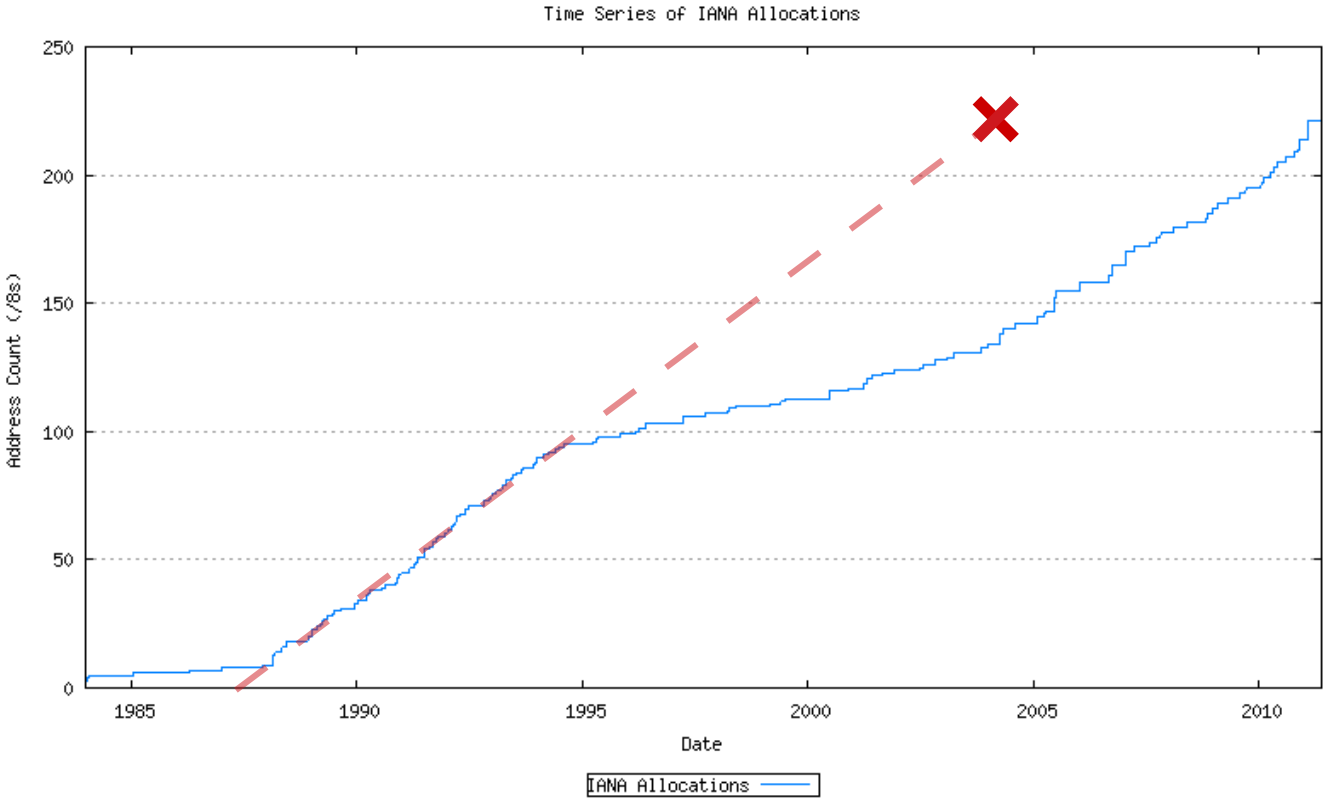
IP verze 6

Motivace

- počátek 90. let – zjevný nedostatek IPv4 adres
- opět aktuální



ipv4.potaroo.net

Vyčerpání adres

- IANA: únor 2011
- RIR
  - APNIC: duben 2011
  - RIPE NCC: září 2012
  - LACNIC: červen 2014
  - ARIN: září 2015
  - AFRINIC: duben 2017

