



**Tomáš Čejka**

cejkat@cesnet.cz

# Monitorování sítě pomocí OpenWrt

# 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 balíčků
- 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

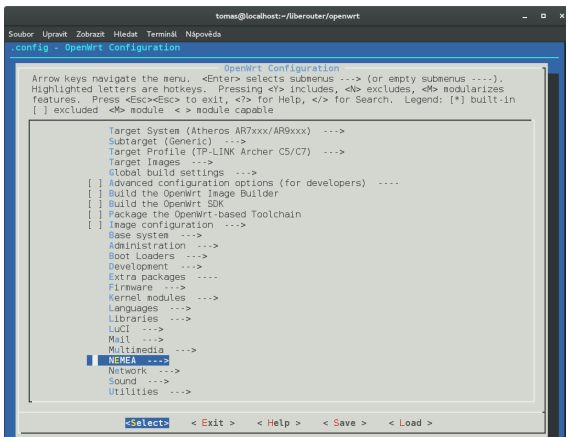
```
scripts/feed update  
scripts/feed install -a
```

# Sestavení OpenWrt

# Konfigurace

- „textová konfigurace“: `make config`
- „grafická konfigurace“: `make menuconfig`

Zdroj. kódy v `scripts/config/`, binárka `mconf`, `ncurses`  
Spouští se: `mconf Config.in`



```
tomas@localhost:~/liberouter/openwrt
Soubor Upravit Zobrazit Hledat Terminál Nápověda
.config - OpenWrt Configuration

OpenWrt Configuration
Arrow keys navigate the menu. <Enter> selects submenus --- (or empty submenus ----).
Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes, <M> modularizes
features. Press <Esc><Esc> to exit, <?> for Help, </> for Search. Legend: [*] built-in
[ ] excluded <M> module < > module capable

Target System (Atheros AR7xxx/AR9xxx) --->
Subtarget (Generic) --->
Target Profile (TP-LINK Archer C5/C7) --->
Target Images --->
Global build settings --->
[ ] Advanced configuration options (for developers) ----
[ ] Build the OpenWrt Image Builder
[ ] Build the OpenWrt SDK
[ ] Package the OpenWrt-based Toolchain
[ ] Image configuration --->
  Base system --->
  Administration --->
  Boot Loaders --->
  Development --->
  Extra packages ----
  Firmware --->
  Kernel modules --->
  Languages --->
  Libraries --->
  LuCI --->
  Mail --->
  Multimedia --->
  NEMEA --->
  Network --->
  Sound --->
  Utilities --->

<Select> < Exit > < Help > < Save > < Load >
```

