

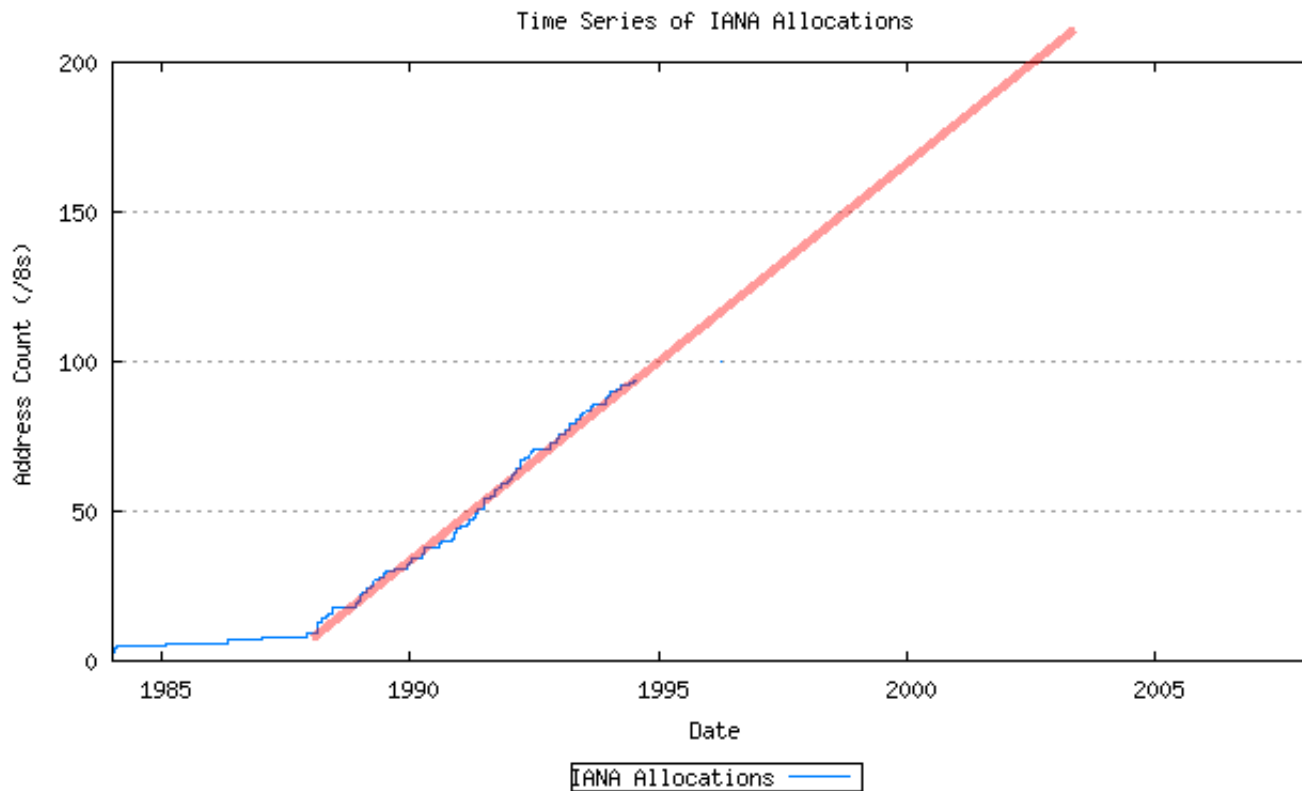
# Úvod do IPv6

Pavel Satrapa

Pavel.Satrapa@tul.cz

# 1. polovina 90. let

- IPv4 adresy dojdou kolem roku 2003
  - některé kategorie (třída B) mnohem dříve

