Analýza DNS provozu ve vysokorychlostních sítích

Internet a Technologie (18)

Jan Dražil

Vysoké učení technické v Brně, Fakulta informačních technologií
Božetěchova 1/2, 612 66 Brno
idrazil@fit.vutbr.cz

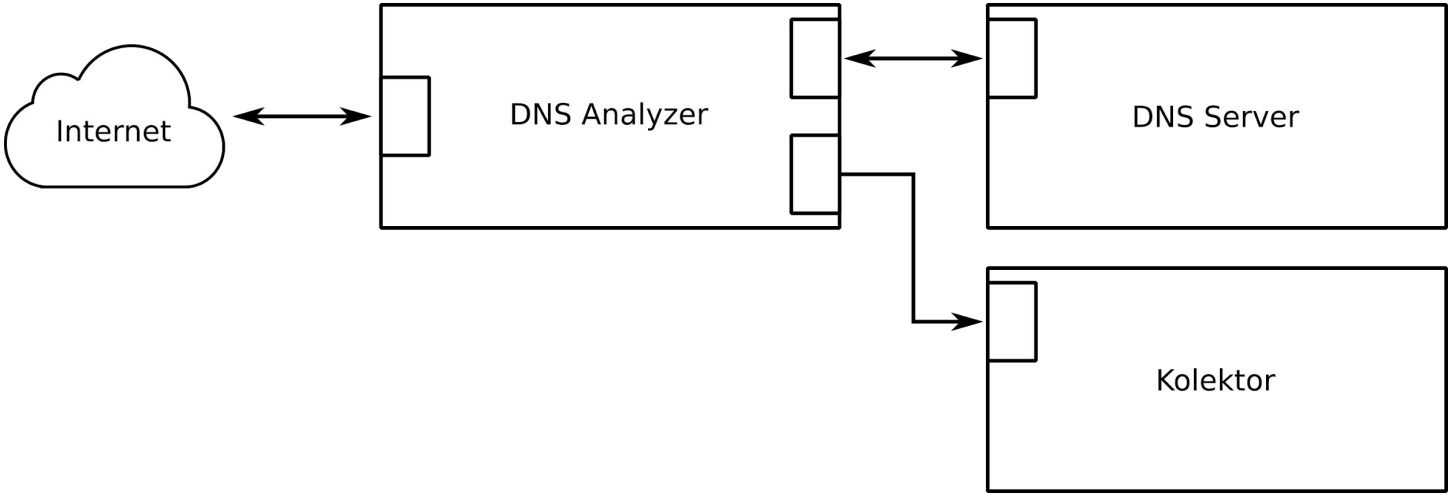
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

