartě:

- Příjem paketů ze sítě
- Extrahování informací z hlaviček paketů
- Z klíčových polí toku vytvořena hash, která je přímo adresa v paměti pro daný tok
- Kolize toků v paměti jsou řešeny přepsáním novým tokem
- Expirované nebo kolizní toky jsou přeneseny do paměti hostitelského osobního počítače

- v hostitelském osobním počítači:

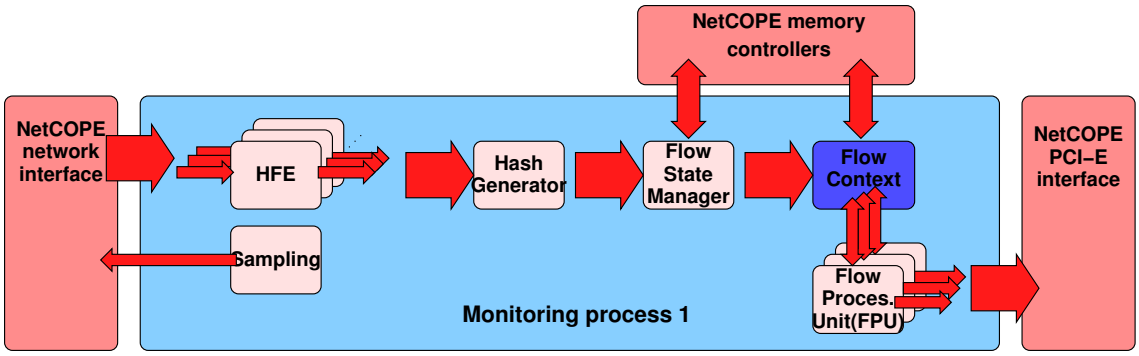
- Příjem toku pomocí přímého přístupu do paměti (DMA)
- Druhá část monitorovacího procesu - agregace příchozích toků s odpovídajícími toky v paměti počítače
- Export expirovaných toků na kolektory

Rozdělení úlohy na dvě části snižuje výskyt fragmentovaných toků, tedy toků, které expirovaly z jiného důvodu než na základě aktivního či neaktivního timeoutu (např. kolize, nedostatek paměti). Na základě testů bylo zjištěno, že agregace kartou sníží rychlost příchozích paketů na méně než jednu desetinu původní hodnoty, což umožní procesoru počítače zpracovávat všechny příchozí toky z karty a sondě zpracovávat celý provoz 10 Gb/s linky.

3.3 Architektura firmwaru

Firmware Flexibilní FlowMon sondy využívá firmwarové platformy NetCOPE a FlowContext. [9] Firmware NetCOPE přijímá pakety, které je schopen vzorkovat na základě požadavku z firmwaru FlowMon sondy, jenž tento požadavek získá od uživatele prostřednictvím programové vrstvy na hostitelském počítači. Na vstupu je paketům přiřazena časová značka a jsou posílány do FlowMon firmware. Zde dochází k jejich parsování (HFE procesor) a jsou získávány informace nezbytné k vytvoření záznamu o toku, ostatní informace

jsou zahozeny. Informace získané z paketu jsou předány FlowContext firmwaru, jenž zajistí vyčtení existujícího záznamu o toku z paměti a jeho přidělení (společně s daty o paketu) FlowProcessingUnit jednotce (FPU). FPU zajistí aktualizaci hodnot v záznamu a uloží záznam zpět, pokud není důvod k jeho expiraci. V případě expirace je záznam přeposlán do výstupního bufferu, odkud je proveden přenos do softwaru hostitelského počítače. [11, 12]



Obrázek 3.2: Blokové schéma firmwaru [12]

Postup zpracování:

- Pakety s časovou značkou jsou získávány od NetCOPE
- Pakety jsou distribuovány mezi několik HFE instancí
- HFE extrahuje informace z paketu a vytvoří UH hlavičku, následuje zbytek paketu
- HashGenerator spočítá hash, která je používána jako adresa/identifikátor toku
- FlowStateManager podle záznamu upraví časové údaje o toku
- FlowContext připraví záznam o toku z paměti a pošle ho do FPU
- FPU jednotka upraví statistiky, či expiruje záznam a předá ho části NetCOPE, která provede DMA přesun do softwaru

