

IPv6 a IPv4 na Linuxu

Pavel Šimerda

pavlix@pavlix.net

LinuxAlt 2011

Brno

<http://data.pavlix.net/linuxalt2011/>

- 1995 RFC 1883 (IPv6)
- 1996 Prvotní podpora IPv6 v Linuxu
- 1998 Spuštění projektu KAME, Japonsko, IPv6 pro BSD
- 2000 USAGI project, Japonsko, IPv6 pro Linux
- 2005 Podpora IPv6 v Linuxu na produkční úrovni
- 2006 Ukončení projektu KAME
- 2011 Vyčerpání IPv4 rozsahů IANA a APNIC
- 2011 The IPv6 Day (8. června)

Zeroconf

- „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

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

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

Linux: iproute2

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

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
```

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

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
```

Linux: radvd.conf na routeru

```
interface eth0
{
    AdvSendAdvert on;
    prefix 2001:db8:0:1::/64
    {
        AdvOnLink on;
        AdvAutonomous on;
    };
};
```

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
```

- 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
- DHCPv6 se používá v kombinaci s RA

Dynamický routing

- Propojení místních sítí bez práce (OSPFv3)
- Software pro výměnu směrovacích informací
 - BIRD
 - Quagga
 - XORP

BIRD: /etc/bird6.conf

```
protocol ospf MyOSPF {  
    area 0.0.0.0 {  
        interface "eth0" {  
            };  
        };  
    }  
}
```

Firewall

- iptables a ip6tables
- Nezávislý firewall
- Stejný pohled jako u IPv4
- Velmi podobné možnosti
- Absence NAT (postupně se mění)

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

- Autentizace počítačů či uživatelů
- integrita a utajení síťového provozu
- Nezávislost na transportním protokolu
- Implementace IPsec v kernelu
- Software pro domlouvání tunelů
 - Racoon (zastaralý, složitá konfigurace)
 - Openswan (problémy s IPv6)
 - Strongswan
 - Racoon2

/etc/ipsec.d/test.conf

```
conn test
    type=transport
    left=2001:db8::a
    leftid=@a.example.com
    leftrsasigkey=0sAQ01EFgL5Od...7DvKohvAwd
    right=2001:db8::b
    rightid=@b.example.com
    rightrsasigkey=0sAQPGT6JIYP0...wZfx7bBGER
    ikev2=yes
    auto=add
```


Distribuce

- Univerzální distribuce (server, desktop i router)
- Mnoho odvozených distribucí
- Výtečně řešená konfigurace sítě
- Integrované síťové skripty
- Pro podporu IPv6 je potřeba vyladit konfiguraci

- Opensource linuxový OS/firmware pro routery
- Ovládání pomocí SSH a konfiguračních souborů
- Základní nastavení dostupné ve webovém UI
- Lze koupit předinstalované nebo flashovat

Závěrem...

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

<http://data.pavlix.net/linuxalt2011/>

pavlix@pavlix.net