CZ.NIC | SPRÁVCE DOMÉNY CZ

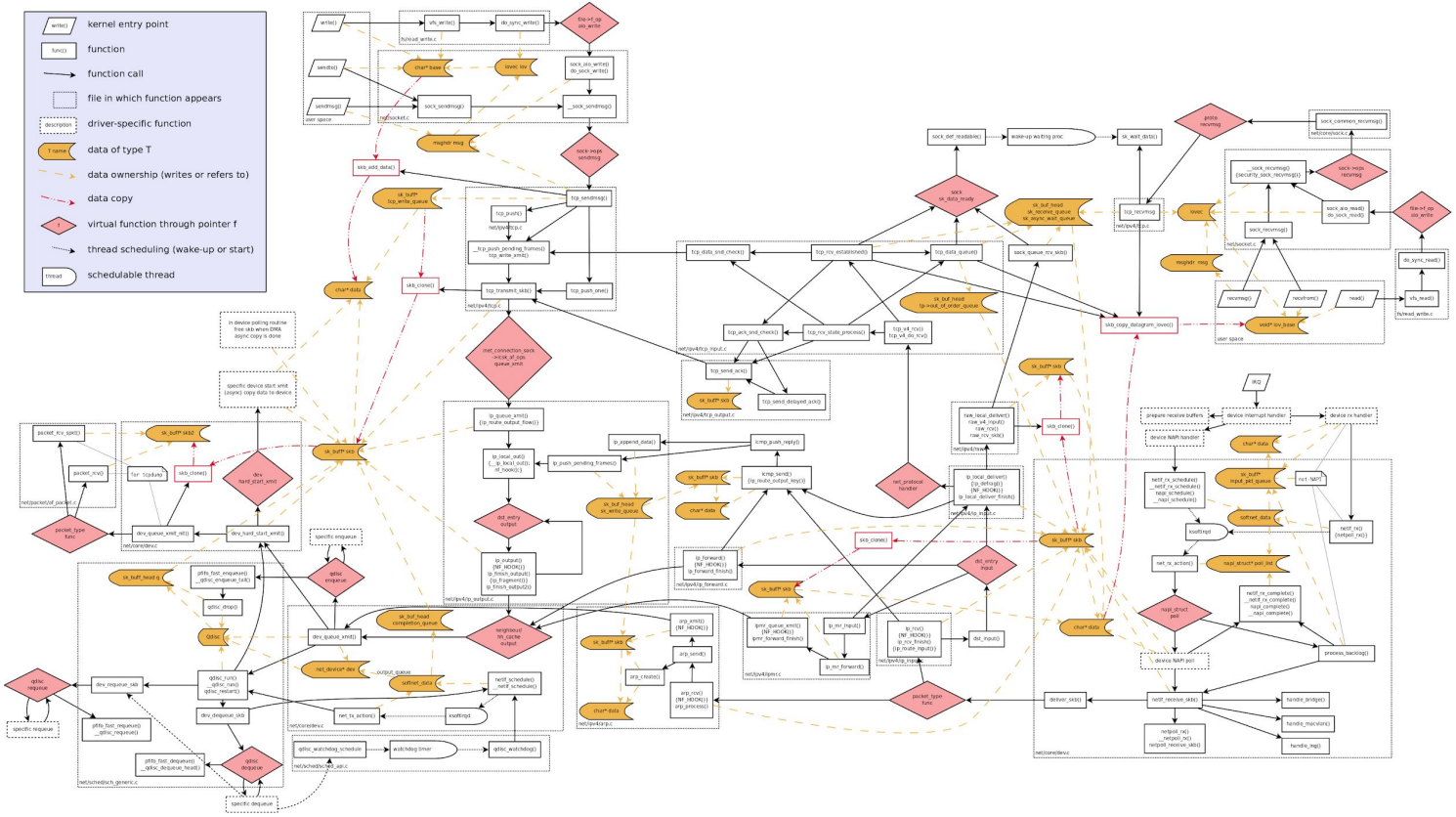
Cíle

- Sonda pro statistickou analýzu DNS provozu
  - Analýza při plné zátěži linky (včetně DDoS)
  - Záchyt s přesnými timestampy
  - Párování dotazů s odpověďmi
  - Forwarding
  - Možnost změny konfigurace za běhu
  - Vhodný výstupní formát
    - Parquet
  - Export nevalidních/neočekávaných paketů
- Nasadit HW akcelerátor do sítě CZ.NIC

