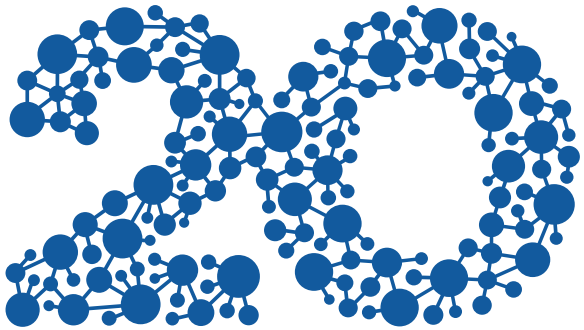
Dual-stack jako řešení přechodu?

Ondřej Caletka



1996–2016
CESNET
SPOLUPRÁCE
VÝZKUM
KOMUNITA

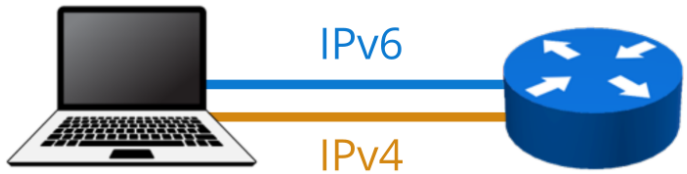
6. června 2016

Přecházíme na IPv6

- nový protokol síťové vrstvy
- ostatní vrstvy zůstávají nedotčeny
- může koexistovat s IPv4

Best transition mechanism?

Dual Stack



Zdroj: RIPE NCC IPv6 training

1996–2016 CESNET

Nevýhody dual-stack přístupu

- **všechno dvakrát**
  - adresování
  - konfigurace služeb
  - firewally
  - **dohled**
  - řešení problémů uživatelů
- práce navíc, kterou málo kdo ocení
  - nejdříve zprovozňujeme IPv4
  - podporu IPv6 doplňujeme *později*
  - když nenajdeme čas, služba běží na IPv4-only
  - často netestujeme funkčnost bez IPv4
- nelze využít výhod IPv6 nekompatibilních s IPv4