Vlastnosti IPv6

- rozhodnuto zahájit vývoj nového protokolu, cíle:
  - dostatek adres (pokud možno navždy)
  - hierarchické směrování a adresace
  - zvýšení bezpečnosti (šifrování a autentizace přímo v IP)
  - služby se zajištěnou kvalitou
  - vysokorychlostní směrování
  - podpora mobilních zařízení
  - automatická konfigurace

IPv6 datagram

<table>
<tr><td>verze</td><td>třída provozu</td><td colspan="3">značka toku</td></tr>
<tr><td colspan="2">délka dat</td><td colspan="2">další hlavička</td><td>max. skoků</td></tr>
<tr><td colspan="5">adresa odesilatele</td></tr>
<tr><td colspan="5">cílová adresa</td></tr>
</table>

Položky hlavičky

- RFC 8200
- **verze:** identifikuje verzi protokolu
- **třída provozu:** pro služby s definovanou kvalitou
- **značka toku:** identifikuje tok (proud souvisejících datagramů) pro vysokorychlostní směrování
- **délka dat:** počet bajtů za hlavičkou
- **další hlavička:** řetězení hlaviček (viz dále)
- **max. skoků:** analogie TTL, omezuje dosah

IPv4 datagram

<table>
<tr><td>verze</td><td>délka hlavičky</td><td>TOS</td><td colspan="2">celková délka [B]</td></tr>
<tr><td colspan="3">identifikátor</td><td>přízn.</td><td>posun fragmentu</td></tr>
<tr><td colspan="2">TTL</td><td>protokol</td><td colspan="2">CRC hlavičky</td></tr>
<tr><td colspan="5">odesilatel (IP adresa)</td></tr>
<tr><td colspan="5">adresát (IP adresa)</td></tr>
<tr><td colspan="5">volby (nepovinné, proměnlivé složení)</td></tr>
<tr><td colspan="5">data</td></tr>
</table>

Řetězení hlaviček

- délka hlavičky je konstantní (40 B) – urychluje zpracování
- případné **volitelné hlavičky** se připojují za ni
- položka **další hlavička** určuje typ hlavičky, která následuje, nebo protokol vyšší vrstvy
- každá rozšiřující hlavička obsahuje položku další hlavička – co je za ní
- pořadí hlaviček urychluje zpracování

Příklad řetězení

základní hlavička další = 44 (Fragmentace)
hlavička Fragmentace další = 60 (Volby pro cíl)
hlavička Volby pro cíl další = 6 (TCP)
TCP data

Problémy řetězení hlaviček

- **zneužitelné**
  - dlouhé řetězce hlaviček zatěžují
  - RFC 7112: všechny hlavičky v prvním fragmentu
- zvyšují pravděpodobnost, že **datagram nedojde**
  - firewally a různé nestandardní prvky
  - výsledky měření v RFC 7872 velmi depresivní – ztrátovost v řádu desítek procent

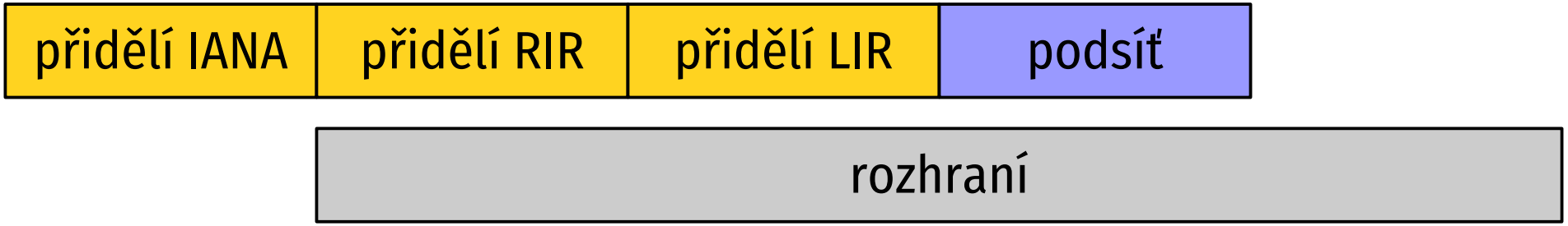
Adresy v IPv6

- délka 128 bitů (16 bajtů)
- zápis v šestnáctkové soustavě, čtveřice číslic odděleny dvojtečkou
- **2001:0718:1c01:0005:020b:dbff:fea1:d52c**
- úvodní nuly ve čtveřici lze vynechat
- jednu skupinu nulových čtveřic lze vynechat a nahradit dvěma dvojtečkami (např. smyčka je ::1)
- prefixy v obvyklém tvaru 2001:718::/32

