

# Historie a současnost IPv6

Pavel Satrapa

Pavel.Satrapa@tul.cz

# Vznik IPv6

- první úvahy v roce 1990
- základní koncepční rozhodnutí přijata v 1. polovině 90. let
- hlavní motivací bylo hrozící vyčerpání adres
  - odhadováno na 2002 až 2003
- první generace RFC (1883 a spol.) vydána v prosinci 1995

# Plánované vlastnosti (1)

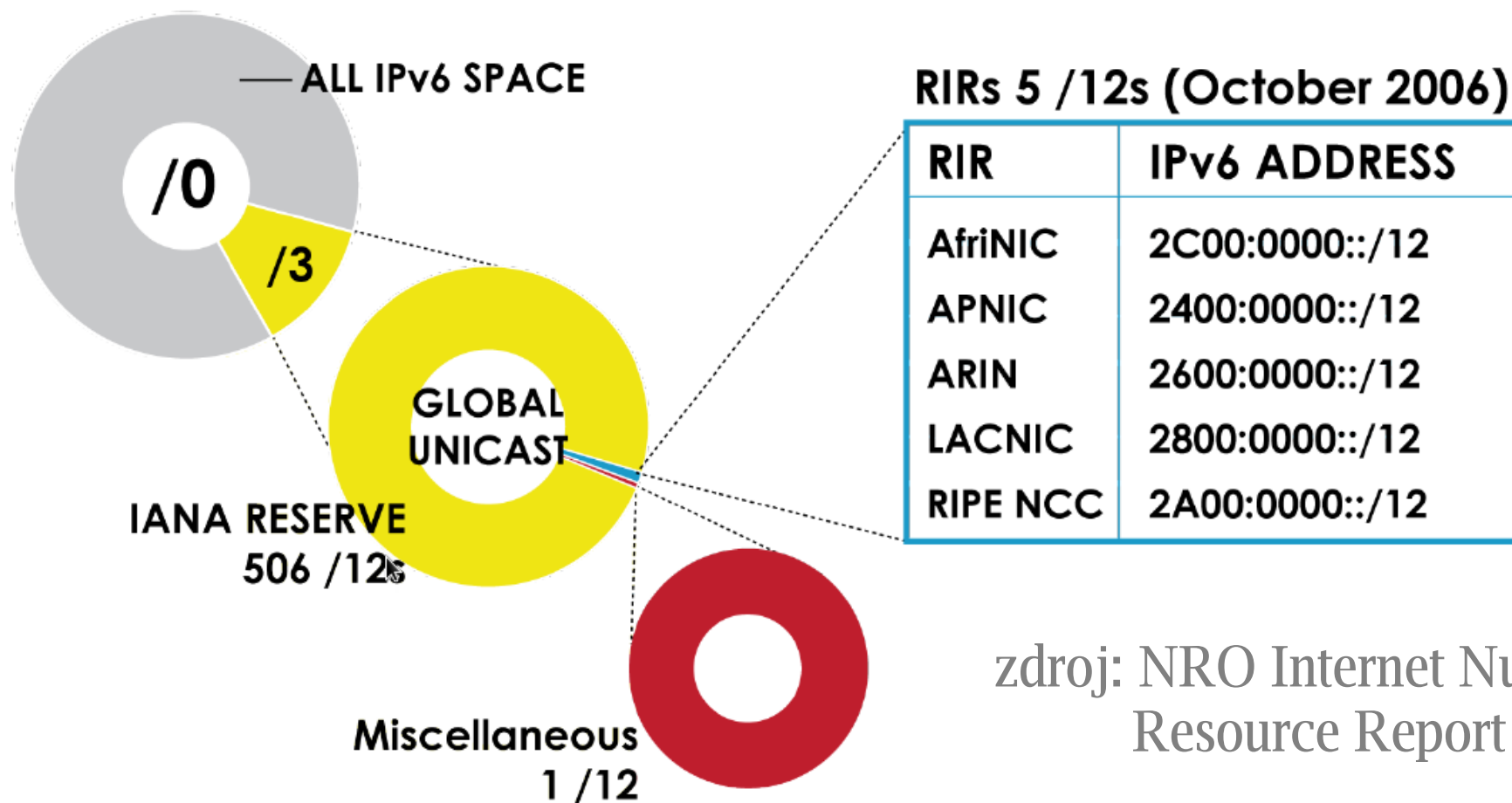
- „nekonečný“ adresní prostor
- tři typy adres – individuální, skupinové, výběrové
- jednotné adresní schéma pro Internet a LAN
- hierarchické směrování
- bezpečnostní prvky součástí IP
- podpora služeb se zajištěnou kvalitou
- vysokorychlostní směrování

# Plánované vlastnosti (2)

- automatická konfigurace
- podpora mobilních zařízení
- hladký přechod z IPv4
  
- **jak se je podařilo realizovat?**

# Adresní prostor (1)

- 128 bitů dlouhé adresy – spousta místa



zdroj: NRO Internet Number  
Resource Report 1/2011

# Adresní prostor (2)

- $79 \cdot 10^{27}$  větší než IPv4
- piha krásy: 64 bitů věnováno identifikátoru rozhraní
  - potřebujeme podsítě velikosti 4 miliard současných Internetů?
  - původní motivace (jednoduché odvození z L2 adresy – snadná automatická konfigurace) překonána – náhodně generované adresy (RFC 4941)
  - vestavěno v řadě prvků – není snadné změnit
  - velká část adresního prostoru nepřirázena, případná změna je do budoucna možná