Klasifikace single-stack protokolů

IPv4 s překládaným IPv6

obecně nelze

IPv4 s tunelovaným IPv6

- 6to4
- Teredo
- 6rd

IPv6 s překládaným IPv4

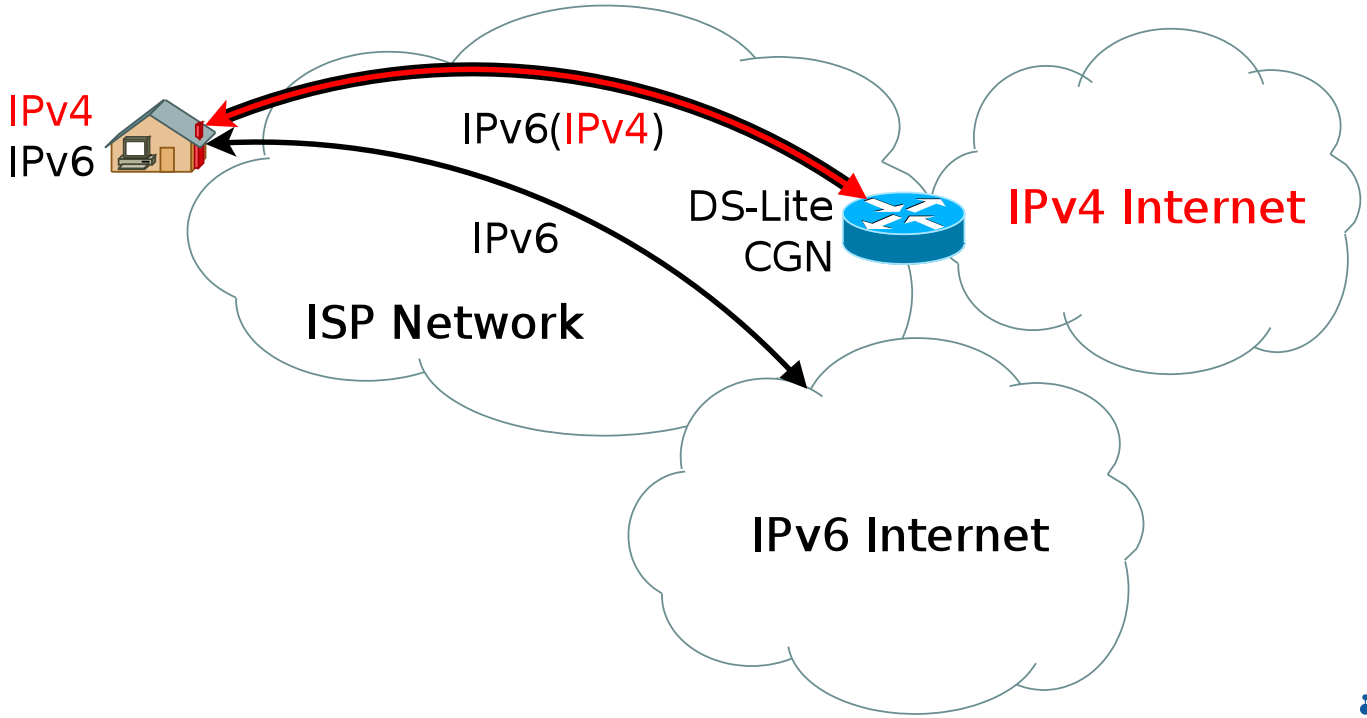
- NAT64
- 464XLAT
- MAP-T
- SIIT-DC

IPv6 s tunelovaným IPv4

- DS-Lite
- MAP-E
- lw4over6

Dual-stack lite

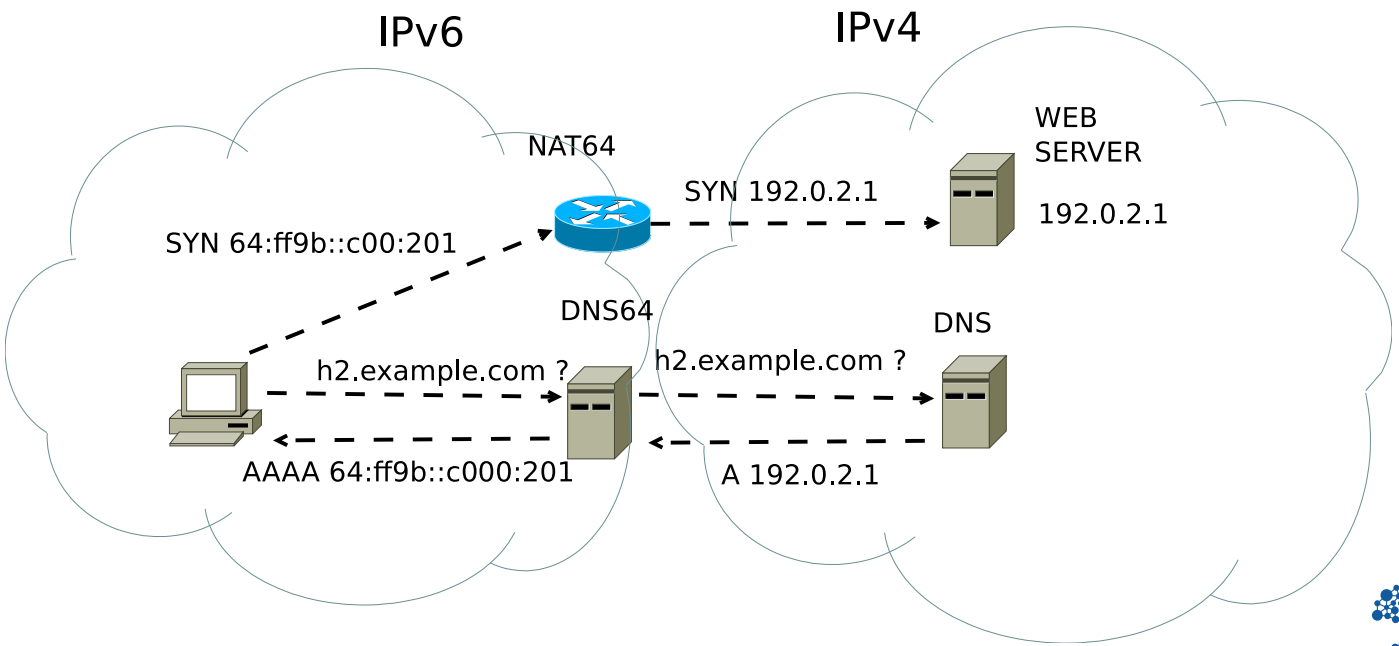
- IPv4 provoz klienta je tunelován IPv6-only přístupovou sítí k *Address Family Translation Router*
- eliminuje NAT u klienta a dual-stack v přístupové síti
- používaný nejčastěji v DOCSIS (v Německu)



