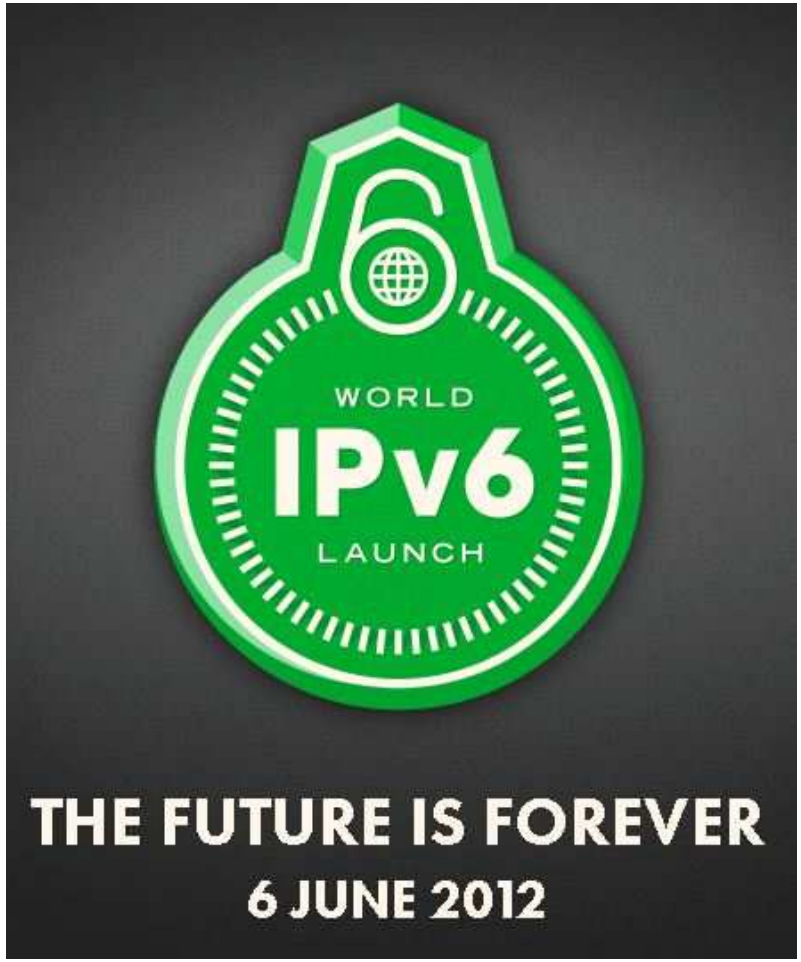
Služby správce .eu přes IPv6

Prague, **June 6th 2012**

.eu
Your European Identity

Proč jsme zde …



http://www.worldipv6launch.org/

.eu Your European Identity

Přehled

- EURid
- Čeho jsme již dosáhli
  Čemu jsme se již přiučili
- Bezpečnost!
  IPv6 : nový protokol přinášející
  nové výzvy a příležitosti
- Vybraná čísla

EURid

- Správce domény nejvyšší úrovně .eu
  - ~ 3.600.000 domén
  - Mezi deseti největšími TLD na světě
  - DNSSEC
  - Organizace: 4 pobočky / podpora ve všech oficiálních jazycích EU

- Moje role:
  - Regional manager Central Europe
    - Pobočka v Praze pro CZ, SK, PL, HU, BG a RO

Čeho jsme již dosáhli
Čemu jsme se již přiučili

Čeho jsme již dosáhli

- Autoritativní služby DNS pro zónu .eu přes IPv6:
  - Od 2007: 2001:1470:8000:100::1
    (l.eu.dns.be. Námi provozovaný server v Lublani)
  - Od 2010: 2001:67c:1010:23::53
    (y.nic.eu. anycast provider NetNod)

- Náš veřejný web server: www.eurid.eu.
  - Od června 2011: 2001:67c:40:1::210
    (neodstranili jsme AAAA record po World IPv6 Day, 8. června)