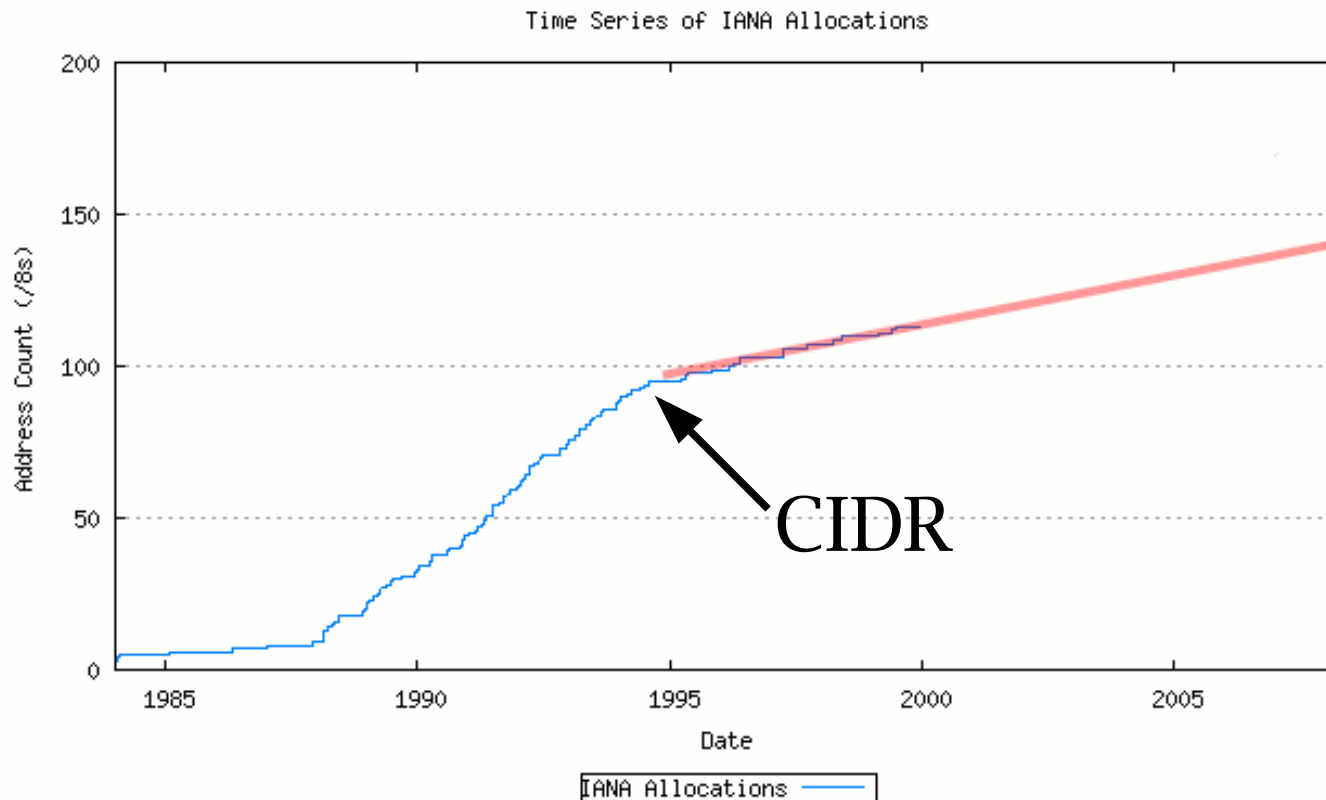


# Návrh nové verze IP

- času je dost – neomezí se jen na prodloužení adresy
- lze začlenit **nové vlastnosti**
  - obrovský adresní prostor (128b adresa)
  - lepší směrování – vysoké rychlosti, QoS
  - automatická konfigurace
  - vestavěné bezpečnostní mechanismy (IPsec)
  - podpora mobility
  - umožnit postupný přechod z IPv4 na IPv6

