Report z testování prototypu 100Gb/s sondy pro zákonné odposlechy

Testovací report

Roman Vrána, Lukáš Kekely, Martin Žádník

Technická dokumentace FIT-TR-2015-1

Report z testování prototypu 100Gb/s sondy pro zákonné odposlechy

Roman Vrána, Lukáš Kekely, Martin Žádník

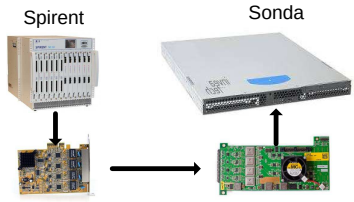
Fakulta informačních technologií
Vysoké učení technické v Brně
Božetěchova 1/2, 612 66 Brno
{xvrana20, ikekely, izadnik}@fit.vutbr.cz

Abstrakt Testovací report shrnuje výsledky testování vysokorychlostní sondy pro zákonné odposlechy určené pro rychlosti linek 100 Gb/s.

1 Testovací prostředí, zapojení a konfigurace

Testování proběhlo v srpnu 2015 v laboratoři Q301 Fakulta informačních technologií Vysokého učení technického v Brně, Božetěchova 2, 612 00 Brno, Česká republika.

Cílem testů bylo určit propustnost (tj. rychlost zpracování paketů) měřena v počtech bytů za sekundu. Rychlost zpracování byla měřena na základě ztrátovosti paketů sondou v několika základních konfiguracích a případech použití. Testy vycházejí z RFC 2544 Benchmarking methodology a RFC 1242 Benchmarking Terminology. Pro účely testování bylo využito zařízení pro generování paketů na plné rychlosti linky, Spirent TestCenter N11U (dále jen Spirent). Spirent byl osazen kartou HYPERMETRICS FX 100G CFP 1-PORT. Přes tuto kartu byl generován provoz do testované sondy. Spirent byl napřímo propojen se sondou (konkrétně se vstupním portem karty Combo 100G) optickým kabelem, vizte obrázek 1.



Obrázek 1. Propojení Spirent a sondy.

Sonda se skládá z hardwarové a softwarové části. Hardwarová část se sestává z hardwarově akcelerované karty s dedikovaným firmwarem. Firmware realizuje

záměrné zahození nezájmového provozu, díky čemuž není nutné tento provoz přenášet do hostitelského počítače. Softwarová část sondy se sestává z jednotlivých procesů. Nejdůležitějším procesem je proces filterd, který běží ve více vláknech (počet vláken odpovídá počtu jader v serveru) a realizuje zahození nezájmových paketů v software a komunikaci s procesem, který zajišťuje vkládání filtračních pravidel do karty. Koncept softwarově definovaného měření je popsán v publikaci [1]. Mezi další důležité procesy se řadí irid, který realizuje tzv. TCP reassembling a zpracování aplikačních protokolů.

2 Výsledky

Výsledky byly získány na základě odečtů čítačů zachycených a zahozených paketů v sondě. Zároveň byly tyto výsledky porovnány s počtem odeslaných paketů ze zařízení Spirent, aby byla vyloučena ztráta paketů před příchodem do sondy.

2.1 Propustnost hardware

Propustnost hardware vyjadřuje propustnost, kterou sonda dosáhne po dosažení stabilizovaného stavu. Stabilizovaný stav je takový, kdy objem provozu zasílaný z karty do software je nižší než propustnost software. Například, v okamžiku, kdy je sonda vložena do linky, je veškerý síťový provoz zpracováván v software a postupně jsou do hardware vkládána pravidla, která nezájmový provoz zahodí již v kartě. Měření doby než se sonda dostane do stabilního stavu je uvedeno v sekci 2.2.

