


Tomáš Čejka
cejkat@cesnet.cz

Monitorování sítě pomocí OpenWrt

LinuxDays 2016

Úvod

OpenWrt

- linuxová distribuce pro embedded zařízení (typicky WiFi routery)
- vyvíjeno komunitou
- opensource, zdarma, GPL (https://openwrt.org/)
- OpenWrt poskytuje zapisovatelný filesystem
- přizpůsobení na úrovni balíků i zdrojových kódů
- repozitář obsahuje „toolchain“ umožňující kompilaci pro různé cílové architektury/platformy
- 1147 podporovaných modelů: https://wiki.openwrt.org/toh/start

OpenWrt build system

Build system

- Obsahuje Makefile soubory a patche, které umožňují vygenerovat toolchain pro cross-kompilaci a kořenový filesystem pro embedded zařízení.

Toolchain

- překladač (GCC wikipedia)
- binutils (as, ld, ar, nm, . . . wikipedia)
- musl libc (https://en.wikipedia.org/wiki/Musl)

OpenWrt feeds

Feed

- připojení externích zdrojů
- kolekce balíků
- umístění: vzdálený server, lokální FS nebo VCS
- seznam feedů: `feeds.conf` nebo `feeds.conf.default`
- src-git, src-svn, svn-link, src-cpy, ...

```
src-git nemea https://github.com/CESNET/Nemea-OpenWRT
```

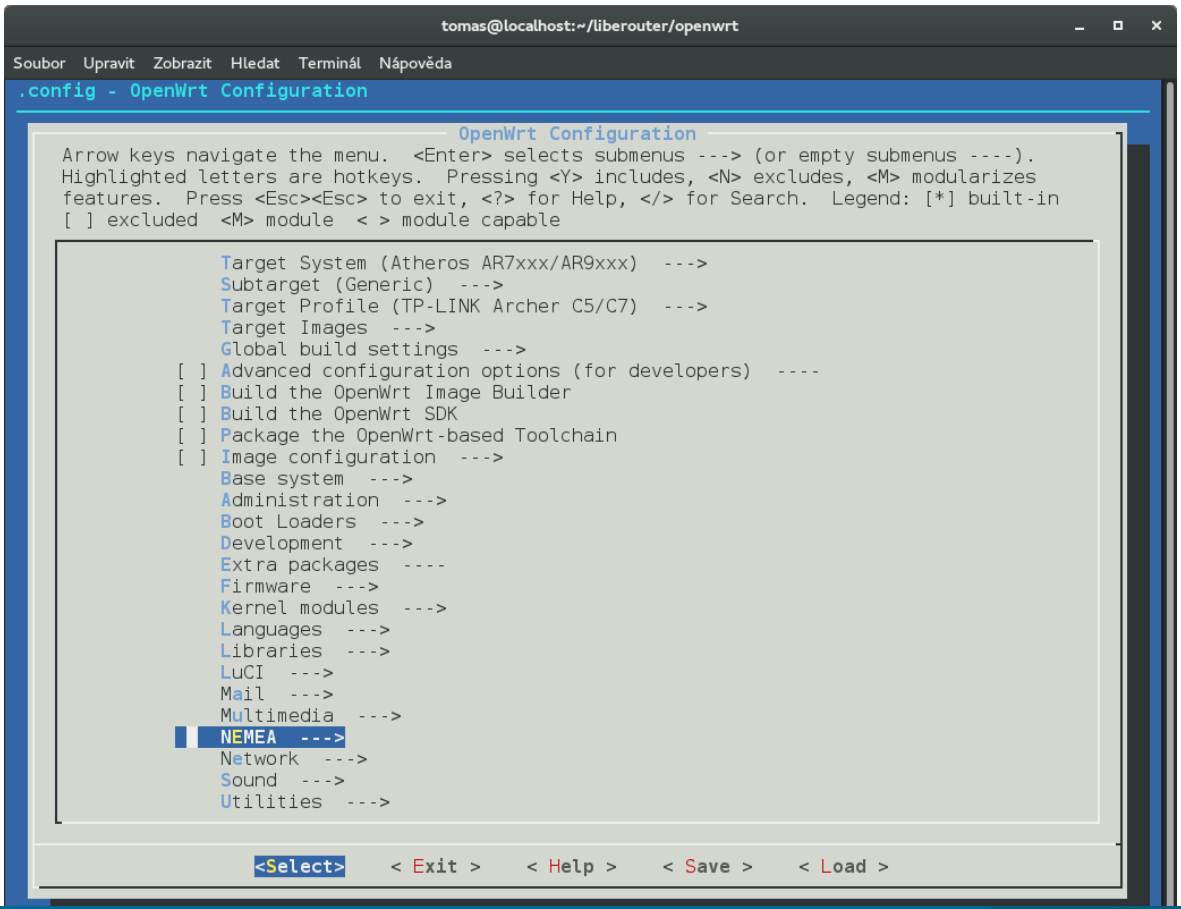
Inicializace feedů

```
scripts/feed update
scripts/feed install -a
```

