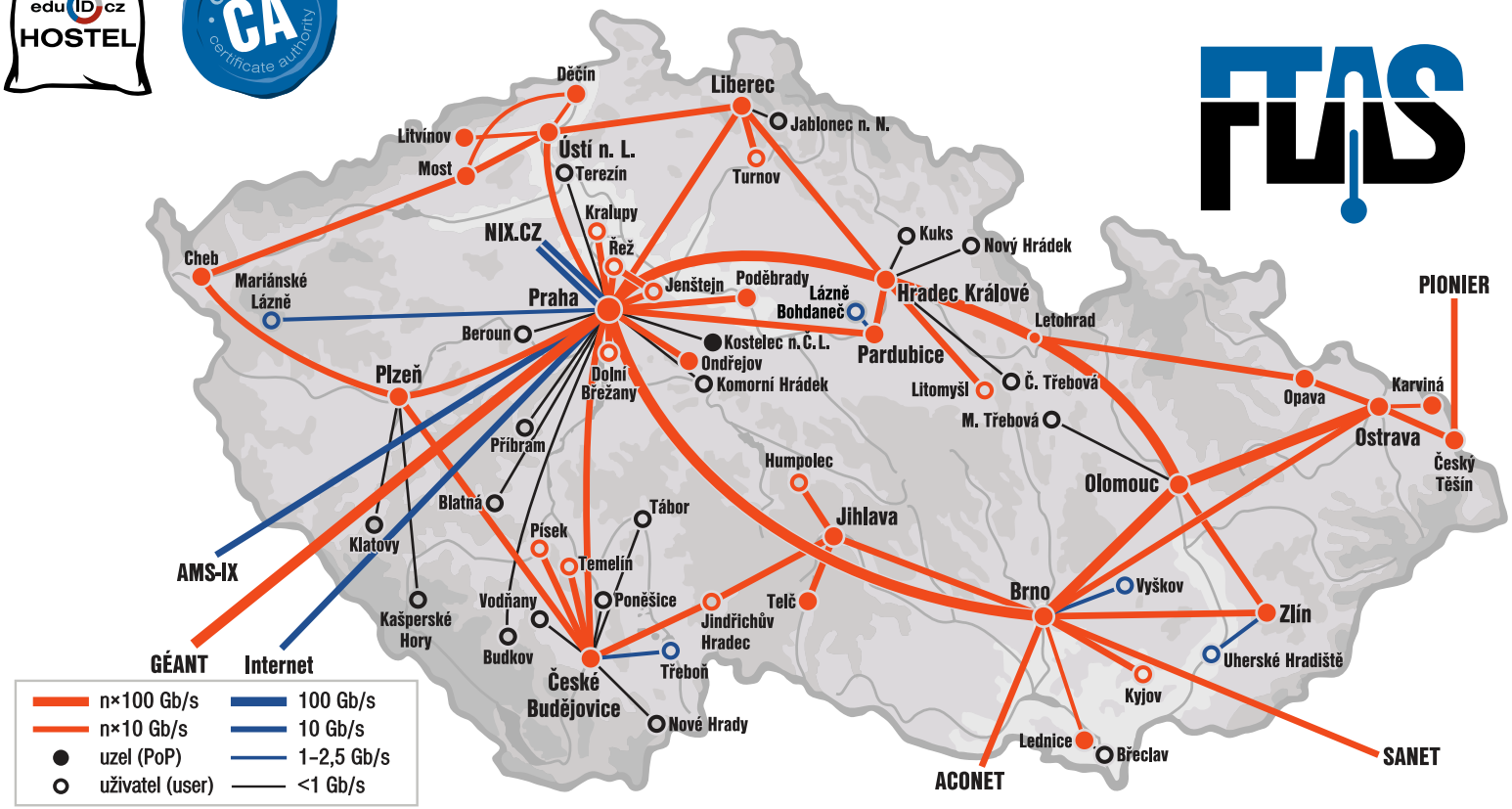
Nejčastější mýty o IPv6

Ondřej Caletka

25. května 2017

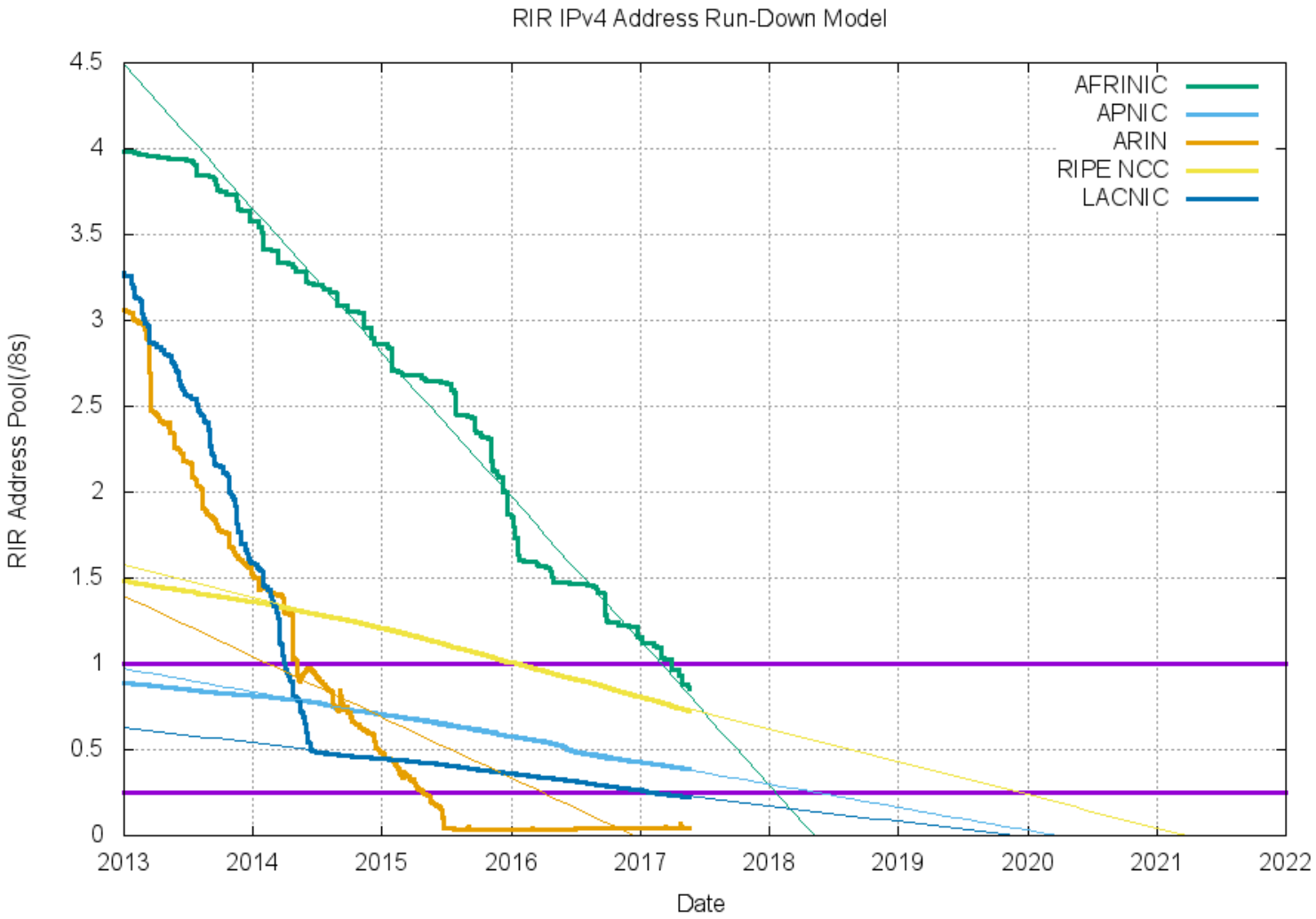
O sdružení CESNET



IPv6 nepotřebujeme, máme dost IPv4 adres

IPv6 nasadíme, až nám dojdou IPv4 adresy

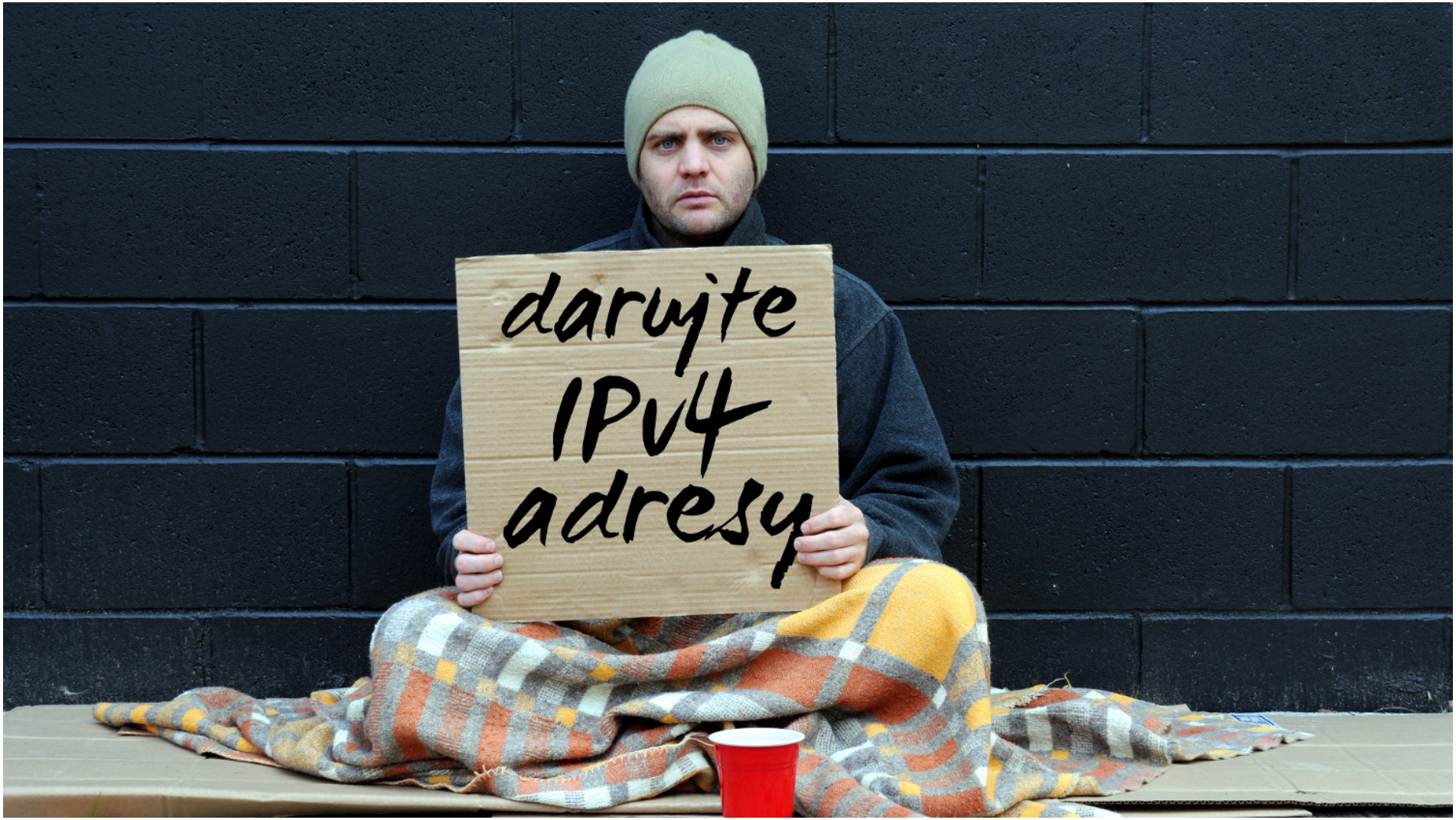
Stav zásob IPv4 adres



Zdroj: `https://ipv4.potaroo.net/`

IPv6 je nekompatibilní s IPv4

- IPv6 je prostředek k eliminaci nedostatečně dimenzovaného IPv4
- IPv6 je **nutnou, nikoli postačující** podmínkou k opuštění IPv4
- je před námi **dlouhý a bolestivý proces**, kde je potřeba podporovat oba protokoly zároveň
- internet se zatím **raději přizpůsobuje nedostatku** IPv4
  - striktní rozdělení na servery a klienty
  - klientům stačí NAT
  - servery potřebují veřejnou adresu
  - přímá komunikace klientů není možná
  - co dělat, až nebudou **adresy ani pro servery**?



