

# Pasivní monitorování zátěže linky

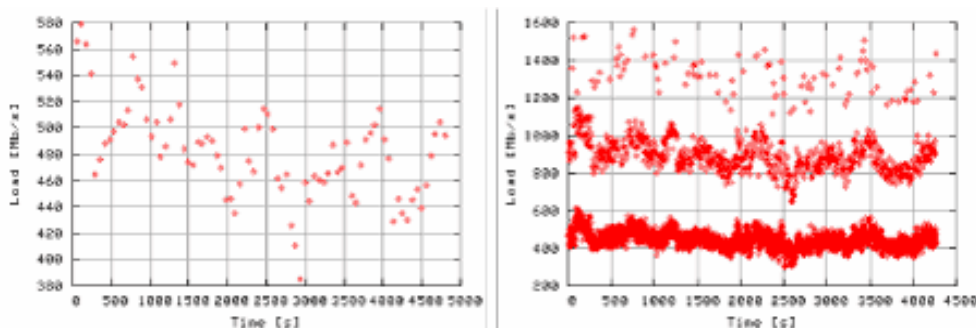
Sven Ubik (CESNET), Arne Oslebo (UNINETT), Demetres Antoniadis (ICS-FORTH)  
Olomouc, 29.-30. května 2007

## Úvod

Monitorování zátěže linky je užitečné při ladění výkonostních problémů a při plánování infrastruktury sítě. Tradiční metodou je čtení čítačů přenesených bajtů na rozhraních směrovačů protokolem SNMP. Tímto způsobem ale můžeme získat pouze relativně dlouhodobou průměrnou zátěž bez informace o její struktuře.

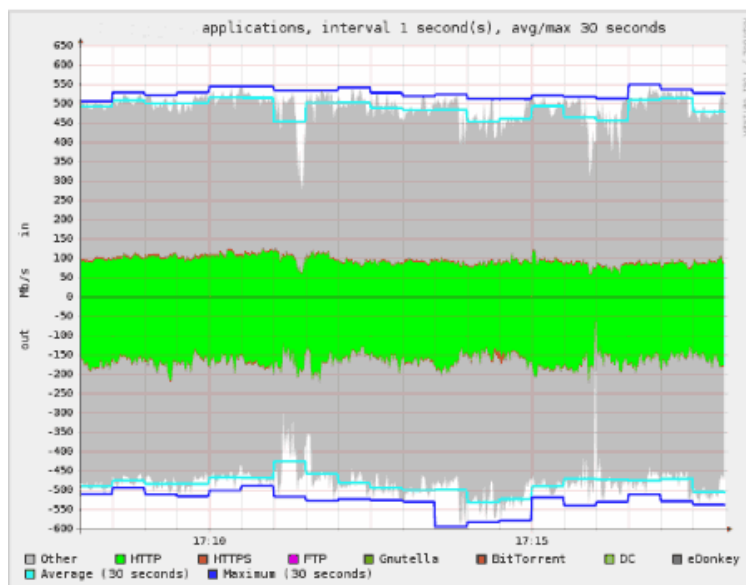
Tento příspěvek popisuje aplikaci ABW pro pasivní monitorování zátěže linky, které umožňuje detekovat krátkodobé špičky zátěže a poskytuje informaci o rozložení zátěže mezi protokoly a aplikace včetně aplikací používajících dynamicky přidělované porty.

Směrovače aktualizují svoje čítače v rámci úlohy, která obvykle nemá nejvyšší prioritu a dochází k nepravidelnému zpoždění několika sekund mezi přenesenými pakety a jejich započtením v čítačích v MIB databázi. Nejkratší interval pro který můžeme spolehlivě určit průměrnou zátěž linky pomocí čítačů v MIB databázi je asi 30 sekund. Při častějším čtení získáme zkreslené výsledky. Například obrázek 1 znázorňuje vlevo 60-sekundové průměry zátěže a vpravo výsledek čtení čítačů každou sekundu, který obsahuje mnoho interferencí mezi čtením čítačů a jejich aktualizací.



Obr. 1: Vzorke čítače přenesených bajtů v MIB databázi čtené každých 60 sekund (vlevo) a každou sekundu (vpravo).

Netflow záznamy mohou být použity pro zjištění podílu zátěže pro jednotlivé protokoly odpovídající TCP a UDP portům. V současné době je ale velká část provozu v Internetu přenášena protokoly, které používají dynamické porty, jejichž identifikace vyžaduje kombinaci hlavičkové klasifikace a hledání řetězců v tělech paketů. Obrázek 2 znázorňuje typické rozložení provozu dle protokolů na páteřní lince sítě CESNET určené pouze podle čísel portů. Šedá oblast znázorňuje část provozu, kterou není možné na základě čísel portů klasifikovat.



