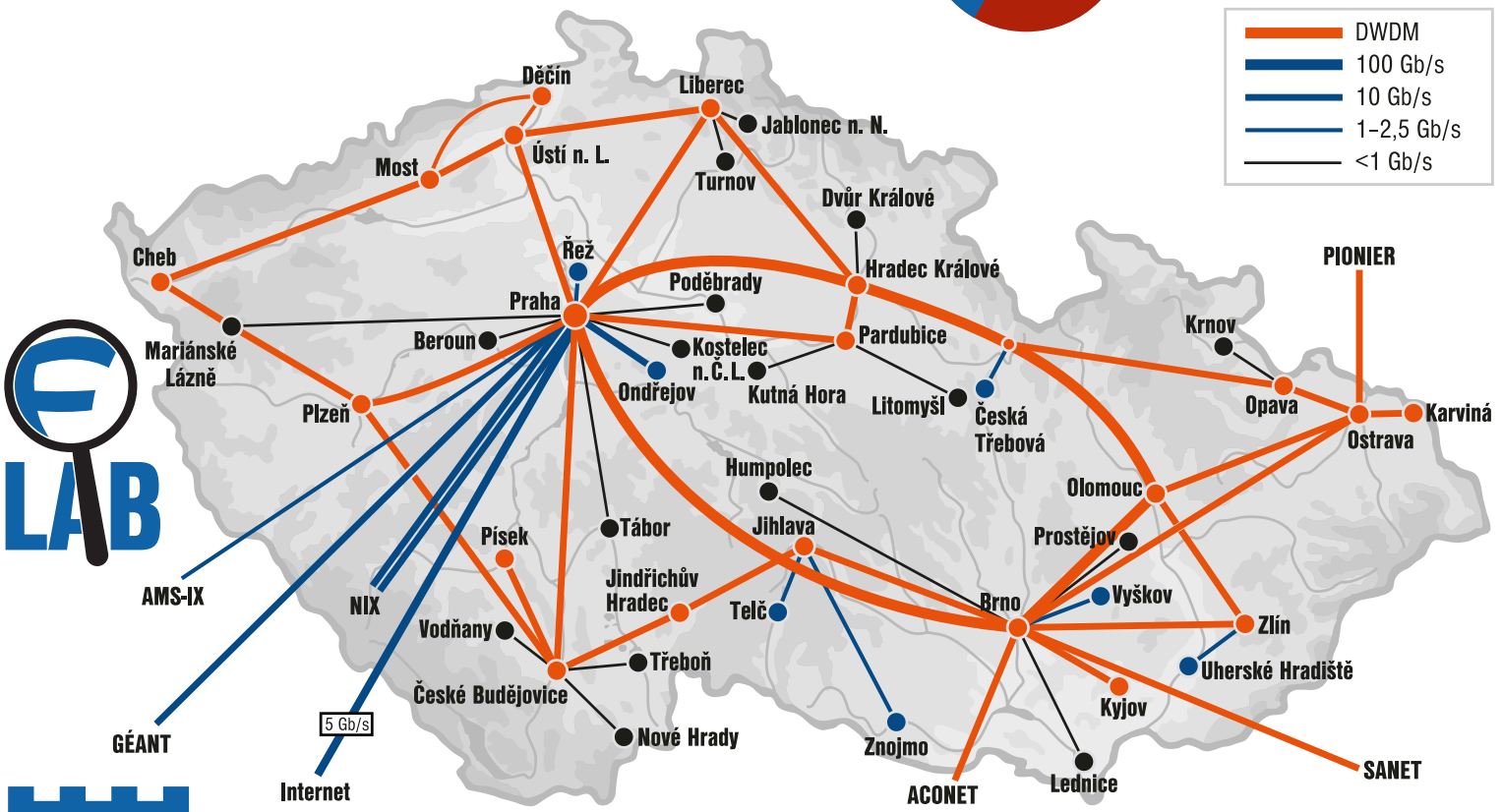
Jak se měří Internet

Ondřej Caletka

1. listopadu 2014

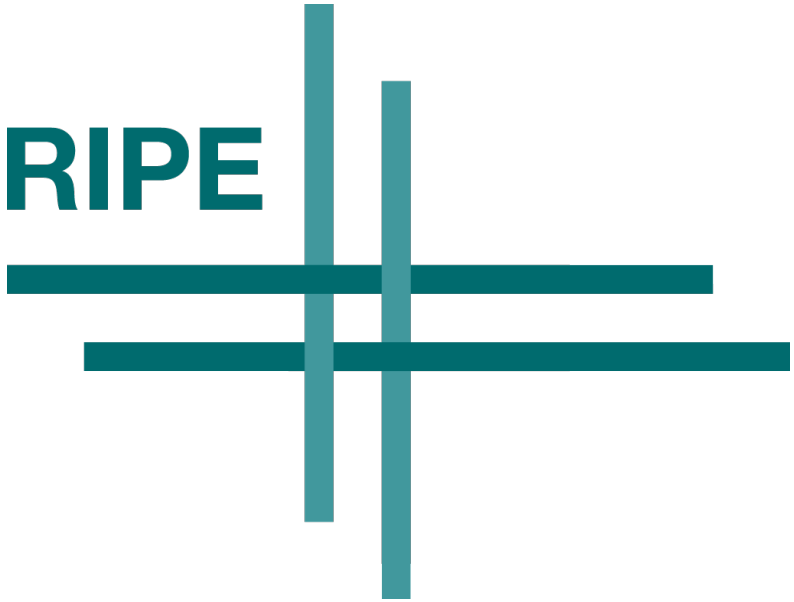
O sdružení CESNET



Obsah

Réseaux IP Européens

- otevřená komunita zaměřená na rozvoj internetového protokolu v Evropě a dále
- založena v roce 1989 za účelem technické a administrativní koordinace IP sítí
- bez formálního členství, čestný předseda Rob Blokzijl, současný předseda Hans Petter Holen
- určuje politiky řízení Internetu v regionu