- Naše registrační testovací prostředí (http / https):
  - 2. dubna 2012: tryout6.registry.eu. is 2001:67c:40:1::201
  - 2. května 2012: tryout.registry.eu. has both A and AAAA record

Co plánujeme

- Náš „ostrý“ registrační systém
  - Umístěn ve stejném data centru jako testovací → IPv6 je možný
  - Všechny servery mohou mít jak IPv4 tak IPv6 adresu
  - Čekáme na zkušenosti v testovacím registračním prostředí
- Veřejné registrační služby: whois a das
  - V plánu, nutno vyřešit rate limiting
- Autoritativní jmenné servery pro .eu:
  - V plánu mít IPv6 adresu pro každý autoritativní NS
    (v rámci projektu navýšení počtu vlastních anycastových serverů)

Čemu jsme se již přiučili

- Zavedení IPv6 vyžaduje plánování:
  - Z hlediska databáze jsou IP adresy na překvapivě mnohých místech (zadání/změna/uložení/zobrazení/…). Na všechny je třeba myslet.
- Síť IPv6 ještě není tak provázaná jako síť IPv4.
  - Z toho důvodu nemusí být dva subjekty na IPv6 schopny komunikovat
    - Nepropagujeme IPv6 adresu x.nic.eu.
      Protože v některých částech sítě IPv6 byla nedostupná!
- Jiné služby mohou pociťovat vedlejší efekty:
  - Např. v začátcích při odděleném webu přes IPv4 a IPv6 problémy s absolutními URL
  - Webové služby by měly mít relativní URL, absolutní URL přepojují návštěvníky zpět na IPv4 pokud je tam pouze IPv4 adresa (A record).

Bezpečnost!

IPv6 :
Nový protokol přinášející nové výzvy a příležitosti

Nový protokol

- Ačkoliv byl vznik IPv6 motivován především předpovědí nedostatku volných IPv4 adres (v současné době stále více a více reálného), nejde o pouhé rozšíření délky adresy, ale jde o nový protokol s novými principy.
  - Například automatická konfigurace přináší nové bezpečnostní výzvy

- Obrovský adresní rozsah u IPv6 vyžaduje změnu přístupu ke konfiguraci:
  - Problém: Rate limiting
  - Výzva:
    být o krok napřed před layer 2 útoky.
  - Příležitost:
    ochrana před nežádoucími adresami.

Rate limiting ?

- Správci TLD uplatňují limity proti data miningu z databáze. Postižené služby: whois a das.

- V IPv4:
  - Uplatnění horního limitu pro počet událostí (např. spojení) z jedné (1) IPv4 adresy.
- V IPv6:
  - Vzhledem k síti /64, může klient provádět každý dotaz z jiné IPv6 adresy v rozmezí! (množství dostupných adres….)

Výzva: layer 2 útok

- Obrovské sítě (/64) → vyhledávání layer 2 adres (MAC)!
  - Vyhledání Layer 2 adresy vyžaduje zdroje:
    - Paměť pro uložení paketu, pro který je adresa vyhledávána
    - CPU
  - Zdroje jsou blokovány dokud není adresa vyhledána
  - Ale co se stane, když útočník posílá pakety na neexistující adresy?
    - Pro každý paket jsou zdroje blokovány maximální čas (všechny pokusy)
    - Máme dost zdrojů, když útočník pošle hodně paketů?
  - IP(v4) má implicitní ochranu: malé sítě
    - /29 mezi externím routerem a firewallem
  - IPv6: lokální síť /64
    - Dává útočníkovi hodně prostoru pro vyvolání procesu vyhledání layer 2 adresy!