Zdroj: Wikimedia commons

NAT64

- překlad části IPv6 adresního prostoru do IPv4
- při použití DNS64 nevyžaduje úpravy na straně většiny klientů (veškerý obsah se zdá být dostupný prostřednictvím IPv6)
- používán nejčastěji v mobilních sítích (Slovinsko, USA, Polsko, Norsko…)



Zdroj: Wikimedia commons

Problémy NAT64/DNS64

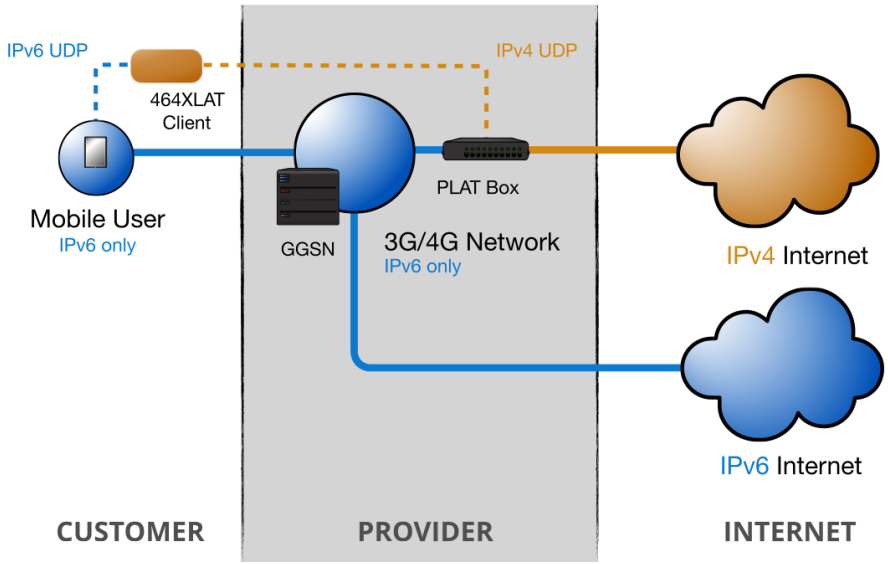
- klientská aplikace musí podporovat IPv6
  - vyžadováno v iOS App Store od 1. 6. 2016
- je nutné používat DNS jména
- vyžaduje *Application Layer Gateway* pro protokoly jako FTP, SIP,...
  - stejně jako u NAT44
- problematická kombinace DNS64 s validací DNSSEC
  - syntézu je třeba dělat až po validaci
  - problém zjištění použitého prefixu
  - nejde o zdaleka největší problém validace DNSSEC na koncovém bodu

Volba prefixu NAT64

- síťově specifický prefix (NSP)
  - možnost použití více nezávislých překladačů
  - možnost překládat RFC1918 adresy
  - možnost použití na dálku
  - bezpečnostní konsekvence – obtížná validace prefixu, možnost vzdáleného zneužití
- dobře známý prefix (WKP) 64:ff9b::/96
  - preferované řešení pro obecné nasazení
  - neutrální ke kontrolním součtům TCP/UDP
  - pouze lokální použití
  - obtížnější vyvažování zátěže

464XLAT

- rozšíření NAT64 o druhý překladač u klienta
  - bezestavový překlad
  - nepotřebuje DNS64
  - potřebuje druhou IPv6 adresu
    - problém v DHCPv6-only sítích
  - kompatibilní s IPv4-only aplikacemi
  - implementován v Androidu (pro mobilní data)

