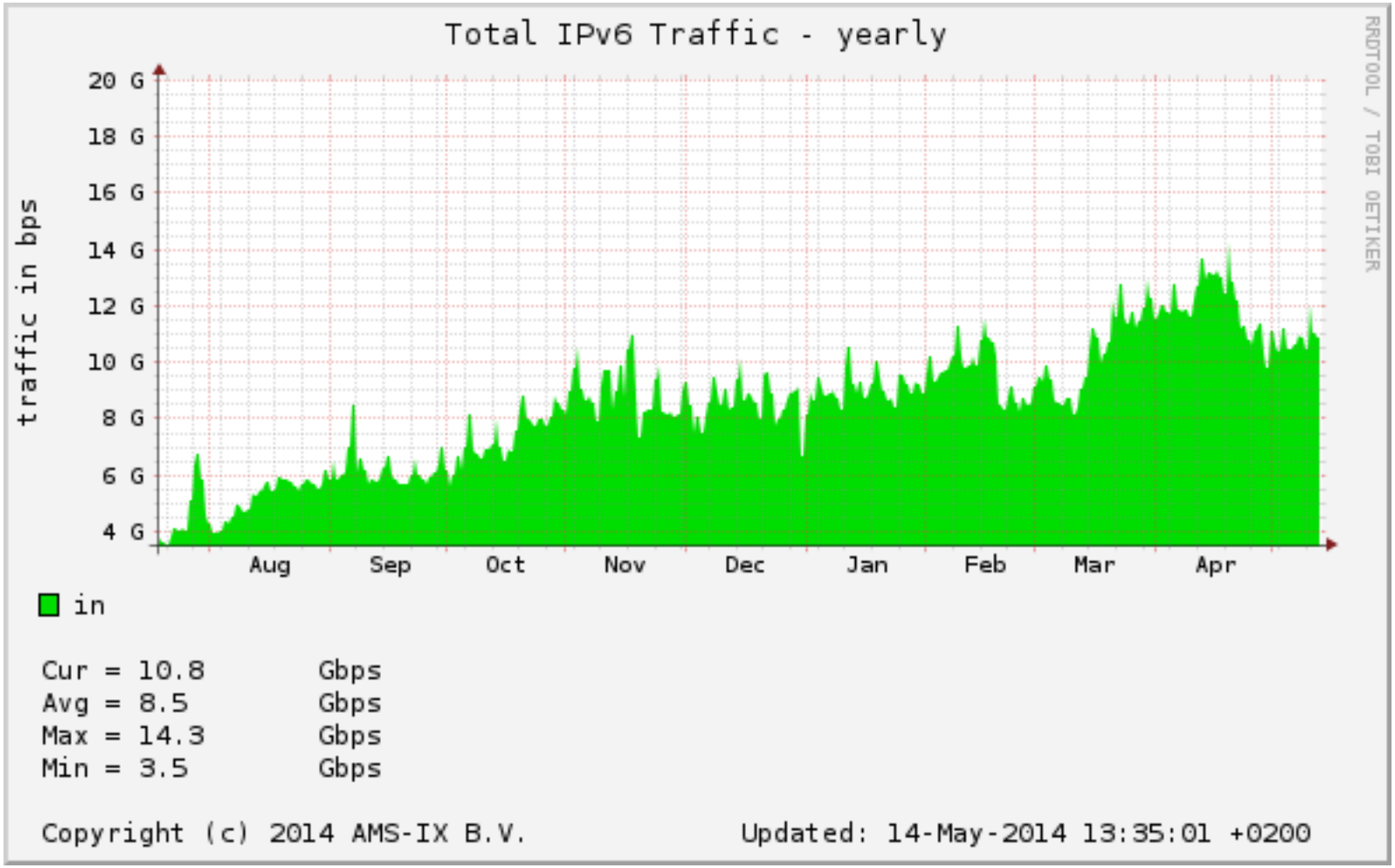
IPv6: Už tam budeme?