Typy adres

- 3 typy adres:
- **individuální (unicast)**
  - určují jedno rozhraní
- **skupinové (multicast)**
  - určují skupinu rozhraní, data se doručují všem
- **výběrové (anycast)**
  - určují skupinu rozhraní, data se doručují nejbližšímu členovi

Globální individuální adresy



- první tři bity 001 (binárně)
- na začátku je **globální směrovací prefix**, politiku určují RIR (doporučeno: 48 b)
- identifikátor **podsítě** (zbytek do 64 b)
- identifikátor **rozhraní** (64 b)

Identifikátor rozhraní

- původně: vycházel z MAC adresy
  - modifikované EUI-64
  - problém: uživatele lze sledovat
- **krátkodobé náhodné adresy** (RFC 4941)
  - problém pro správce sítí
- **stabilní náhodné adresy** (RFC 7217)
  - hash z několika údajů (včetně prefixu)
  - stabilní, ale v různých sítích jiný – doporučeno

Objevování sousedů

- **Neighbor Discovery, ND**
- nahrazuje ARP + další možnosti
- **hledání linkové adresy:**
  - pošle **výzvu sousedovi** na skupinovou adresu s prefixem ff02:0:0:0:0:1:ff00::/104, k němuž připojí posledních 24 b hledané adresy (adresa pro vyzývaný uzel)
  - oslovený pošle **ohlášení souseda**
  - vyzyvatel si zapíše do **cache sousedů** (a udržuje si zde informaci o jeho dosažitelnosti)

Automatická konfigurace

- **stavová (DHCPv6)**
  - podobně jako v IPv4 (pošle dotaz, server odpoví)
- **bezstavová (SLAAC)**
  - vše si obstará sám
  - východiskem **ohlášení směrovače** obsahující prefixy adres a jeho ochotu být implicitním směrovačem
  - počítač přidá své rozhraní k prefixu, ověří (objevováním sousedů) zda je volná a příp. začne používat
  - udržuje si tabulku implicitních směrovačů a střídá je

Směrovací protokoly

- nic speciálního, adaptace existujících protokolů
- **RIPng**
  - RIPv2 upravený pro IPv6 adresy
- **OSPFv3**
  - univerzální pro IPv4 i IPv6
- **BGP4+**
  - jediný používaný externí směrovací protokol (mezi autonomními systémy)

DNS

- záznamy **AAAA** pro IPv6 adresy
  - pc AAAA 2001:718:1c01:5:20b:dbff:fea1:d52c
- **reverzní:**
  - šestnáctkový zápis adresy včetně nul se obrátí
  - každá číslice se stává doménou
  - přípona **ip6.arpa**
  - c.2.5.d.1.a.e.f.f.f.b.d.b.0.2.0.5.0.0.0.1.0.c.1.8.1.7.0.1.0.0.2.ip6.arpa

IPsec

- bezpečnostní mechanismy, dvě rozšiřující hlavičky:
- **Authentication Header (AH)**
  - ověření odesilatele
  - ochrana před změnou obsahu a opakováním
- **Encapsulating Security Payload (ESP)**
  - navíc šifrování obsahu – zašifruje vše za sebou
  - povinná a preferovaná
- databáze bezpečnostní politiky určuje pravidla pro zpracování datagramů

Mobilita

- mobilní počítač má domácí síť (zde je veden v DNS)
- po dobu nepřítomnosti jej zastupuje **domácí agent**
- pošle-li někdo datagram adresovaný cestujícímu počítači, domácí agent jej předá ESP tunelem
- mobilní počítač provede **optimalizaci cesty** – ohlásí partnerovi, že jeho aktuální adresa je jiná
- po optimalizaci budou data přenášena přímo