# Tři typy adres

- splněno
- IPv4 je má ovšem také
- míra podpory srovnatelná
  - individuální a výběrové masově používány
  - problémové jsou zejména skupinové adresy

# Jednotné adresování

- splněno
- díky spoustě adres není třeba dělat kompromisy
- původně (RFC 3177) velmi unifikováno: síť 48 b, podsíť 16 b, rozhraní 64 b
- dnes volnějšší (RFC 6177): síť určuje registr, typicky 48/56/64 b, podsíť 16/8/0 b, rozhraní 64 b
- pokud by byl zájem o privátní adresy, lze použít ULA (RFC 4193)



# Hierarchické směrování

- splněno
- adresy od počátku přidělovány se zřetelem na agregaci
- místa je dost, lze dělat koncepčně
- stav IPv4 směrování se bude zhoršovat (převody a prodeje adres)

# Bezpečnostní prvky

- splněno na papíře – IPsec
- definovány hlavičky AH a ESP, oficiálně povinné
- řada implementací nepodporuje nebo podporuje jen částečně
  - postupně se zlepšuje
- stav v IPv4 srovnatelný

# Definovaná kvalita

- v základní hlavičce Třída provozu a Značka toku
- třída provozu využívána pro DiffServ
  - stejně jako TOS v IPv4
- toky jsou velká neznámá
  - aktuálně pracovní skupina 6man pracuje na změně existujících specifikací
- proti IPv4 zatím žádný velký pokrok

# Vysokorychlostní směrování

- jednodušší hlavička
  - odstraněn kontrolní součet
- problém s řetězením hlaviček
  - uměle protažený řetěz rozšiřujících hlaviček může směrovač významně zatížit

# Automatická konfigurace (1)

- **bezstavová – plug and play**
- stačí nastavit směrovač, aby posílal ohlášení
- nově doplněny DNS informace (RFC 6106)
- široce podporována, funguje všude
- správce ztrácí kontrolu nad připojovanými stroji
  - možné řešení: IEEE 802.1X

# Automatická konfigurace (2)

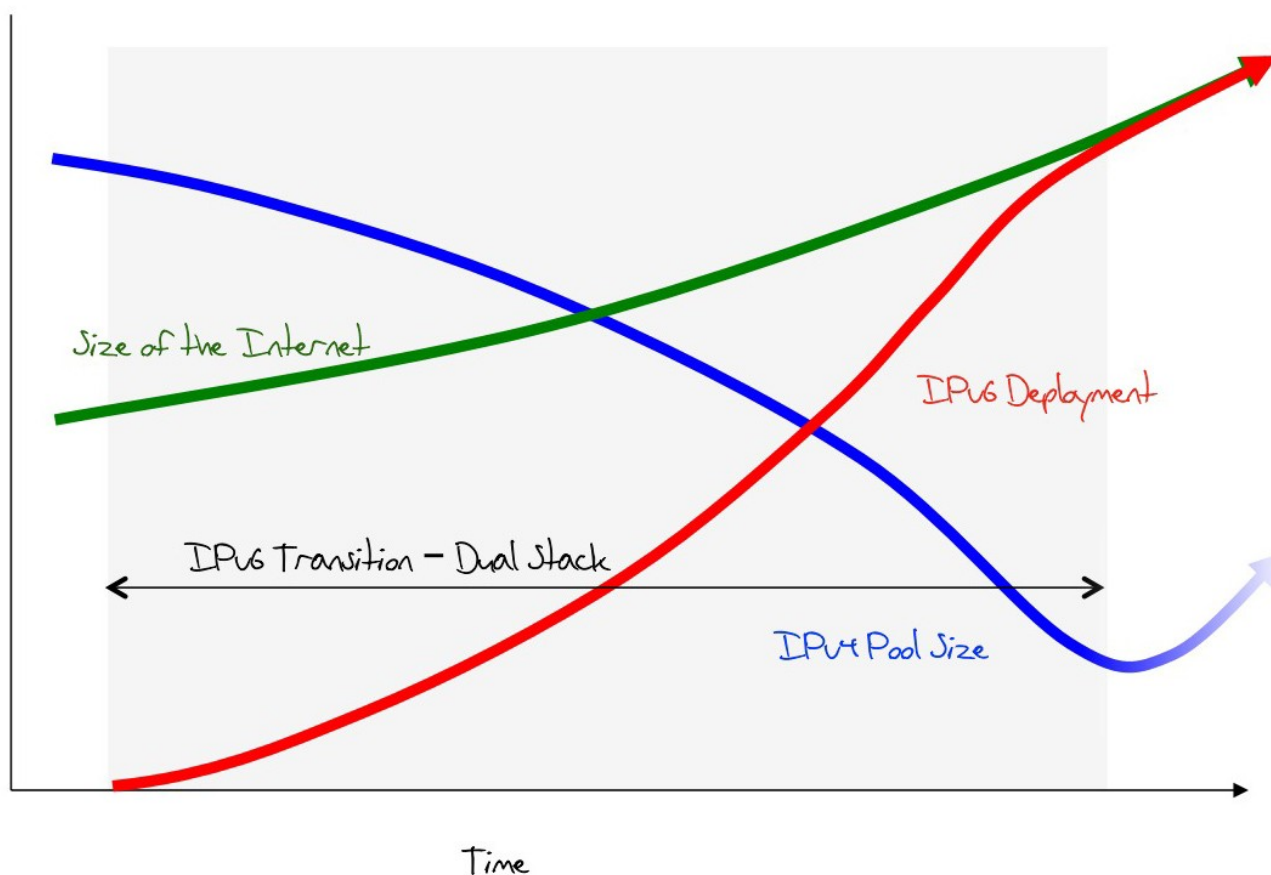
- **stavová – DHCPv6**
- některé pěkné vlastnosti (delegace prefixů)
- celkově ale velmi problematické
  - DUID místo MAC adresy
  - chybějící implicitní brána