Pavel Satrapa, TU v Liberci

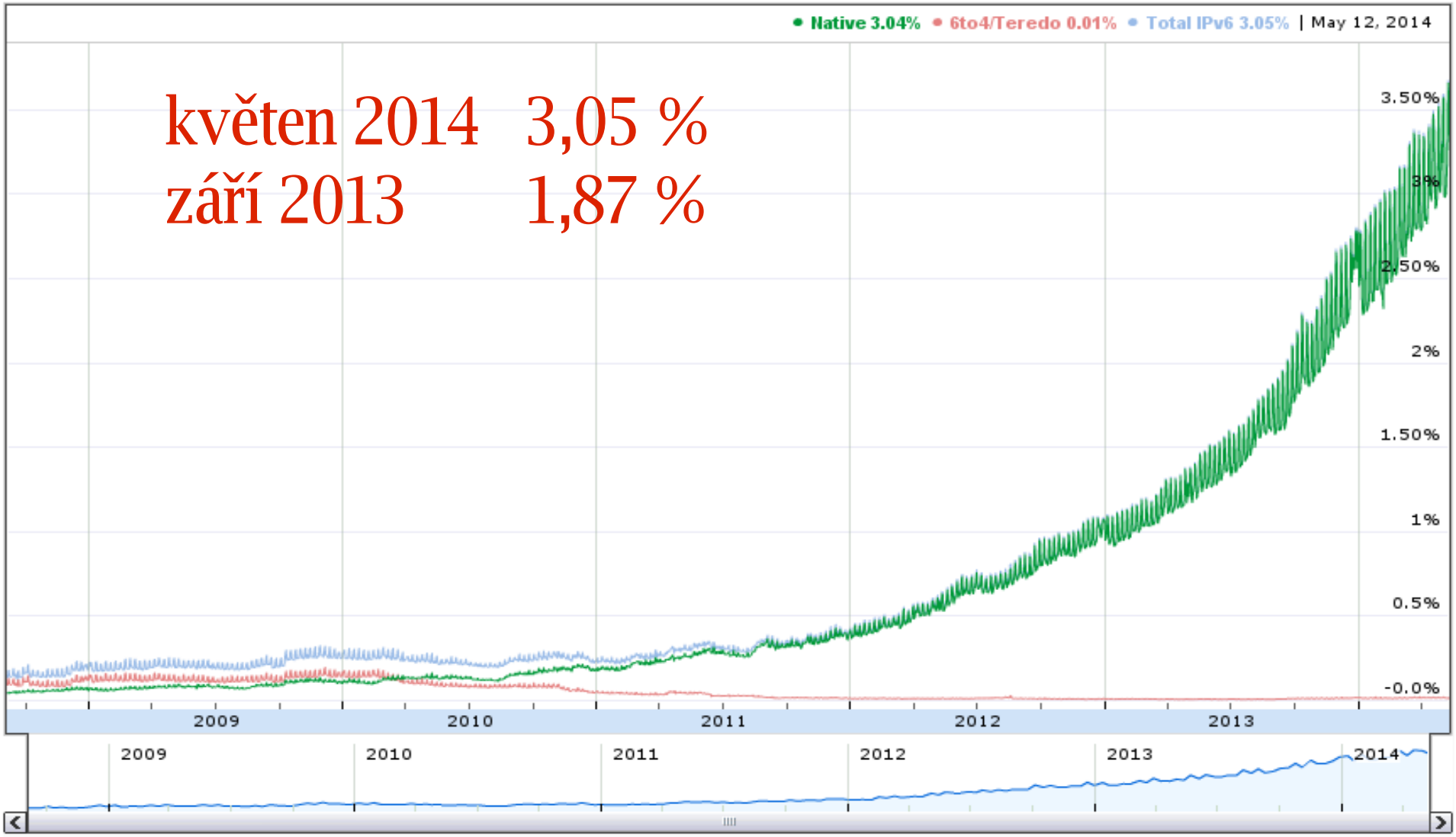
Pavel.Satrapa@tul.cz

AMS-IX



- IPv6 lehce přes 0,5 % provozu

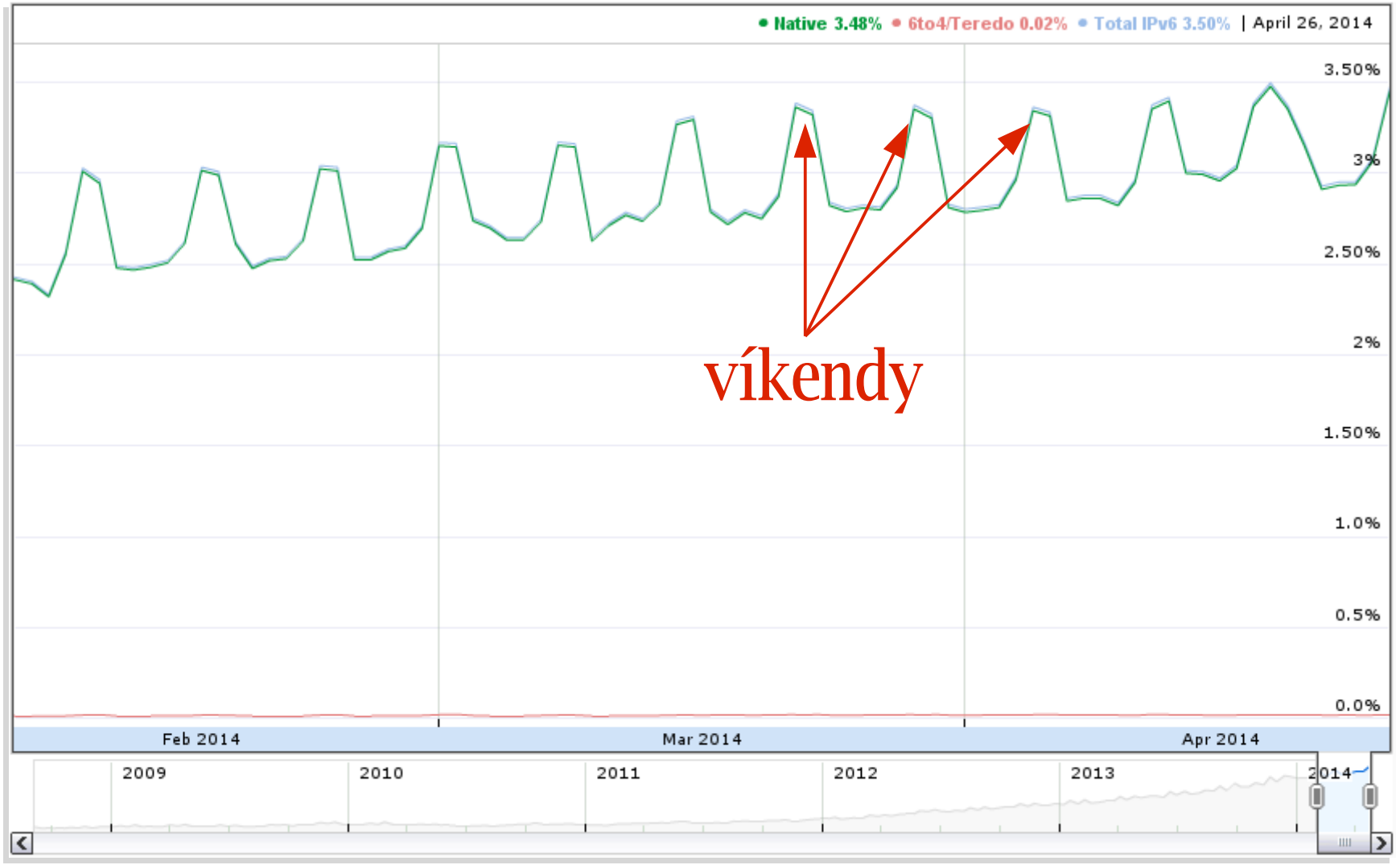