Přechodové mechanismy

- jak přejít od IPv4 k IPv6
- problém: IPv6 není zpětně kompatibilní
- **dual-stack** – podporují se oba protokoly, dnes nejčastější
- **tunelování** – oba konce hovoří stejným protokolem, sít mezi nimi ne
- **překlad** – datagramy se překládají z jednoho do druhého a naopak

Tunelování

- jeden protokol zabalen do druhého, přenesen „cizí“ sítí a na druhém konci vybalen
- statické tunely (tunel servery apod.)
- **6rd** – automatické, z jedné IPv4 adresy se vytvoří prefix pro adresování celé IPv6 sítě, RFC 5969
- **DS-Lite** – páteřní síť poskytovatele jen IPv6, IPv4 (s neveřejnými adresami) se zákazníkům doručuje tunely na centrální IPv4 NAT, RFC 6333

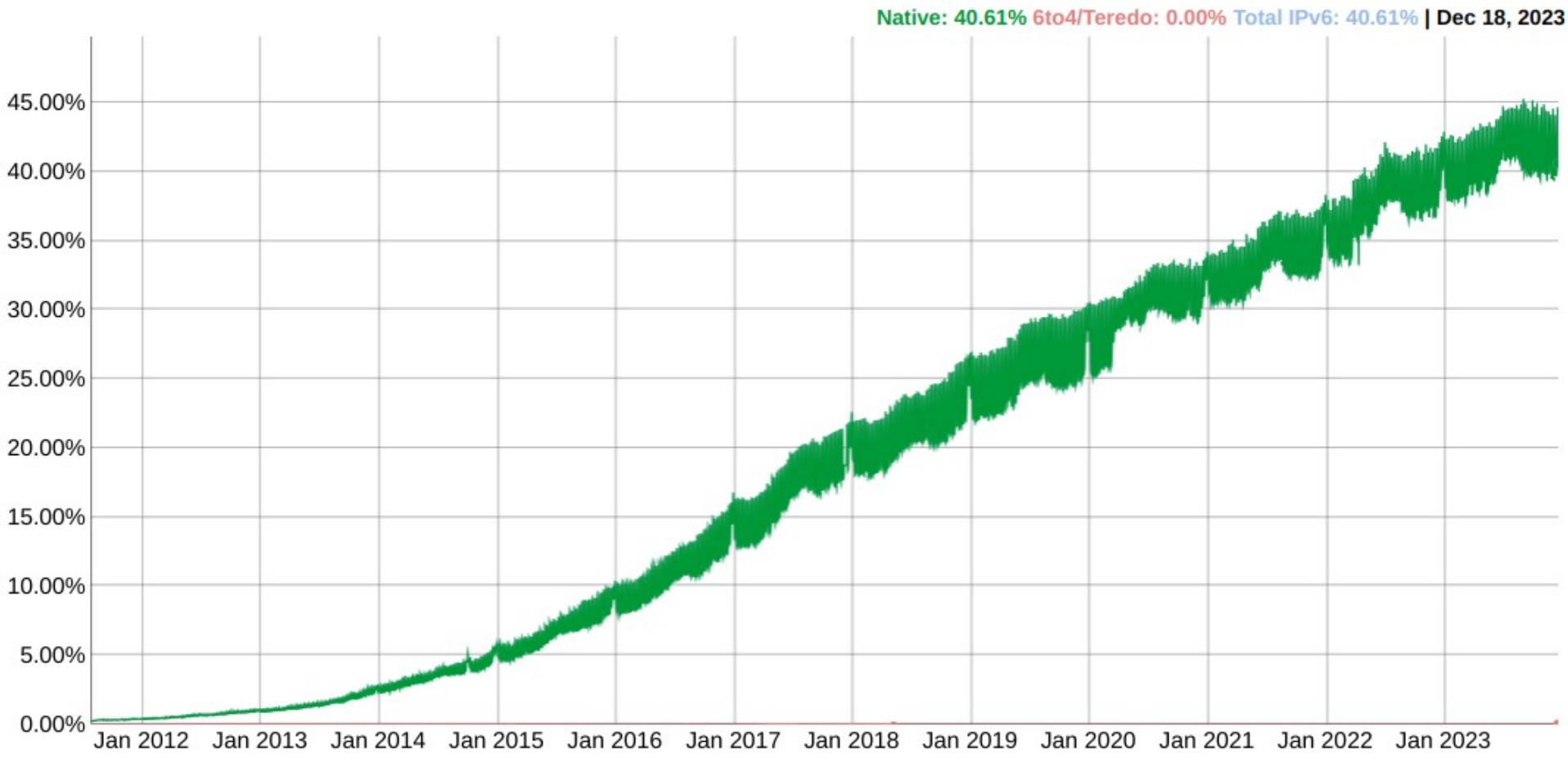
Překlad

- **SIIT** – pravidla, jak překládat kterou položku, neřeší adresy, využíváno ostatními, RFC 6145
- **NAT64 + DNS64** – překlad adres podobný IPv4 NATu, jednosměrné (přístup z koncové IPv6 sítě do IPv4 Internetu), RFC 6146 a 6147
- **464XLAT** – dvojitý překlad, páteřní síť poskytovatele jen IPv6, IPv4 se u zákazníka přeloží na IPv6 a na centrálním zařízení zpět do IPv4, používá T-Mobile v USA (70 mil. zákazníků), RFC 6877

