



# Připojení IPv6 sítě do e-infrastruktury sítě CESNET

**Martin Pustka**

6.12.2013  
Seminář IPv6 WG, Olomouc

[Martin.Pustka@vsb.cz](mailto:Martin.Pustka@vsb.cz)

# Role CESNETu

- poskytování IPv6 konektivity (primární i záložní)
- plnohodnotná implementace a provozní podpora
- poskytování statistik
- podpora i v MPLS VPN
- podpora v serverových službách (DNS, SMTP, antispam filtry, ...)

# Proč podporovat IPv6 v LAN

- není-li podpora IPv6 v lokální síti, tak uživatelské systémy se k IPv6 konektivitě pravděpodobně nějak a neřízeně dostanou
- externí tunely TEREDO, 6to4
- nekontrovalé systémy se mohou prohlásit za běžné IPv6 směrovače
- na hranici IPv4 lze omezit (protokol 41)

# Postupy

- získat konektivitu a adresy
- adresní plán
- zajistit podporu IPv6 v infrastruktuře počítačové sítě
  - směrovače, přepínače
  - firewally, VPN, IDS/IPS
- podpora serverových systémů
- podpora uživatelských zařízení

# Získání konektivity a adres

- u CESNETu jednoduché, analogie s IPv4
- žádost o přidělení IPv6 adres <http://www.cesnet.cz/nic>
- institucím se přiděluje obvykle síť s délkou prefixu 48 (65536 podsítí /64) nebo 56 bitů (256 podsítí)
- IPv6 adresy na propojovací podsít'
- CESNET podporuje i záložní připojení, BGP

# Adresní plán

- přidělení sítě /48
- koncové sítě /64 =  $2^{16}$  podsítí, tj. 65536
- jak rozdělit?
  - s ohledem na geografické lokality
  - často se uplatňuje metoda půlení intervalu
- spojovací sítě /127 (dříve /64)
- dva světy, dva protokoly, dva adresní plány

# Adresace sítí

- je zbytečné budovat IPv6 only nebo IPv4 only sítě a implementovat meziprotokolové brány
- jednodušší je podporovat oba protokoly
- veřejné IPv4 a veřejné IPv6 adresy
- privátní IPv4 a veřejné IPv6 adresy

# Infrastruktura počítačové sítě

- hraniční dual-stack směrovače
- firewally, VPN
- směrovače vnitřní sítě
- přepínače
- budování shodných topologií pro IPv4/6
- přechodové mechanismy
- dva oddělené směrovací protokoly, dodržovat stejné metriky (např. interní OSPF/OSPFv3, externí BGP)



# Serverová infrastruktura v síti

- odlišný pohled na serverové a uživatelské sítě
- nepodporovat v síti autokonfigurace koncových systémů, lze nastavit na směrovači LAN sítě
- statické nastavení IP adres, problémy s DHCPv6
- manuálně vypínat u systémů Windows tunely a autokonfigurace

# Sít'ová podpora v uživatelských sítích

- obvykle není možno konfigurovat koncové stanice, zvláště v univerzitním prostředí
- vhodné implementovat ISATAP tunely uvnitř organizace
- blokovat tunelování IPv6 provozu mimo sít'
- oznámení směrovače s vysokou preferencí
- autokonfigurace, DHCPv6
- RA guard v sít'ové L2 infrastruktuře

# Problémy při implementaci

- administrativní problémy a financování obnovy
- jedná se o dlouhodobý proces, opora v instituci
  
- technicky starší aktivní prvky bez podpory IPv6
  - multicastový provoz je rozесílán na všechny porty
- podpora IPv6 v HW, SW podpora může snižovat výkon

# Problémy při implementaci

- dohledatelnost uživatelů
- uživatelé se sdíleným připojením a externí IPv6 konektivitou
- přístupy ke špatným IPv6 zdrojům (např. justice.cz)
- First-hop security (FHS)
- WiFi sítě a podpora IPv6

# Problémy při NEimplementaci

- uživatelé nějakým způsobem získají nekvalitní tunelovanou IPv6 konektivitu
  - obtížné dohledávání problémů s přístupem k cizím IPv6 zdrojům
- dostupnost interních systémů přes IPv6
- First-hop security, Man-in-the-middle útoky
- infrastruktura Active Directory

# A na konec...

- je potřeba vědět zda a proč se IPv6 nasazuje
- požádat o IP adresy a udělat test připojení/nasazení
- připojit se (a neodpojit) a začít nasazovat ve vybraných částech sítě
- nepodceňovat od počátku bezpečnost, zvláště je-li řešena v IPv4
- ve všech oblastech může CESNET pomoci

# Zavěr a dotazy

Děkuji za pozornost.