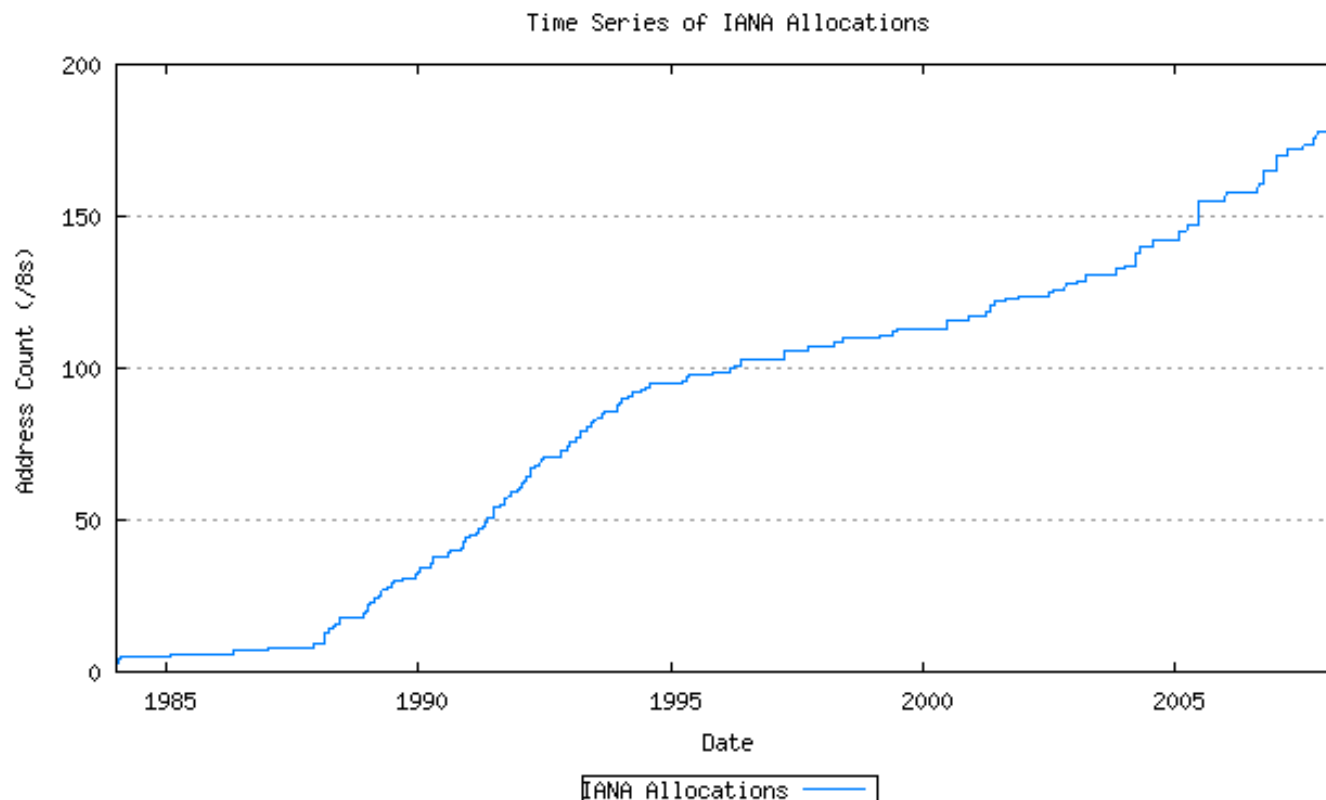
# Kolem roku 2000

- IPv6 nebylo samo – CIDR, NAT
  - IPv4 adresy vydrží do roku 2030, pohoda, klídek, tabáček



# Současnost

- **IPv4 adresy dojdou kolem poloviny roku 2012**
  - **Houstone máme tu problém**



zdroj:  
Geoff Huston,  
[ipv4.potaroo.net](http://ipv4.potaroo.net)

# Adresy a jejich zápis

- definuje RFC 4291 (4. generace)
- 128 bitů dlouhé
- zapisují se v šestnáctkové soustavě, čtveřice číslic oddělovány dvojtečkami  
**2001:0718:1c01:0005:020b:dbff:fea1:d52c**
  - úvodní nuly ve čtveřici lze vynechat
  - souvislou skupinu nulových čtveřic lze nahradit ::  
::1 = 0:0:0:0:0:0:0:1
- uživatelsky nepřítulné – DNS je nutnost

