Infrastuktura IPv6 na otevřených systémech

Pavel Šimerda
pavlix@pavlix.net

38. konference EurOpen.CZ

Letopočty

- 1995 RFC 1883 (IPv6)
- 1996 Prvotní podpora IPv6 v Linuxu
- 1998 Spuštění projektu KAME, Japonsko, IPv6 pro různé varianty BSD
- 2000 USAGI project, Japonsko, moderní implementace IPv6 po Linux
- 2005 Podpora IPv6 v Linuxu na produkční úrovni
- 2006 Ukončení projektu KAME

Zeroconf

Linkové adresy

- „Plug and play“
- Adresace v rámci linkového segmentu
- Nedílná součást IPv6 (oproti IPv4)
- Nezávislé na infrastruktuře IPv6 či IPv4
- Prefix `ff80::/64`
- Identifikátor počítače tvoří MAC adresa

Multicast DNS a DNS-SD

- Původně od Applu
- Systémový démon Avahi
- Objevování sousedů
- Obsluha domény `.local`
- Objevování služeb

Použití LL, mDNS a DNS-SD

- Okolní počítače a služby
- Nenakonfigurované routery a servery
- Síťové tiskárny, disky a další periferie
- Lokální alternativa klasického DNS
- Nouzová práce při selhání síťové infrastruktury

Konfigurace globálních IP adres

Ruční konfigurace

- Ruční zadání konfiguračních hodnot
  - IPv6 adresa
  - Délka prefixu (obdoba masky)
  - Výchozí brána
  - Další konfigurace
- Hodí se pro routery a servery

Ruční konfigurace – dočasná

Linux: iproute2

```
ip address
    add 2001:db8:85a3::8a2e:370:7334/64
    dev eth0
ip route add default via 2001:0db8:85a3::1
```

BSD: ifconfig

```
ifconfig fxp0
    inet6 2001:db8:85a3::8a2e:370:7334
    prefixlen 64
route -n add -inet6 default 2001:db8:85a3::1
```

Ruční konfigurace – stálá

Debian: /etc/network/interfaces

```
iface eth0 inet6 static
    address 2001:db8:85a3::8a2e:370:7334
    netmask 64
    gateway 2001:0db8:85a3::1
```

OpenWRT: /etc/config/network

```
config interface wan
    option ifname eth0
    option proto static
    option ip6addr
        2001:db8:85a3::8a2e:370:7334/64
    option ip6gw 2001:0db8:85a3::1
```

Mikrotik RouterOS

```
/ipv6 address
    add address=2001:db8:85a3::8a2e:370:7334/64
    interface=ether1
/ipv6 route
    add dst-address=::/0
    gateway=2001:0db8:85a3::1
```

Automatická konfigurace – bezstavová

- Výchozí způsob konfigurace na moderních distribucích
- Server vysílá RA, klient konfiguruje adresu samostatně
- Adresy, které obsahují MAC adresu
- Náhodné dočasné adresy
- Kryptografické adresy (pouze experimentální projekty)

Automatická konfigurace – bezstavová

Linux: náhodné dočasné adresy

```
sysctl net.ipv6.conf.all.use_tempaddr=2
```

BSD: náhodné dočasné adresy

```
sysctl net.inet6.ip6.use_tempaddr=1
sysctl net.inet6.ip6.prefer_tempaddr=1
```

Řízená konfigurace (DHCPv6)

- Podpora v distribucích přichází pozvolna
- NetworkManager 0.8.1 podle všeho DHCPv6 umí aktivovat
- Několik známých opensource DHCPv6 klientů a serverů
  - WIDE-DHCPv6
  - ISC DHCP 4.1
  - Dibbler
- Funguje hladce s RA

Dynamický routing

Dynamický routing

- Routovací démon Quagga, BIRD
- OSPFv3 (OSPF pro IPv6)
- BGP

Firewall

- iptables a ip6tables
- Nezávislý firewall
- Stejný pohled jako u IPv4
- Velmi podobné možnosti
- Absence NAT

ip6tables

```
ip6tables -A FORWARD
    -m state --state INVALID -j DROP
ip6tables -A FORWARD
    -m state --state ESTABLISHED,RELATED
    -j ACCEPT
ip6tables -A FORWARD
    -p ipv6-icmp --icmpv6-type echo-request
    -j ACCEPT
ip6tables -A FORWARD
    -j LOG
    --log-prefix "Rejecting in FORWARD: "
ip6tables -A FORWARD
    -j REJECT
    --reject-with icmp6-adm-prohibited
```

IPsec

- Transport a tunelování
- Implementace IPsec v kernelu
- Výměna klíčů v userspace: Racoon