# 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

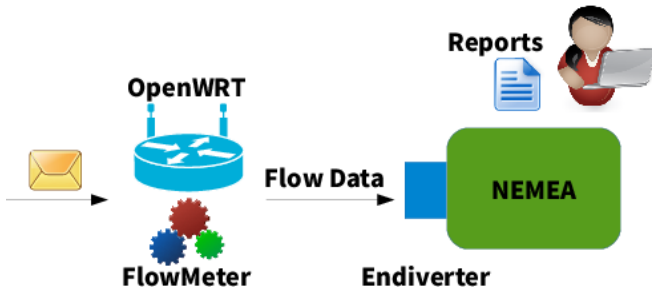
# NEMEA Flow\_meter

- <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

The screenshot displays a terminal window with several panes. The top pane shows a terminal session where the user has connected to a remote host via SSH. The middle pane shows a network flow netter visualization, which is a complex graph of nodes and edges representing network traffic. The bottom pane shows a terminal session where the user has run a command to view network flow data. The right pane shows a log file with a list of IP addresses and timestamps, likely representing network traffic logs.

```

Pondělí, 25. července, 20:02:54

tomasa@localhost:~/fiberouter/openwrt
Soubor Upravit Zobrazit Hledat Terminál Nápověda
root@openwrt:~# ssh root@192.168.1.1

BusyBox v1.23.2 (2015-07-25 15:09:46 CEST) built-in shell (ash)

-----
CHAOS CALMER (15.05, r46767)
-----
+ 1/2 oz Gin           Shakes with a glassful
+ 1/4 oz Triple Sec   of broken ice and pour
+ 3/4 oz Lime Juice   unstrained into a goblet.
+ 1/2 oz Orange Juice
+ 1 tsp. Grenadine Syrup

root@openwrt:~# /usr/bin/nemea/flow_netter -i br-lan -t 1:234

-----
tomasa@localhost:~/fiberouter/nemea/modules/flow_netter
Soubor Upravit Zobrazit Hledat Terminál Nápověda
root@flow_netter:~# /ndivterter -h
root@flow_netter:~# /ndivterter -i 1:192.168.1.1:1234,ubcc

-----
tomasa@localhost:~/fiberouter/nemea/modules/flow_netter
Soubor Upravit Zobrazit Hledat Terminál Nápověda
root@flow_netter:~# /ndivterter -h
root@flow_netter:~# /ndivterter -i 1:192.168.1.1:1234,ubcc

-----
tomasa@localhost:~/fiberouter/nemea/modules/flow_netter
Soubor Upravit Zobrazit Hledat Terminál Nápověda
192.168.1.233,192.168.1.1,363,0,2016-07-25T18:01:06.290,3,39912,1234,0,5,26,0,0
192.168.1.233,192.168.1.1,832,0,2016-07-25T18:01:09.939,2016-07-25T18:01:09.939,11,42501,123,0,17,0,0
192.168.1.233,192.168.1.1,177,156,0,2016-07-25T18:01:08.441,2016-07-25T18:01:08.441,5,58804,443,0,16,0,0
192.168.1.233,192.168.1.1,233,135,0,2016-07-25T18:01:08.444,2016-07-25T18:01:08.444,2,443,58804,0,6,25,0,0
80.79.25.111,192.168.1.233,76,0,2016-07-25T18:01:09.896,1,123,42501,0,17,0,0,0
192.168.1.1,192.168.1.1,983,2400,0,2016-07-25T18:01:08.983,2016-07-25T18:01:08.983,20,22,5596,0,6,24,0,0
192.168.1.233,147.32,232.238,46,0,2016-07-25T18:01:11.101,2016-07-25T18:01:11.101,1,49999,993,0,6,16,0,0
147.32,232.238,192.168.1.233,52,0,2016-07-25T18:01:11.102,2016-07-25T18:01:11.102,1,993,49998,0,6,16,0,0
192.168.1.233,192.168.1.1,832,0,2016-07-25T18:01:09.939,2016-07-25T18:01:11.637,16,35966,22,0,6,16,0,0
192.168.1.1,192.168.1.233,124,0,2016-07-25T18:01:14.963,2016-07-25T18:01:14.966,2,53,43711,0,17,0,0,0
192.168.1.233,192.168.1.1,472,0,2016-07-25T18:01:14.963,2016-07-25T18:01:14.986,2,43711,53,0,17,0,0,0
192.168.1.233,192.168.1.1,366,0,2016-07-25T18:01:13.915,2016-07-25T18:01:15.144,6,46844,443,0,6,24,0,0
173.252.90.36,192.168.1.233,1197,0,2016-07-25T18:01:13.980,2016-07-25T18:01:15.146,7,443,46844,0,6,24,0,0