Koncept nasazení



Dosáhnutí plné propustnosti

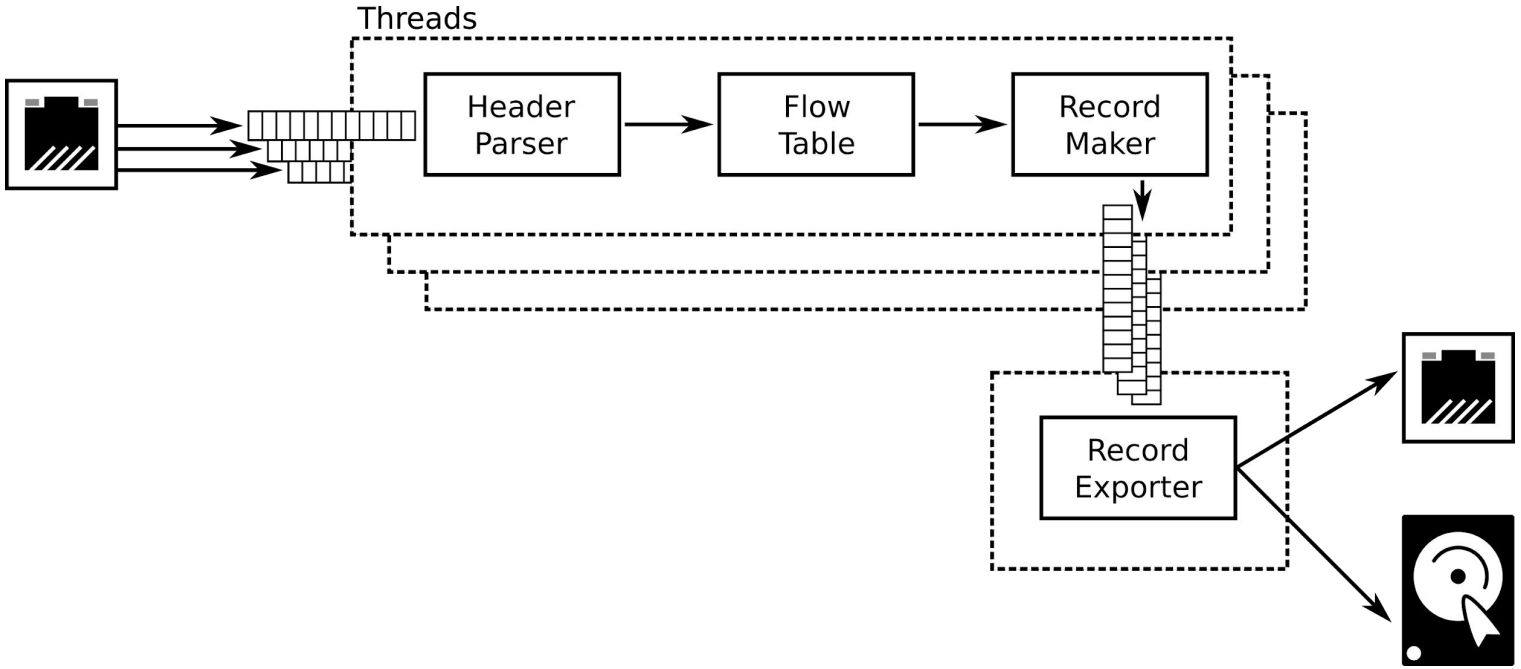


Zdroj: https://wiki.openwrt.org/doc/networking/praxis

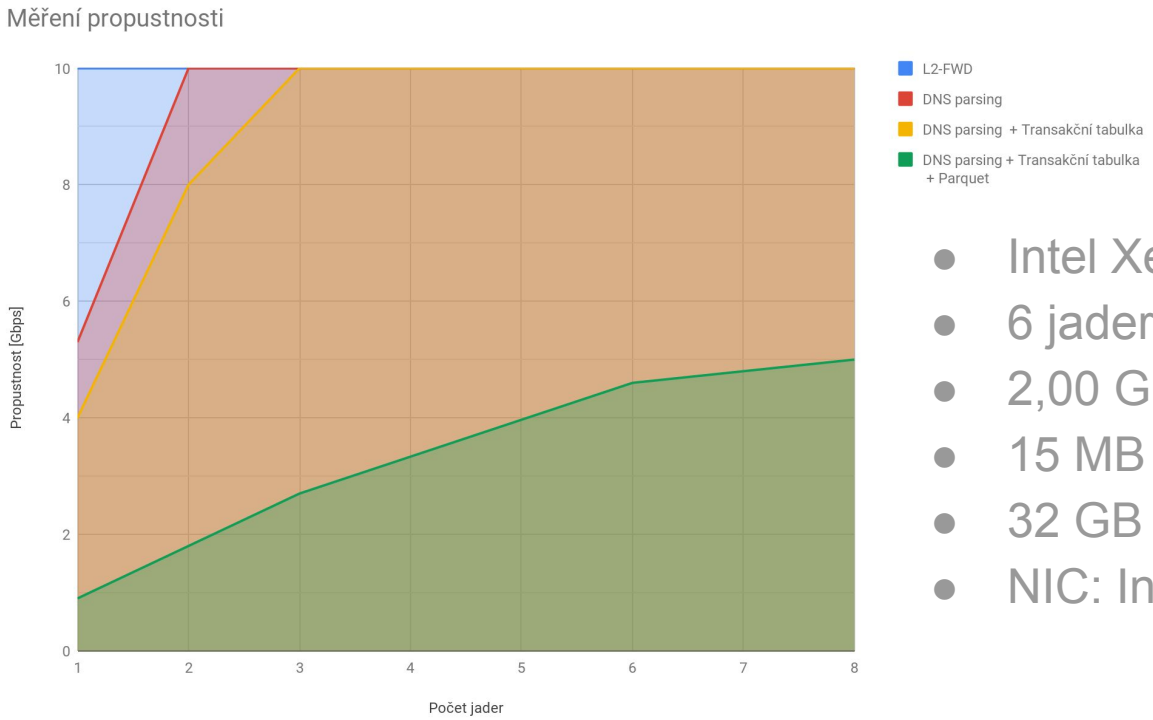
Postup implementace

- Fáze I
  - Vytvořit kompletní softwarovou aplikaci
  - Jednodušší přístup komunity
  - Umožní identifikovat komponenty potřebné pro HW
  - Příprava testů
- Fáze II
  - Přenést SW aplikaci na HW platformu