# Mobilita

- koncepčně vyřešena lépe než v IPv4
- implementace vážnou
- LISP (Locator/Identifier Separation Protocol)  
možná pošle celý koncept mobility do důchodu

# Přechod z IPv4 (1)

- těžký zádrhel
- teorie:

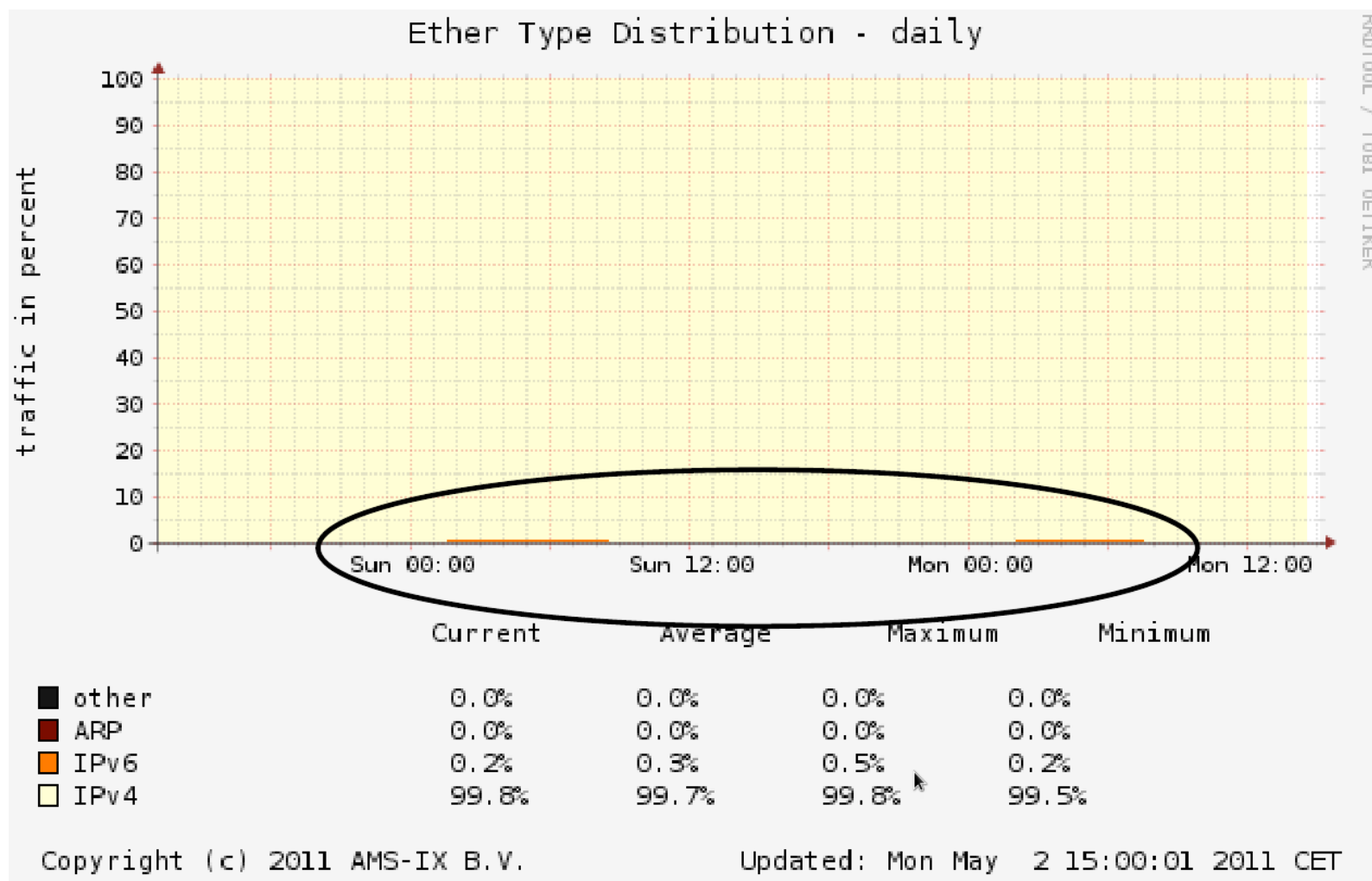