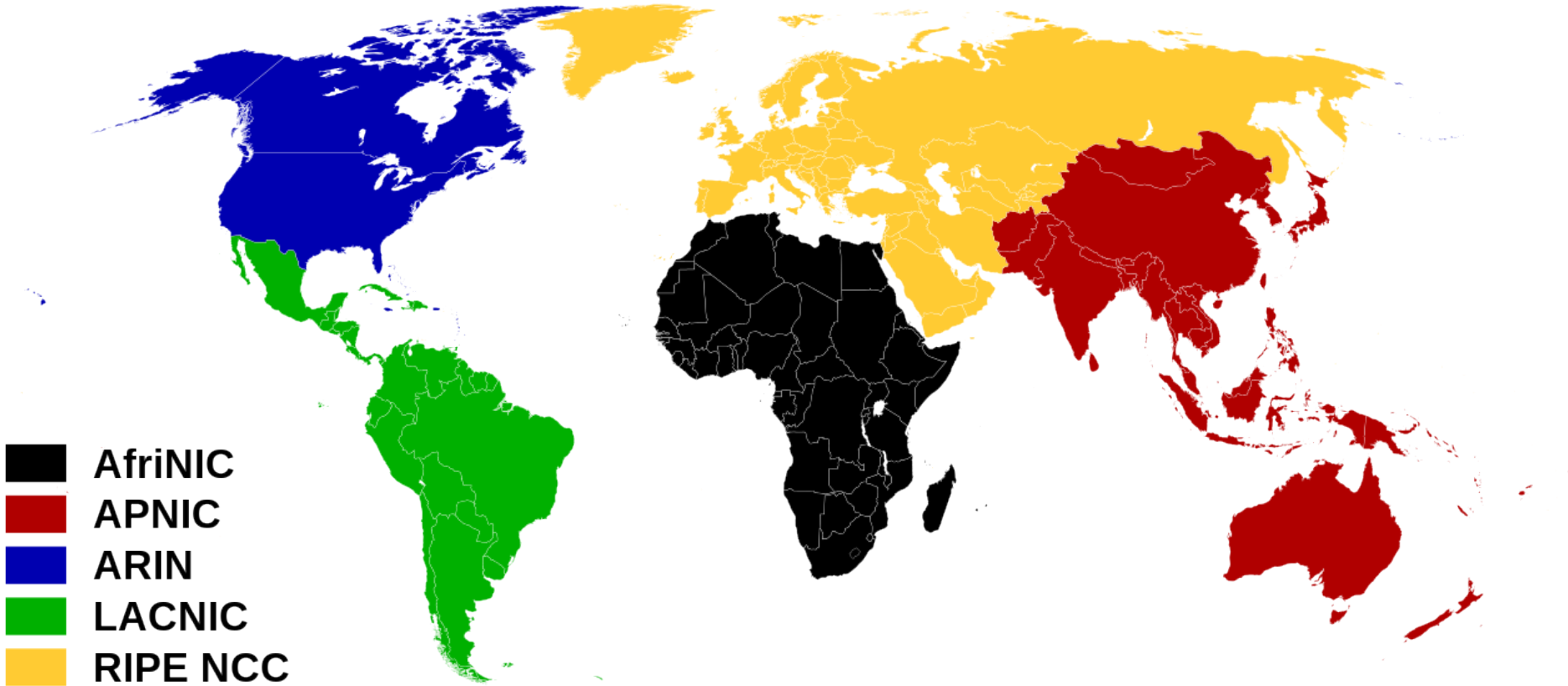
RIPE Network Coordination Centre

- sekretariát pro potřeby RIPE komunity
- neziskové sdružení se sídlem v Amsterdamu
- členy jsou ISP alias *Local Internet Registry*
- vykonává funkci registru IP rozsahů pro Evropu a Střední východ
- výzkumné projekty zaměřené na zkvalitňování Internetu

RIPE NCC

CESNET

Regionální registry



RIPE Atlas

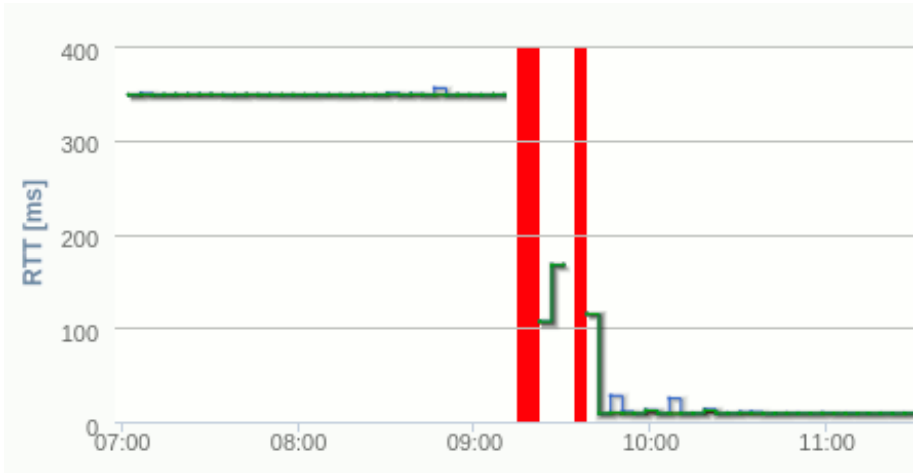
- systém aktivního měření Internetu
- budován od roku 2010
- používá hardwarové sondy hostované u dobrovolníků
- více než 7000 připojených sond (230 v ČR)
- vestavěná a uživatelsky definovatelná měření
- zaměřeno na nejnižší úroveň funkce IP sítí
  - ping
  - traceroute
  - DNS

Sonda RIPE atlas

- speciální hardware použitý s ohledem na nízkou spotřebu a cenu
- napájení z USB, 10/100Mbps připojení do sítě
- žádné ovládací prvky, žádné ovládací rozhraní, žádný otevřený port
- může být zapojena za NAT
- udržuje spojení s řídicími servery u RIPE NCC
- provádí měření a posílá výsledky řídicím serverům

Co sondy měří

- Ping vybraných cílů
- Traceroute k vybraným cílům
- DNS dotazy ke kořenovým serverům
- HTTP dotazy na `ripe.net`
- SSL spojení k `ripe.net`
- Uživatelská měření



Uživatelská měření

- možnost spouštět měření na celé síti sond
- platba virtuální měnou
- získání kreditu za hostování sond
- kompletní přístup pomocí JSON REST API
- oficiální knihovna Sagan pro Python

Uzly v síti RIPE Atlas

Sondy verze 1 a 2

- založeny na Lantronics Xport Pro
- procesor bez MMU, uClinux
- měřicí software založený na Busyboxu
- výroba zastavena v roce 2012

Lantronics Xport Pro

Síťové rozhraní

- 10Base-T a 100Base-TX Link
- Konektor: RJ45
- Protokoly: TCP / IP, UDP / IP / **IPv6 (ve verzi s Linuxem)**, ARP, ICMP, SNMPv2, HTTP, SMTP, SSHv2, SSLv3, PPP, AutoIP, RSS a SYSLOG