Google



květen 2014 3,05 %

září 2013 1,87 %

Google – detail

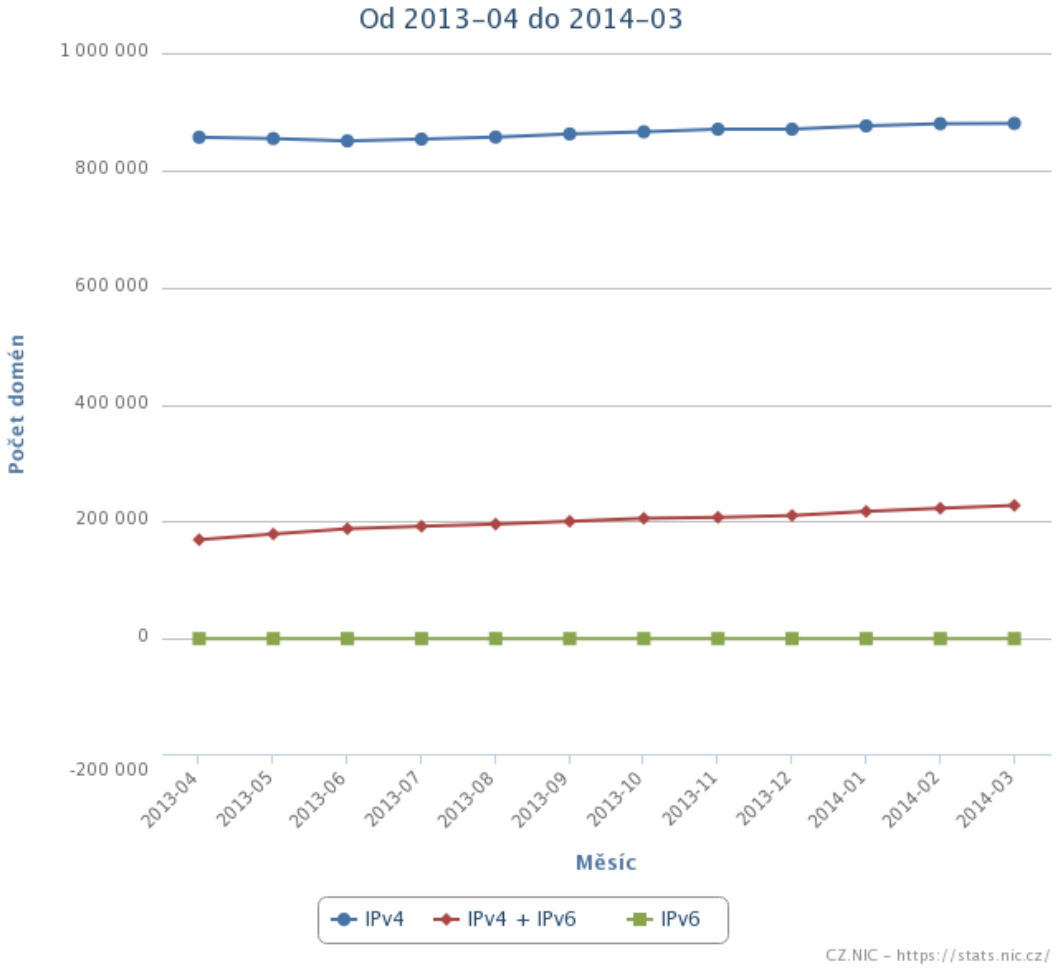


Závěry ze statistik

- **Černého Petra mají provozovatelé služeb**
  - dual-stack služba: přes 3 %
  - objem provozu v páteřní síti: 0,5 %
- **domácí sítě podporují IPv6 více než firemní**
  - víkendová navýšení