zdroj: Geoff Huston



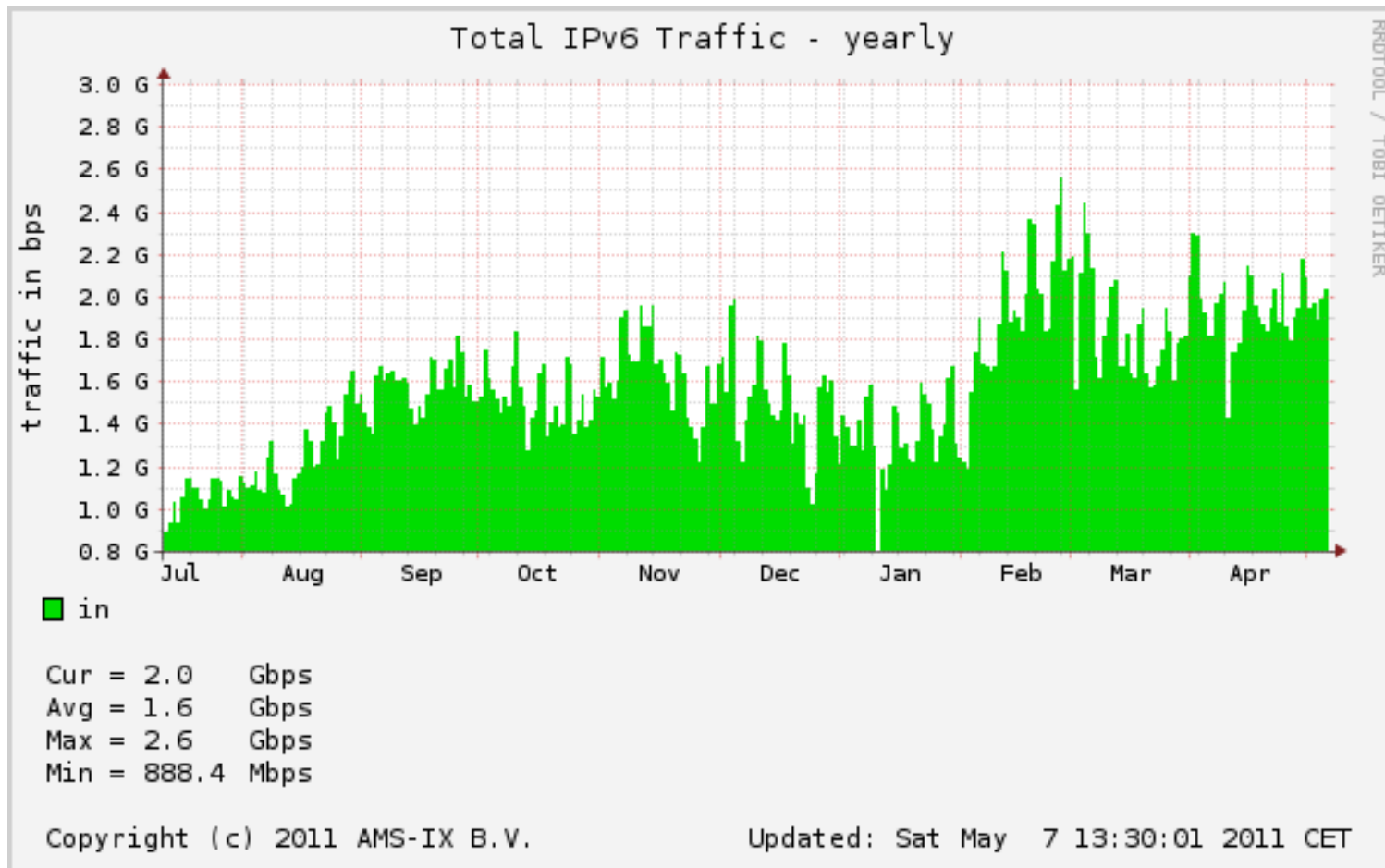
# Přechod z IPv4 (2)

- realita:



zdroj: AMS-IX

# IPv6 provoz (1)

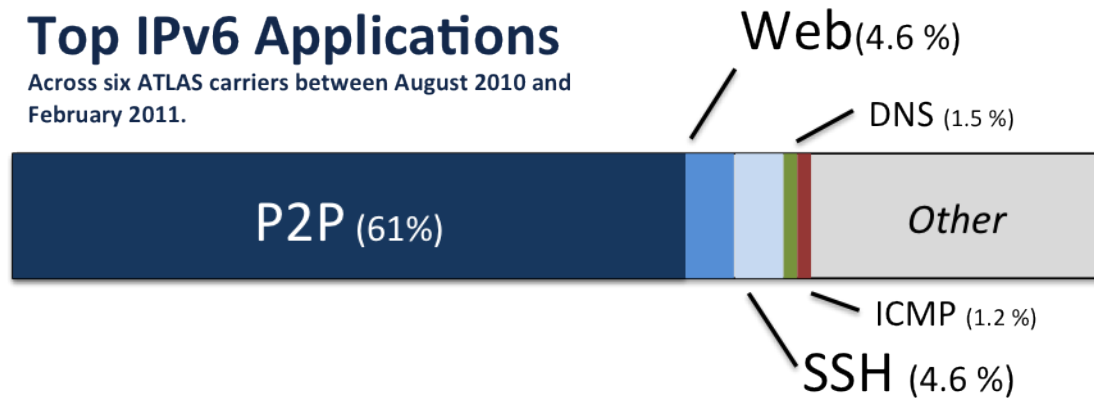


<http://www.ams-ix.net/sflow-stats/ipv6/>

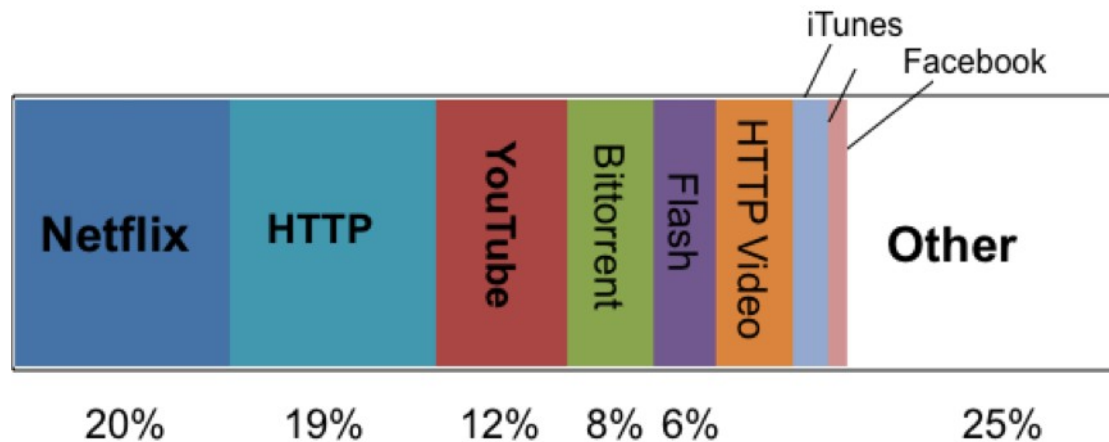
# IPv6 provoz (2)