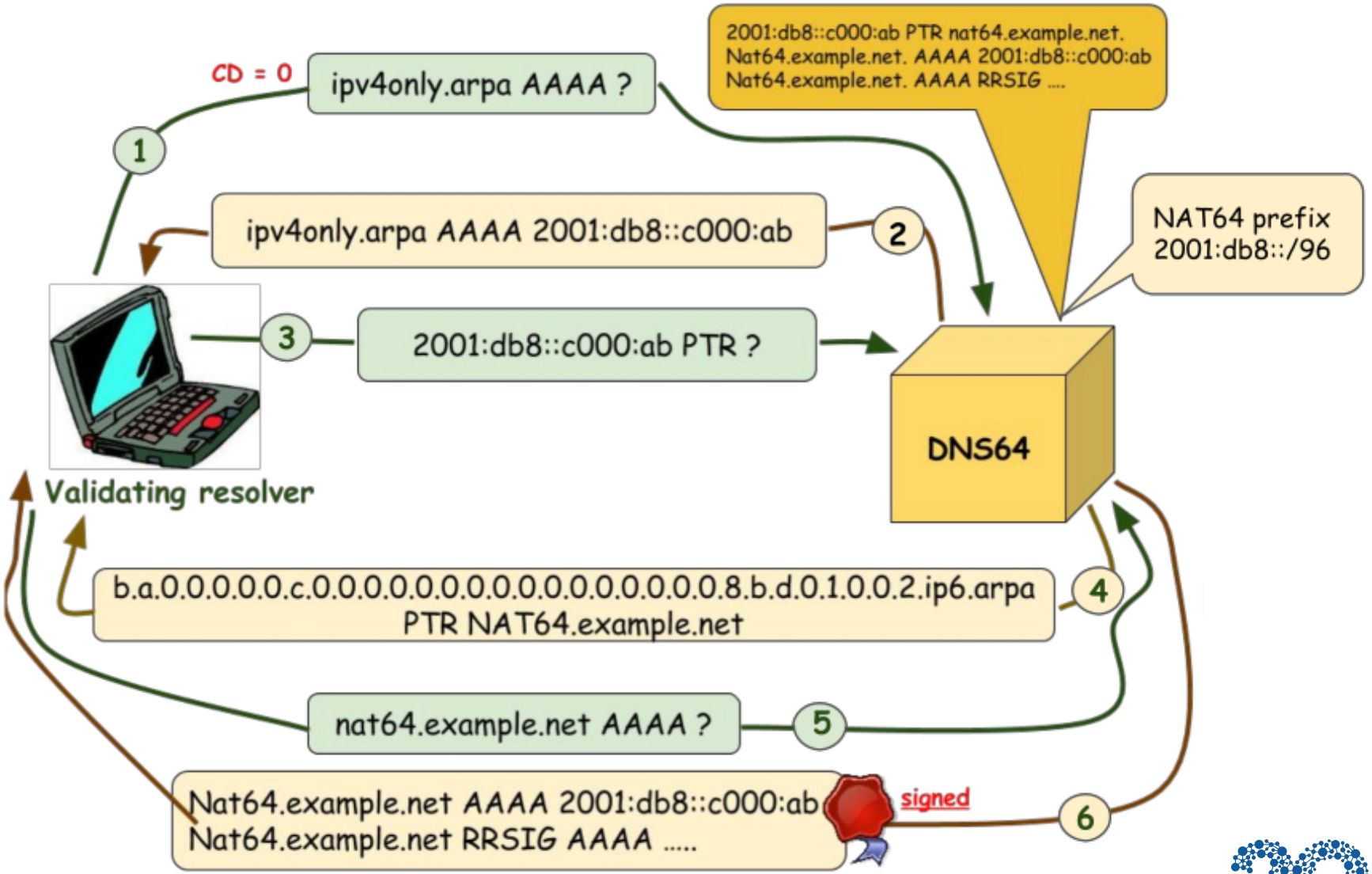


Zdroj: RIPE NCC IPv6 training

Detekce NAT64 prefixu klientem

- nutné pro konfiguraci CLAT a/nebo DNS64
- RFC 7051 navrhuje několik řešení:
  1. DNS dotaz na dobře známé jméno
  2. volba v rozšíření EDNS0
  3. volba v DHCPv6
  4. volba v ohlášení směrovače
  5. aplikační protokol typu STUN
- RFC 7050 popisuje řešení podle 1:
  1. dotaz na `ip4only.arpa IN AAAA`
  2. zjištění prefixu analýzou odpovědi
- nové bezpečnostní hrozby (odklonění IPv4 provozu do sítě útočníka) *při nesprávné implementaci detekce*