Zdroj: `https://www.root.cz/clanky/stav-ipv4-drancovani-a-vsudypritomny-nat/`

Koupit? – *No problem*, 500 Kč za adresu

Small Blocks for Purchase

Select a block from the table, then fill out the rest of the form and submit your request. Your block will be reserved if possible, and we will contact you with further instructions.

Block Size	Address Range	Price/IP (USD)	IPv4 Cost (USD)	Region	
/24	To Be Determined	$24.00	$6144	RIPE	
/23	To Be Determined	$19.00	$9728	RIPE	Select
/22	To Be Determined	$18.00	$18432	RIPE	Select
/21	To Be Determined	$15.00	$30720	RIPE	Select

results current as of 05/22/2017 13:51 utc+0

Zdroj: `https://ipv4marketgroup.com`

Bez IPv6 spočívá budoucnost vašeho podnikání pouze v nakupování adres **od těch, kteří je dříve dostali zdarma**.

...za předpokladu, že bude *od koho* nakupovat.

Všem dnes stačí IPv4

IPv6 po nás nikdo nechce

Prosím, přestaňte obtěžovat náš helpdesk dotazy, kdy zavedeme IPv6. Naši operátoři nestíhají odpovídat, že o to není zájem.

Výhody pro poskytovatele připojení

- snížení objemové náročnosti CGN
- eliminace problémů s blacklistováním od velkých CDN sítí
- udržitelný rozvoj
- méně problémů s *data retention*
- konkurenční výhoda

Výhody pro poskytovatele obsahu

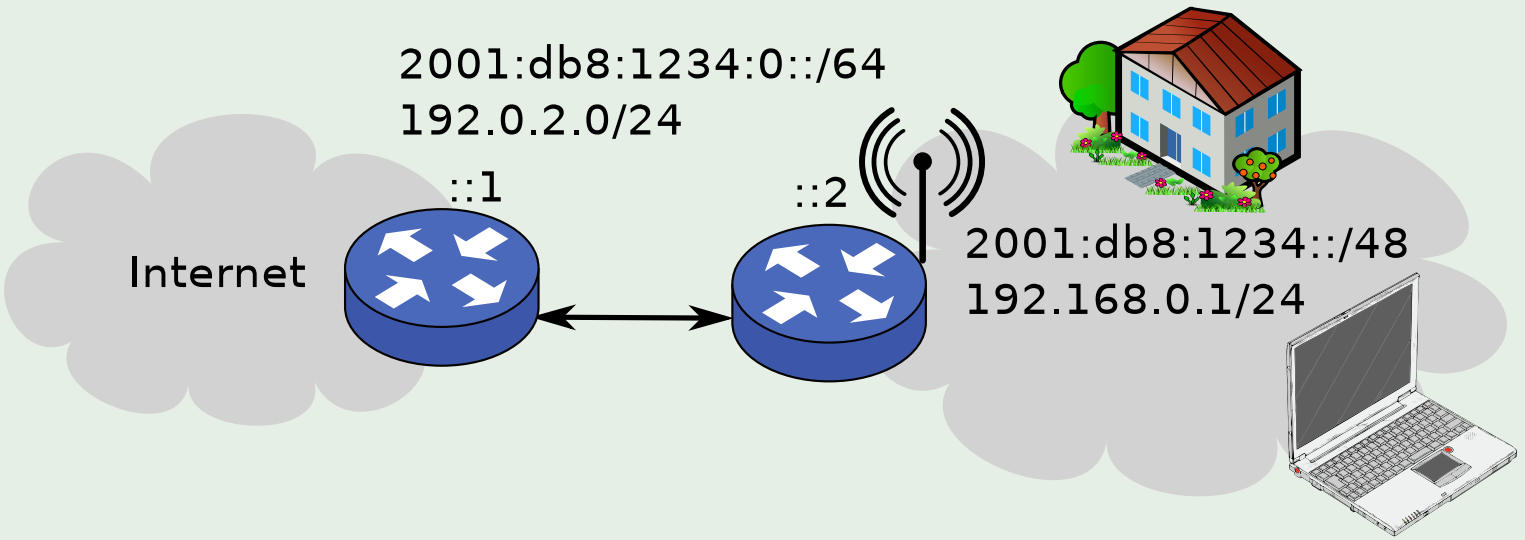
- minimální přidané náklady
- funkčnost pro IPv6-only zákazníky
  - například při přetížení IPv4 technologie velkých ISP
  - změna může přijít bez dostatečného předstihu
- přesnější geolokace zákazníka

IPv6 je zbytečně složité

Proč není IPv6 pouze IPv4 s delší adresou?

Spousta problémů, které IPv6 řeší, **nemá v IPv4 obdoby**.

Adresování domácí sítě



IPv6 v lokální síti

- sebekonfigurující *link-local* adresy
- objevování sousedů i konfigurace adresy je součástí protokolu
  - plnohodnotná náhrada ARP: NDP
  - částečná náhrada DHCP: SLAAC
- použití multicastu
  - reakce na časté problémy velkých *broadcast domén*
  - broadcast je speciální formou multicastu
  - v dnešní realitě jde stejně o broadcast

Komplexnost autokonfigurace

- IPv6 automaticky nastavuje výchozí bránu a volitelně také adresu
- dva standardy konfigurace DNS serveru
  - volba (bezestavového) DHCPv6
  - RDNSS volba v ohlášení směrovačů
- kontroverze stavového přidělování jedné adresy pomocí DHCPv6
  - zvládá přidělit pouze jedinou adresu
  - nepoužívá MAC adresy jako identifikátory
  - politický boj Google vs. zbytek světa