192.168.1.1,192.168.1.233,114,0,2016-07-25T18:01:18.051,2016-07-25T18:01:18.051,2,53,59744,0,17,0,0,0
192.168.1.233,192.168.1.1,336,0,2016-07-25T18:01:18.072,2016-07-25T18:01:18.072,2,59744,53,0,17,0,0,0
192.168.1.233,216.58,214,206,244,0,2016-07-25T18:01:26.389,2016-07-25T18:01:26.398,4,42216,443,0,6,20,0,0
216.58,214,206,192.168.1.233,331,0,2016-07-25T18:01:26.381,2016-07-25T18:01:26.391,4,443,42216,0,6,25,0,0
192.168.1.233,173.252.90.6,257,0,2016-07-25T18:01:33.664,2016-07-25T18:01:33.806,2,34502,443,0,6,24,0,0
173.252.90.6,192.168.1.233,416,0,2016-07-25T18:01:33.666,2016-07-25T18:01:33.847,3,443,34502,0,6,24,0,0
52.40,174.67,192.168.1.233,290,0,2016-07-25T18:01:12.586,2016-07-25T18:01:38.901,5,443,52274,0,6,17,0,0
192.168.1.233,52,40,174,67,343,0,2016-07-25T18:01:12.775,2016-07-25T18:01:37.148,6,52274,443,0,6,25,0,0
192.168.1.233,192.168.1.1,990,0,2016-07-25T18:01:41.293,2016-07-25T18:01:41.287,2,49481,53,0,17,0,0,0
192.168.1.1,192.168.1.233,129,0,2016-07-25T18:01:41.281,2016-07-25T18:01:41.287,2,53,49481,0,17,0,0,0
199.16.156.198,192.168.1.233,1310,0,2016-07-25T18:01:18.651,2016-07-25T18:01:40.496,9,443,50124,0,6,24,0,0
192.168.1.233,199.16.156.198,1992,0,2016-07-25T18:01:18.159,2016-07-25T18:01:40.492,9,56124,443,0,6,24,0,0
fd7c:e770:9e8a::1,fd7c:e770:9e8a::88e0:fc1b:32f6:925,46,0,2016-07-25T18:02:03.097,2016-07-25T18:02:03.117,1,39
90350,0,17,0,0,0
fd7c:e770:9e8a::88e0:fc1b:32f6:925,fd7c:e770:9e8a::1,211,0,2016-07-25T18:02:03.117,2016-07-25T18:02:03.117,1,39
953,53,0,17,0,0,0
173.252.90.4,192.168.1.1,43,331,0,2016-07-25T18:01:58.477,2016-07-25T18:02:03.067,6,443,44777,0,6,28,0,0
192.168.1.233,192.168.1.1,43,49,5865,0,2016-07-25T18:02:01.400,2016-07-25T18:02:08.472,12,95750,443,0,6,27,0,0
192.168.1.233,192.38.253.125,135,0,2016-07-25T18:02:04.292,2016-07-25T18:02:04.405,2,34490,443,0,6,24,0,0
192.168.1.233,192.38.253.125,135,0,2016-07-25T18:02:04.262,2016-07-25T18:02:04.373,2,36542,443,0,6,24,0,0
164.244.43.49,192.168.1.233,1362,0,2016-07-25T18:02:01.390,2016-07-25T18:02:08.458,11,443,20310,0,6,17,0,0
192.168.1.233,192.38.253.124,135,0,2016-07-25T18:02:04.236,2016-07-25T18:02:04.348,2,40776,443,0,6,24,0,0
192.168.1.233,192.38.253.125,135,0,2016-07-25T18:02:04.262,2016-07-25T18:02:04.375,2,50984,443,0,6,24,0,0
192.168.1.233,192.38.253.125,135,0,2016-07-25T18:02:04.376,2016-07-25T18:02:04.491,1,52939,0,6,24,0,0
192.30.253.125,192.168.1.233,87,0,2016-07-25T18:02:04.379,2016-07-25T18:02:04.379,1,443,39909,0,6,24,0,0
fd80:a62b:b0ff:fedc:53e,fd7c:e770:9e8a::88e0:fc1b:32f6:925,24,0,2016-07-25T18:02:08.399,2016-07-25T18:02:08.39
9,1,0,0,58,0,0,0
192.168.1.1,192.168.1.233,124,0,2016-07-25T18:02:14.966,2016-07-25T18:02:14.966,2,53,43442,0,17,0,0,0
192.168.1.233,192.168.1.1,472,0,2016-07-25T18:02:14.968,2016-07-25T18:02:14.987,2,43442,53,0,17,0,0,0

```

Více na stránku CESNETu...

# Kontakty

E-Mail: [cejkat@cesnet.cz](mailto:cejkat@cesnet.cz)

Mailinglist: [nemea@cesnet.cz](mailto: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](#)