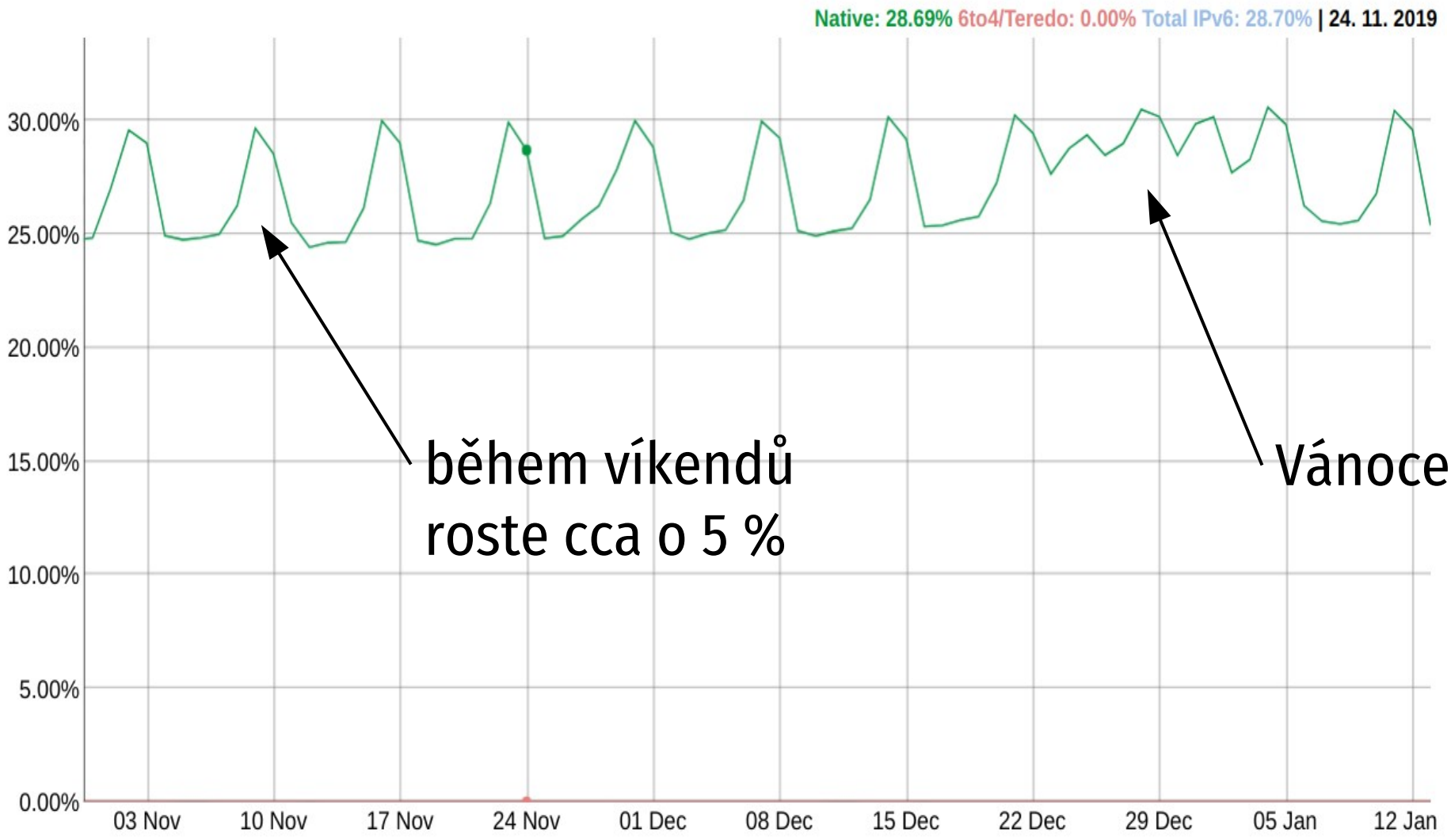
IPv6 v praxi

- Internet měl už dávno používat IPv6
- podporováno všemi současnými platformami
- dlouho se motalo v kruhu
  - proč bychom zpřístupňovali služby, když nejsou uživatelé
  - proč bychom doručovali uživatelům, když nejsou služby
- obavy z technických problémů
- World IPv6 Launch – 8. 6. 2011, nasadili velcí hráči (Google, Facebook, Akamai,...)