3.3.1 HFE procesor

HFE (Header Field Extractor) procesor je hardwarová jednotka sloužící pro získávání informací z hlaviček příchozích paketů, ze kterých vytváří tzv. UH hlavičky. Nadále se již pracuje právě s těmito hlavičkami, neboť pro monitorování na základě datových toků nejsou potřeba celé pakety, ale pouze informace z jejich hlaviček. U Flexibilní FlowMon sondy je možné, aby si uživatel před vytvořením firmwaru definoval strukturu HFE hlavičky včetně jejího obsahu a tím si vybral položky z hlaviček paketů, které jej při monitorování zajímají. HFE jednotka je implementována v jazyce Handel-C, který je modifikací standardního jazyka C pro popis paralelních výpočtů. Vlastní zdrojový kód HFE procesoru je velmi složitý, proto bylo uživateli umožněno definovat strukturu UH hlavičky prostřednictvím konfiguračního souboru, jenž je používán při překladu této jednotky. [11, 12]

3.3.2 HashGenerator

HashGenerator je velmi jednoduchá jednotka, která podle bitového pole zadaného při konfiguraci firmwaru vybere klíčová slova (vymaskuje neklíčová) z UH hlavičky. Na těchto slovech vypočítá pro každou UH hlavičku hash, kterou před ní následně uloží. Tato hash slouží k adresaci toku příslušného paketu, proto hash musí být co nejkvalitnější (např. MD5 či CRC). Vstupem HashGenerator jednotky je UH hlavička a výstupem pak také UH hlavička, ale s přidaným identifikátorem (hash). [11, 12]

Maska pro výpočet hash musí být nastavena prostřednictvím programového vybavení hostitelského počítače a je možné ji i měnit během používání sondy. Při startu sondy je také nutné hash funkci inicializovat náhodnou hodnotou.

3.3.3 FlowStateManager

Jednotka FlowStateManager slouží pro expiraci již nepoužívaných toků, tedy takových, které neobdrželi po určitou dobu žádný paket. Tato doba se nazývá neaktivní timeout a je možné její hodnotu volit kdykoliv během používání sondy. Jednotka kontroluje všechny toky vzhledem k hodnotě neaktivního timeoutu a informuje FlowProcessingUnit o tocích, které mají být uvolněny.

FlowStateManager přijímá UH hlavičky paketů z jednotky HashGenerator. Příchozí pakety způsobují obnovu časového příznaku pro daný tok. Aktualní čas mínus časový příznak toku značí délku neaktivity toku. Pokud je tok neaktivní po dobu delší než je nastavený neaktivní timeout, pak je k toku poznačen příznak neplatnosti časové značky. FlowStateManager na takový tok vygeneruje požadavek na expiraci, který zašle FlowProcessingUnit přes FlowContext. [11, 12]

3.3.4 FlowProcessingUnit

Jednotka FlowProcessingUnit (FPU) má za úkol aktualizovat záznam o toku informacemi získané z příchozího paketu. Záznam i informace o paketu, jsou jí poskytnuty FlowContextem. Neboť zpracování záznamu se jeví jako časově náročný úkol je tato jednotka instancována dvou a vícekrát, na což je FlowContext připraven.

FPU jednotka musí být vygenerována na základě informací o struktuře UH hlavičky, vlastního záznamu o tocích (flow context) a definicí operací nad položkami. [11, 12]

Jednotka provádí kontroly nad klíčovými poli (identifikující tok) pro shodu záznamu o toku (context) a UH hlavičkou - zda daný paket reprezentovaný UH hlavičkou skutečně náleží danému toku a nedošlo ke kolizi. Tyto kontroly včetně dalších jako např. aktivní timeout jsou popsány v konfiguračním xml souboru (viz [11]) a jsou prováděny FPU jednotkou, která musí být podle toho korektně vygenerována v době přípravy firmware - tzn. před vlastní monitorovací činností sondy.

3.4 Flexibilita u FlowMon sondy

Výstupy monitorovacího procesu na základě datových toků lze použít mnoha způsoby, přičemž v každé síti a pro každého správce sítě mohou být důležité jiné informace o síti. Avšak vzhledem k jasným omezením, jak na straně hardware i software není možné do monitorování zahrnout veškeré možné informace. Proto bylo rozhodnuto o poskytnutí uživateli jistý stupeň flexibility. Tato flexibilita ovšem nemohla být pouze v programovém vybavení v hostitelském osobním počítači, ale bylo nutné určitou flexibilitu zabudovat i do vlastního

firmwaru sondy. Ta spočívá v nastavení (spoluvytvoření) firmwaru před zahájením vlastního monitorování. Po nahrání firmwaru do akceleračních karet a zahájení monitorování není již možné firmware měnit.