# Kategorie adres

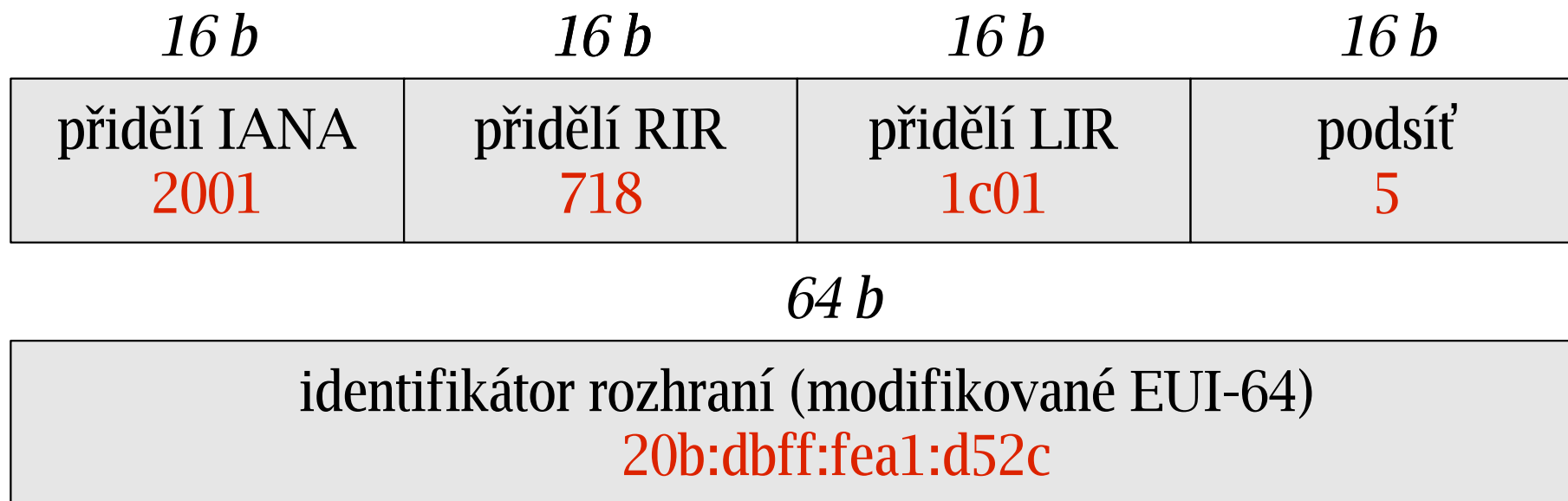
- **individuální (unicast)**
  - označují jedno rozhraní – běžné adresy
- **skupinové (multicast)**
  - označují skupinu rozhraní, data se doručují všem členům skupiny
  - broadcast je speciálním případem multicastu
- **výběrové (anycast)**
  - označují skupinu rozhraní, doručuje se nejbližšímu členovi

# Rozdělení adresního prostoru

- `::/128`      nedefinovaná adresa
- `::1/128`      smyčka (loopback)
- `ff00::/8`      skupinové
- `fe80::/10`    individuální lokální linkové
- ostatní      individuální globální

# Globální individuální adresa

- typicky s prefixem 2001::/16
- přidělují se stejnou cestou jako IPv4



# Identifikátor rozhraní

- 64 bitů – zběsile plýtvá, ale usnadňuje některé mechanismy
- standard: modifikované EUI-64
  - odvozeno z MAC adresy
  - nezapamatovatelné
  - umožňuje sledovat mobilní stroj – RFC 4941 zavádí dočasné náhodně generované identifikátory, aby se chránilo soukromí uživatelů
- rozhraní má v IPv6 několik adres

