# IPv6 tunely pomocí OpenVPN

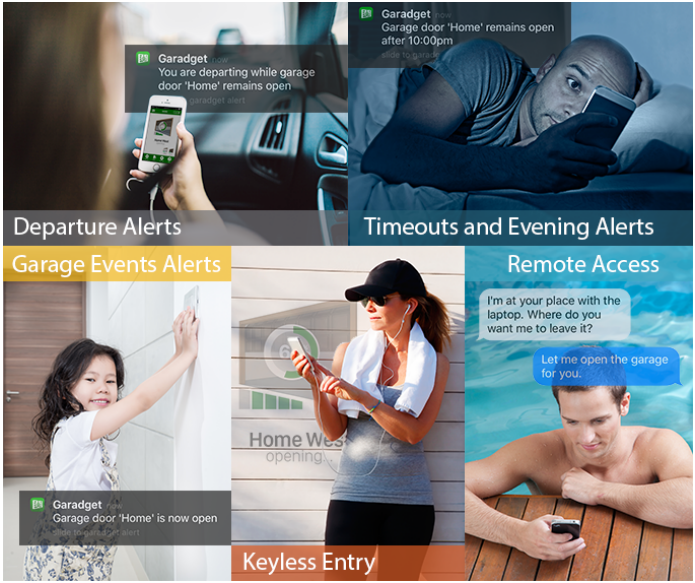
Ondřej Caletka


8. října 2017

# Potřebuje Internet IPv6?

- podle představ z 90. let: **nepochybně ano**
- podle současné reality: ¯_😒_/¯
- už pět let jsme bez IPv4 adres
- úspěšné služby se přizpůsobily
- distribuované CDN sítě snižují atraktivitu globálního tranzitu
- bez potřeby globální komunikace není třeba globální adresace


Zdroj: Indiegogo




Zdroj: Amazon

# Garadget

## Hodnocení zákazníka na Amazon.com

Junk - DO NOT WASTE YOUR MONEY - iPhone app is a piece of junk, crashes constantly...

## Reakce výrobce

The abusive language here and in your negative Amazon review, submitted minutes after experiencing a technical difficulty, only demonstrates your poor impulse control...
At this time **your only option is return Garadget** to Amazon for refund. Your unit ID 2f0036... **will be denied server connection**.

Zdroj: Business Insider

# Přizpůsobený internet

- v garáži máme internet
- v mobilu máme internet
- přesto nelze z mobilu garáž ovládat
- místo zařízení musíme koupit **balík zařízení a služby**
- jak spolehlivě a dlouho bude fungovat **služba, kterou neplatíme**?
- co, až se provozovatel služby rozhodne dělat něco jiného?
- co když se mu přestane líbit náš *tón v diskuzích*?

# NAT jako bezpečnostní prvek

Zdroj: Wired

# IPv6 jako *lepší* internet

- připojená zařízení komunikují přímo
- cloudová služba je možnost, nikoli povinnost
- výrobci nespoléhají, že *bezpečnost* bude zastoupena *nedokonalostí* přístupové sítě

# Stav IPv6 u českých ISP

- bez velkých problémů v datacentrech
- s problémy pro firemní zákazníky
- téměř nemožné pro rezidentní zákazníky
  - nasazeno u xDSL přípojek
    - dobře u T-Mobile
    - špatně u O2
    - vůbec u ostatních
  - pilotní provoz v síti UPC
    - bez možnosti vypnout router v modemu
    - bez možnosti rozdělit síť
  - **žádné plány** u mobilních sítí
    - *chcete-li IPv6 jako v Polsku, odstěhujte se do Polska*
    - v USA n×10 milionů iPhonů zcela bez IPv4

# Tunelování IPv6 uvnitř IPv4

- služba přístupu k Internetu poskytovaná přes internet
- automatické a manuální tunely
  - 6to4
  - Teredo
  - tunnelbroker.net
  - SixXS