Obr. 2: Klasifikace protokolů podle čísel portů

Hlavní výhody aplikace ABW pro pasivní monitorování zátěže linky jsou následující:

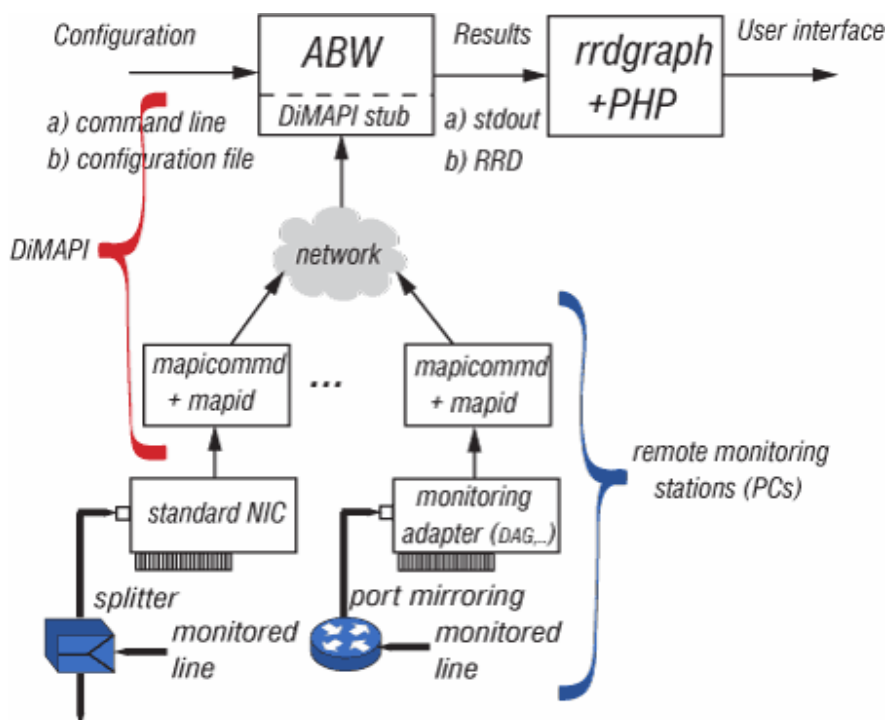
- Určení zátěže linky v různých časových měřících včetně detekce krátkodobých špiček
- Klasifikace nejvýznamnějších protokolů využívajících dynamické porty

### 3 Architektura

Aplikace ABW využívá middleware DiMAPI (Distributed Monitoring Application Interface) a knihovnu trackflib pro detekci protokolů. Aplikace je napsaná v jazyce C a používá sadu skriptů v jazyce PHP a nástroj rrdtool pro uživatelské rozhraní.

Struktura aplikace je znázorněna na obrázku 3. Pakety jsou z monitorované linky odbočeny pomocí optického rozbočovače nebo pomocí monitorovacího portu na přepínači nebo směrovači. Pakety jsou následně odchyceny síťovou kartou, což může být běžná karta typu Ethernet nebo specializovaná monitorovací karta typu DAG nebo COMBO. Výhodou monitorovacích karet je jejich schopnost zachytit veškerý provoz až do plné rychlosti linky a počítač vybrané statistiky přímo v hardware kartě. Pakety jsou dále zpracovány v DiMAPI, které je rozděleno mezi démony mapid a mapicommd běžící na počítači se síťovými kartami a knihovnu, která je přilinkována k aplikaci, která může běžet na jiném centrálním počítači.

Vlastní aplikace ABW monitoruje vybraný provoz podle zadání v konfiguračním souboru a ukládá výsledné statistiky do RRD databáze. Skripty uživatelského rozhraní získávají statistiky z databáze a prezentují je formou grafů ve webovském prohlížeči podle požadavků uživatele.



Obr. 3: Architektura aplikace ABW

DiMAPI je sada knihoven pro tvorbu monitorovacích aplikací na vysoké úrovni abstrakce. Aplikace si nejprve otevře jeden nebo více *flow*. Každý *flow* je zpočátku tvořen všemi pakety přicházejícími na jednu nebo více zadaných síťových karet (v případě více karet se tento *flow* nazývá *scope*).

Aplikace následně nasadí na každý *flow* jednu nebo více monitorovacích funkcí. Výběr a pořadí těchto monitorovacích funkcí určují výslednou funkčnost aplikace. Jsou k dispozici funkce pro hlavičkovou filtraci (BPF\_FILTER), prohledávání paketů (STR\_SEARCH), počítání paketů (PKT\_COUNTER) a další. Programátor může definovat svoje vlastní monitorovací funkce.