Pro uživatele je především důležité definovat:

- jaké položky z hlaviček paketů budou zpracovávány (podoba UH hlavičky)
- a které z nich budou klíčové pro tvorbu jednotlivých toků
- jak bude vypadat vlastní záznam o jednotlivých tocích (jaké bude obsahovat položky)
- jak bude docházet k aktualizaci záznamů o tocích

Tyto vlasnosti není možné nastavovat bez zásahu do firmware sondy. Bylo vytvořeno xml schéma [11, 12], které umožňuje uživateli zcela tyto vlastnosti monitorování popsat a definovat. Na základě tohoto xml souboru je následně třeba pomocí programového vybavení vytvořit konfigurační soubor pro jednotku HFE (popis UH hlavičky), nastavit HashGenerator jednotku (klíčové položky) a vytvořit odpovídající FPU jednotku (záznam o toku, aktualizace toků atp.). Nyní je nutné celý firmware FlowMon sondy provést procesem syntézy pomocí komerčních syntezačních nástrojů a tím z něj vytvořit binární soubory nahratelné do programovatelných polí akceleračních karet. Následně musí být celý firmware inicializován a nastaven prostřednictvím programového vybavení hostitelského počítače. Sonda začne monitorovat síť na základě datových toků a to přesně podle požadavků uživatele. Během činnosti může uživatel měnit vlastnosti sondy (timeouty, vzorkování, export na kolektory atp.), ale pokud chce změnit vlastní monitorovací proces, tak je nutné jej opět definovat prostřednictvím xml konfiguračního souboru, na základě něj vytvořit popis části firmwaru, přeložit firmware a ten nahrát do akcelerační karty.

Kapitola 4

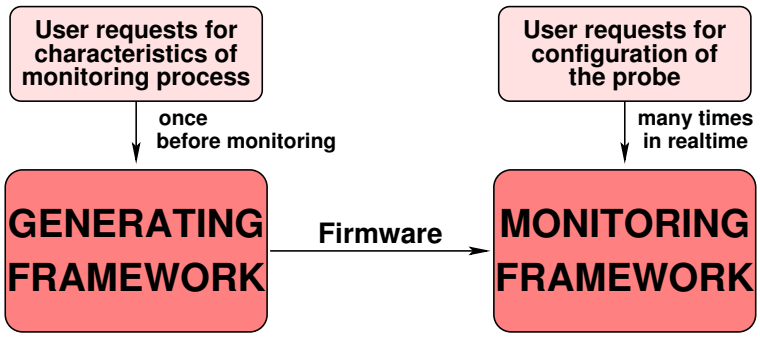
Návrh programového vybavení pro Flexibilní FlowMon sondu

Z rozboru pevné části Flexibilní FlowMon sondy a jejích požadavků na programové vybavení hostitelského počítače je zřejmé, že navazující programovou část je možné rozdělit do dvou logických částí:

- přípravná (popisná, generační) část
- monitorovací část

Přípravnou částí se rozumí činnosti nutné před vlastním prvním spuštěním Flexibilní FlowMon sondy. Zahrnuje specifikaci požadavků na monitorovací proces uživatelem, což znamená především určení toho, jaké položky z paketů se mají sledovat a jak s nimi pracovat. Následně je na základě této specifikace třeba vytvořit (vygenerovat) firmware odpovídající požadavkům uživatele. Tuto činnost je nutné provést pouze jedinkrát při určování požadavků na monitorování a následně až v okamžiku, kdy dojde k jejich změně. V případě, že uživatel nechce přesně specifikovat činnost sondy, tak může použít některý z firmwarů již vytvořených a poskytovaných tvůrci sondy.

Monitorovací část obsahuje nahrání vygenerovaného firmware do akceleračních karet, jeho inicializaci, nastavení a vlastní monitorování sítě. Tato činnost probíhá neustále, a proto je třeba, aby poskytovala co nejpříjemnější uživatelské rozhraní.



Obrázek 4.1: Rozdělení na přípravnou a monitorovací činnost

4.1 Přípravná část

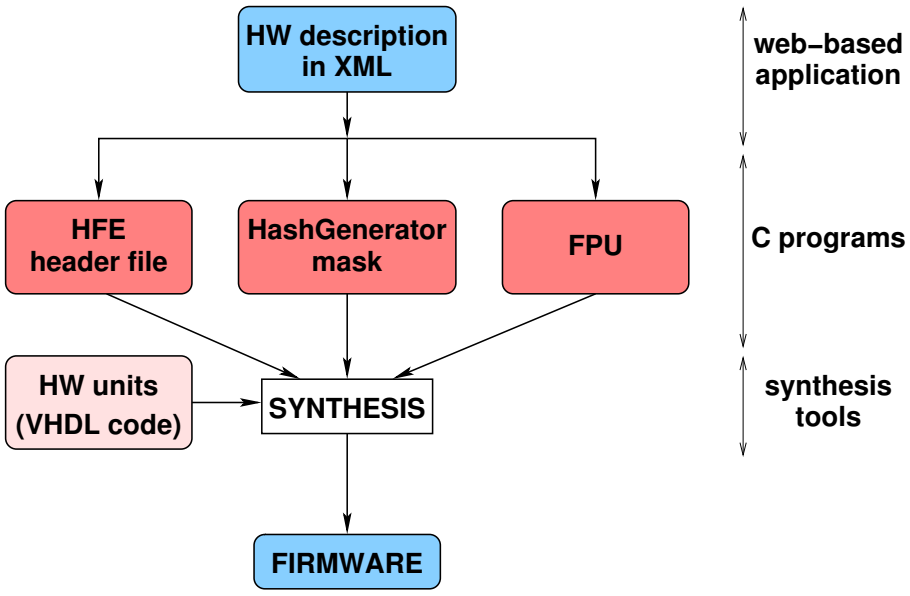
Tato část bude tvořena sadou nástrojů pro popis monitorovacího procesu a syntézu firmwaru. Vlastním popisem procesu se rozumí zapsání požadavků uživatele v podobě jediného xml souboru, který byl pro tuto úlohu navržen (viz [11, 12]). Tento soubor bude zpracován a na základě něj bude programově:

- vytvořen hlavičkový soubor pro jednotku HFE procesor
- vytvořena maska pro výpočet hash v HashGenerator jednotce
- vygenerována FlowProcessingUnit jednotka

Vytvoření hlavičkového souboru pro jednotku HFE procesor vlastně představuje převedení informací o UH hlavičce z xml souboru do vhodného formátu a podoby hlavičkového souboru použitelného při překladu jednotky HFE, jenž je psána v jazyce Handel-C.

Vytvoření masky pro výpočet HashGenerator jednotky znamená nalezení v xml polí, která jsou označena jako klíčová, a na základě jejich pozice v záznamu o tocích vytvořit bitovou masku. Tato maska bude zapsána do souboru a bude nahrávána do HashGenerator jednotky při inicializaci sondy.

Generování FlowProcessingUnit jednotky je složitou činností, kdy se na základě popsaného monitorovacího procesu v xml souboru generuje zdrojový kód jednotky v jazyce VHDL. Tato část není předmětem této práce, ale jiné bakalářské práce na FIT VUT v Brně, proto se jí nebude detailněji věnováno.



Obrázek 4.2: Schéma přípravné části programového vybavení

Po provedení těchto operací je již možné spustit nástroje sloužící pro syntézu firmwaru celé sondy. Tyto nástroje nejsou běžně volněs dostupné a i vlastní překlad trvá řádově desítky minut. Výstupem jsou binární soubory přímo nahratelné do hradlových polí akceleračních karet.

Je vidět, že během přípravné fáze je nutné provést poměrně velké množství operací, přičemž chyba v jakékoliv z nich způsobí následnou nefunkčnost sondy. Proto je vhodné, aby všechny operace prováděla jediná aplikace, čímž se zajistí konzistence všech činností. Ale vzhledem k nutnosti používat složité překladové nástroje třetích stran je toto prakticky nemožné. Stejně tak je nemožné tvořit ručně xml soubor popisující monitorovací proces, neboť není vůbec triviální a musí být zcela korektní a konzistentní.

Jako vhodným řešením se jeví zastřešení všech těchto jednotlivých částí jediným webovým rozhraním, přičemž navíc celá tato sada nástrojů bude umístěno jen na vyhrazeném serveru tvůrců sondy. To z důvodu složitosti a dostupnosti překladových nástrojů a ne příliš častému generování firmware. Uživatel tedy nebude muset instalovat žádné nástroje a pouze prostřednictvím svého webového prohlížeče přistoupí na daný server. Zde výběrem z nabízených možností popíše monitorovací proces a zadá požadavek na vytvoření odpovídajícího firmwaru. Webová aplikace vytvoří xml soubor, který bude jinak uživateli zcela skryt, a předá jej spuštěnému programu pro tvorbu součástí zdrojových kódů jednotek firmwaru (HFE procesor, HashGenerator, FPU). Po jejich vytvoření webová aplikace spustí syntézu celého firmware. Po dokončení celé činnosti bude uživatel informován prostřednictvím elektronické pošty o úspěšném ukončení tvorby firmware a možnosti si balíček s tímto firmwarem stáhnout.

Balíček bude obsahovat binární soubory nahratelné do hradlových polí akceleračních karet, konfigurační soubor pro jednotku HashGenerator a konfigurační xml soubor.

4.2 Monitorovací část

Monitorovací část vychází z původní softwarové architektury FlowMon sondy („neflexibilní“, viz [13]). Zásadní změny sebou ovšem přináší flexibilita záznamu o tocích a také změna v rozdělení monitorovacího procesu mezi hardware a software. Tato část zahrnuje všechny činnosti následující po vytvoření a stažení balíčku s firmwarem z vyhrazeného serveru. Již zcela probíhá na straně uživatele.