Statistiky CZ.NIC

- https://stats.nic.cz/stats/ipv6_domains/



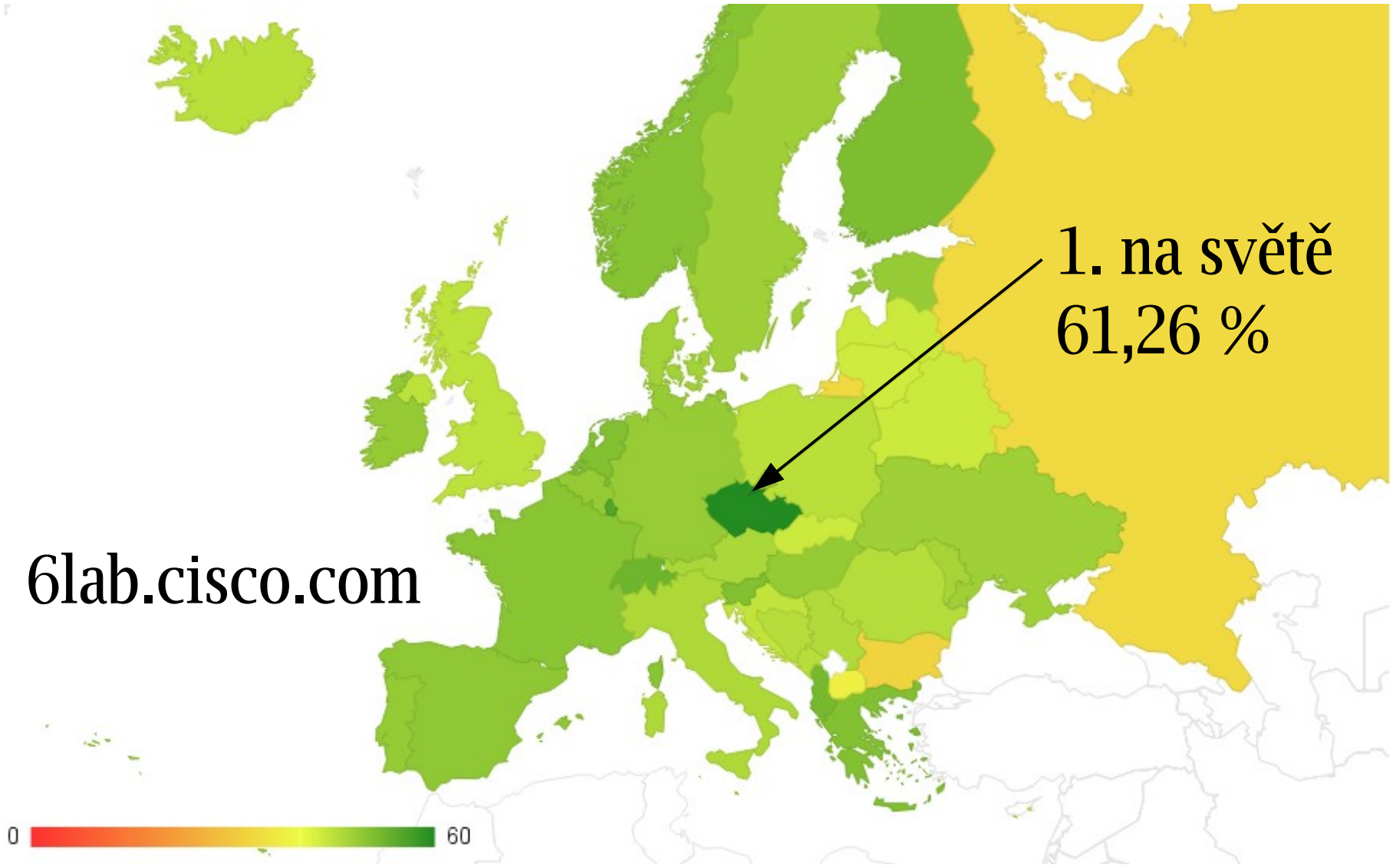
1,11 mil. domén .cz

231 tisíc (21 %)
podporuje IPv6

164 tisíc (15 %)
má IPv6 mail

Webový obsah

- 6lab.cisco.com



Co je nového?

Bezpečnost

Omezení hlaviček

- dlouhé řetězce rozšiřujících hlaviček jsou oblíbeným nástrojem útočníků všeho druhu
- bezstavový firewall nedokáže paket posoudit, pokud nemá kompletní hlavičky
- RFC 7112: **všechny rozšiřující hlavičky se musí vejít do prvního fragmentu**
- jinak zahodit datagram a poslat ICMPv6 zprávu

Bezpečnost objevování sousedů

- triky s objevováním sousedů umožňují falšovat automatické konfigurační mechanismy
- RFC 6980: **zákaz fragmentace všech ND paketů**
  - porušující pakety potichu ignorovat
  - výjimka: ohlášení certifikační cesty v SEND
- RFC 7113: **vylepšení RA-Guard**
  - je třeba prohlížet všechny hlavičky datagramu
  - zahazovat pakety, kde hlavičky přesahují 1. fragment

SAVI (1)

