

# IPv6 v OpenWRT

Ondřej Caletka



5. října 2014



Uvedené dílo podléhá licenci Creative Commons Uvedte autora 3.0 Česko.



# Novinky v Barrier Breaker

- procd: správce procesů
- netifd: správce síťových rozhraní
  - nyní spravuje i Wi-Fi síť
- block: správce filesystemů
- snapshot: alternativa k overlayi s JFFS2
  - podobné LiveCD
  - základ v SquashFS, overlay v RAM
  - snapshoty RAM se ukládají jako série TARů
- podpora DNSSEC validace (ale v DNSmasq ☹ )
- **nativní a úplná podpora IPv6**

# Nativní podpora IPv6

- vypnuta automatická konfigurace v kernelu
- DHCPv6 klient obstarává i SLAAC
- server odhcpd umí RA, DHCPv6 i NDproxy
- policy routing a ingress filtering pro zamezení smyček „*Pomoc, nemám ve směrovací tabulce výchozí bránu!*“
- tip: prozkoumání stavů síťových rozhraní příkazem `ifstatus`

# Konfigurace IPv6 – netifd

- 2 upstreamy – wan a wan6
  - umožňuje použití různých protokolů
  - základní nastavení: DHCPv4 a DHCPv6 klient
- volba `ip6prefix` u upstream rozhraní určuje nadelegovaný prefix pro router
- tento prefix je automaticky rozdělen downstream rozhraním
  - volba `ip6assign` určuje délku prefixu pro downstream
  - volba `ip6hint` umožňuje přesně zvolit číslo podsítě (např. `bab0`)
- je nastaven policy routing zahazující nepřidělené adresy z downstream rozhraní



# Konfigurace IPv6 – odhcpd

- dříve se jmenoval 6relayd
- kombinace DHCPv6 a RA serveru
- má-li upstream port IPv6 konektivitu, vysílá do sítě RA
- je-li na downstream portu kratší prefix než /64, nabízí delegaci prefixu na podřízený router
- podpora IPv4 DHCP není ve výchozím stavu aktivní

## Pevné vyhrazení IPv6 adresy

```
config host
    option name 'latte'
    option duid '0001000119f682940c8bfd600e9b'
    option hostid '1a1e'
```

# Relaying ND

- pro nouzové případy, kdy upstream síť má IPv6, ale neposkytuje prefix
- LAN zařízení dostávají adresy ze stejného /64 prefixu, jako má WAN

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

```
config dhcp wan6
    option dhcpv6 relay
    option ra relay
    option ndp relay
    option master 1
```

```
config dhcp lan
    option dhcpv6 relay
    option ra relay
    option ndp relay
```

# Source routing

- podpora pro větší množství IPv6 upstreamů
- každý záznam v routovací tabulce obsahuje i údaj o zdrojovém prefixu, pro který platí
- standardně jsou ohlašovány všechny IPv6 upstreamy do všech downstreamů, lze ovlivnit pomocí `ip6class`

## workaround pro statickou IPv6 konfiguraci

```
config route6 'wan6gw'  
  option interface 'wan'  
  option target '::/0'  
  option gateway '<default GW>'  
  option source '<WAN IP prefix/delegated>'
```



# Praktické případy konfigurace

# xDSL přípojka s PPPoE protokolem

```
config interface 'wan'  
    option ifname 'eth0.2'  
    option proto 'pppoe'  
    option username 'adsl'  
    option password 'adsl'  
    option ipv6 '1'
```

```
config interface 'wan6'  
    option ifname '@wan'  
    option proto 'dhcpv6'
```

# Tunel 6in4 (např. HE.net)

```
config interface 'wan6'  
    option ifname '@wan'  
    option proto '6in4'  
    option mtu '1480'  
    option peeraddr '216.66.86.122'  
#    option ip6addr '<adresa tunelu>/64'  
    option ip6prefix '2001:470:nnnn::/48'  
  
# HE.net only  
    option 'tunnelid' '<číslo tunelu>'  
    option 'username' '<username>'  
    option 'updatekey' '<update key tunelu>'
```

# Tunel pomocí AICCU (např. SixXS)

```
config interface 'wan6'  
    option ifname '@wan'  
    option proto 'aiccu'  
    option verbose '1'  
    option username 'OCB-SIXXS/T76490'  
    option password 'heslo'  
#    option ip6addr '<adresa tunelu>/64'  
    option ip6prefix '<delegovaný prefix>/48'
```

# Statická konfigurace IPv4 a IPv6

```
config interface 'wan'  
    option ifname 'eth0.2'  
    option proto 'static'  
    option ipaddr '<IPv4>'  
    option netmask '<IPv4 maska>'  
    option ip6addr '<IPv6 WAN adresa>/64'  
    option ip6gw    '<IPv6 brána>'  
    option ip6prefix '<delegovaný prefix>/48'
```

# Proč NEuvádět ip6addr u tunelů

- většina návodů požaduje odresování místní strany tunelu
- takové adresování nemá u PtP tunelů velký smysl, *cokoli do něj vstoupí, na druhé straně vypadne*
- adresa na rozhraní tunelu bude preferována pro odchozí provoz samotného routeru
- při jejím neuvedení bude systém používat jinou *vhodnou* adresu, například tu z LAN rozhraní
- provoz routeru tedy půjde ze stejného prefixu, jako provoz celé LAN

# Firewall

- základní nastavení zahazuje nevyžádaný provoz zvenku
- plamenná diskuze o výchozím nastavení
- osobně bych doporučoval kompromis: blokovat privilegované porty, dynamické porty propouštět

## Příklad konfigurace

```
config rule
    option src          wan
    option proto        tcpudp
    option dest         lan
    option dest_port    1024:65535
    option family      ipv6
    option target       ACCEPT
```

- možnost zprovoznit NAT64 v engine tayga (včetně netifd integrace)
- ND proxy režim není plně funkční
- neexistuje snadná náhrada funkcionality multiwan

## Integrační skripty netifd

- k nalezení na `/lib/netifd/proto/*.sh`
- načítají se pouze při startu netifd
- prakticky nulová dokumentace ☹



Děkuji za pozornost

Ondřej Caletka

Ondrej.Caletka@cesnet.cz

<http://Ondrej.Caletka.cz>