/etc/racoon/racoon.conf

```
path pre_shared_key "/etc/racoon/psk.txt"

remote 2001:db8:2:2::2
{
    exchange_mode main;
    lifetime time 24 hour;
    proposal
    {
        encryption_algorithm 3des;
        hash_algorithm md5;
        authentication_method pre_shared_key;
        dh_group 2;
    }
}
```

/etc/racoon/racoon.conf – pokračování

```
sainfo address 2001:db8:1:1::1 any
    address 2001:db8:2:2::2 any
{
    lifetime time 1 hour;
    encryption_algorithm 3des;
    authentication_algorithm hmac_md5;
    compression_algorithm deflate;
}
```

/etc/racoon/psk.txt

```
2001:db8:2:2::2 MocTajneHeslo
```

/etc/racoon/setkey.sh

```
#!/sbin/setkey -f
flush;
spdflush;
spdadd 2001:db8:1:1::1 2001:db8:2:2::2 any -P out i
spdadd 2001:db8:2:2::2 2001:db8:1:1::1 any -P in  i
```

Distribuce

Debian

- Univerzální distribuce (server, desktop i router)
- Mnoho odvozených distribucí
- Výtečně řešená konfigurace sítě
- Integrované síťové skripty
- Zaměření na podporu IPv6 teprve nové, mnoho třecích ploch

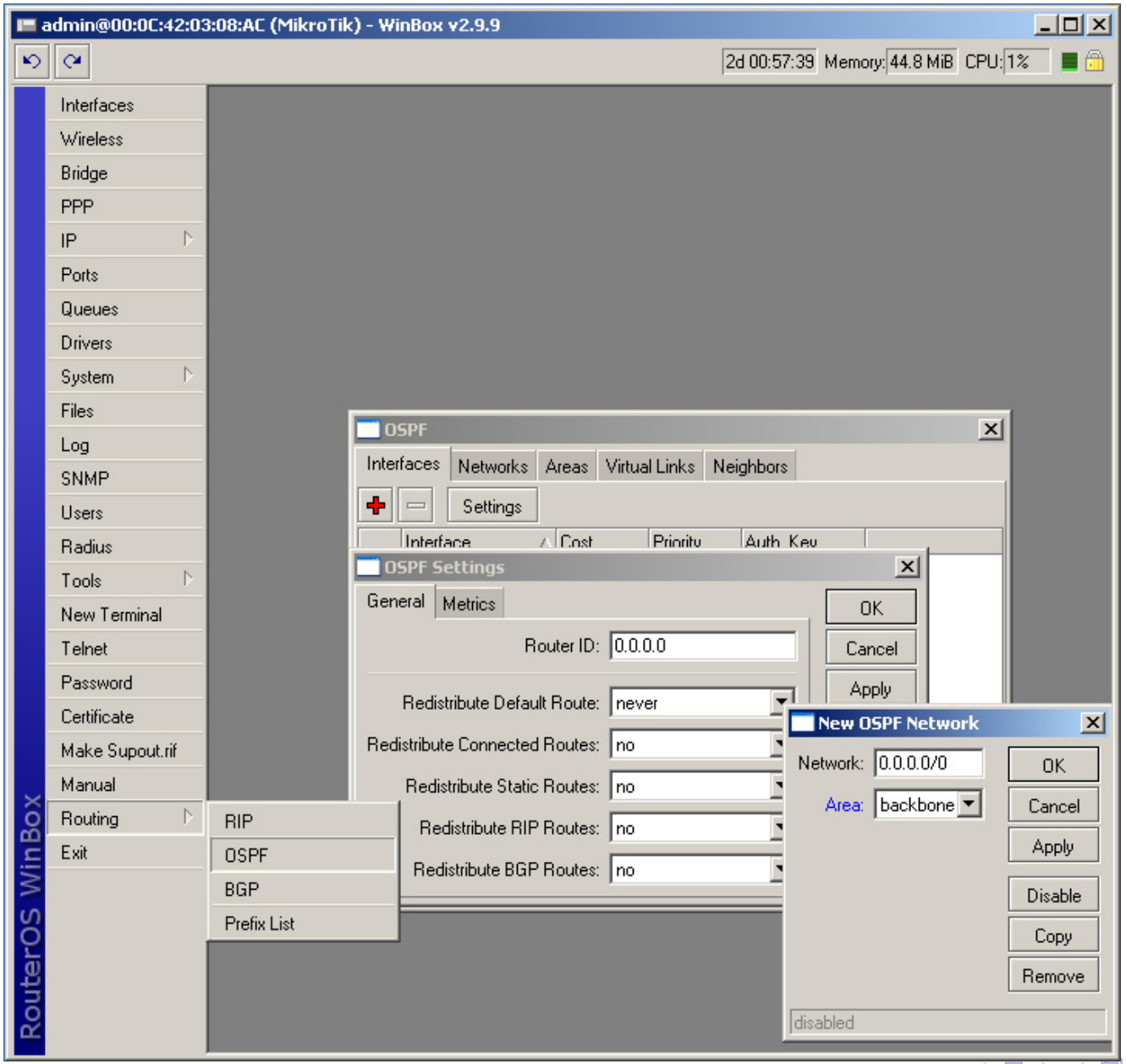
OpenWRT

- Opensource linuxový firmware
- Ovládání pomocí SSH a konfiguračních souborů
- Webová UI ve vývoji
- Lze koupit předinstalované (ale spíše výjimečně)