- Source Address Validation Improvement, RFC 7039
- ověření adresy odesilatele **pro lokální provoz**
- 3 kroky:
  1) zjistit, jaké IP adresy je stroj oprávněn používat
  2) svázat je s vlastnostmi linkové vrstvy
  3) vynutit, aby pakety odpovídaly vazbě podle 2)
- lze implementovat v různých místech, nejlépe v přepínačích připojujících koncové stroje

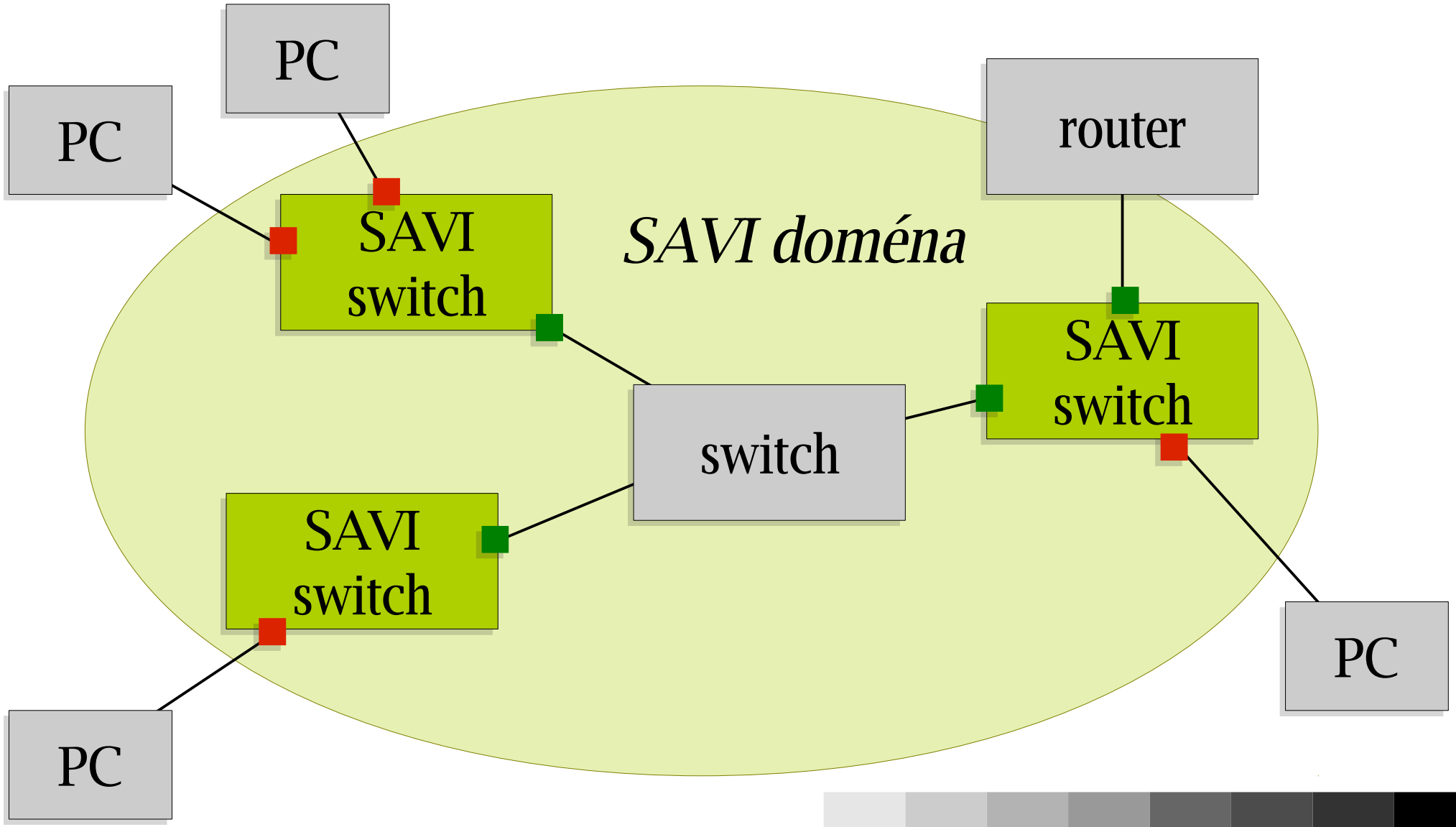
SAVI (2)

- **zjištění korektních adres**
  - závisí na použité metodě přidělování
  - např. sledování DHCPv6 komunikace nebo paketů automatické autokonfigurace
- **vazba IP adresy na L2 prvky**
  - různé metody, různá úroveň bezpečnosti
  - typicky číslo portu na přepínači
  - EUI-64 nebo podobný identifikátor
  - identifikátor tunelu, ...