Sestavení OpenWrt

Konfigurace

- „textová konfigurace“: `make config`
- „grafická konfigurace“: `make menuconfig`
  Zdroj. kódy v `scripts/config/`, binárka `mconf`, ncurses
  Spouští se: `mconf Config.in`



Kompilace

Spuštění kompilace:

```
make
```

Jak probíhá sestavení

- tools (automake, autoconf, sed, cmake)
- toolchain/binutils
- toolchain/gcc (gcc, g++, cpp)
- target/linux (kernel modules)
- package (základní balíky)
- target/linux (kernel)
- target/linux/image (firmware image file)

Monitorování

Jak můžeme sbírat data?

- čítače síť. karet: muninlite (čte z `/proc/net/dev`)
- packet-base: tcpdump (menuconfig -> Network -> tcpdump)
- flow-based:
  - iptables modul (`https://github.com/aabc/ipt-netflow/`)
  - softflowd (packages feed, Network -> softflowd, 2.10.2016: musel jsem snížit verzi na 0.9.8 a změnit md5sum v Makefile)
  - NEMEA flow_meter (viz dále)

NEMEA

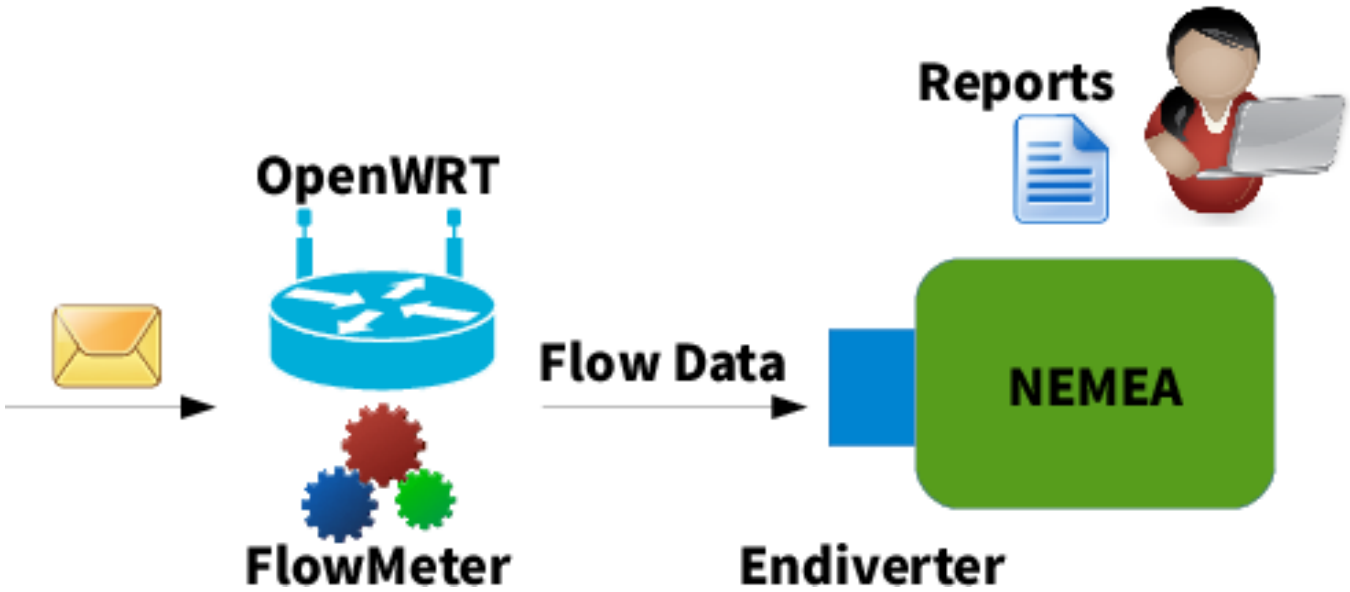
NEMEA Flow_meter

- http://nemea.liberouter.org/openwrt
- https://github.com/CESNET/NEMEA

Co umí Flow_meter?