Stejně jako u současné verze FlowMon sondy bude i u Flexibilní FlowMon sondy dána uživateli možnost zvolit si ze dvou základních přístupů, jak ji ovládat a konfigurovat. Prvním z nich je použití terminálového rozhraní, kdy se uživatel přímo na sondu přihlásí pomocí SSH (Secure Shell) a za pomocí skriptů a dalších nástrojů spouštěných přímo z příkazové řadky na sondě bude provádět veškeré operace s ní.

Druhým přístupem bude vzdálená konfigurace prováděná prostřednictvím webového rozhraní, která bude pro nezkušeného uživatele sondy intuitivnější a uživatelsky přívětivější. Bude ji tvořit:

- webové konfigurační rozhraním na vzdáleném webovém serveru
- konfiguračním démon na sondě
- systém NETCONF

4.2.1 Webové konfigurační rozhraní

Webové konfigurační rozhraní představuje aplikaci tvořenou v jazyce PHP, která využívá služeb serveru apache a slouží uživateli pro zadávání jeho požadavků na konfiguraci sondy. Webové rozhraní bude uživateli umožňovat komfortní a snadnou editaci konfiguračního souboru krok za krokem. Z jediného rozhraní bude možné nastavovat libovolný počet sond.

Po zadání požadavku na realizaci změn provedených v konfiguračním souboru, bude soubor odeslán prostřednictvím systému NETCONF na sondu, aby mohly být vyžadované změny provedeny, což zajistí konfigurační démon. Konfigurační démon informuje webový frontend opět prostřednictvím systému NETCONF o výsledku přenastavení sondy, o němž bude následně vyrozuměn i uživatel. Webové rozhraní také bude prezentovat stavové informace ze sondy získané vzájemnou komunikací s konfiguračním démonem.

Uživatel bude moci pracovat přes webové rozhraní se dvěma ruznými konfiguracemi (konfiguračními soubory) sondy - tzv. running a startup - a vždy si nejprve vybere, s kterou z nich chce právě pracovat. Jejich rozdíl spočívá v tom, že změny v running konfiguraci se provádí okamžitě, zatímco změny ve startup konfiguraci se provedou až po restartu sondy. Tento princip je použit proto, aby uživatel mohl nejprve ozkoušet korektní funkčnost nové konfigurace sondy, a proto bude pracovat s konfigurací running. V případě, že vlivem provedených změn dojde k problémům na sondě, tak bude možnost se velmi snadno vrátit k předchozí konfiguraci pouhým restartem sondy. Ověřená a funkční running konfigurace bude moci být uložena jako startup a tedy bude následně používána jako základní.

Podobné webové rozhraní je již používáno pro současnou verzi FlowMon sondy, avšak aby bylo použitelné i pro Flexiblní FlowMon sondu, tak v něm bude nutné provést určité změny. Odlišnosti budou spočívat především ve změnách v množině nastavitelných parametrů sondy a návratových stavových hodnot ze sondy, ale také v možnosti prostřednictím webového rozhraní instalovat nový a vybírat z nainstalovaných firmwarů na sondě.

Jak již bylo zmíněno, tak flexibilita sondy je realizována mimo jiné i použitím různých firmwarů v akceleračních kartách. Proto je nutné, aby webové rozhraní umožňovalo i instalaci a výběr firmwarů použitých na sondě. Součástí konfigurovatelných vlastností sondy bude tedy i výběr jednoho z nainstalovaných firmwarů na sondě. Výběr této možnosti způsobí nahrání nového firmwaru do programovatelných polí akceleračních karet, čímž dojde ke změně v monitorovacím procesu. Webové rozhraní bude umožňovat i přímo instalaci balíčku na sondu, kdy uživatel zadá cestu k balíčku, který se má na sondu nainstalovat. Prostřednictvím systému NETCONF dojde k nakopírování a instalaci balíčku na sondě a následně bude tento firmware již nabízen i k výběru na webovém rozhraní.

4.2.2 Konfigurační démon

Na sondě bude spuštěn jako programový démon konfigurační program, jenž bude provádět vlastní konfiguraci sondy na základě údajů v konfiguračních souborech. Také bude získávat stavové informace ze sondy. Konfigurace sondy spočívá v těchto akcích:

- nahrání binárních souborů firmware do akceleračních karet
- inicializace firmware
  - nahrání masky do HashGenerator jednotky
  - inicializace hodnoty pro výpočet hash v HashGenerator jednotce
  - další činnosti spojené s inicializací jednotlivých jednotek i celé sondy
- nastavení aktivního a neaktivního timeoutu
- nastavení vzorkování paketů na vstupu
- nastavení exportu dat o tocích

  - IP adresa a port kolektoru
  - verze NetFlow protokolu
  - atd.
- atd.