→ Možností je konfigurace /125 na zařízeních ve vnější síti

Příležitost: nežádoucí adresy

- Alokace adres v IPv4 světě je komplikovaná
  - Mnoho bloků adres, které nejsou použitelné ve veřejném Internetu, je náhodně rozeseto v adresním prostoru:
    ~ privátní adresový prostor:
    10/8, 172.16/12 a 192.168/16
    ~ IPv4 link local adresy:
    169.254/16
    ~ (a mnoho dalších rozsahů, které jsou z historických důvodů nepoužitelné)

  - Poznámka: tyto rozsahy není možné agregovat! Vytváření routovacích nebo filtrovacích pravidel je komplikovanější, takovéto seznamy jsou dlouhé
    → každý používá 0.0.0.0/0 jako default destination

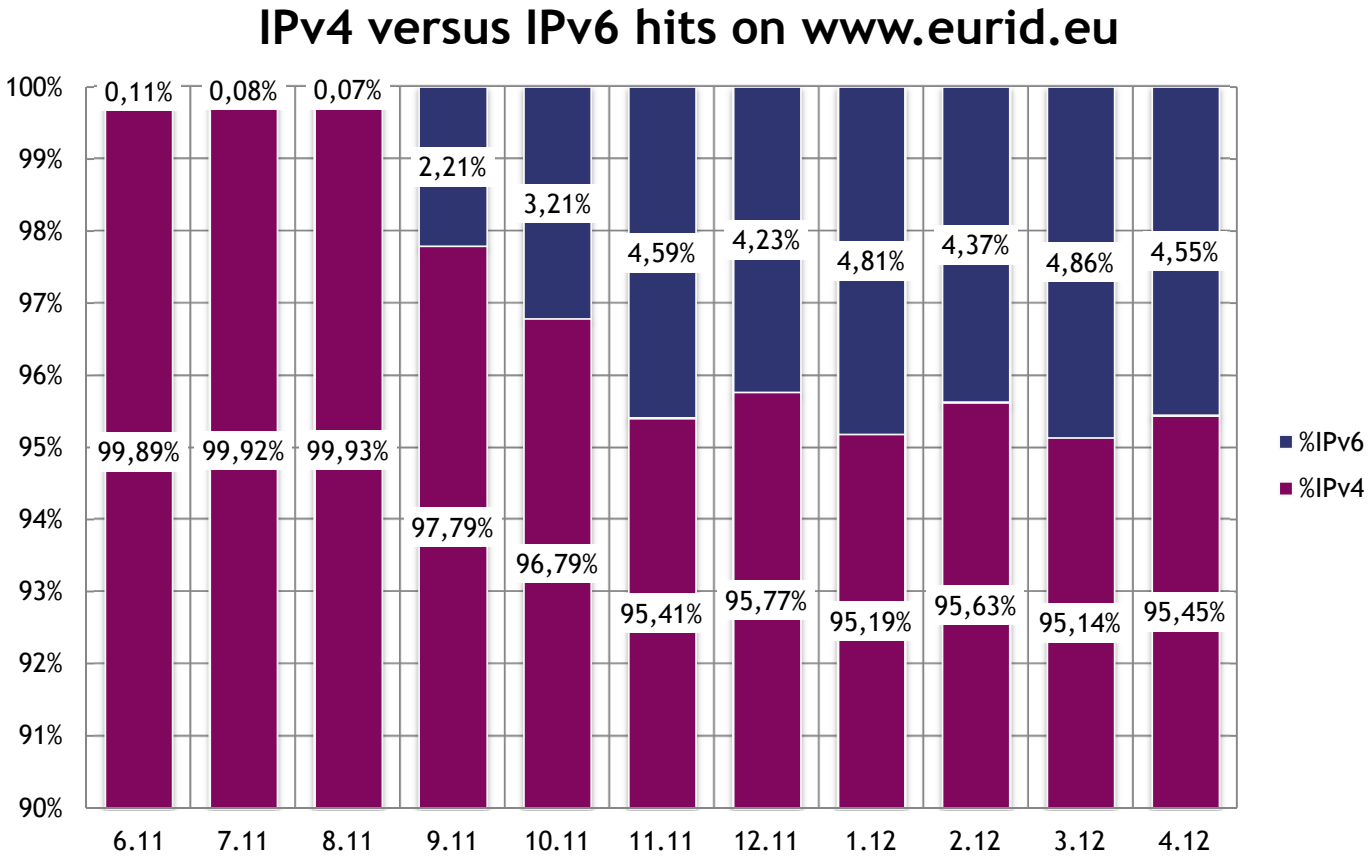
Příležitost: nežádoucí adresy

- V IPv6 je adresování mnohem lépe uspořádané
  - Ekvivalentní rozsahy (k IPv4) jsou blízko u sebe:
    - ~ privátní adresní rozsah:
      FC00::/7 (Universal Local Addresses – RFC 4193)
    - ~ IPv6 link local adresy:
      FE80::/10
    - ~ Mnoho dalších rozsahů není z historických důvodů použitelných, ale … veřejný adresní prostor v IPv6 je: 2000::/3
- Z toho vyplývá:
  - Na veřejných serverech není nutné používat ::/0 jako default gateway, ale lze použít 2000::/3 (a ::/0 směrovat do /dev/null)

  → Pokud útočník propaguje (bgp) nějaký, např. 7000::… rozsah, tato konfigurace automaticky zabraňuje komunikaci (myšlenka původně od Freda Bakera, Cisco, v IETF mailing listu)