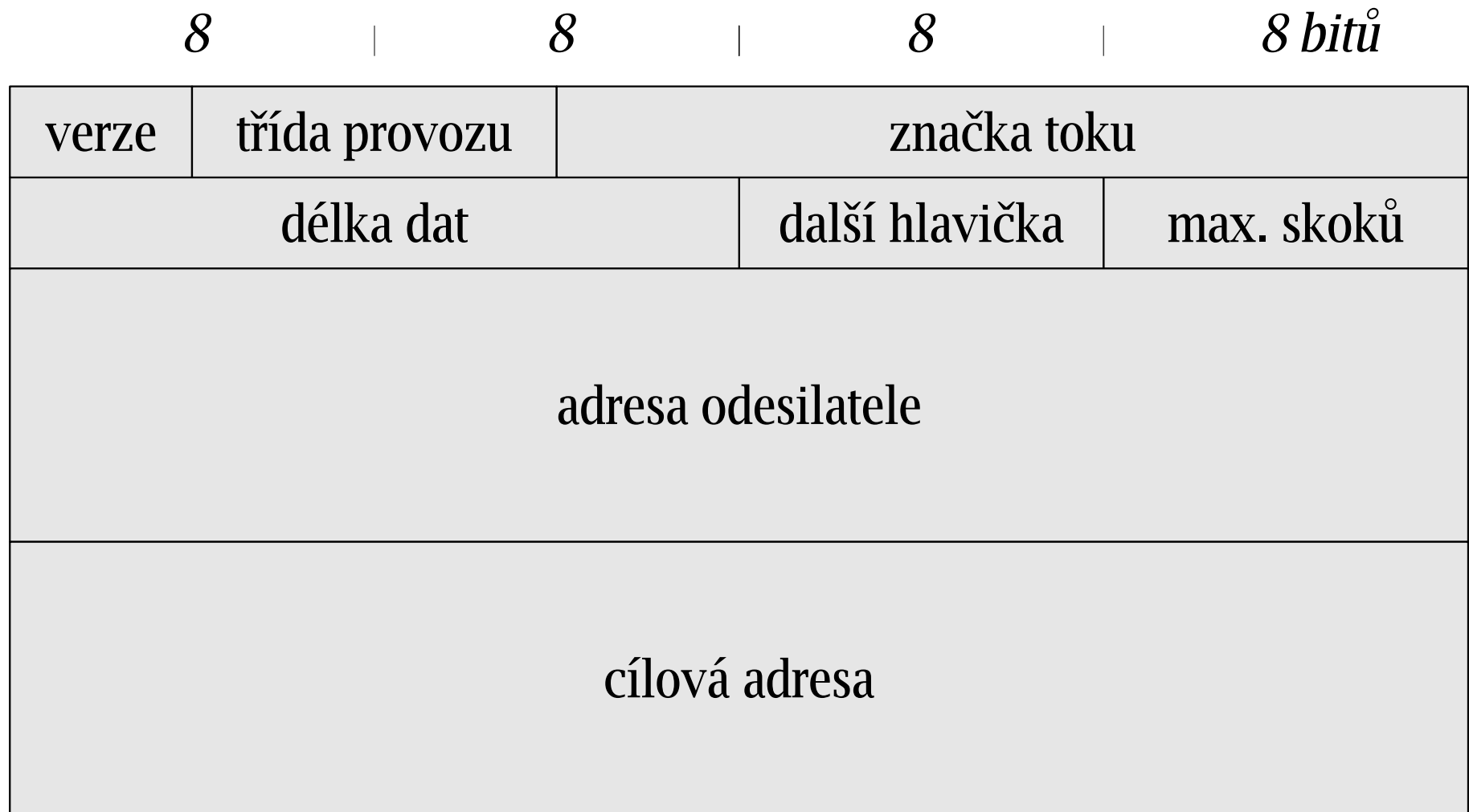
# Skupinové adresy

- samostatný adresní prostor – prefix ff00::/8
- součástí adresy je dosah (4. číslice)
  - od rozhraní až po globální
  - nahrazuje triky s TTL ze světa IPv4
- obsahuje též příznak, zda se jedná o dobře známou (trvalou) nebo dočasnou adresu
- správu skupin řídí MLD – Multicast Listener Discovery

# Výběrové adresy

- cíl: zastupitelnost serverů, distribuované poskytování služeb
- sdílí prostor s individuálními adresami
  - nutno odlišit konfigurací
- řada praktických problémů
  - reálně používány (a použitelné) jen v omezeném měřítku