Získávané a prezentované stavové informace ze sondy jsou:

- počet přijatých paketů
- počet chybných paketů
- počet navzorkovaných paketů
- stav linky
- atd.

Programový démon bude přistupovat na akcelerační karty, provádět konfiguraci a získávat stavové informace prostřednictvím knihovny (viz Kapitola 4.2.4), která bude pro tuto úlohu vytvořena.

Konfigurační démon po svém spuštění načte startup konfigurační soubor a podle údajů z něj začne provádět nastavení sondy. Nahraje vybraný firmware do akceleračních karet, provede jeho inicializaci a následně i nastaví žádoucí vlastnosti sondy. Spustí také exportovací program s parametry odpovídající hodnotám v konfiguračním souboru. Démon zkopíruje startup konfigurační soubor a vytvoří z něj running konfigurační soubor. Nyní již sonda začíná monitorovat síť.

Konfigurační démon čeká na požadavky na přenastavení sondy, které mu budou od uživatele doručovány prostřednictvím komunikace se systémem NETCONF, který je spouštěn webovým rozhraním.

4.2.3 Systém NETCONF

Komunikace mezi konfiguračním démonem a webovým rozhraním bude tvořena systémem NETCONF, což je implementace komunikačního protokolu NETCONF vytvořená v rámci projektu Liberouter (viz [8]).

Protokol NETCONF je určen pro konfiguraci síťových zařízení. Poskytuje jednoduchý mechanismus, pomocí kterého lze provádět nejrůznější změny konfigurace určitého zařízení. Jde nejen o nastavení různých parametrů daného zařízení nebo získání konkrétních konfiguračních či stavových informací, ale hlavně o komplexní změny v konfiguracích síťových zařízení. Protokol NETCONF je postaven na formátu xml. Hierarchické uspořádání dat v xml protokol využívá pro vytváření RPC (Remote Procedure Call) zpráv s popisem požadovaných funkcí. Komunikace v rámci protokolu NETCONF má podobu klasické aplikace klient-server. Klientem je zařízení vznášející požadavky a serverem je konfigurované zařízení. NETCONF je postaven nad protokolem SSH (Secure Shell). [8]

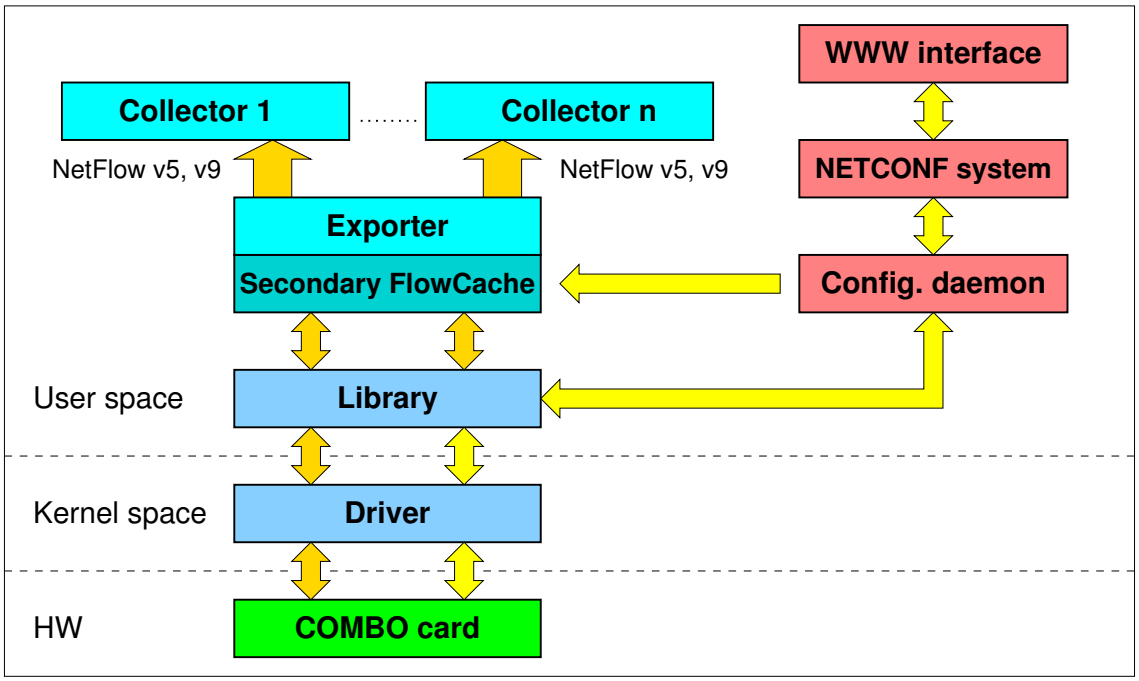
Při zadání požadavku uživatele na provedení změn na sondě spustí webový frontend NETCONF klienta a předá mu konfigurační soubor obsahující dané změny. NETCONF klient se připojí na svůj server na Flexibilní FlowMon sondě a přenese na ní daný konfigurační soubor. NETCONF server předá požadavek na přenastavení sondy konfiguračnímu

démonovi prostřednictvím programové roury fifo a ten změny provede. Stejným způsobem, ale opačným směrem, odesílá démon odpověď i stavové informace ze sondy.