# Automatické tunely

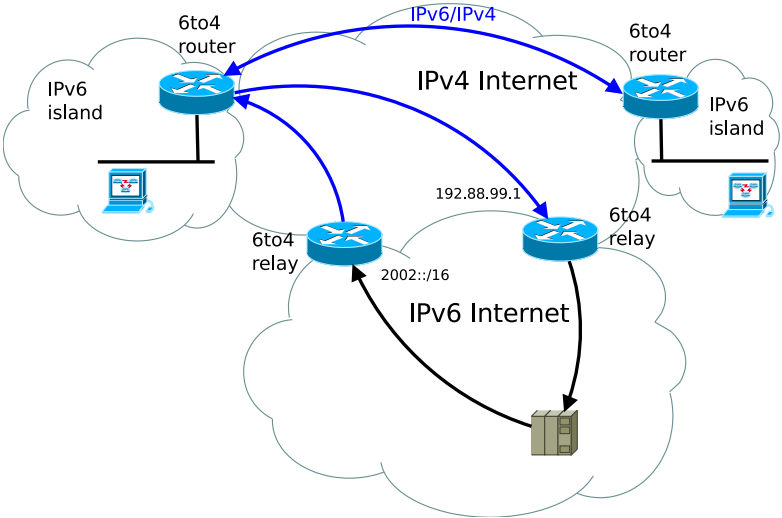
## 6to4

- jednoduchý a bezestavový
- potřebuje veřejnou IPv4 adresu
- problém anonymních bran
- chyby implementací ve Windows

## Teredo

- extrémně komplikovaný
- nepotřebuje veřejnou IPv4 adresu
- problém anonymních bran
- extrémně nespolehlivý

# 6to4


6to4
router
IPv6/IPv4
6to4
router
IPv6
island
IPv4 Internet
IPv6
island
192.88.99.1
6to4
relay
6to4
relay
2002::/16
IPv6 Internet

# Konfigurované tunely

- existovaly před IPv6
- mají pevně definované konce
- stabilní cesta dat
- spolehlivost určená jen koncovými body
- mnoho technologií
  - IPv6-in-IPv4 (proto-41, sit)
  - IPv6-in-UDP-in-IPv4 (AYIYA)
  - IPSec
  - Wireguard
  - L2TP
  - PPP-over-X
  - OpenVPN

# O službě SixXS

- již od roku 2000
- odrazový můstek pro rozjezd nového protokolu
- desítky tunelovacích serverů
- možnost získat IPv6 i bez veřejné IPv4 adresy
  - statický tunel V6V4
  - V6V4 s *heartbeatem*
  - V6UDPV4 tunel
- vypnuto 6. 6. 2017
  - začalo být kontraproduktivní
  - nativní konektivity je dostatek

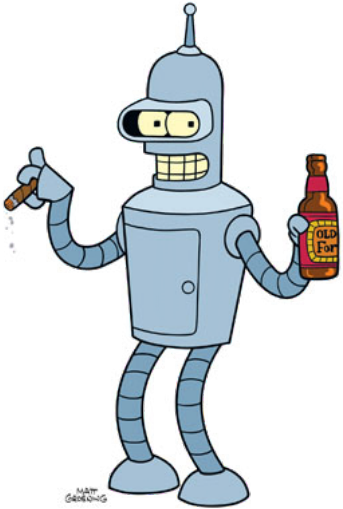
# Pohřbeno se SixXS

- protokol TIC pro komunikaci s tunnel brokerem
- protokol AYIYA pro tunelování IPv6-over-UDP-over-IPv4
- klient `aiccu` (open source)
- registrační systém (propriertární)
- server `sixxsd` (propriertární)
  - tunelování V6V4, V6UDPV4 a heartbeat tunel v jednom procesu
  - směrování v userspace, vysoký výkon

# Návykovost IPv6

- IPv6 používám od roku 2009
- 2 lokality nativně, 3 tunelem
- HE.net, kde je veřejná IPv4 adresa (1 lokalita)
- SixXS, kde není (2 lokality)
  - od 6. 6. 2017 offline ☹

# Postavíme si vlastní tunel



# Co budeme potřebovat

- dostatek IPv6 adres
  - minimálně /64 na jeden tunel + spojovačku
- IPv4 adresu
- nějaký software

# Kde získat adresy

- běžná nabídka VPS hostingů: nejvýše /64 na VPS
- navíc bez možnosti *naroutovat* podrozsah
- delegování adres podléhá pravidlům registrace

## Pravidla registrace v RIPE regionu

- držitel příslušné adresy musí být registrován v RIPE Whois databázi
- adresy mohou být alokované, nebo přiřazené
- jednou přiřazené adresy nejde pod-přiřadit

# 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*

# Jak přiřazovat adresy (a nezbláznit se z toho)

**IPv4**
- použití CGN ☺
- výjimky z pravidel pro *broadband pools* a *PtP spoje*

**IPv6**
- možnost agregovaného přiřazení, typicky pro *broadband pools*
- povinná evidence počtu použitých adres

## Příklad přiřazení rozsahu adres

```
inet6num:       2001:718:e::/48
netname:        CESNET-6BLUEBOX
status:         ASSIGNED
…
```