# Formát datagramu



# Rozšiřující hlavičky

- údaje, které nejsou potřeba vždy, byly přesunuty do rozšiřujících hlaviček
- položka *Další hlavička* obsahuje typ následující hlavičky, ta opět obsahuje tuto položku
- poslední v řetězci identifikuje protokol vyšší vrstvy
- definováno pořadí tak, aby směrovač mohl co nejrychleji ukončit průchod řetězcem a zpracovat datagram

# Objevování sousedů

- Neighbor Discovery (ND), RFC 2461
- řeší několik odlišných úkolů
  - zjišťování MAC adres sousedů (náhrada ARP)
  - ověřování dosažitelnosti
  - detekce duplicitních adres
  - automatická konfigurace
  - přesměrování

# Automatická konfigurace

- **stavová**
  - DHCPv6, RFC 3315
  - server: dhcp6s pro Linux
  - klient: Dibbler (<http://klub.com.pl/dhcpv6/>)
- **bezstavová**
  - uživatelský počítač se nastaví sám
  - plug-and-play
  - umí snad každá implementace IPv6

# Bezstavová autokonfigurace

- základem **ohlášení směrovače**
  - prefixy místních (pod)sítí – první polovina adresy
  - zda (jak dlouho) je ochoten dělat implicitní směrovač
- **počítač**
  - z MAC adresy vytvoří modifikované EUI-64
  - přidá fe80:: (lokální linková) a ověří jednoznačnost adresy
  - spojí místní prefixy s EUI-64 – globální adresy
  - udržuje si seznam implicitních směrovačů (střídá je)

# IPv6 a DNS

- IPv6 adresy v záznamech AAAA, např.  
jmeno AAAA 2001:718:1c01:5:20b:dbff:fea1:d52c
- revrezní DNS
  - vychází z kompletní adresy (včetně všech nul)
  - obrácené pořadí číslic, každá číslice je jednou doménou
  - přípona ip6.arpa
  - příklad – v doméně 1.0.c.1.8.1.7.0.1.0.0.2.ip6.arpa záznam  
c.2.5.d.1.a.e.f.f.f.b.d.b.0.2.0.5.0.0.0 PTR jmeno.kdesi.cz.

# Jak zavádět do DNS?

- dvě adresy pro jedno jméno – A i AAAA záznamy pro stejné jméno
  - neviditelný přechod na nový protokol
  - zviditelní se, pokud jsou problémy s IPv6 (některé systémy mu dávají přednost)
- odlišná jména – např. `www.kdesi.cz` a `www.ip6.kdesi.cz`
  - explicitní zdůraznění protokolu

# Směrování

- rozšíření stávajících protokolů
- **interní protokoly**
  - RIPng
  - OSPFv3
  - IS-IS
- **externí protokoly**
  - BGP4+

# Bezpečnostní prvky – IPsec

- standardní součástí IPv6
- definice společná pro IPv4 i IPv6 (RFC 4301 a spol.)
- rozšiřující hlavičky
  - **Authentication Header (AH)** – ověření totožnosti odesilatele, ochrana proti změně obsahu
  - **Encapsulating Security Payload (ESP)** – zejména šifrování obsahu (ale umí i služby jako AH)