Veřejné IP adresy jsou bezpečnostní riziko

- globálně unikátní adresa ≠ globálně dostupná adresa
- chování NATu lze plnohodnotně emulovat stavovým firewallem
- neexistují problémy s kolizemi privátních rozsahů
- není problém s protokoly IPSEC, FTP, SIP,…
- zředění adresního prostoru znesnadňuje horizontální skenování

Bezpečnost patří na koncový bod

- *bezpečná lokální síť* ve skutečnosti neexistuje
- problém je stejný i v IPv4 – lokální útoky

NAT/CGN chrání soukromí uživatelů

- IPv6 v klientských systémech implementují ochranu soukromí na podobné úrovni, jako NAT
- sdílení adresy stylem CGN přináší provozní komplikace
  - společné blacklistování
  - ratelimitting ze strany obsahu
  - nutnost udržovat databázi překladů
- uživatelé jsou mnohem snáze sledovatelní na vyšších vrstvách (reklamy, supercookies, apod.)

Stačí nakupovat zařízení s podporou IPv6

Podpora IPv6 není binární

- jedná se o velkou rodinu standardů
- je třeba zkoumat podporu/nepodporu konkrétních funkcí
- pozor na dostatečnou kapacitu
  - např. router s kapacitou 8k ARP záznamů a 4k NDP záznamů
- nejistá podpora funkčnosti bez IPv4

Jak vybírat IPv6-ready zařízení v tendrech?

RIPE-554: Requirements for IPv6 in ICT Equipment

CESNET

Podsíť /64 přece musí stačit každému

- podsíť velikosti /64 je **dále nedělitelnou** jednotkou adresování
  - neumožňuje ani např. vytvoření oddělené sítě pro hosty
- všechny regionální registry **schvalují a doporučují** přidělování prefixu až /48 na zákazníka
- pro rezidentní zákazníky je zvykem používat /56
  - z obchodních, nikoli technických důvodů
- přidělování jiné délky prefixu *pouze na požádání* je **zbytečná komplikace** pro obě strany

Nechceme platit RIPE NCC, vystačíme si s /48

- takové jednání je **porušením pravidel** registrace
- kdo poskytuje připojení zákazníkům, měl by být LIR
- výjimky z IPv4 pro bod-bod spoje a *pooly* neplatí

Alokace vs. přiřazení (assignment)

alokace adres slouží k agregaci adresního prostoru

- alokované adresy jsou stále *volné*
- je možné vytvářet subalokace
- není možné je používat bez přiřazení

přiřazení znamená obsazení daného prostředku konkrétním účelem

- typicky zákazníkovi
- nesmí být používány jiným subjektem
- nelze dělat sub-přířazení
- maximální velikost /48 na *end site*

Varianty získání IPv6 alokace

- založení LIR – alokace od RIPE NCC
- subalokace od jiného LIRa
  - na jeho zodpovědnost
- založení společného LIRa – rozdělení alokace od RIPE NCC
  - například osmičlenný spolek – každý /32

Zakázané praktiky

- přiřazení *Provider Independent* adres od RIPE NCC (`2001:67…/48`)
- přiřazení /48 přídělu od upstream ISP