Protokol NETCONF umožňuje definovat rozšíření. Pro potřeby Flexibilní FlowMon sondy bude třeba implementovat rozšíření v podobě instalace balíčku firmware na sondě. Tedy instalace balíčku bude probíhat zcela v režii NETCONF systému, stejně jako nyní operace restart a vypnutí sondy.

4.2.4 Programová architektura

V přechozích sekcích byly popsány tři základní bloky monitorovací části programového vybavení sondy z pohledu jejího ovládání. Nyní bude popsáno, z jakých jednotlivých vrstev bude tvořena programová architektura přímo umístěná na sondě (Obrázek 4.3).



Obrázek 4.3: Architektura programového vybavení sondy

Přístup ke kartě bude zajišťován specialním modulem linuxového ovladače, který bude optimalizován pro tuto činnost. Vznikne úpravou stávajícího modulu ovladače pro FlowMon sondu. Hlavní změnou z pohledu ovladače bude uzpůsobení přenosu různě velkých (variabilních) záznamů o tocích z akcelerační karty do osobního počítače podle použitého firmware.

Na modul ovladače bude přímo navazovat knihovna, která bude poskytovat funkce pro vyčítání záznamu o tocích z firmwaru sondy, ale také bude sloužit pro vyčítání všech stavových informací a pro nastavování vlastností sondy. Tato knihovna využije sadu již existujících funkcí, jež jsou používány pro přístup do adresového prostoru akceleračních karet na projektu Liberouter. Konfigurační démon i exportovací program sloužící pro zasílání dat na kolektory budou přistupovat na akcelerační karty právě prostřednictvím této knihovny.

Konfigurační démon při inicializaci a nastavování sondy spouští také exportovací program. V předchozích verzích FlowMon sondy sloužil tento program pouze pro vyčítání dat

o tocích z karty, jejich zabalení do zvolené verze NetFlow protokolu a odeslání na jediný kolektor. V případě, že bylo žádáno zasílat data na více kolektorů, potom muselo být spuštěno více exportovacích programů a každý vyčítal záznamy o tocích a zasílal je na jediný kolektor (pozn.: modul ovladače byl uzpůsoben tak, aby bylo možné vyčítat z karty stejná data několika aplikacemi současně). Ovšem pro Flexibilní FlowMon sondu bylo z objektivních důvodů (viz Kapitola 3.1) rozhodnuto o rozdělení monitorovacího procesu mezi hardware a software, tedy vlastně o vytvoření sekundární cache pro záznamy o tocích (sekundární flowcache) v software (primární flowcache je ve firmwaru). Není vhodné, aby každý z kolektorů samostatně tuto sekundární flowcache tvořil a ani aby byla jediná sekundární flowcache sdílena více programy, protože to výrazně komplikuje její implementaci. Proto nová verze exportovacího programu bude podporovat zasílání dat na více kolektorů zároveň, tedy nebude nutné ani možné spustit více instancí exportovacího programu. Navíc bude exportovací program obsahovat nový programový modul, který bude zajišťovat funkci sekundární flowcache.

Exportovací program také bude modifikován s ohledem na variabilitu záznamu o tocích. Po svém spuštění nejprve zjistí z xml souboru, ze kterého byl vytvořen používaný firmware, obsah a pozici jednotlivých položek v záznamu o tocích a až od tohoto okamžiku bude schopen s těmito daty korektně pracovat. Modul zajišťující sekundární FlowCache bude z xml soubor navíc vyčítat i informace týkající se agregace dat na základě datových toků, aby mohl v této agregaci korektně pokračovat.