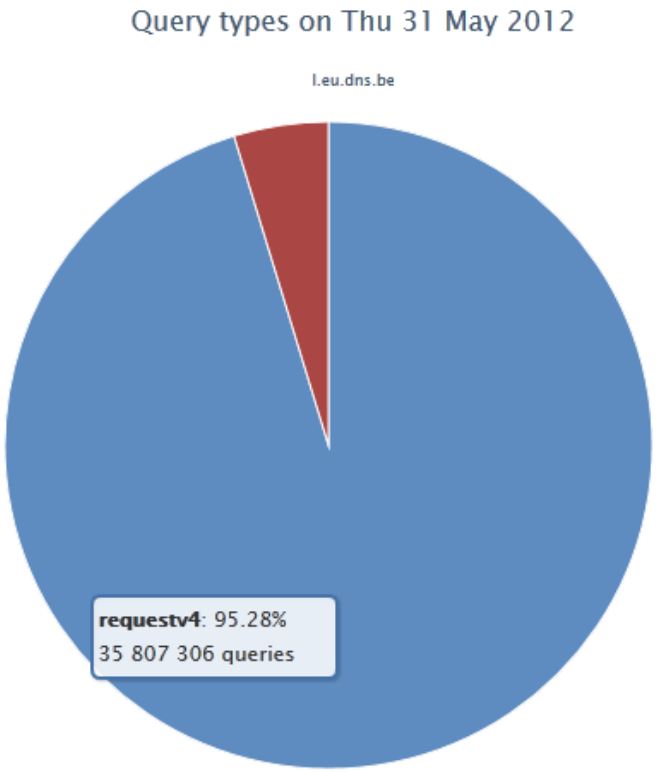
Vybraná čísla

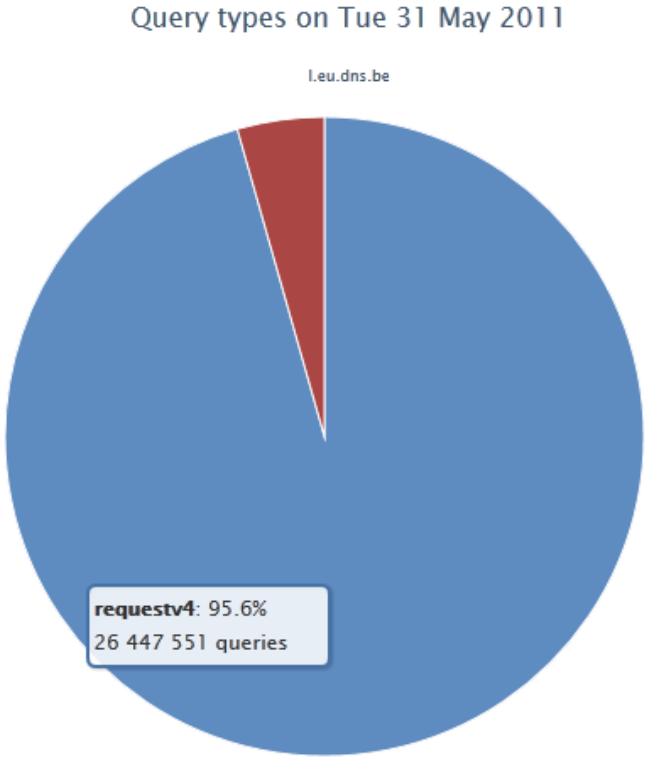
Webový server



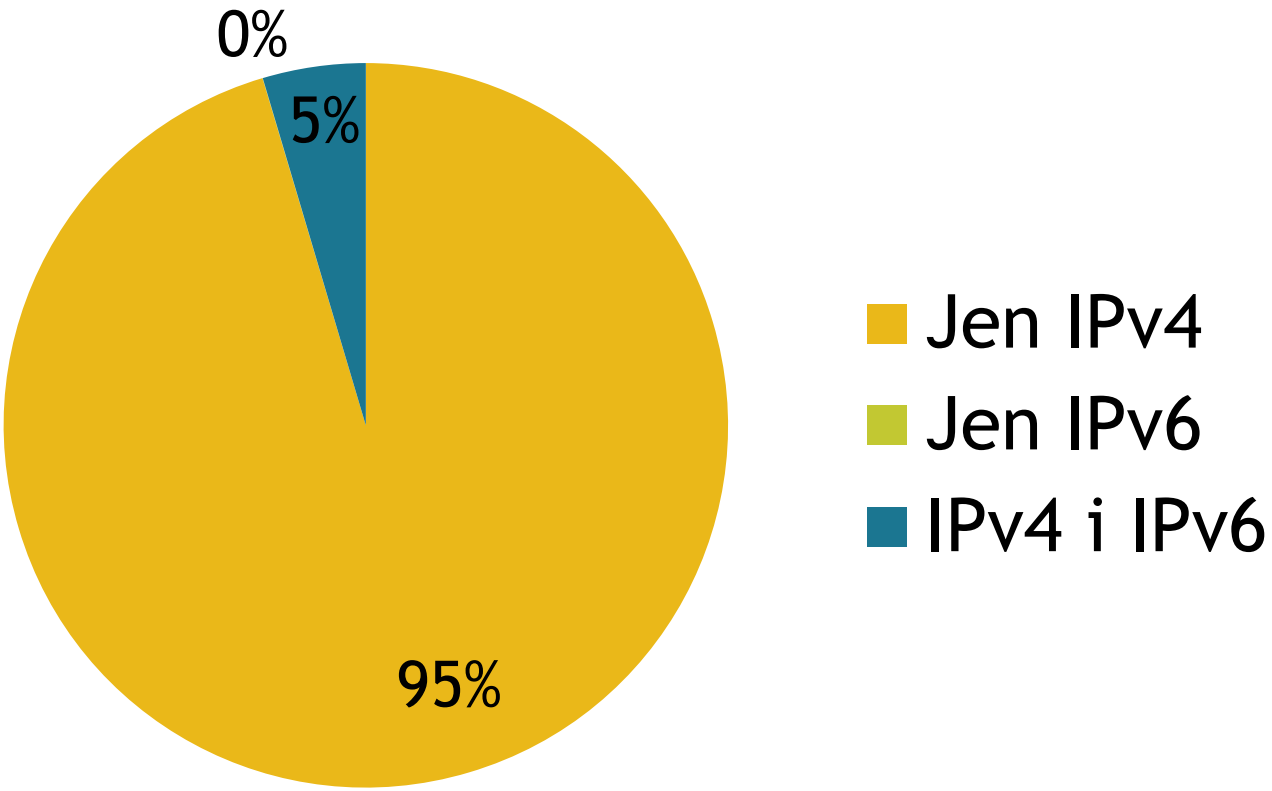
.eu Your European Identity

l.eu.dns.be: % IPv4 dotazů





Glue záznamy v zóně



Dotazy?

regina.fuchsova@eurid.eu