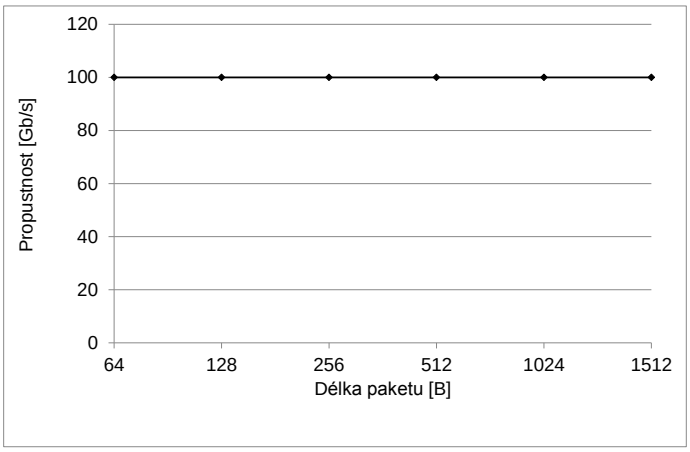
Propustnost byla měřena pro délky paketů 64 B, 128 B, 256 B, 512 B, 1024 B a 1512 B. Spirent generoval pakety na plné rychlosti linky, tj. 100 Gb/s. Každé měření probíhalo 30 s. Celkem proběhlo 10 měření. Propustnost sondy byla spočítána na základě počtu přijatých paketů, tj. paketů, které nebyly zahozeny.

Na obrázku 2 lze vidět, že na všech paketových délkách dosahuje sonda ve stabilizovaném stavu propustnosti 100 Gb/s bez ztráty paketu.

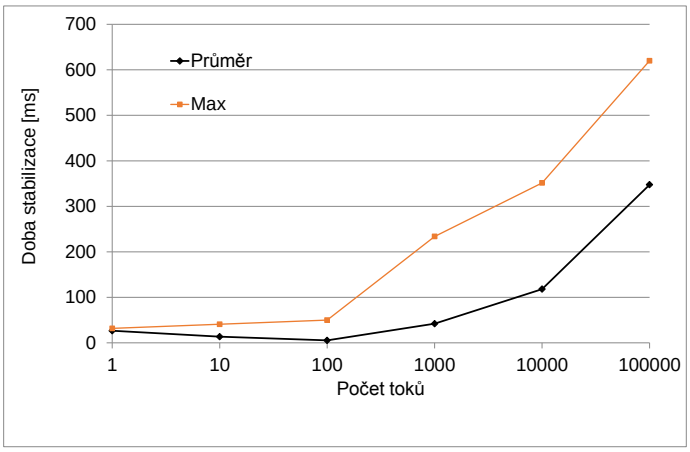
2.2 Doba stabilizace

Doba stabilizace udává za jakou dobu se sonda dostane do stabilizovaného stavu. Tato doba náběhu závisi především na složení síťového provozu, především na počtu toků. Z tohoto důvodu byla doba stabilizace měřena pro síťový provoz, který postupně obsahoval 1, 10, 100, 1000, 10000, 100000 toků. Síťový provoz byl generován na plné rychlosti linky 100 Gb/s a délkou paketů 128 B. Celkem bylo provedeno deset měření.

První měření doby stabilizace probíhalo tak, že veškeré procesy na sondě byly spuštěny před zahájením testu. Následně byl generován provoz do sondy. Výsledky doby stabilizace lze vidět v grafu na obrázku 3. V grafu je zobrazen průměr z deseti provedených měření i maximum, tedy nejdelší změřená doba stabilizace. V grafu můžeme pozorovat, že délka stabilizace roste úměrně s počtem



Obrázek 2. Propustnost sondy po době náběhu.

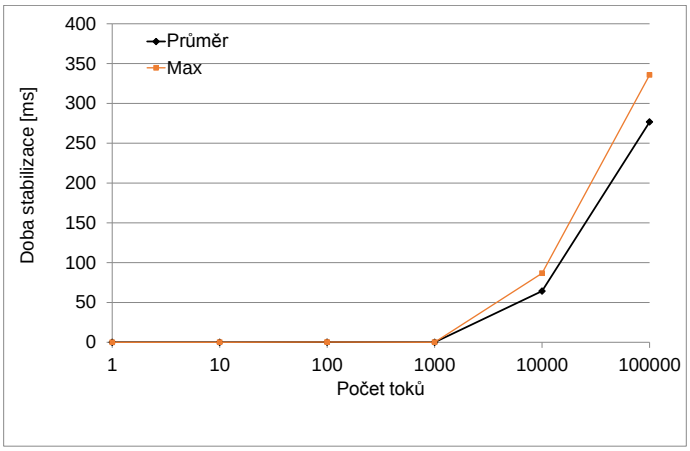


Obrázek 3. Doba stabilizace plně připravené sondy.

toků (x-ová osa grafu je v logaritmickém měřítku). Doba stabilizace i v případě provozu obsahující 100 000 toků trvá přibližně 350 ms a je tedy velmi rychlá.