4.2.5 Sekundární FlowCache

Sekudární flowcache v softwaru bude výraznou změnou v monitorovacím procesu sondy. Celková velikost flowcache je při monitorování na vysokorychlostních sítích jedním z nejdůležitějších parametrů sondy a neboť není možné a efektivní neustále tuto cache rozšiřovat ve firmwaru, tak bude podpořena v softwaru. Do sekundární flowcache budou přicházet již předagregované záznamy o tocích, které musely být již z flowcache firmwaru expirovány, neboť:

- došlo k uplatnění aktivního či neaktivního timeout
- došlo ke kolizi dvou toků při ukládání v primární flowcache ve firmwaru
- primární flowcache ve firmwaru je již plná

V sekundární flowcache bude rozhodnuto o jejich další agregaci s odpovídajícími toky. Agregace již dále nebude probíhat v případě, že k expiraci došlo z důvodu uplatnění aktivního či neaktivního timeoutu a záznam o toku bude zařazen k exportu na kolektory. V opačném případě dojde k zařazení záznamu o toku do sekundární flowcache. Se zařazenými záznamy o tocích se bude pracovat principielně zcela stejně jako ve flowcache ve firmware a i jejich expirace bude probíhat na základě stejných timeoutů, přičemž časové hodnoty toků se budou z firmwaru i sekundární flowcache sčítat.

Tímto způsobem dojde k výraznému posunutí limitu monitorování velkého množství toků na vysokých rychlostech.

Kapitola 5

Závěr

Cílem této práce bylo navrhnout architekturu programového vybavení monitorovací sondy na bázi toků - Flexibilní FlowMon sondy, což je zařízení monitorující vysokorychlostní sítě na základě datových toků a vzniká v rámci projektu Liberouter. Tohoto cílu bylo dosaženo.

Nejprve bylo nutné seznámit se s problematikou monitorování počítačových sítí na bázi toků. Nastudovat používané technologie a také protokoly NetFlow verze 5 a NetFlow verze 9 s variabilním záznamem. Tato problematika je popsána a rozebrána v první části této práce.

Následující část práce představuje hardwarovou architekturu monitorovací sondy Flexibilní FlowMon a požadavky kladené na její ovládání a konfiguraci. Právě na základě hardwarové architektury a požadavků byla navržena architektura programového vybavení sondy, která je prezentována v závěrečné části této práce. Při návrhu bylo dbáno na modularitu celého systému a také na návaznost na již existující nástroje.

Nyní bude následovat proces implementace navrženého systému a jeho propojení s již existujícími částmi.

Literatura

[1] CASE, J.; FEDOR, M.; SCHOFFSTAL, M.: *Simple Network Management Protocol (SNMP)*. RFC 1157 (1990) [online], [cit. 2007-12-20].
URL http://www.faqs.org/rfcs/rfc1157.html

[2] Cisco systems, Inc.: *Webové stránky společnosti Cisco*.
URL http://www.cisco.org

[3] Cisco systems, Inc.: *NetFlow Export Datagram Format*. 1992-2002, [online], poslední aktualizace 16.4.2002, [cit. 2007-12-20].
URL http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/nfc/nfc_3_0/nfc_ug/nfcform.htm

[4] Cisco systems, Inc.: *Cisco IOS NetFlow Version 9 Flow-Record Format*. 1999-2004, [online], [cit. 2007-12-20].
URL http://www.cisco.com/en/US/products/ps6601/products_white_paper09186a00800a3db9.shtml

[5] Cisco systems, Inc.: *Introduction to Cisco IOS NetFlow Overview*. 1999-2005, [online], poslední aktualizace únor 2006, [cit. 2007s-12-20].
URL http://www.cisco.com/en/US/products/ps6601/products_white_paper0900aecd80406232.shtml

[6] Claise, B.: *RFC 3954 - Cisco Systems NetFlow Services Export Version 9*. 2004, [online], poslední aktualizace listopad 2004, [cit. 2007-12-20].
URL http://rfc.net/rfc3954.txt

[7] KOŠŇÁR, T.: Notes to Flow-Based Traffic Analysis System Design. Technická zpráva, CESNET, prosinec 2004, [online], poslední aktualizace 7.12.2004, [cit. 2007-12-20].
URL http://www.cesnet.cz/doc/techzpravy/2004/ftas-design/

[8] KREJČÍ, R.: *Konfigurace síťových zařízení protokolem NETCONF*. bakalářská práce, FI MUNI, 2007.

[9] Liberouter: Webové stránky projektu Liberouter.
URL http://www.liberouter.org

[10] ŠPRINGL, P.: *Návrh a implementace programového vybavení pro ovládání a konfiguraci sondy NetFlow*. bakalářská práce, FIT VUT v Brně, 2006.

[11] ŽÁDNÍK, M.: *Design of Flow Monitoring Probe*. diplomová práce, FIT VUT v Brně, 2007.

[12] ŽÁDNÍK, M.; ŠPRINGL, P.; ČELEDA, P.: Flexible FlowMon. Technická zpráva, CESNET, prosinec 2007.

[13] ŽÁDNÍK, M.; ČELEDA, P.; etc.: FlowMon Probe. Technická zpráva, CESNET, prosinec 2006.
URL http://www.cesnet.cz/doc/techzpravy/2006/flowmon-probe/