Mikrotik

- Řada RouterOS 5.x (2011) připravená na provoz s IPv6
- Dodávaný s routery Mikrotik
- Ne až tak opensource
- Linuxové jádro a další nástroje
- Konfigurace přes SSH se speciálním shellem
- Konfigurace přes utilitu Winbox (pod Wine či Windows)
- Příklad pro OSS komunitu
- Občas zůstávají dlouho neopravené chyby

Mikrotik – screenshot



Něco z praxe

Jak si ulehčit práci

- Adresy routerů konfigurovat staticky
- Používat bezstavovou konfiguraci v koncových sítích
- Vnitřní routing řešit pomocí OSPF
- Vnější routing řešit pomocí BGP
- Omezovat konektivitu po celých subnetech
- Konfigurovat problémové spoje jako NBMA

Jak si ulehčit práci

- Adresy routerů konfigurovat staticky
- Používat bezstavovou konfiguraci v koncových sítích
- Vnitřní routing řešit pomocí OSPF
- Vnější routing řešit pomocí BGP
- Omezovat konektivitu po celých subnetech
- Konfigurovat problémové spoje jako NBMA

Jak si ulehčit práci

- Adresy routerů konfigurovat staticky
- Používat bezstavovou konfiguraci v koncových sítích
- Vnitřní routing řešit pomocí OSPF
- Vnější routing řešit pomocí BGP
- Omezovat konektivitu po celých subnetech
- Konfigurovat problémové spoje jako NBMA

Jak si ulehčit práci

- Adresy routerů konfigurovat staticky
- Používat bezstavovou konfiguraci v koncových sítích
- Vnitřní routing řešit pomocí OSPF
- Vnější routing řešit pomocí BGP
- Omezovat konektivitu po celých subnetech
- Konfigurovat problémové spoje jako NBMA

Jak si ulehčit práci

- Adresy routerů konfigurovat staticky
- Používat bezstavovou konfiguraci v koncovýh sítích
- Vnitřní routing řešit pomocí OSPF
- Vnější routing řešit pomocí BGP
- Omezovat konektivitu po celých subnetech
- Konfigurovat problémové spoje jako NBMA

Jak si ulehčit práci

- Adresy routerů konfigurovat staticky
- Používat bezstavovou konfiguraci v koncovýh sítích
- Vnitřní routing řešit pomocí OSPF
- Vnější routing řešit pomocí BGP
- Omezovat konektivitu po celých subnetech
- Konfigurovat problémové spoje jako NBMA

Praktické problémy v sítích

- Nefunkční IPv6 způsobuje problémy
- DUID není stálé!
- RA může posílat kdokoli

Praktické problémy v sítích

- Nefunkční IPv6 způsobuje problémy
- DUID není stálé!
- RA může posílat kdokoli

Praktické problémy v sítích

- Nefunkční IPv6 způsobuje problémy
- DUID není stálé!
- RA může posílat kdokoli

Bonusy

- IPv6 pro malého poskytovatele nabízí méně prostoru
- IPv6 poslední záchrany
- Přechodové mechanismy v OSS systémech
- NAT mezi IPv6 a IPv4
- Testování s ULA adresami

Bonusy

- IPv6 pro malého poskytovatele nabízí méně prostoru
- IPv6 poslední záchrany
- Přechodové mechanismy v OSS systémech
- NAT mezi IPv6 a IPv4
- Testování s ULA adresami

Bonusy

- IPv6 pro malého poskytovatele nabízí méně prostoru
- IPv6 poslední záchrany
- Přechodové mechanismy v OSS systémech
- NAT mezi IPv6 a IPv4
- Testování s ULA adresami

Bonusy

- IPv6 pro malého poskytovatele nabízí méně prostoru
- IPv6 poslední záchrany
- Přechodové mechanismy v OSS systémech
- NAT mezi IPv6 a IPv4
- Testování s ULA adresami

Bonusy

- IPv6 pro malého poskytovatele nabízí méně prostoru
- IPv6 poslední záchrany
- Přechodové mechanismy v OSS systémech
- NAT mezi IPv6 a IPv4
- Testování s ULA adresami