## Top IPv6 Applications

Across six ATLAS carriers between August 2010 and February 2011.



**IPv6**



**IPv4**

<http://asert.arbornetworks.com/2011/04/six-months-six-providers-and-ipv6/>

# Přechodové mechanismy (1)

- cíl: usnadnit přechod z IPv4 na IPv6 a koexistenci obou protokolů
- 3 skupiny:
  - dual stack
  - tunelování
  - překlad
- **Máme víc přechodových mechanismů než IPv6 paketů.** (Randy Bush)

# Přechodové mechanismy (2)

- **dual stack**
  - podpora obou protokolů
  - standardní řešení současnosti, funguje
  - neodstraňuje potřebu IPv4
- **manuální tunely**
  - poměrně funkční a spolehlivé
  - vyžaduje aktivitu uživatele
  - neškáluje

# Přechodové mechanismy (3)

## ■ 6to4

- automatické tunelování IPv6 sítí IPv4 Internetem
- strašlivá nespolehlivost (kolem 15 %)
- zvažuje se odmítnutí (draft-ietf-v6ops-6to4-to-historic)

## ■ 6rd

- vycházející hvězda, staví na 6to4
- vše pod kontrolou jednoho ISP – předvídatelnější a spolehlivější
- potřebuje IPv4 síť – neřeší vyčerpání IPv4 adres

# Přechodové mechanismy (4)

## ■ Teredo

- automatické tunelování IPv6 z koncových počítačů
- počítá s NATy
- ještě strašlivější nespolehlivost (kolem 40 %), navíc velmi pomalé

## ■ NAT-PT

- překlad IPv6 na IPv4 a naopak – vzájemné zpřístupnění
- řada provozních problémů
- zavrženo 2007 (RFC 4966)

# Problém motivace

- **proti**
  - všechny služby jsou dostupné po IPv4
  - čistě IPv6 zákazník uvidí jen zlomek Internetu
- **pro**
  - IPv4 adresy reálně docházejí
  - IPv4 síť se komplikuje (stále více NATů)
- aktuální potřeba:  
zpřístupnit IPv6 zákazníkům IPv4 služby