Zabezpečení

- SSLv3 a SSHv2 Client & server, volitelné 128/256/512/1024 Bit certifikáty
- Šifrování: AES, 3DES a RC4
- Autentizace: SHA-1, MD5, Base-64 šifrovaný seznam uživatelů

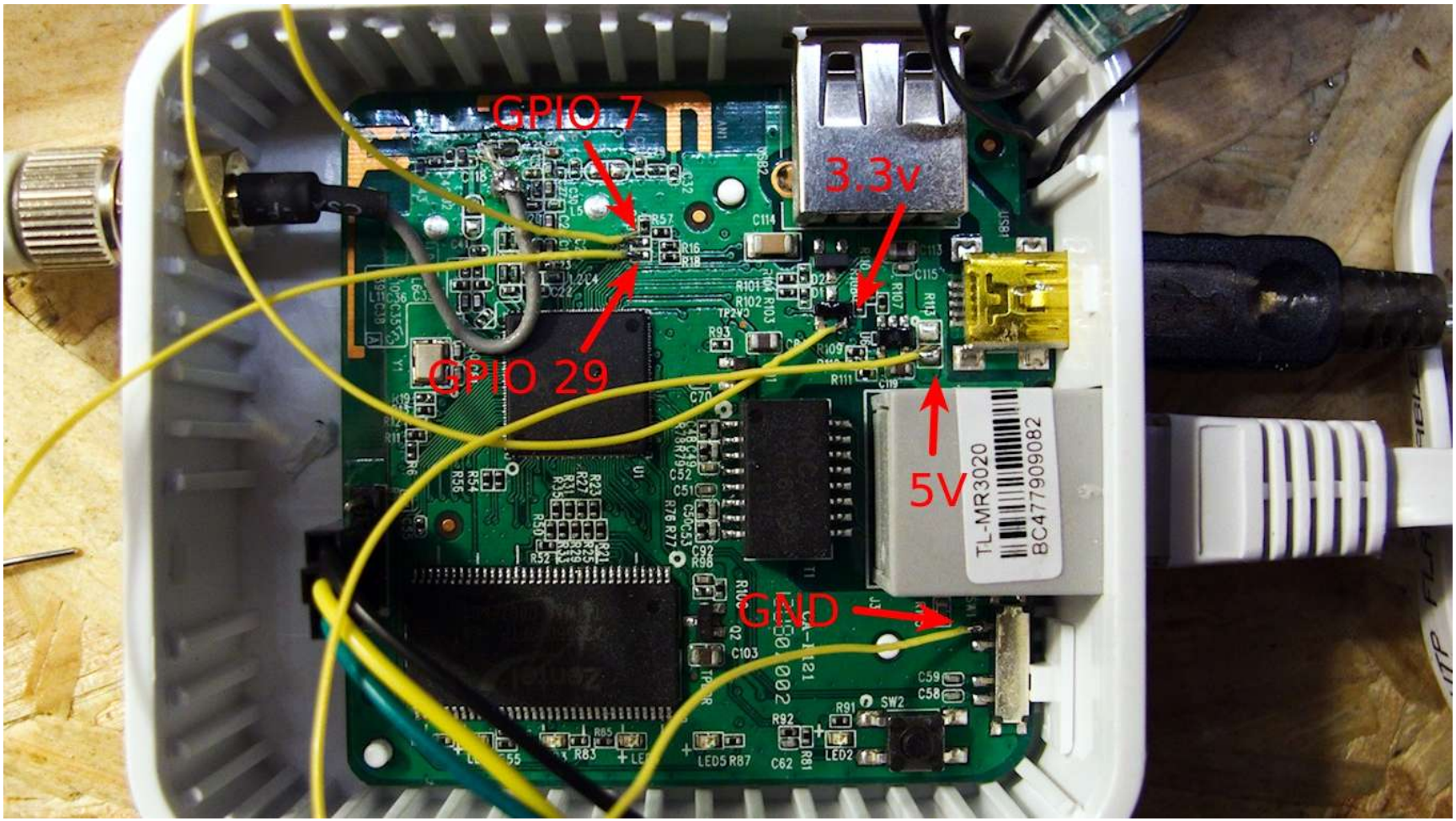
zdroj

CESNET

Sondy verze 3

- založeny na TP-Link MR3020
- výkonnější a levnější
- firmware založený na OpenWRT
- USB flash disk pro OS a data
- vestavěná Wi-Fi není SW podporovaná