Dual-stack je jediná možnost nasazení IPv6

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

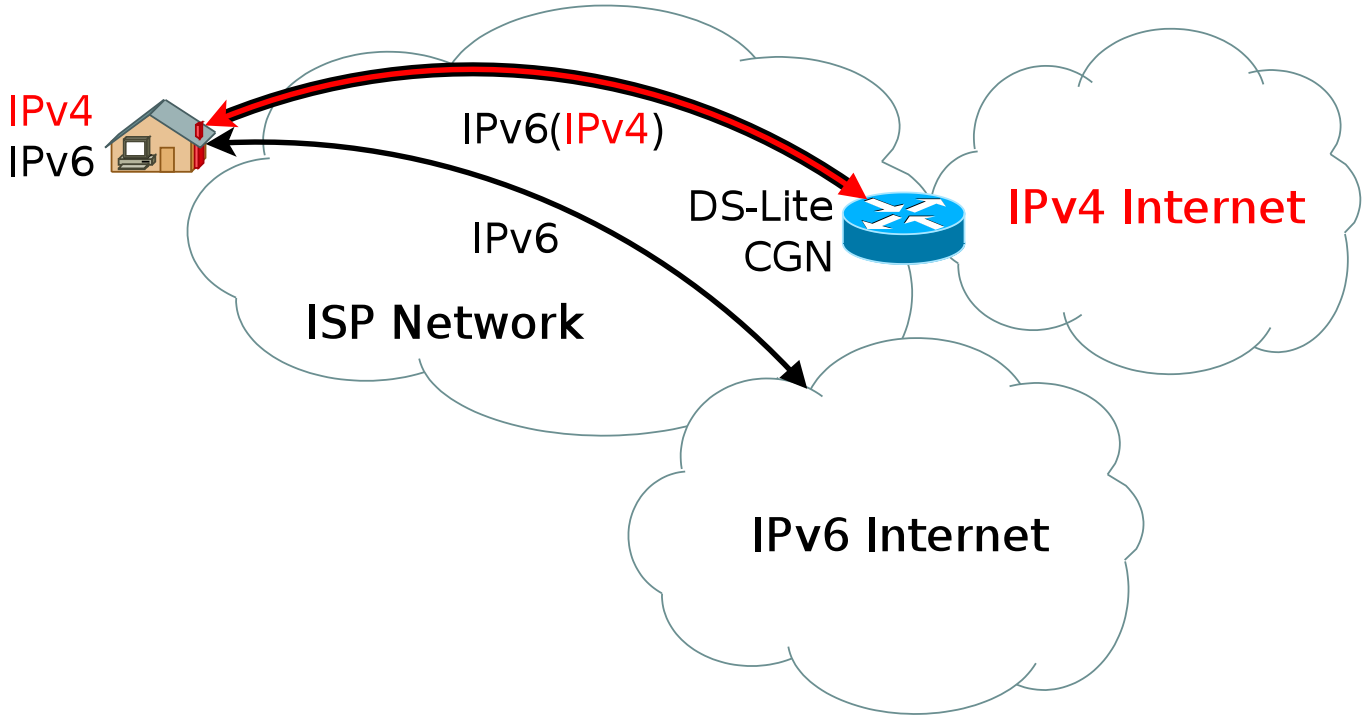
- NAT64
- 464XLAT
- MAP-T
- SIIT-DC

IPv6 s tunelovaným IPv4

- DS-Lite
- MAP-E
- lw4over6

Dual-stack lite

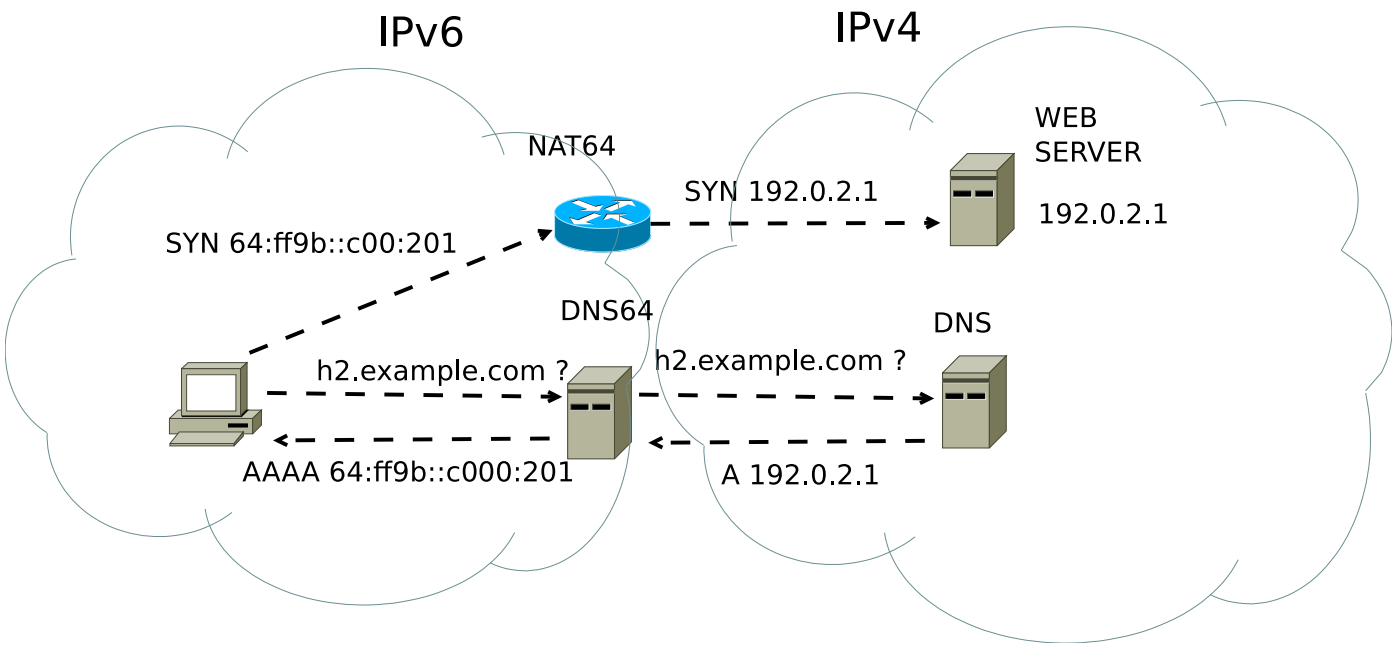
- IPv4 provoz klienta je tunelován IPv6-only přístupovou sítí k *Address Family Translation Router*
- eliminuje NAT u klienta a dual-stack v přístupové síti
- používaný nejčastěji v DOCSIS (brzy i u nás)



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

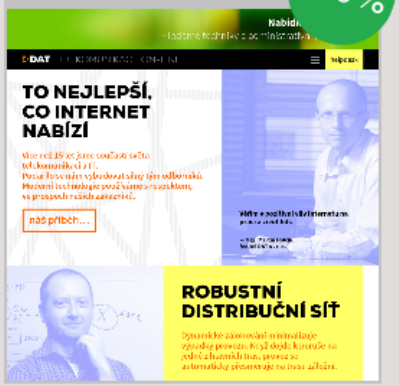
NAT64check

www.dat.cz

Test again

Last test finished:
23 May 2017, 16:43 CEST

Image match

NAT64	IPv4-only	IPv6-only
100%		
		

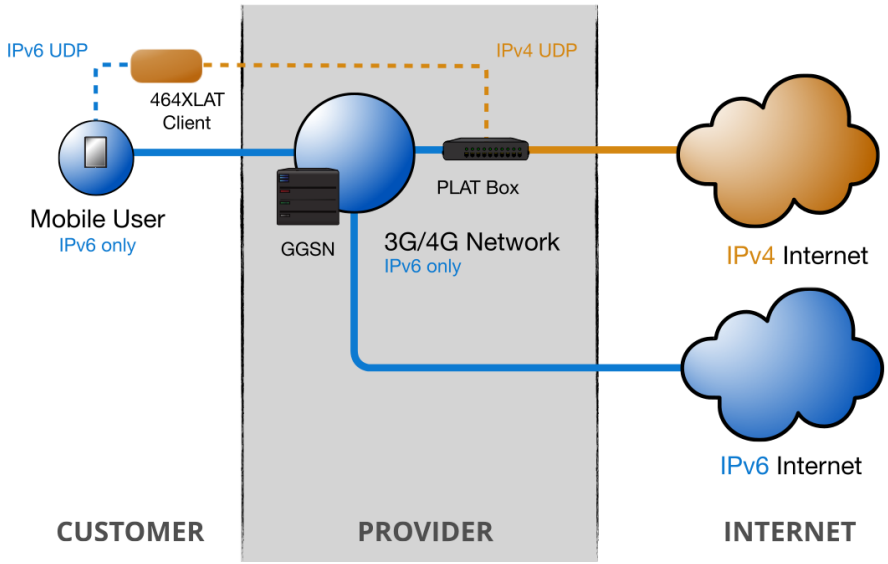
Resources match ▶

	NAT64	IPv4-only	IPv6-only
	100%		IPv6 not implemented
DNS records		80.251.240.49	None
Ping		26.6 ms 26.6 ms 26.7 ms 26.6 ms 26.6 ms	No measurement
Ping (1500 byte		27.2 ms 27.0 ms 27.0 ms 27.0 ms 27.1 ms	No measurement