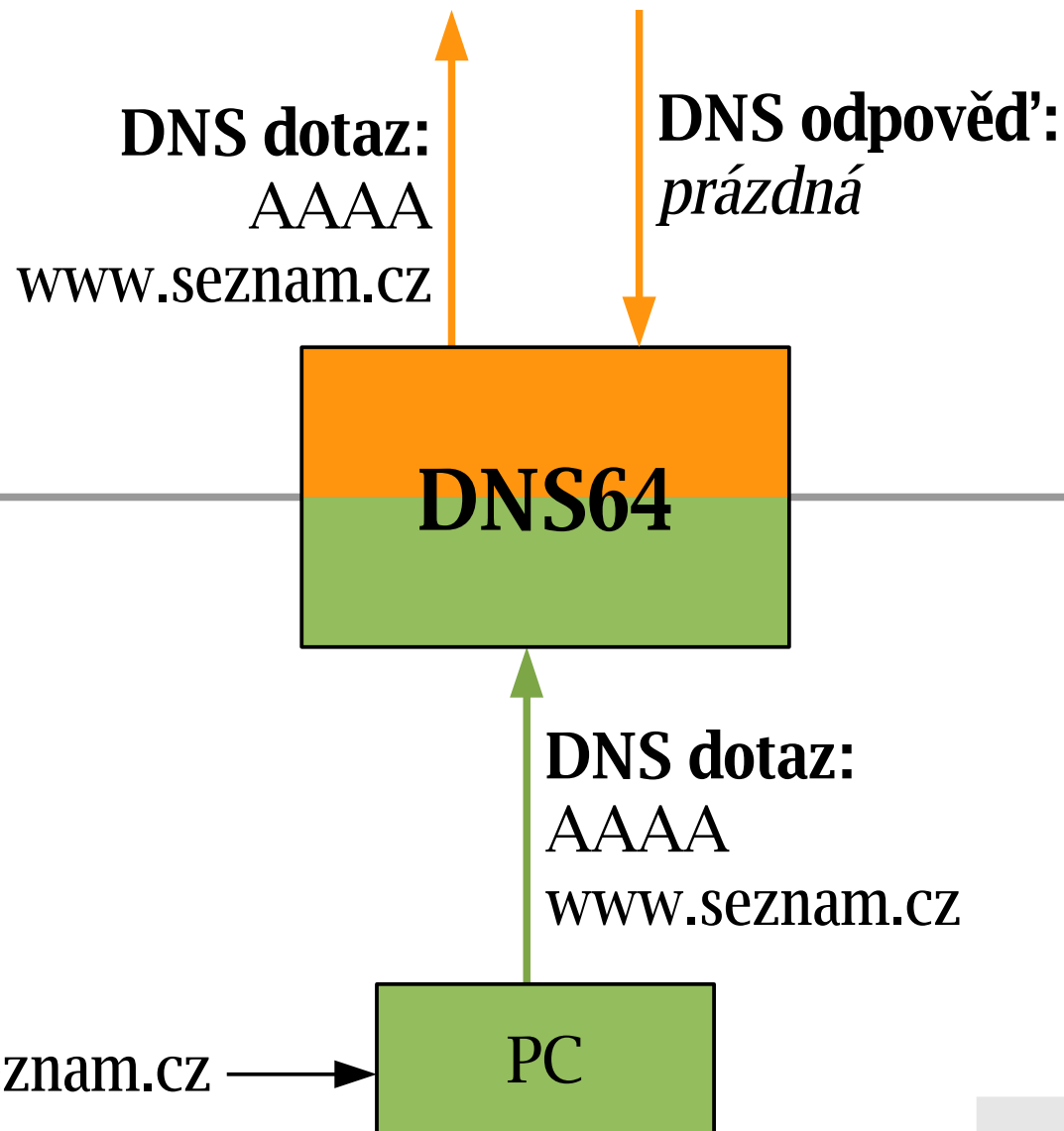
# Pracovní skupiny IETF

- IPv6 Maintenance (**v6man**) – protokoly
- IPv6 Operations (**v6ops**) – provoz
- Behavior Engineering for Hindrance Avoidance (**Behave**) – překlad protokolů, NAT64
- **Softwires** – tunelování, Dual-Stack Lite
- Site Multihoming by IPv6 Intermediation (**Shim6**)
- IPv6 over Low Power WPAN (**6lowpan**)

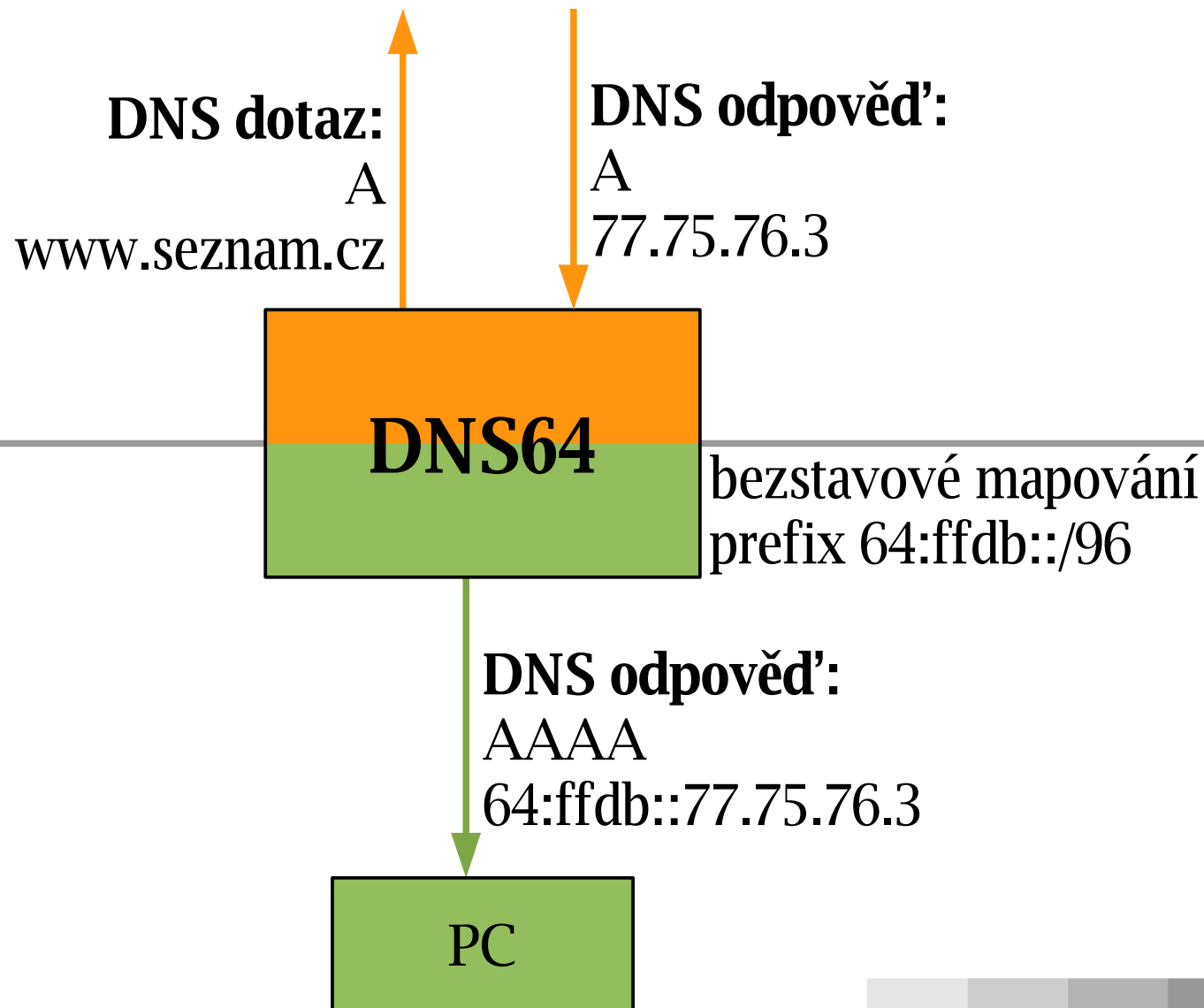
# NAT64 + DNS64 (1)