Validace NSP pomocí DNSSEC



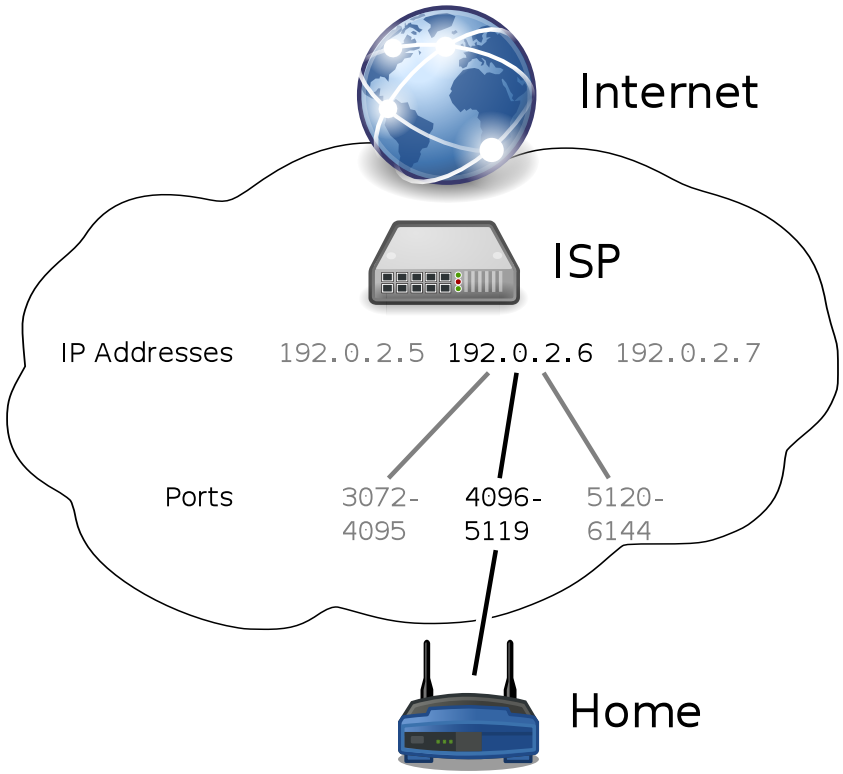
Zdroj: RIPE 72: IPv6-only and DNS[SEC|64]

NAT64 na vlastní kůži

- zde – TAYGA a Unbound na OpenWRT Chaos Calmer
- veřejné demo Go6 Lab
  - Ecdysis, PaloAlto Networks, Cisco ASR1000 na samostatných prefixech
  - stačí vypnout IPv4 a nastavit adresu DNS resolveru podle požadovaného NAT64 překladače
- Apple OS X 10.11 – option-click Internet Sharing
  - primárně pro vývojáře iOS aplikací
- clatd implementace CLAT pro Linux

Address plus Port (RFC 6346)

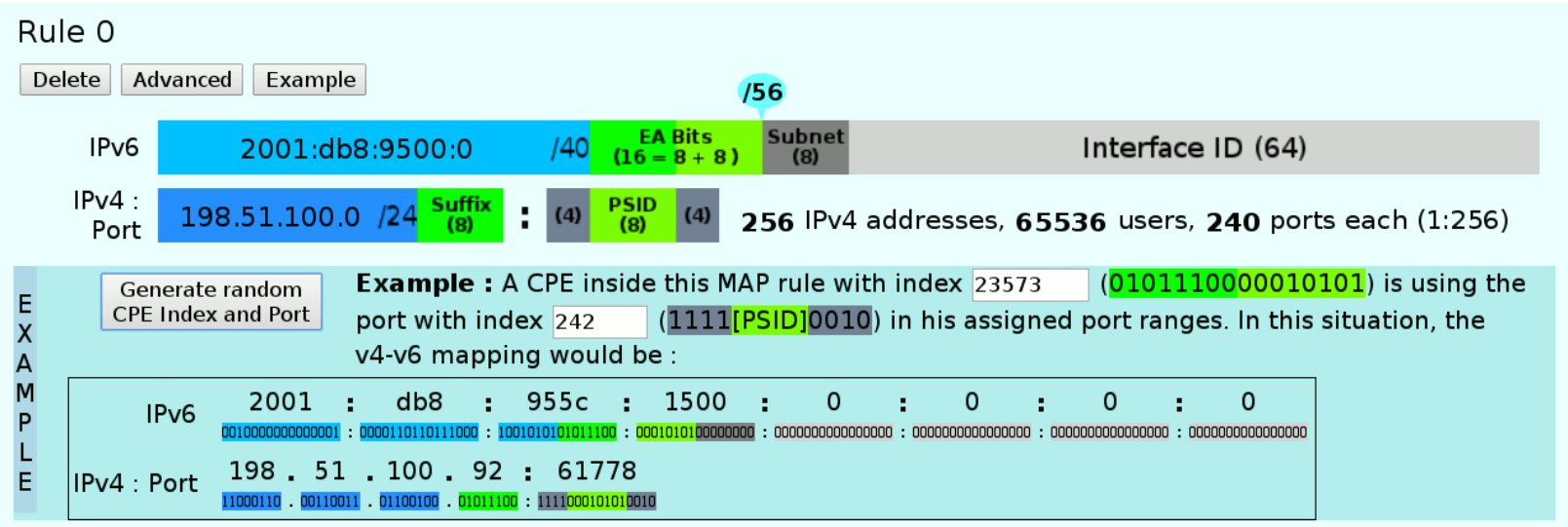
- šetření IPv4 adres při eliminaci CGN
- čísla portů TCP/UDP jako rozšíření IPv4 adresy
- implementace: MAP, 4rd, Lightweight 4over6