CESNET

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



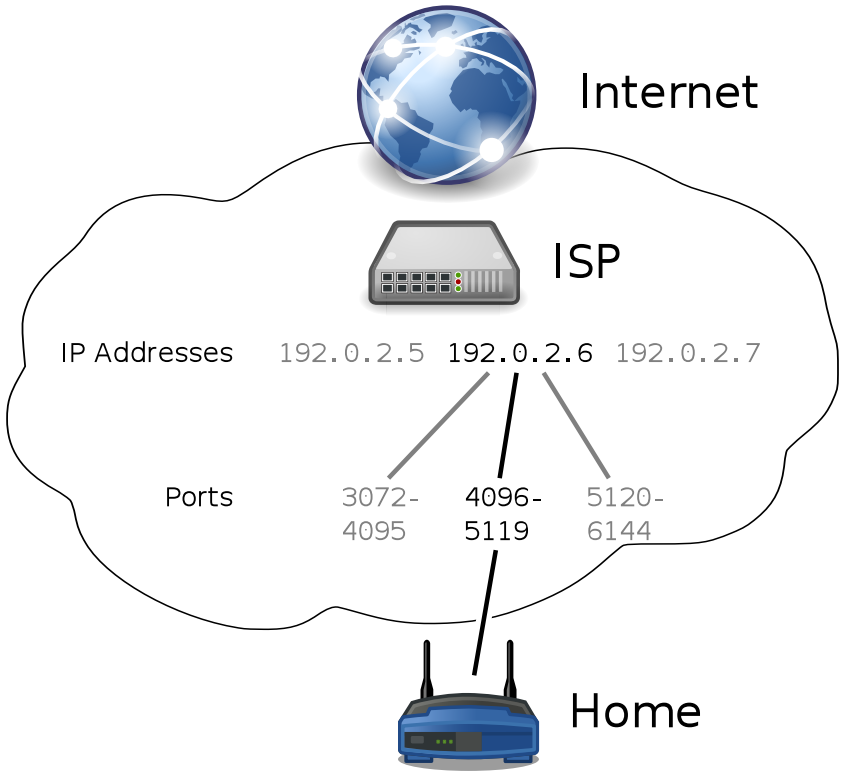
Zdroj: RIPE NCC IPv6 training

NAT64 na vlastní kůži

- veřejné demo Go6 Lab
  - Jool, PaloAlto Networks, Cisco ASR1000, A10 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)

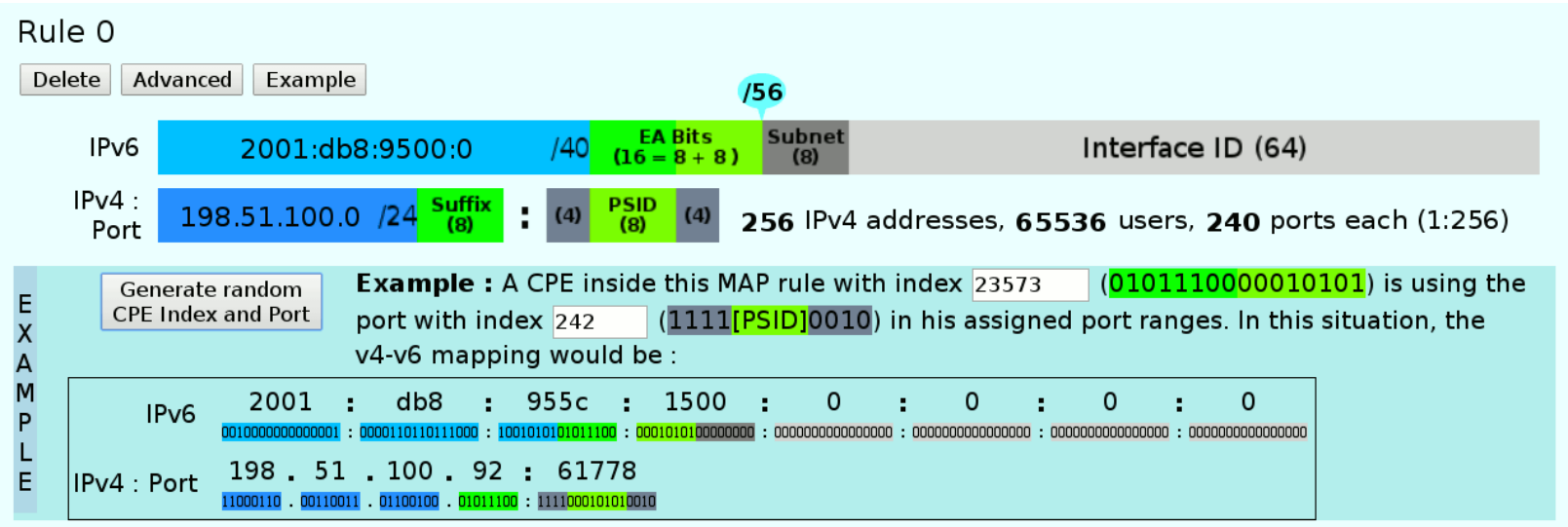
- šetření IPv4 adres při eliminaci CGN
- čísla portů TCP/UDP jako rozšíření IPv4 adresy
- implementace: MAP, 4rd, Lightweight 4over6