- překlad datagramů mezi IPv6 a IPv4
- cíl: zpřístupnit IPv6 klientům IPv4 služby (a v omezené míře i opačně)
- RFC 6144 – obecný rámec
- RFC 6145 – překlad datagramů
- RFC 6146 – NAT64
- RFC 6147 – DNS64

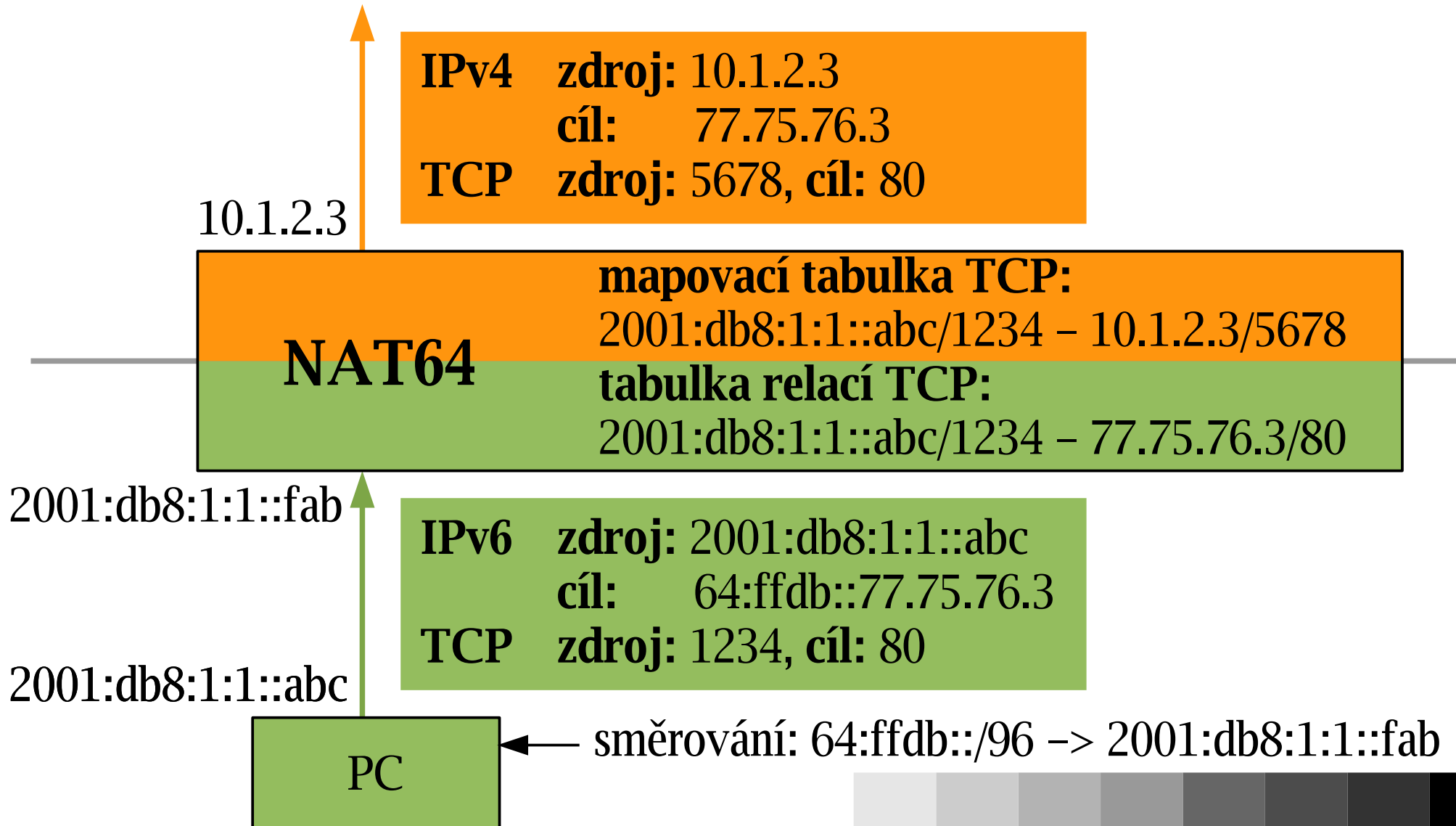
# NAT64 + DNS64 (2)