## Příklad agregovaného záznamu

```
inet6num:       2a03:3b40:200::/39
netname:        VPSFREE-IPV6-TUNNELS
status:         AGGREGATED-BY-LIR
assignment-size:48
…
```

# Adresní plán

- celkem k dispozici 512×/48
- první /48 vyhrazena pro koncové body tunelů
- další přiřazujeme v rastru /44
- prostor pro růst každého přídělu

| ID | Certifikát | Spojovačka | Přidělený prefix |
|---|---|---|---|
| 200 | spojovačka | | |
| 210 | oskar1 | 2a03:3b40:200::210 | 2a03:3b40:210::/48 |
| 220 | krcmar1 | 2a03:3b40:200::220 | 2a03:3b40:220::/48 |
| 230 | | 2a03:3b40:200::230 | 2a03:3b40:230::/48 |
| 240 | | 2a03:3b40:200::240 | 2a03:3b40:240::/48 |
| 250 | | 2a03:3b40:200::250 | 2a03:3b40:250::/48 |
| 260 | | 2a03:3b40:200::260 | 2a03:3b40:260::/48 |
| 270 | | 2a03:3b40:200::270 | 2a03:3b40:270::/48 |

## Ping-pong

```
$ ping 2a03:3b40:300::300
PING 2a03:3b40:300::300(2a03:3b40:300::300) 56 data bytes
From 2a01:430:0:fe0b::2 icmp_seq=1 Time exceeded: Hop limit
From 2a01:430:0:fe0b::2 icmp_seq=2 Time exceeded: Hop limit
```

## Eliminace ping-pongu

```
iface lo inet loopback
        up ip -6 route add unreachable 2a03:3b40:200::/39
```

# OpenVPN

- univerzální tunelovací nástroj
- režim TUN point-to-multipoint
- bezproblémový průchod NATy, minimální problémy s MTU
- autentizace X.509 certifikáty
- možnost vypnout šifrování a autentizaci provozu
  - hlavně kvůli výkonu a latenci

# Vydávání certifikátů

- samostatná certifikační autorita easyRSA3
- generování privátního klíče i certifikátu na serveru
- platnost certifikátu 1 rok
  - TODO: upozornění na konec platnosti
  - motivace 1× ročně kontaktovat ISP
- volba `unique_subject = no` pro snadné obnovování certifikátů
- generování konfiguračního souboru klienta
- možnost poslání žádosti o certifikát

# Konfigurace OpenVPN serveru

```
mode server
dev tun0
ifconfig 169.254.200.200 255.255.255.255
ifconfig-ipv6 2a03:3b40:200::200/64 2a03:3b40:200::200
route-ipv6 2a03:3b40:200::/40
client-config-dir /home/ansible/data/ccd
ccd-exclusive
…
auth none
cipher none
ncp-ciphers AES-256-GCM:AES-256-CBC
```

## Soubor s konfigurací pro daného klienta

```
iroute-ipv6 2a03:3b40:200::210/128
iroute-ipv6 2a03:3b40:210::/48
```

## Konfigurace OpenVPN klienta

```
client
remote ipv6tun01.vpsfree.cz 1194
remote-cert-tls server
auth none
cipher none
ncp-disable
```

# První zkušenosti

- funguje dle očekávání
- vestavěné filtrování BCP38 v OpenVPN
- snadná integrace s OpenWRT/LEDE
- vysoké paměťové nároky (problém 4/32)
- nízká dosažitelná rychlost (150 Mbps)

# Integrace s OpenWRT/LEDE/TurrisOS

## /etc/config/network

```
config interface 'ipv6tun'
        option ifname 'tunipv6'
        option proto 'static'
        option ip6addr '2a03:3b40:200::2xx/64'
        option ip6gw '2a03:3b40:200::200'
        option ip6prefix '2a03:3b40:2xx::/48'
```

# Reverzní DNS

- skrytý master server přímo na tunelovacím serveru
- přenos na veřejné servery spolku
- ručně spravovaná zóna
- možno automatizovat v budoucnu

# Jak se zapojit

- zejména pro lidi bez veřejné IPv4 adresy
- nutné rozumné koncové zařízení (OpenWRT/Linux)
- vhodná ochota aktivně řešit problémy, zejm. v beta verzi

**kontaktní adresa**:
`ipv6tun@vpsfree.cz`

# Další rozvoj

- ideálně **útlum**
- testování jiných tunelovacích protokolů (např. Wireguard)
- podpora pro V6V4 tunely
  - vestavěná v Linuxu
  - minimální overhead
  - neperzistentní konfigurace
- přemlouvání ISP, aby pohli s IPv6
  - ¾úspěch s A-net Liberec

Děkuji za pozornost


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