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

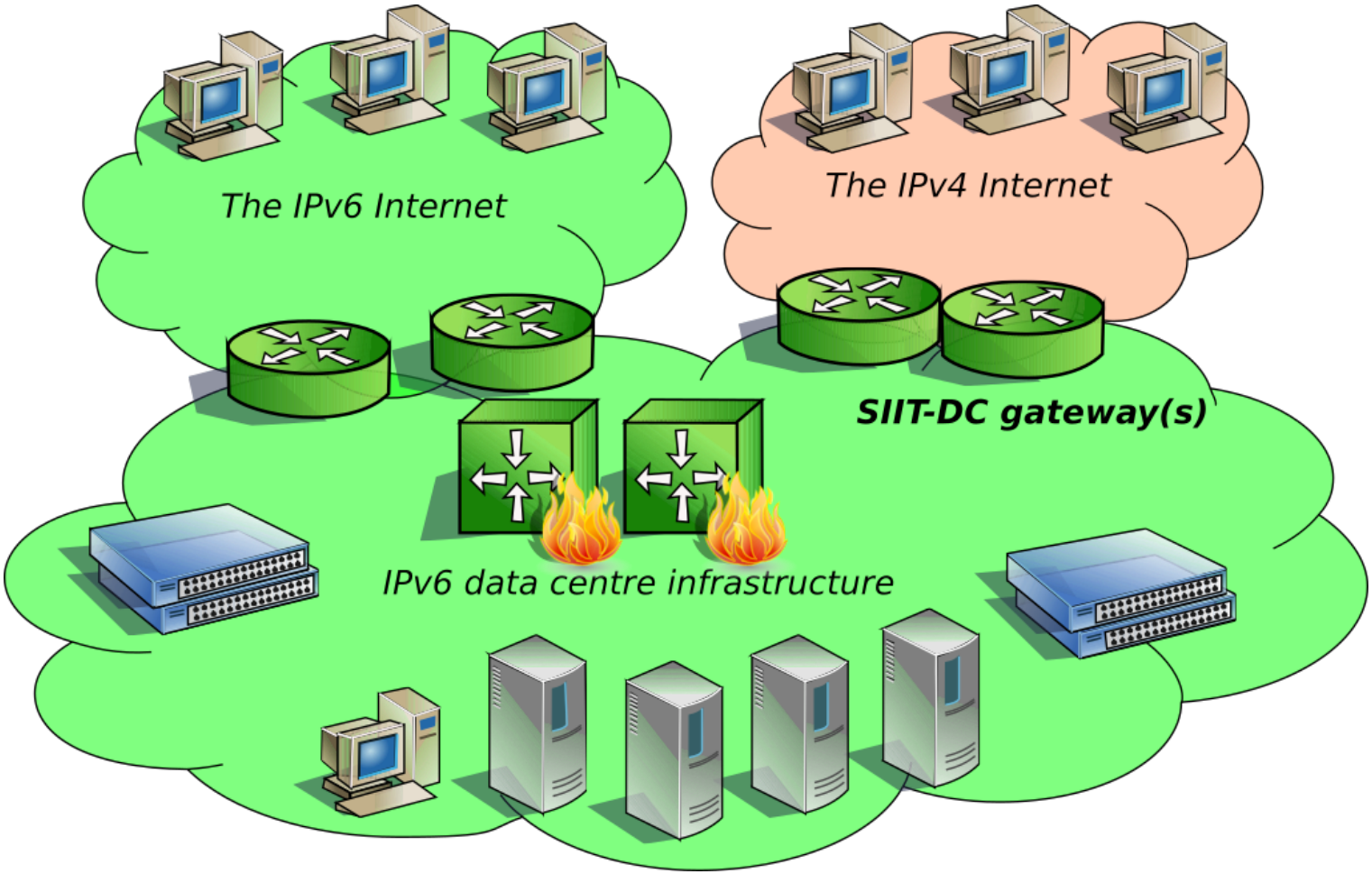
IPv4 Residual Deployment via IPv6 (RFC 7600)

- 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

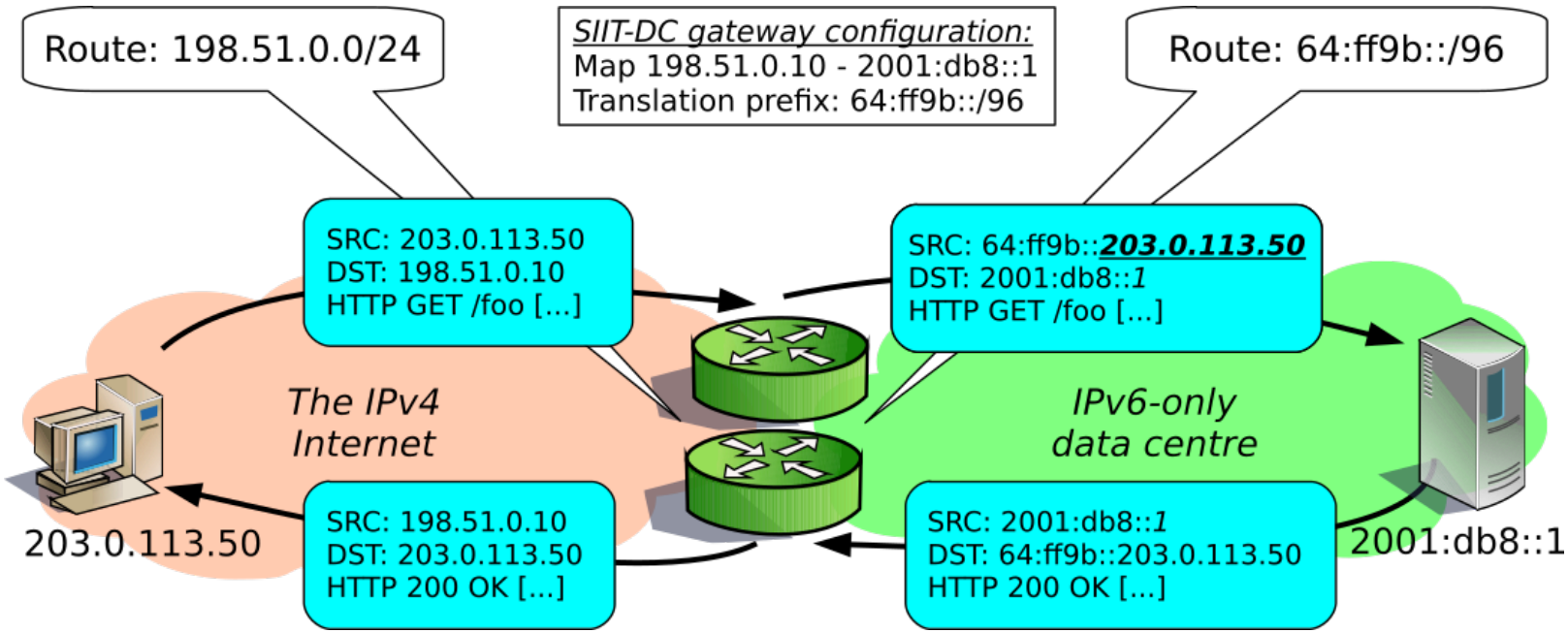
IPv6-only v datacentrech



Zdroj: RIPE72: SIIT-DC

SIIT-DC (RFC 7755)