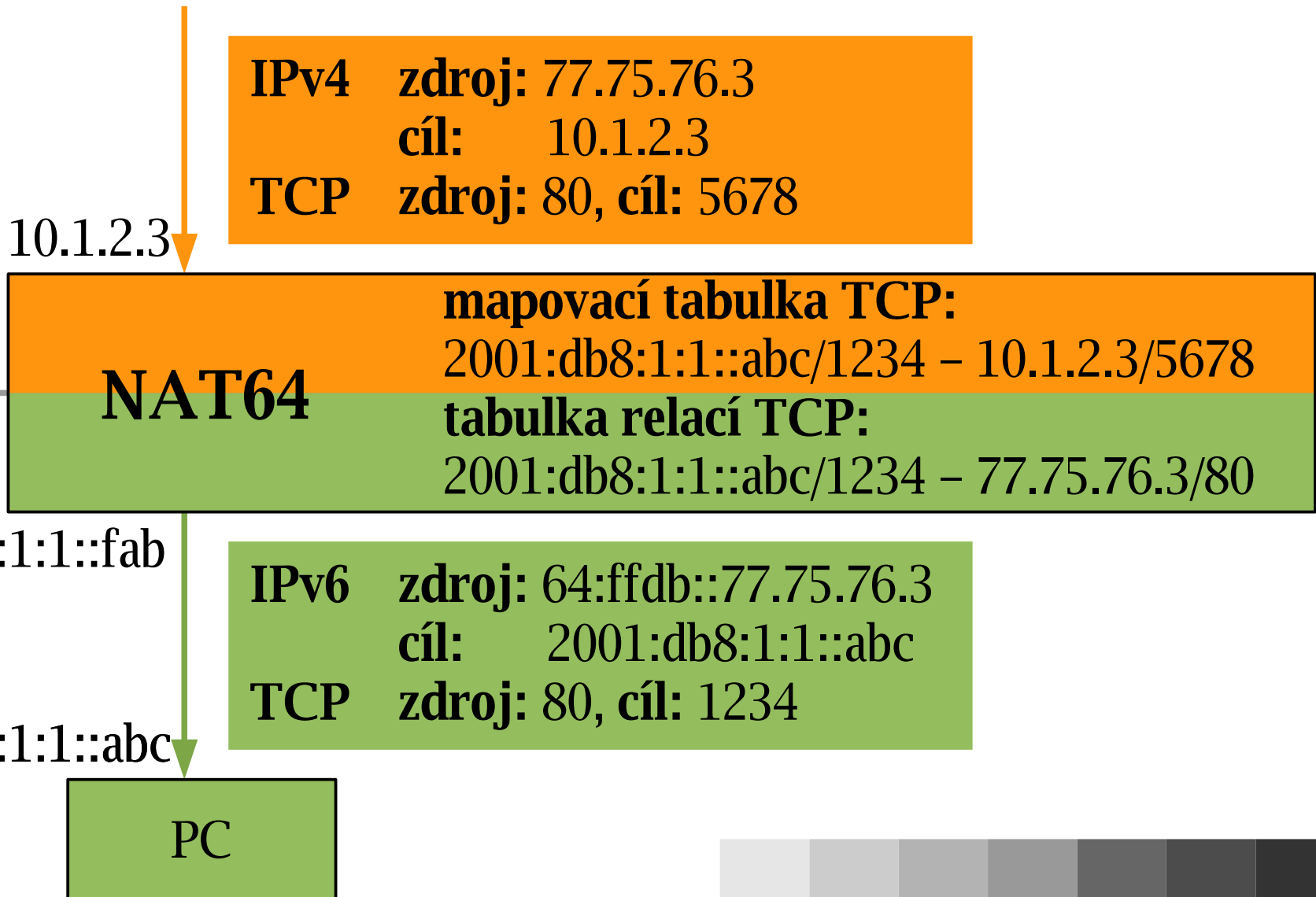
# NAT64 + DNS64 (3)



# NAT64 + DNS64 (4)



# NAT64 + DNS64 (5)



# NAT64 + DNS64 (6)

- asymetrické
  - mapování IPv4 do IPv6 staticky (prefix)
  - mapování IPv6 do IPv4 dynamicky (překládová tabulka)
- NAT64 a DNS64 nemusí běžet na stejném stroji
- bezproblémově lze navázat spojení jen z IPv6 (protější směr lze pevnými položkami v tabulce)
- podporuje jen protokoly UDP, TCP, ICMP
- počítá se i s filtrováním a dalšími obvyklými vlastnostmi NATů

# Dual-Stack Lite (1)

- domácí síť bude provozovat oba protokoly
  - IPv4 nejspíš s neveřejnými adresami
- páteřní síť poskytovatele je jen IPv6
- IPv4 bude tunelováno v IPv6 a dopraveno na centrální NAT
  - nepřekládá protokoly, jen adresy
  - identifikace zákaznického stroje podle jeho neveřejné IPv4 adresy a IPv6 adresy přístupového směrovače – umožňuje kolidující adresní rozsahy



# Dual-Stack Lite (2)

IPv6 zdroj: 2001:db8:5:ff::cd  
cíl: 2001:db8:5:ff::1

IPv4 zdroj: 10.5.6.1  
cíl: 77.75.76.3  
TCP zdroj: 1234, cíl: 80

IPv4 zdroj: 147.230.1.2  
cíl: 77.75.76.3  
TCP zdroj: 5678, cíl: 80

147.230.1.2

domácí  
směrovač

2001:db8:5:ff::1

2001:db8:5:ff::cd

mapovací tabulka TCP:

2001:db8:5:ff::cd,  
10.5.6.1/1234 - 147.230.1.2/5678

centrální NAT

10.5.6.1

IPv4 zdroj: 10.5.6.1  
cíl: 77.75.76.3  
TCP zdroj: 1234, cíl: 80

10.5.6.3

PC

# Prosadí se IPv6?

- **uživatelé IPv6 nesmí být znevýhodněni**
  - přístup k IPv4 zdrojům
  - srovnatelný výkon (u nativního je už dnes)
- **poskytovatelům se musí vyplatit**
  - poroste cena IPv4 – nákupy adres, složitá síť
  - náklady IPv6 nejsou dramatické
    - nový HW obvykle umí IPv6
    - školení personálu, konfigurace

# Co s tím?

- tunelování a překlady jsou problematické, nejlépe se chová nativní protokol
- nasad'te **dual stack** (čím dříve, tím lépe)
- funguje, provozujeme v síti TU v Liberci cca 5 let
- pomocí DNS si říd'te přístup
- několik let máme AAAA pro DNS, WWW i mail

Děkuji za pozornost.

Dotazy?