DiMAPI automaticky využije hardwarovou podporu vybraných typů monitorovacích adaptérů DAG nebo COMBO a použije softwarovou implementaci v případě běžných síťových karet nebo pokud není možné hardwarovou podporu pro určité monitorovací funkce použít vzhledem k jejich počtu a pořadí. Pro aplikace je toto zcela transparentní.

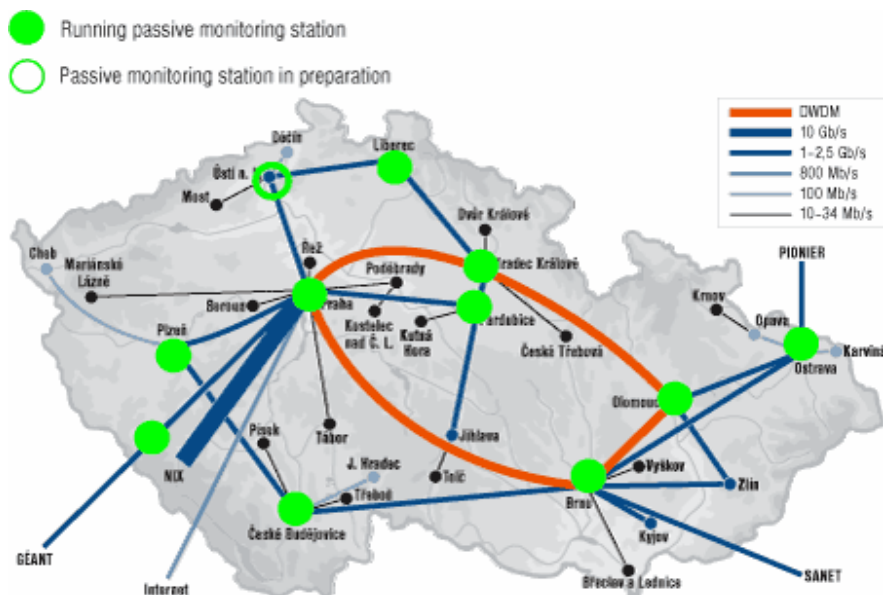
Knihovna tracklib pro detekci protokolů je součástí DiMAPI. Používá se aplikací funkce TRACK na jednotlivé *flow*. Vzorky dat potřebné pro detekci protokolů se obvykle nachází blízko začátku paketu, pro spolehlivou detekci protokolů proto postačí odchyťovat a prohledávat pouze určitý prefix paketů. Detekované protokoly jsou shrnuty v tabulce 1. FTP zahrnuje i pasivní FTP a WEB zahrnuje přenosy protokolem HTTP, což nemusí být shodné se spojeními na portech 80 a 443, které jsou někdy využívány jinými protokoly.

Gnutella DC++  
BitTorrent WEB  
eDonkey FTP  
Skype IP-in-IP

Tabulka 1: Protokoly detekované knihovnou trackflib

## 4 Nasazení v síti CESNET

V síti CESNET je aplikace ABW nasazena na 10 monitorovacích stanicích v hlavních uzlech sítě a na jedné stanici pro monitorování linky do sítě GN2, viz obrázek 4. Aplikace trvale běží a ukládá výsledky do RRD databáze.



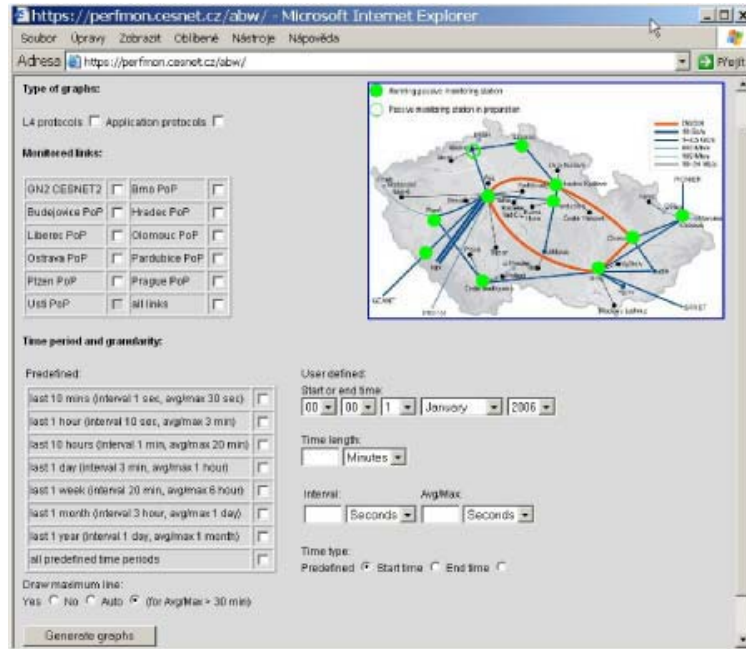
Obr. 4: Nasazení aplikace ABW v síti CESNET