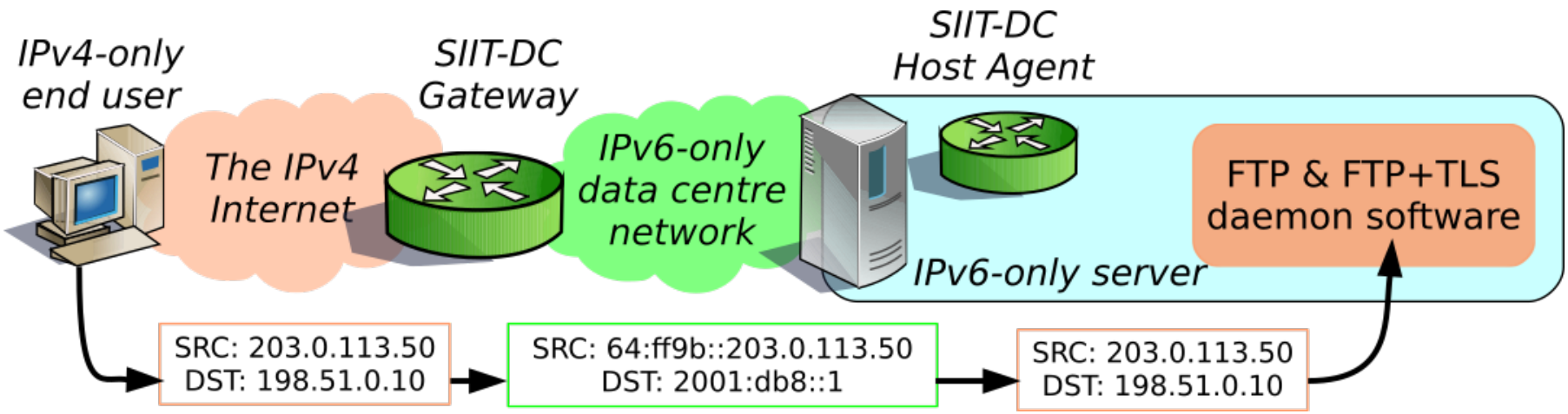
- bezestavový překlad IPv4-IPv6 na hraně datacentra
- NAT64 s explicitním mapováním páru IPv4-IPv6
- pro klienty zcela transparentní



Zdroj: RIPE72: SIIT-DC

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

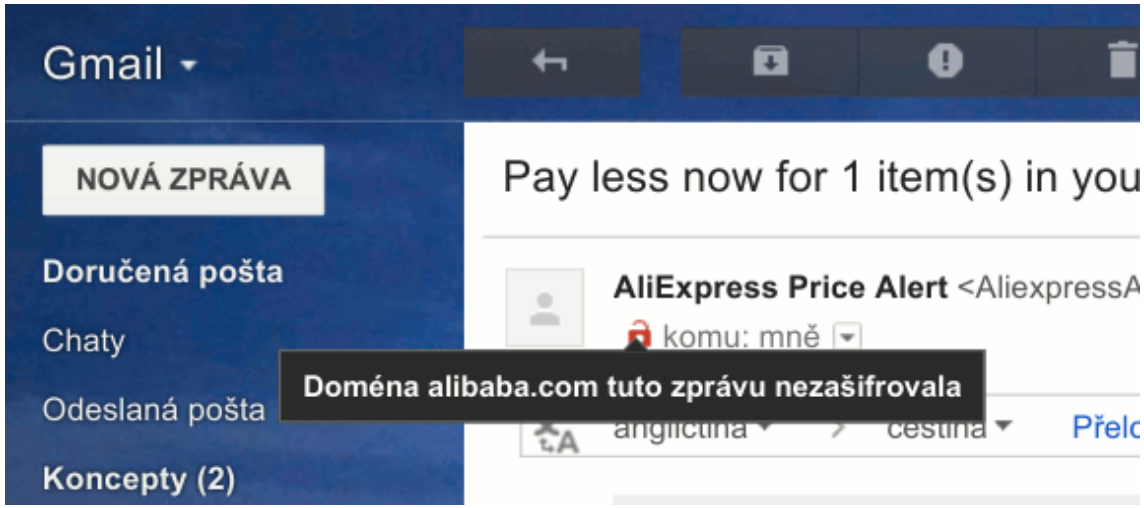


Zdroj: RIPE72: SIIT-DC

Shrnutí

Shrnutí

- IPv6 je **jediná známá** možnost dalšího rozvoje internetu
- velcí hráči dokazují, že **IPv6 je možné nasadit** v současné podobě
- podpora hardwaru je problematická a **sama se nezlepší**
- k odklonu od IPv4 **může dojít velmi rychle**



Pozvánka

Sdružení CESNET pořádá 6. 6. 2017 seminář o IPv6

- Tutoriál: Úvod do IPv6
- Tunelování IPv6 dříve a nyní
- Nasazení IPv6 u Mall.cz
- BCOP aneb jak správně nasazovat
- Na cestě za standardem
- Implementace IPv6 u Freenet Liberec, UPC, mobilních operátorů

Podrobnosti a registrace:
`https://www.cesnet.cz/sdruzeni/akce/ipv6-2017/`

Děkuji za pozornost

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

Prezentace je již nyní k dispozici ke stažení.