Zdroj: Wikimedia commons

Mapping of Address and Port (RFC 6346)

- implementace A+P od Cisco
- bezestavové směrování podle IPv4 adresy a portu
- varianty MAP-E (Encapsulation) a MAP-T (Translation)



Zdroj: `http://map46.cisco.com/`

4rd a lw4over6

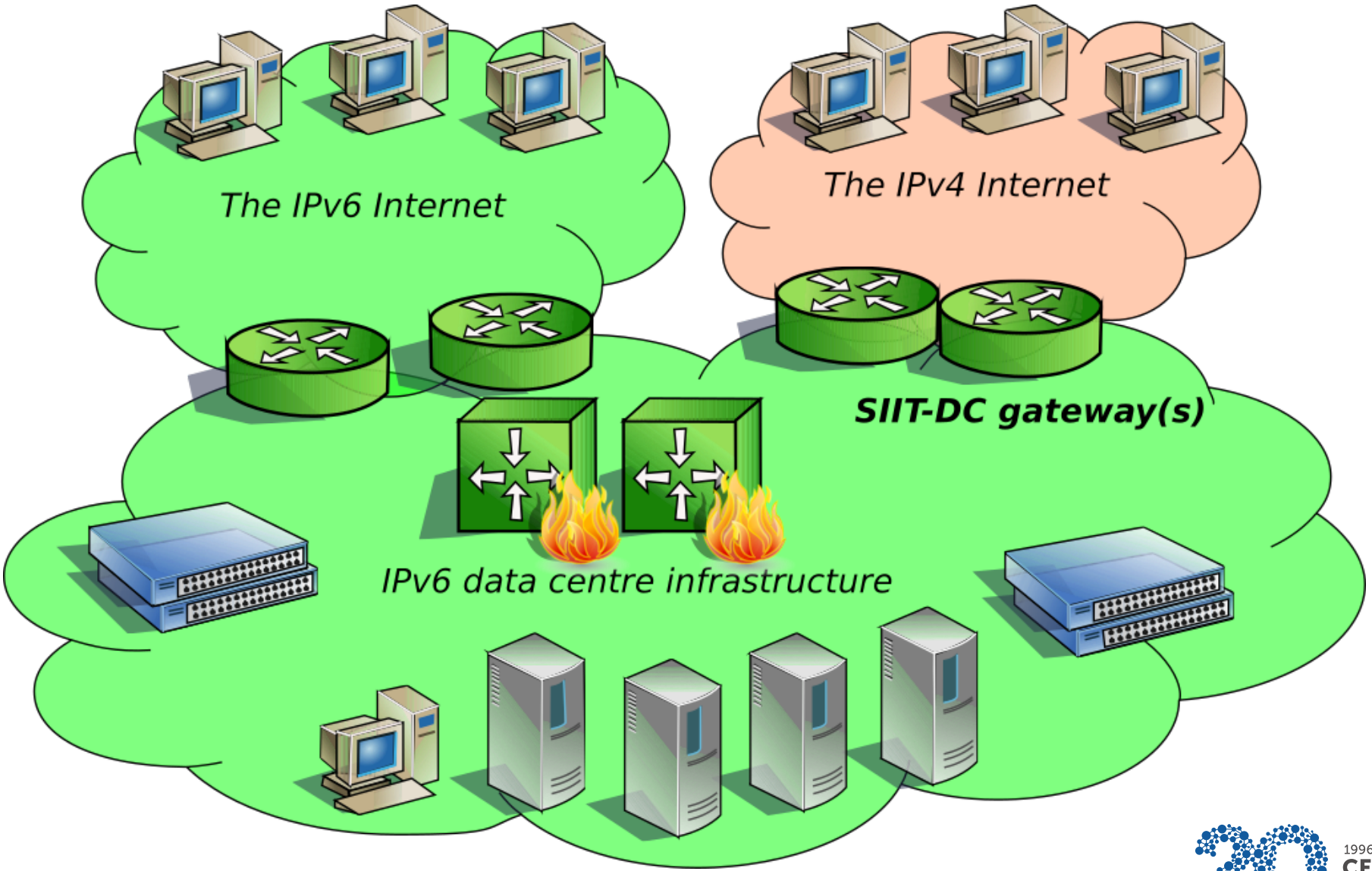
IPv4 Residual Deployment via IPv6 (RFC 7600)