Stanice pro monitorování linky do sítě GN2 je vybavená kartami DAG (10 Gb/s DAG6.2 a 1 Gb/s DAG4.3GE). Ostatní stanice jsou vybaveny běžnými síťovými kartami. Připravujeme stanici pro monitorování nejzatíženější linky Praha - Brno, která bude vybavená kartami 10 Gb/s DAG8.2X. Všechny stanice používají operační systém Linux. Výsledky monitorování jsou k dispozici na adrese <https://perfmon.cesnet.cz>.

## 5 Příklad použití

Uživatelské rozhraní aplikace je znázorněno na obrázku 5. Uživatel si může vybrat dva typy grafů - rozložení L4 protokolů (který rovněž indikuje přítomnost IPv6 a multicastu) nebo aplikačních protokolů. Uživatel si dále vybere jednu nebo více monitorovaných linek a jedno nebo více časových období a časových granularit, pro které budou získány výsledky z databáze a prezentovány. Dále je možné zvolit určité parametry zobrazení, například zda má být zobrazena

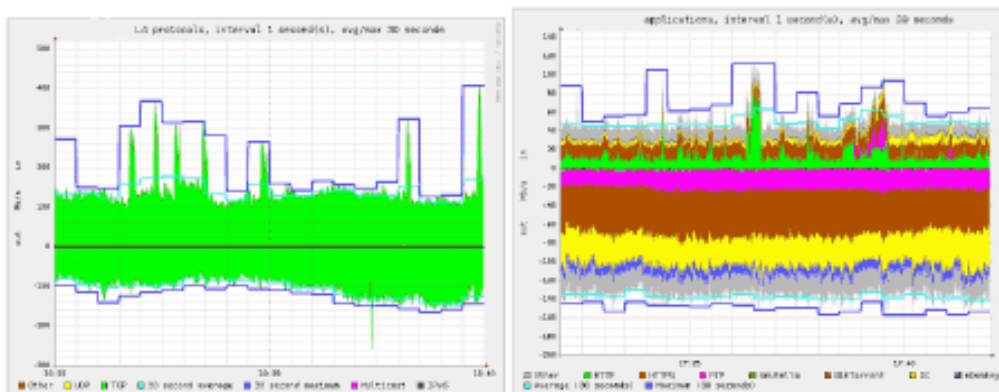
obalová křivka maximálních hodnot, která u grafů pro delší časová období může snížit čitelnost zobrazených hodnot, které jsou hluboko pod maximální hodnotou.



Obr. 5: Uživatelské rozhraní aplikace ABW

Příklad grafu rozložení L4 protokolů je v levé části obrázku 6. Zelená barva znázorňuje protokol TCP, který je ve většině případů převládajícím transportním protokolem. Tmavě modrou čarou je znázorněna obalová křivka maximálních hodnot v tomto případě pro 30-sekundové úseky. Hlavní graf znázorňuje průběh zátěže pro 1-sekundové úseky. Můžeme vidět, že linka obsahuje řadu krátkých a vysokých špiček zátěže, které nemohou být detekovány v 30-sekundových průměrech.

Příklad grafu rozložení aplikačních protokolů je v pravé části obrázku 6. Můžeme vidět, že byla detekována řada protokolů používajících dynamické porty.



Obr. 6: Rozložení L4 protokolů (vlevo) a aplikačních protokolů (vpravo)

## **6 Závěr**

Vytvořili jsme aplikaci pro pasivní neintruzivní trvalé monitorování zátěže síťové linky v širokém rozmezí časových intervalů, včetně detekce krátkodobých špiček a s detekcí rozložení protokolů včetně nejvýznamnějších protokolů používajících dynamické porty. Aplikace automaticky využívá hardwarové podpory vybraných monitorovacích adaptérů, pokud jsou použity. V další práci se chceme věnovat kvantifikaci dynamiky síťového provozu v subsekundové oblasti.

## **7 Poděkování**

Vývoj aplikace ABW byl podpořen aktivitou JRA1 projektu GN2. Vývoj DiMAPI včetně knihovny trackflib byl podpořen projektem IST FP6 LOBSTER (Contract No. 004336).