

IPv6 na OpenWRT

Ondřej Caletka



6. června 2012

Obsah

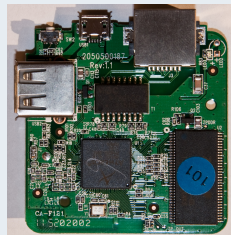
- 1 O OpenWRT
- 2 Realizace IPv6 připojení
- 3 Získání IPv6 konektivity
- 4 Šíření IPv6 po lokální síti
- 5 IPv6-only Wi-Fi síť
- 6 Validace DNSSEC na routeru
- 7 Firewall

OpenWRT

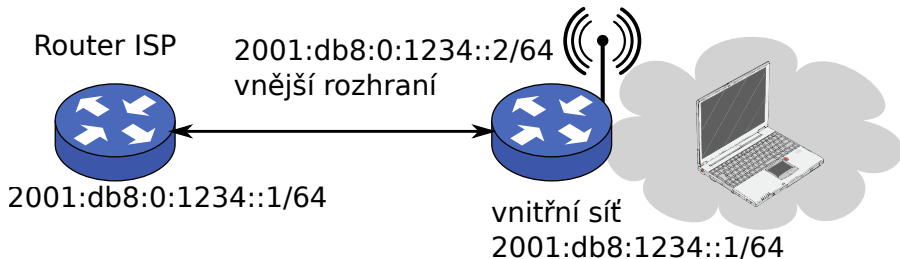
- Linuxová distribuce pro embedded zařízení.
- Zaměřeno na domácí směrovače.
- Nadstandardní možnosti konfigurace.
- Velmi dobrá podpora IPv6.

TP-LINK TL-WR703N

- Kapesní „3G“ router.
- Napájení z USB, spotřeba < 1 W.
- MIPS architektura, 32 MB RAM, 4 MB ROM.
- USB 2.0 port, 802.11n Wi-Fi.
- Ke koupi na <http://www.volumerates.com>



Realizace IPv6 připojení



- Nejčastější řešení: ruční konfigurace
- Nebo delegace prefixu pomocí DHCPv6
- My si předvedeme použití tunelu

Tunelová připojení

6to4

- ✓ není třeba protistrana
- ✓ data tečou téměř vždy optimální cestou
- ✗ vyžaduje veřejnou IPv4 adresu
- ✗ nejistá spolehlivost překladových bran

Hurricane Electric tunnelbroker.net

- ✓ jednoduchá registrace
- ✗ vyžaduje veřejnou IPv4 adresu

Tunelová připojení

SixXS

- ✓ robustní a spolehlivá infrastruktura
- ✓ mnoho PoPů po Evropě
- ✓ podporuje i průchod IPv4 NATem
- ✗ zdlouhavá registrace s ručním schvalováním

Freenet6

- ✓ jednoduchá registrace
- ✓ podporuje i průchod IPv4 NATem
- ✗ PoP v USA

První kroky

- Přeflashování firmware za OpenWRT snapshot.
 - Přihlášení telnetem, nastavení hesla. Tím se telnet vypne a aktivuje se SSH.
 - *Volitelně*: Použití USB disku namísto ROM.
 - Nastavení časového pásma, časových serverů. (Routery nemají HW hodiny reálného času.)
 - Konfigurace sítě, povolení Wi-Fi.
- ⇒ Máme funkční IPv4 router.

Konfigurační systém UCI

- Nadstavba OpenWRT nad konfigurační soubory.
- Cílem je zjednodušit systémovou konfiguraci, umožnit vznik front-endů (např. LuCI).
- Textová konfigurační databáze v `/etc/config/`
- Low-level vs. high-level síťová rozhraní:
 - High-level rozhraní popisují význam, např. `lan`, `wan`
 - Low-level rozhraní jsou skutečné názvy rozhraní viditelné pro OS, např. `eth0`. V UCI se nepoužívají.

Konfigurace 6to4

```
$ opkg update  
$ opkg install 6to4
```

```
/etc/config/network
```

```
config interface 'tun6to4'  
    option proto '6to4'
```

```
/etc/config/firewall
```

```
config rule  
    option src      wan  
    option proto    41  
    option target    ACCEPT
```

Statický tunel (he.net, SixXS)

```
$ opkg update  
$ opkg install 6in4
```

```
/etc/config/network
```

```
config interface 'henet'  
    option proto '6in4'  
    option peeraddr '216.66.86.122'  
    option ip6addr '2001:470:::2/64'
```

```
/etc/config/firewall obdobně
```

UDP tunel procházející NAT (SixXS)

```
$ opkg install aiccu  
$ /etc/init.d/aiccu enable  
$ /etc/init.d/aiccu start
```

```
/etc/config/aiccu
```

```
config aiccu  
    option username 'TunnelID'  
    option password 'TunnelPassword'
```

AICCU vyžaduje přesný čas, jinak se tunel neotevře.

Šíření IPv6 po lokální síti

```
/etc/config/network
```

```
config interface lan
```

```
...
```

```
option ip6addr '2a01:8c00:ffaf:1::1/64'
```

```
$ opkg install radvd
```

```
$ /etc/init.d/radvd enable
```

```
#Odstranit řádky „ignore“ v /etc/config/radvd
```

```
$ /etc/init.d/radvd start
```

IPv6-only Wi-Fi síť

```
/etc/config/network
```

```
config interface lan6
    option proto      'static'
    option ip6addr     '2a01:8c00:ffaf:6666::1/64'
```

```
/etc/config/wireless
```

```
config wifi-iface
    option device      radio0
    option network      lan6
    option mode         ap
    option ssid         IPv6day-6only
```

RADVD nastavíme obdobně.

Stateless DHCPv6 server (pro DNS)

```
$ opkg install wide-dhcpv6-server  
$ /etc/init.d/dhcp6s enable  
$ /etc/init.d/dhcp6s start
```

/etc/config/dhcp6s

```
config 'dhcp6s' 'basic'  
    option 'enabled' '1'  
    option 'interface' 'lan6'  
    option 'config_file' '/etc/dhcp6s.conf'
```

/etc/dhcp6s.conf

```
option domain-name-servers 2a01:8c00:ffaf:6666::1;
```

Validace DNSSEC na routeru

```
$ opkg install unbound
```

```
$ /etc/init.d/unbound enable
```

Unbound není napojen na UCI, přiložená konfigurace pracuje Out-of-the-box. Je však třeba přesunout DNS port programu dnsmasq, který slouží také jako DHCPv4 server.

```
/etc/config/dhcp
```

```
config 'dnsmasq'  
    option 'port' '5353'
```

DNSSEC vyžaduje správně nastavené hodiny. Časové servery je třeba nastavit jako IP adresy.

Firewall

V aktuálním OpenWRT UCI firewall podporuje IPv4 i IPv6. Není však nainstalován nástroj `ip6tables`, takže pravidla pro IPv6 nejsou uplatňována.

```
/etc/config/firewall
```

```
config 'rule'  
    option 'src' 'wan'  
    option 'proto' 'tcp'  
    option 'dest_port' '22'  
    option 'target' 'ACCEPT'  
    option '_name' 'SSH zvenku'
```


Děkuji za pozornost.