SAVI (3)

- princip obranného perimetru
- **porty k ostatním SAVI prvkům jsou důvěryhodné**
- **porty vedoucí k ne-SAVI prvkům jsou prověřovány**
- SAVI zařízení si uchovává jen informace o paketech přicházejících z prověřovaných portů (o přímo připojených ne-SAVI sousedech)

SAVI (4)


PC
PC
router
SAVI
switch
SAVI doména
SAVI
switch
switch
SAVI
switch
PC
PC

FCFS SAVI

- **First-Come First Served**, RFC 6620
- určeno zejména pro bezstavovou autokonfiguraci
- když se **poprvé objeví IPv6 adresa**, zařízení implementující FCFS SAVI si ji **sváže s L2 údaji** (zde povinně číslo portu) a následně propouští s touto adresou jen pakety se stejnými L2 údaji
- **při změně L2** (přepojení do jiného portu) **ověří nedostupnost** původních parametrů

SEND SAVI

- pro sítě používající SEND, RFC 7219
- **váže CGA na L2 port** pokud
  - počítač ověřuje detekcí duplicit unikátnost své adresy
  - přijde jiný paket a SAVI prvek ověří detekcí dosažitelnosti, že odesilatel je pravý
- platnost vazby oživuje detekcí dosažitelnosti

Bezpečnostní dopady na IPv4

- RFC 7123
- určeno pro provozovatele infrastruktur, kteří chtějí setrvat u IPv4
- čím může přítomnost IPv6 v koncových zařízeních narušit bezpečnost IPv4 sítě
- aneb **jak blokovat různé tunelovací mechanismy**
  - 6in4, 6over4, 6rd, ISATAP, TEREDO,...
    srovnání tunelovacích mechanismů viz RFC 7059