- vychází z MAP-T – překladu IPv4 do IPv6
- přidává *Reversible Packet Translation* pro zachování většiny IPv4 parametrů
- experimentálně nasazeno u Free.fr

Lightweight 4over6 (RFC 7596)

- vychází z MAP-E/DS-Lite – tunelování IPv4 v IPv6
- stavové přidělování množiny portů klientům

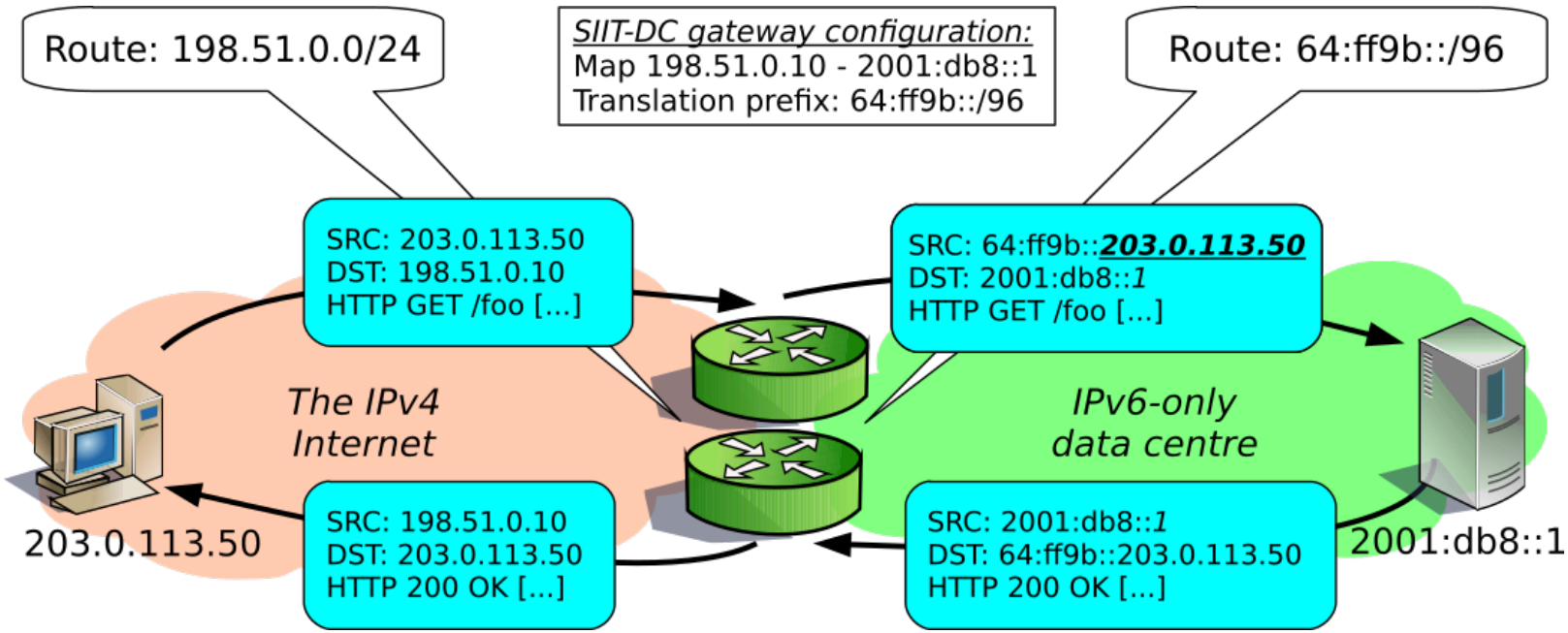
IPv6-only v datacentrech



Zdroj: RIPE72: SIIT-DC

SIIT-DC (RFC 7755)

- bezestavový překlad IPv4-IPv6 na hraně datacentra
- NAT64 s explicitním mapováním páru IPv4-IPv6
- pro klienty zcela transparentní