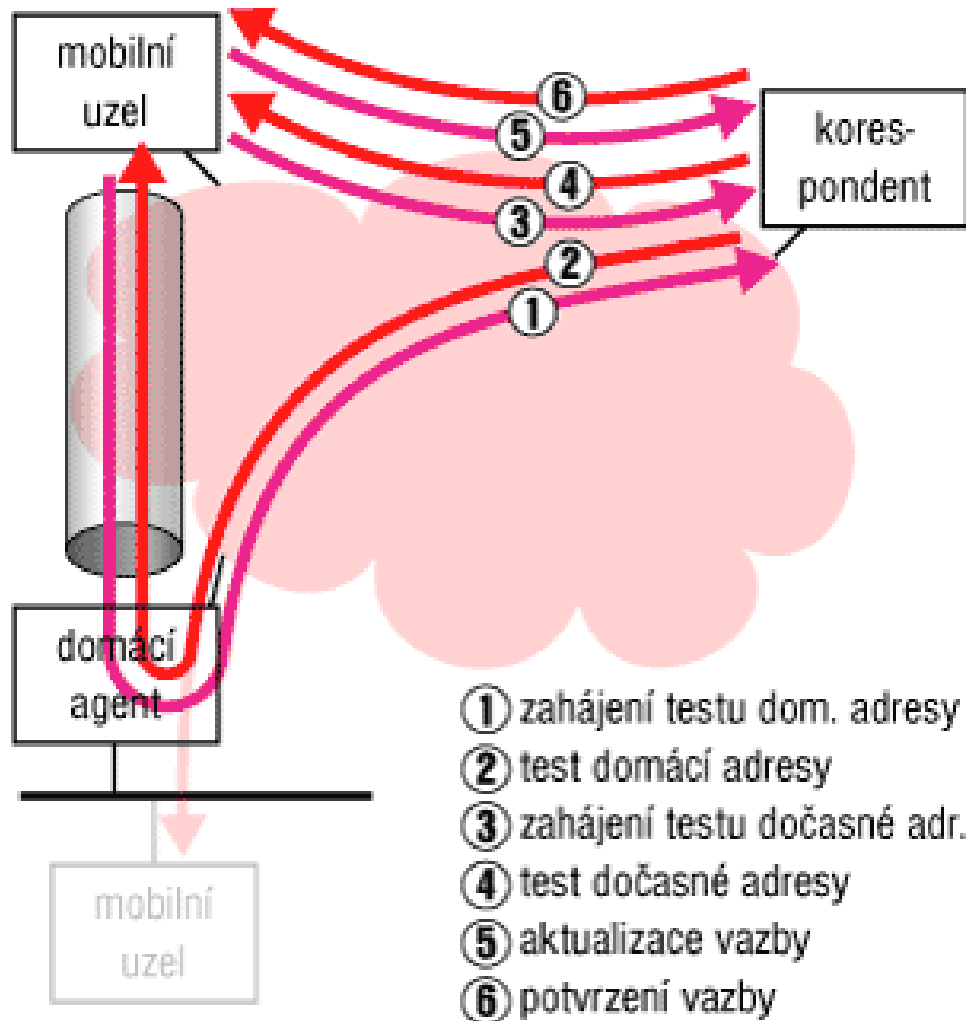
# IPsec v praxi

- dva možné **režimy**:
  - **transportní** – IPsec hlavičky mezi ostatními (připojuje odesílatel datagramu)
  - **tunelující** – celý datagram je zabalen do nového, opatřeného IPsec hlavičkami (tunel mezi směrovači)
- **problémy**
  - nedostatečné implementace
  - správa klíčů (chybí PKI)

# Mobilita

- efektivně podporuje mobilní uzly (RFC 3775)
- každý má určitou domácí síť a **domácí adresu**
- pokud je na cestách, zastupuje jej v domácí síti tzv. **domácí agent** (Home Agent)
  - jeden z místních směrovačů
  - švindluje při objevování sousedů a stahuje na sebe datagramy určené mobilnímu uzlu
  - přeposílá je uzlu šifrovaným tunelem na aktuální adresu

# Optimalizace cesty



- mobilní uzel oznámí protějšku svou dočasnou adresu
- nutno ověřit, že nelže – přijímá data na obou adresách
- další komunikace pak probíhá přímo

# Přechodové mechanismy

- **dual stack**
  - zařízení podporuje oba protokoly
- **tunelovací**
  - oba konce hovoří IPv6, pakety musí přepravit běžným IPv4 Internetem
- **konverzní**
  - překlad mezi IPv4 a IPv6 pokud spolu mají komunikovat počítače hovořící odlišnými protokoly

# Doporučené čtivo

- **Silvia Hagen: IPv6 Essentials**  
O'Reilly, 2006  
popis protokolu a doprovodných mechanismů
- **Iljitsch van Beijnum: Running IPv6**  
Apress, 2005  
praktický popis konfigurace a provozování IPv6
- **Pavel Satrapa: IPv6**  
Neocortex, 2002  
jediná česká kniha na toto téma

# Děkuji za pozornost



Technická univerzita  
v Liberci