Adresy

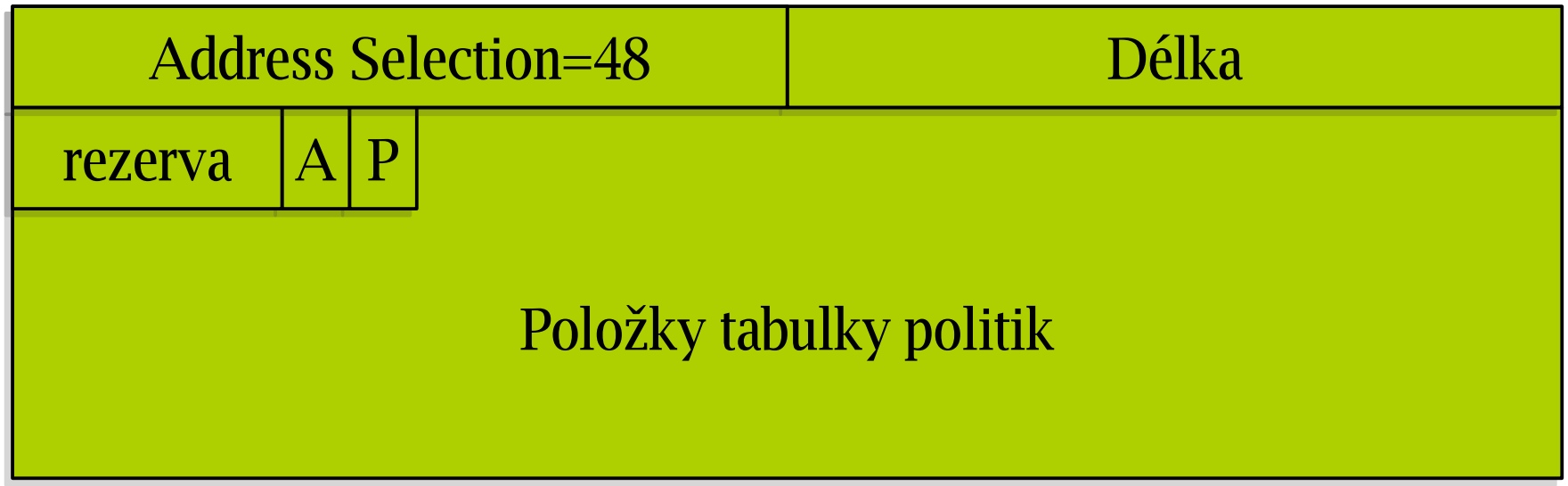
Výběr adresy

- před rokem: RFC 6724 (náhrada RFC 3484)
- změny spíše kosmetické, základní principy zůstávají
- rozšířena tabulka politik
  - potlačení historických prefixů
- bez dynamické správy

- a letos...

Řízení tabulky politik

- nová volba DHCPv6 – Address Selection, RFC 7078
- umožňuje nastavit tabulku automaticky
- **příznak P – preferovat adresy chránící soukromí**



Identifikátory rozhraní (1)

- **současný stav pro globální individuální adresy:**
- pevné identifikátory rozhraní
  - ručně nastavené nebo z EUI-64
  - konstantní – umožňují sledovat stroj
- náhodné identifikátory rozhraní
  - dočasné, stále se mění (RFC 4941)
  - chrání soukromí
  - noční můra pro správce

Identifikátory rozhraní (2)

- nově: konstantní náhodné identifikátory (**RFC 7217**)
- identifikátor je náhodný (bez vazby na MAC)
- v každé (pod)síti jiný
- ve stejné (pod)síti zůstává konstantní
- kompromis mezi ochranou soukromí a spravovatelností
- slouží jako **alternativa EUI-64 adres pro bezstavovou autokonfiguraci**

Identifikátory rozhraní (3)

- generuje hashovací funkce, jejímž vstupem je
  - prefix podsítě
  - identifikátor síťového rozhraní stroje
  - identifikátor sítě (SSID) – nepovinně
  - čítač pro detekci duplicit
  - tajný klíč (vygeneruje se při instalaci operačního systému a zůstává neměnný)

Identifikátor rozhraní (4)

- výpočet zahrnuje prefix – různé identifikátory rozhraní v různých (pod)sítích
- nezahrnuje MAC – výměna karty nezpůsobí změnu
  - MAC je jednou z variant pro „identifikátor rozhraní“
- tajný klíč je svázán s OS
  - změní se reinstalací
  - různé OS na stejném stroji budou mít různý identifikátor rozhraní

Identifikátor rozhraní (5)

- **RFC 7136** oficiálně zrušilo význam bitů U (globální/lokální) a G (individuální/skupinový)
- zrušilo požadavek na používání EUI-64
- nová formulace: **identifikátor rozhraní je dlouhý 64 bitů, pokud je odvozen z MAC identifikátoru, musí se použít modifikované EUI-64**

Další

Domácí krabičky

- aktualizace požadavků na domácí směrovače RFC 6204 → RFC 7084
- povinná podpora přechodových mechanismů **6rd** a **DS-Lite**
- měl by být podporován **Port Control Protocol**
- SNTP → **NTP**
- **BCP 38** (filtrování paketů s padělanou adresou odesilatele) **sníženo z „must“ na „should“**

Na čem se pracuje

6man

- **64bitová hranice pro identifikátor rozhraní**
  - draft-ietf-6man-why64
- **skupinové adresy**
  - draft-ietf-6man-multicast-addr-arch-update
  - draft-ietf-6man-multicast-scopes
- **zlepšená detekce duplicitních adres**
  - řeší smyčky
  - draft-ietf-6man-enhanced-dad

v6ops

- **návrh IPv6 sítě**
  - draft-ietf-v6ops-design-choices
- **nasazení IPv6 v síti organizace**
  - draft-ietf-v6ops-enterprise-incremental-ipv6
- **a v datových centrech**
  - draft-ietf-v6ops-dc-ipv6
- **zkušenosti s NAT64**
  - draft-ietf-v6ops-nat64-experience

Děkuji za pozornost.

Dotazy?