Doba stabilizace se liší dle stavu sondy. Pokud na sondě nejsou spuštěny příslušné procesy a tyto se spouští až po vložení do linky, pak je doba stabilizace

delší. Graf na obrázku 3 zobrazuje právě dobu stabilizace v případě, že procesy se spouští až s příchodem prvního paketu. I přes delší dobu stabilizace přibližně 750 ms je tato doba dostatečně krátká pro nasazení sondy do reálné sítě.



Obrázek 4. Propustnost sondy po době náběhu.

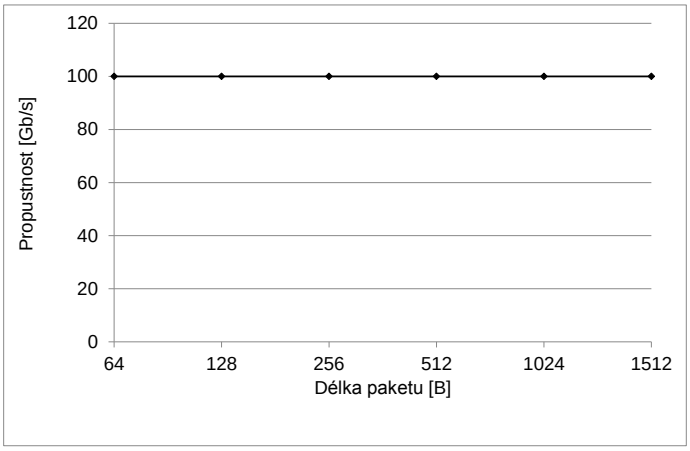
2.3 Propustnost software

Propustnost software vyjadřuje propustnost, kterou sonda dosáhne bez hardwarové podpory karty. Tedy v případech, kdy karta propouští veškerý provoz do software, například během stabilizace. Propustnost byla měřena pro délky paketů 64 B, 128 B, 256 B, 512 B, 1024 B a 1512 B. Spirent generoval pakety na plné rychlosti linky, tj. 100 Gb/s. Každé měření probíhalo 30 s. Celkem proběhlo 10 měření. Propustnost sondy byla spočítána na základě počtu přijatých paketů, tj. paketů, které nebyly zahozeny.

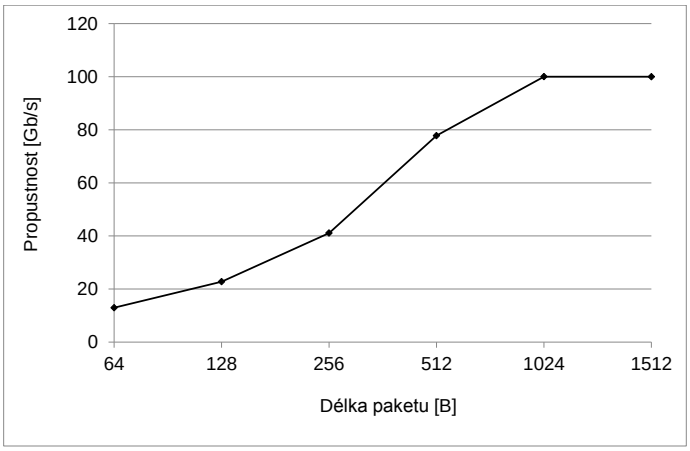
Propustnost je ovlivněna především komplexností zpracování paketu. V případě, že je provoz přenášen pouze do operační paměti hostitelského počítače, pak je propusnost plných 100 Gb/s (vizte obrázek 5).

V případě, že je nutné pakety zpracovávat, například extrahovat IP adresy a rozhodnout o zahození či zachycení paketu, řízení filtrace v kartě apod., pak propustnost čistě softwarového řešení klesá s komplexností zpracování.