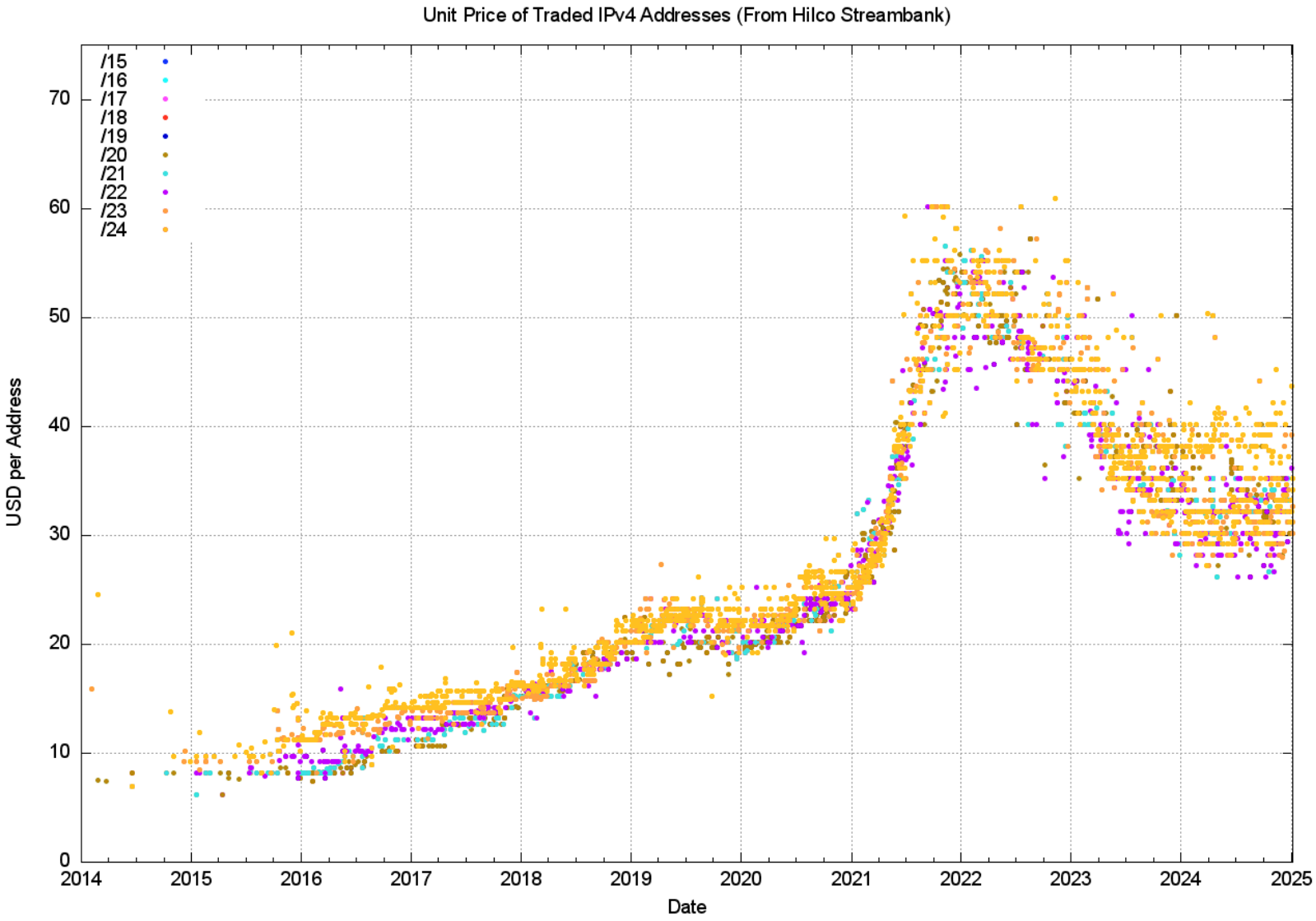
Statistika Google



Firmy jsou konzervativní



Cena IPv4 adresy

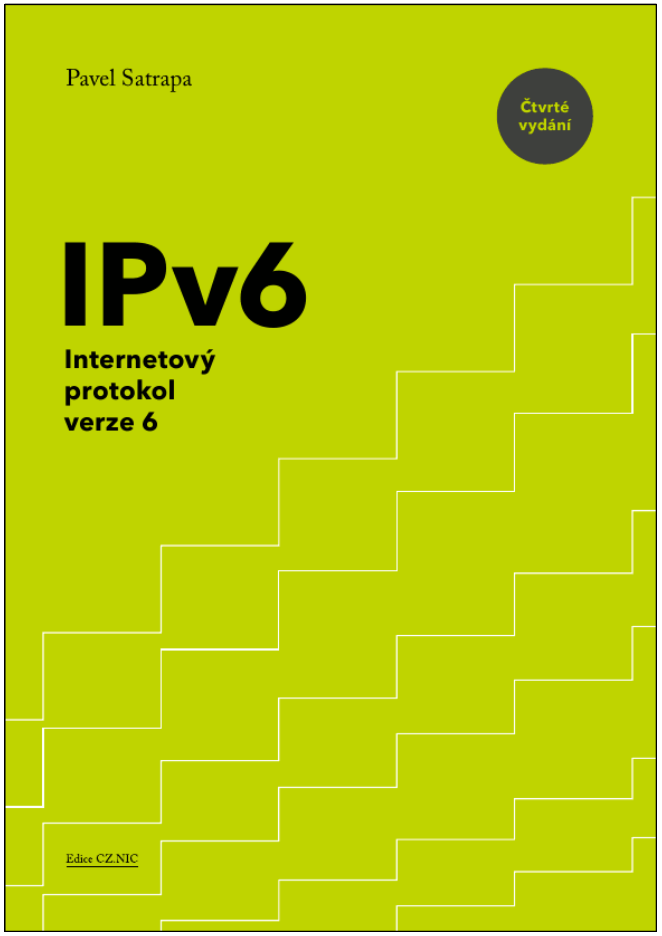


https://www.potaroo.net/ispcol/

Podrobněji

P. Satrapa: IPv6

knihy.nic.cz



vytvořeno s podporou
projektu ESF