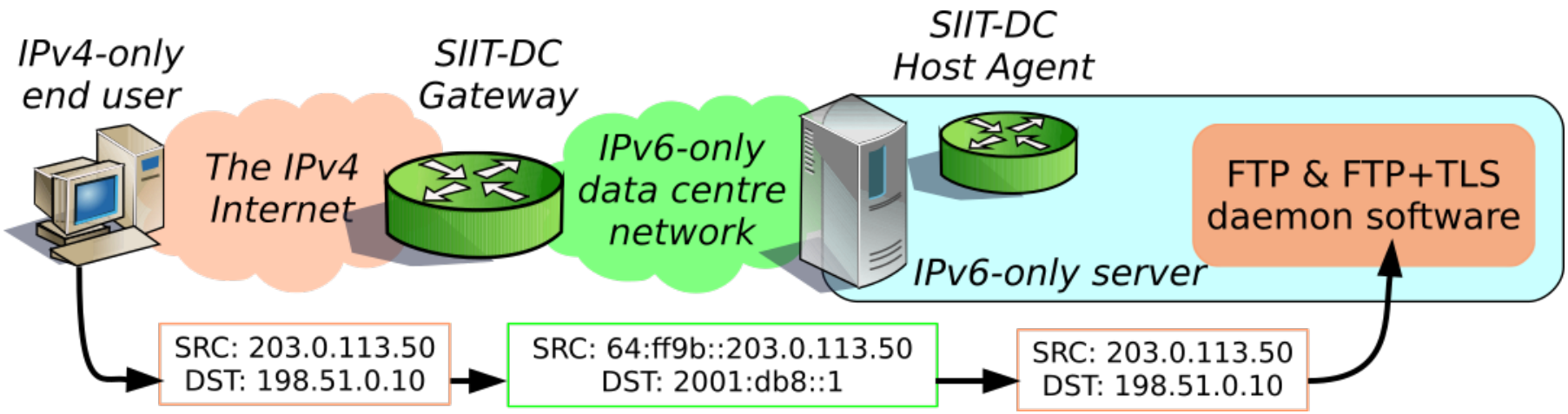
Zdroj: RIPE72: SIIT-DC

Klíčové vlastnosti SIIT-DC

- extrémě úsporné k IPv4 adresám
  - žádné ztráty na adresování infrastruktury
  - IPv4 adresy pouze pro veřejné služby
- brána může být kdekoli v síti
- bezestavové – není problém s vyvažováním zátěže a asymetrickým směrováním
- IPv4 adresa klienta zůstává zachována (mapovaná do IPv6 adresy)
- nezávislost aplikací na IPv4
  - žádné dodatečné náklady při vypínání IPv4

Podpora legacy služeb v SIIT-DC

- pro podporu FTP a podobných protokolů
- SIIT-DC Host agent je totéž co CLAT
  - lze použít clatd, popř. staticky konfigurovaný TAYGA
- téměř k nerozeznání od dual-stacku
  - server vidí svou IPv4 adresu na svém rozhraní



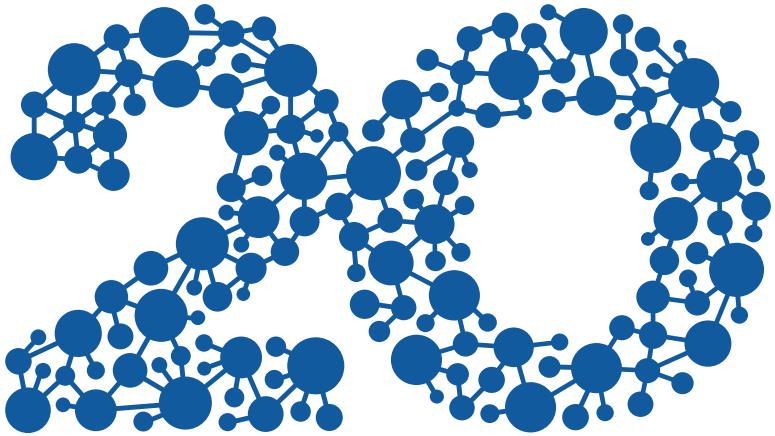
Zdroj: RIPE72: SIIT-DC

Shrnutí

- dual-stack opravdu není *jediná* možnost
- NAT64 funguje velmi dobře
  - ale pořád je to NAT – něco se ztratí v překladu
  - DNS64 je nutné zlo
    - ale neškodí nativnímu IPv6 obsahu
  - 464XLAT je dobrý – lepší je ale opravit aplikace
- IPv6-only datová centra jsou realitou
  - funguje-li služba za NAT, bude fungovat i za SIIT-DC
  - možnost postupného přechodu
  - odpadá dvojí konfigurace firewallů, dohled, atd.
  - jistota, že všechno bude fungovat po vypnutí IPv4
- další čtení
  - ToreAndreson.no: IPv6-only data centre RFCs
  - Root.cz: IPv4 jako služba

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
https://Ondřej.Caletka.cz



1996–2016
CESNET
SPOLUPRÁCE
VÝZKUM
KOMUNITA