Softwarová architektura

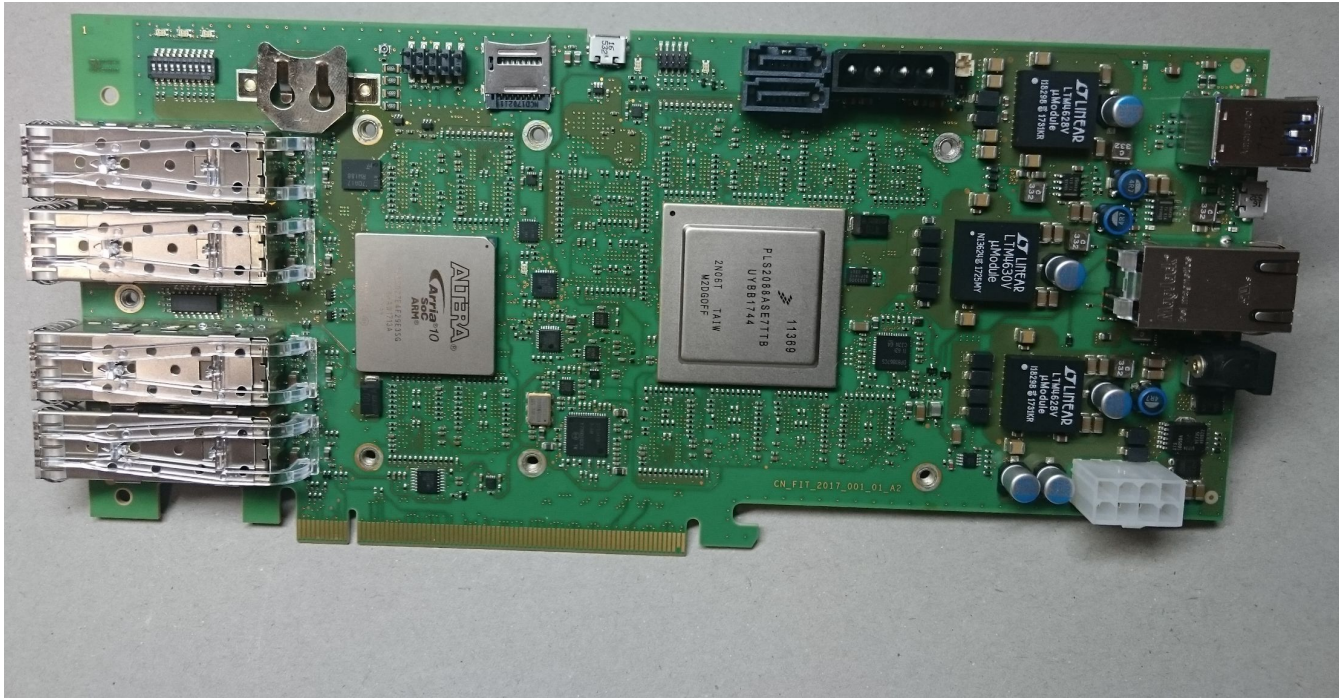


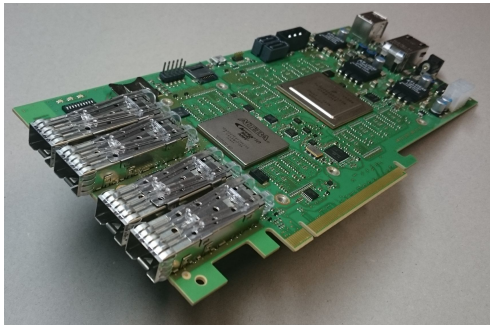
Výkonnostní měření SW



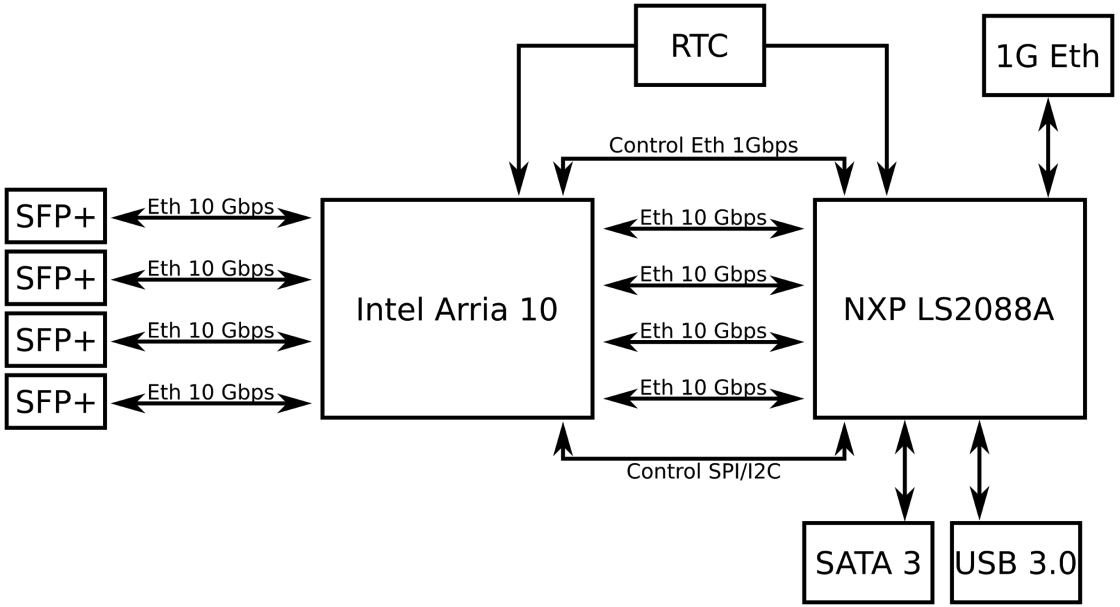
- Intel Xeon E5-2620
- 6 jader (12 vláken)
- 2,00 GHz
- 15 MB cache
- 32 GB RAM
- NIC: Intel X520-SR2