- export flow
  (SRC/DST IPv4/IPv6, SRC/DST port, protokol, čas, bajty, pakety)
- aplikační rozšíření: DNS, HTTP, SIP, NTP (+ exper. ARP)
- online zdroj dat pro NEMEA systém (detekční moduly, . . .)
- ukládání flow do souborů (včetně rotace souborů čas/velikost)

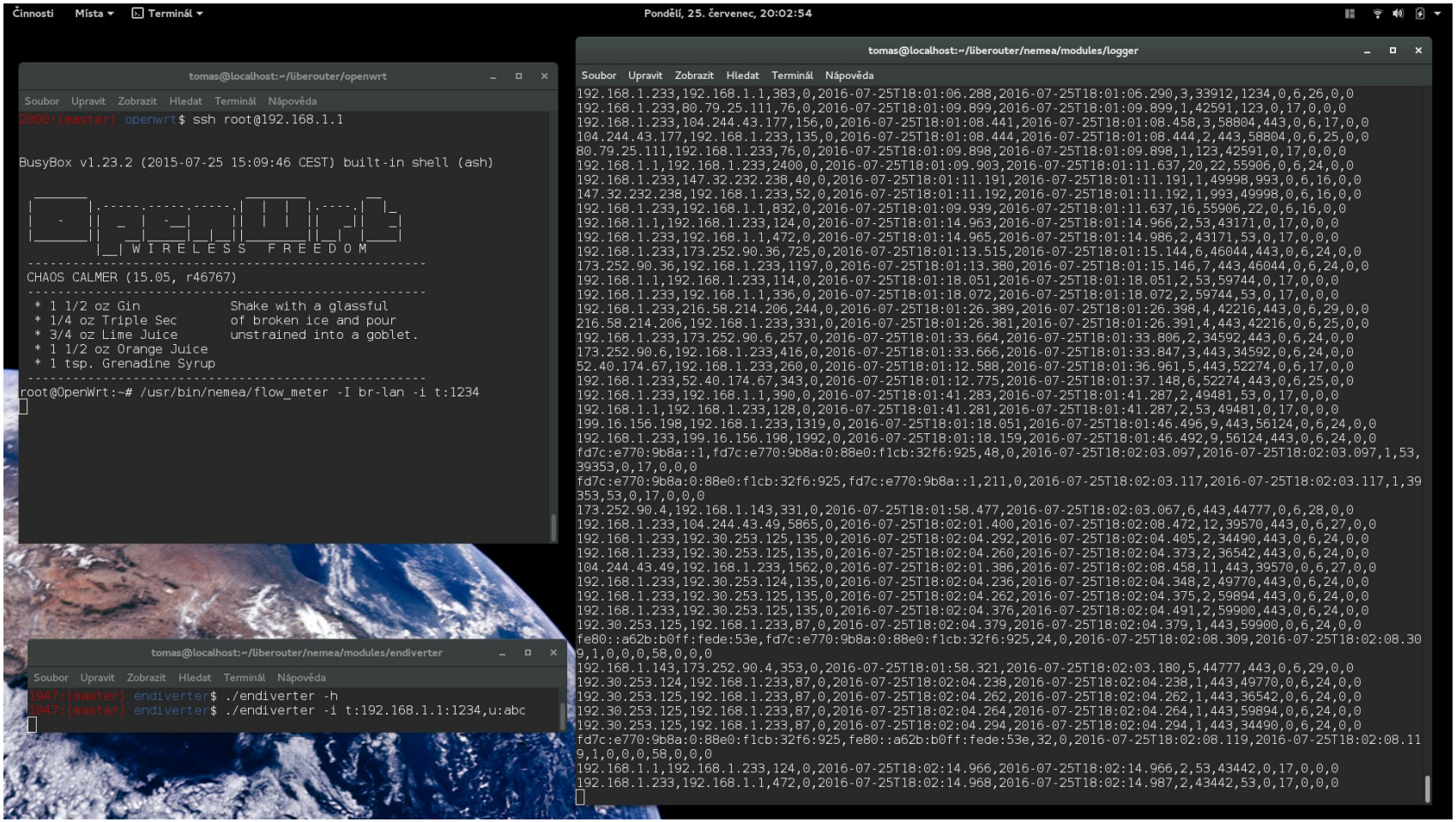
NEMEA nasazení



Konfigurace /etc/config/flow_meter

```
config profile wan
    option interface eth0
    option plugins basic,dns,http
    option ifcspec f:b:w:time=5,f:d:w:time=5,f:h:w:time=5
    option cache_size 0
    option timeouts default
    option respawn 1
    option respawn_threshold 3600
    option respawn_timeout 5
    option respawn_retry 5
    option core unlimited
    option enabled 1
```

Ukázka



Více na stánku CESNETu...

Kontakty

E-Mail: cejkat@cesnet.cz
Mailinglist: nemea@cesnet.cz
Přihlášení:
https://random.cesnet.cz/mailman/listinfo/nemea
Web: http://nemea.liberouter.org
Git: https://github.com/CESNET/NEMEA
Twitter: @tomcejka, @NEMEA_System