Propustnost software v případě, že sonda pracuje pouze do úrovně L4, tedy filtruje pouze na základě síťové a transportní vrstvy, je zobrazena na v grafu na obrázku 6.



Obrázek 5. Propustnost při přenosu paketů do paměti hostitelského počítače.

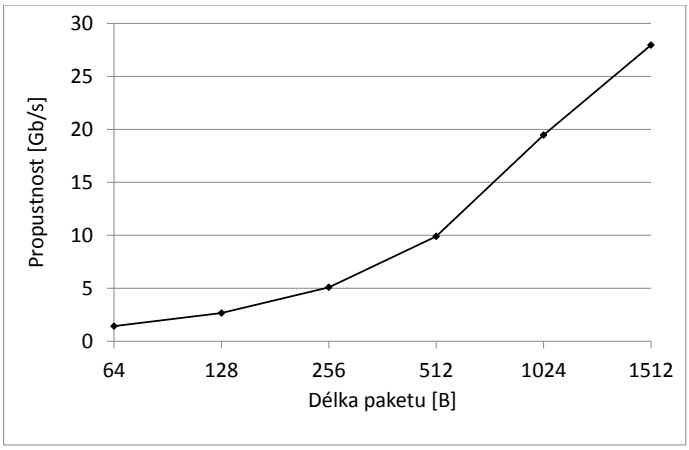


Obrázek 6. Propustnost software filtrující do úrovně L4.

Graf na obrázku 6 ukazuje, že na nejvyšších paketových délkách dosahuje sonda plné propustnosti i při L4 zpracování. Naopak na nejkratší délce paketů (64 B) dosahuje sonda propustnosti pouze 13 Gb/s, což odpovídá přibližně 20 mil. paketům za vteřinu. Důležitá je rovněž hodnota propustnosti pro průměrnou

velikost paketů v síti. Dle studie [2] je průměrná délka paketů na Internetu přibližně 570 B. V takovém případě sonda dosahuje propustnosti 80 Gb/s i bez hardwarové podpory.

Propustnost software v případě, že sonda pracuje až úroveň L7, tedy filtruje na základě síťové, transportní a aplikační vrstvy, je zobrazena na v grafu na obrázku 7. L7 zpracování v sobě zahrnuje proces TCP reasemblingu, tedy poskládání datové proudu a dále extrakci aplikačních identifikátorů z aplikační vrstvy a jejich odeslání přes rozhraní INI2. Ve vyhodnocované verzi bylo aktivováno zpracování protokolu SIP (Session Initiation Protocol).



Obrázek 7. Propustnost software zpracovávající protokol SIP.

V grafu na obrázku 7 lze vidět, že propustnost zpracování nedosahuje plné propustnosti linky ani na nejdelších paketech. Na nejkratších paketových délkách dosahuje propustnost přibližně 1 Gb/s

3 Závěr

Výsledky testování prototypu 100Gb/s sondy pro zákonné odposlechy ukazují, že sonda dosahuje propustnost 100 Gb/s. Testy dále ukazují rychlosti zpracování softwarové části, která bez asistence karty je schopna dosáhnout plné propustnosti pouze pro L4 zpracování nejdelších paketů. Pokud je zapnuta filtrace nezájmového provozu na kartě, pak po době stabilizace, která je velmi krátká (pod 1 s), dochází k dosažení rovnovážného stavu, kdy většina provozu je zahozena na kartě jako nezájmový provoz a malá část je zpracovávána v software, kde již postačuje nižší propustnost.

Reference

1. Kekely, L.; Pus, V.; Korenek, J.: Software Defined Monitoring of Application Protocols. In *Proceedings of IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, IEEE Computer Society, 2014, ISBN 978-1-4799-3360-0, s. 1725–1733.
   URL `http://www.fit.vutbr.cz/research/view_pub.php?id=10657`
2. Lan, K.; Heidemann, J.: A measurement study of correlations of Internet flow characteristics. *Computer Networks*, ročník 50, č. 1, 2006: s. 46 – 62, ISSN 1389-1286, doi:DOI:10.1016/j.comnet.2005.02.008.
   URL `http://www.sciencedirect.com/science/article/B6VRG-4G7X5D3-2/2/68cc7a078b8a785cb729980fe4155d79`