Hardwarová platforma



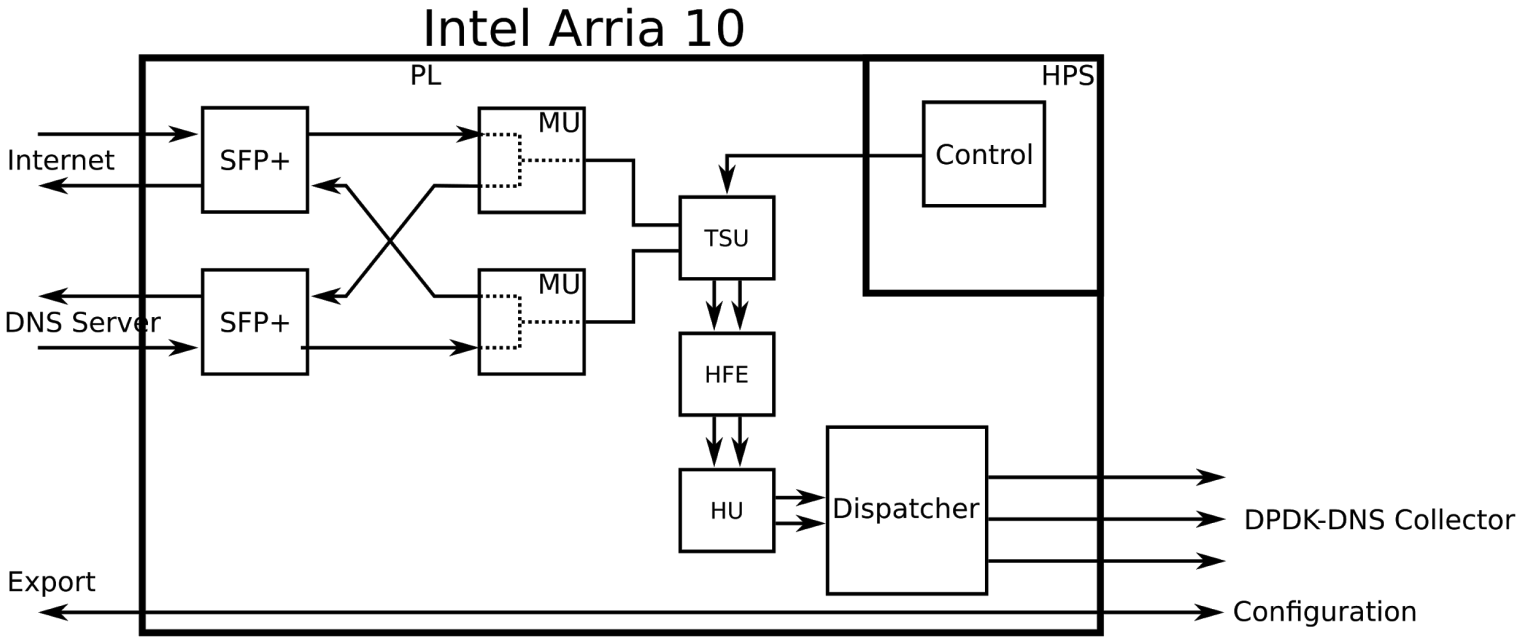


Hardwarová platforma



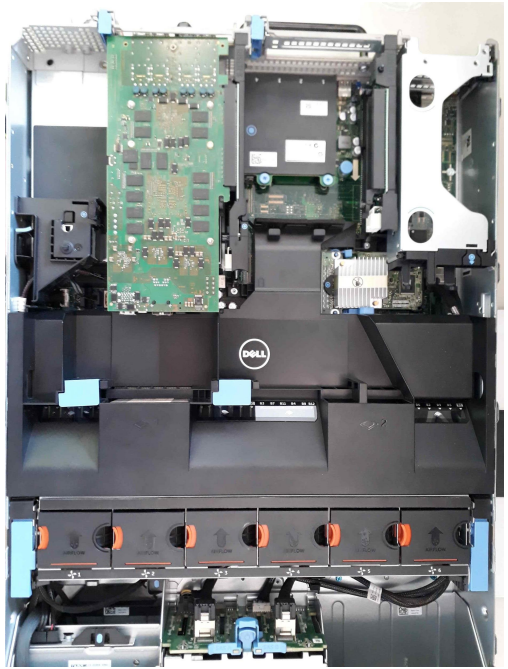
Hardwarová platforma

- NXP LS2088A
  - 8x ARM A-72
  - 80 Gbps switch
  - Akcelerační moduly - komprimace, PM, šifrování, AIO procesory
- Intel Arria 10
  - FPGA
  - Masivně paralelní architektura
  - Vhodné pro signálové zpracování, síťové aplikace do L3, pattern matching


Intel Arria 10
PL
HPS
Internet
SFP+
MU
Control
TSU
DNS Server
SFP+
MU
HFE
HU
Dispatcher
DPDK-DNS Collector
Export
Configuration

Nasazení

Samostatné zařízení



Jako součást serveru

Další možnosti použití

- Filtrace provozu
- DNS cache
- Vzorkování při vysokém zatížení
- Prioritizace provozu