Tohle se sondou neprovádějte ☺

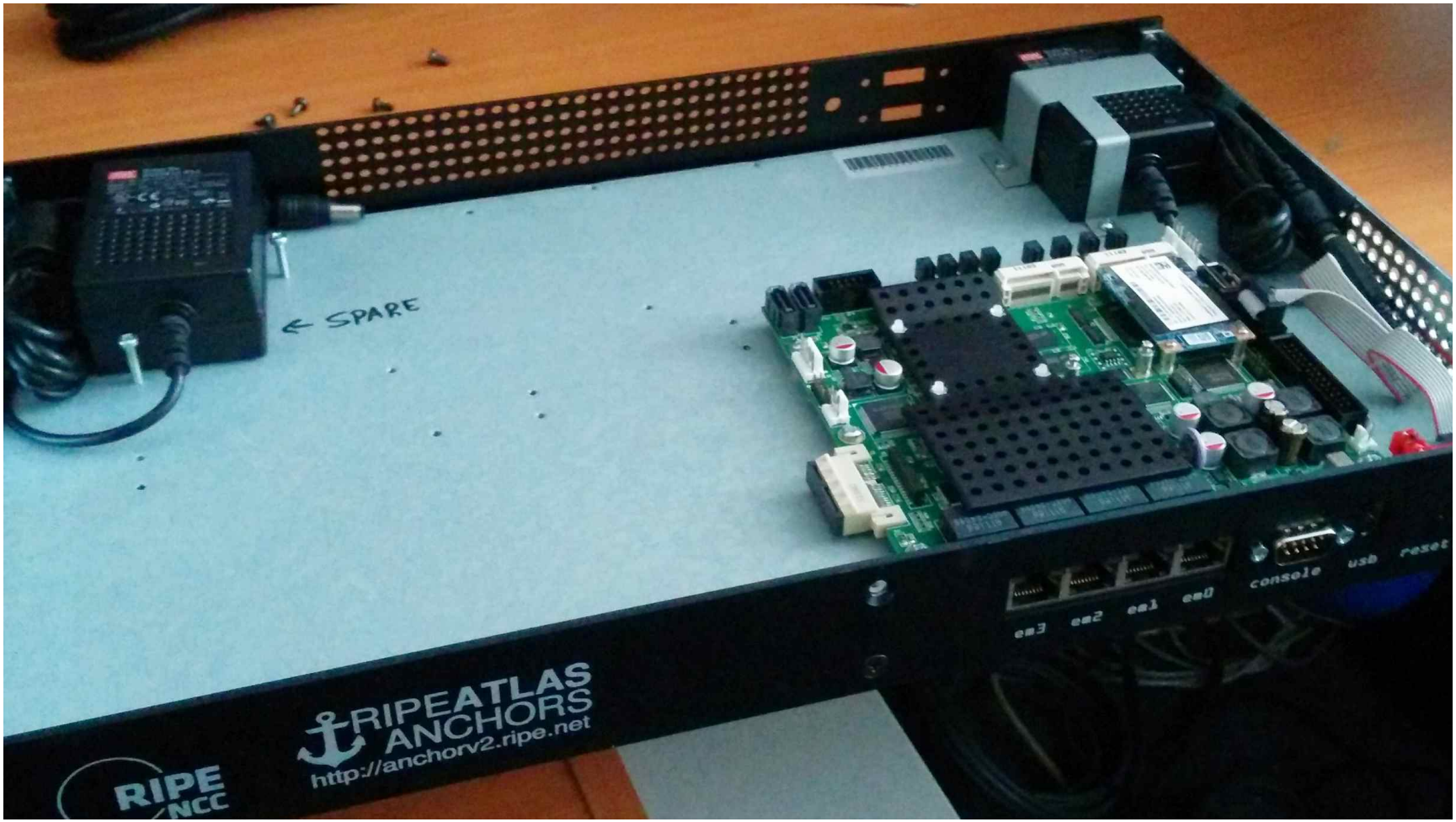


zdroj

Sondy Atlas Anchor

- výkonné sondy určené do datových center
- sondu zakupuje hostující organizace za 770 €
- založeno na x86 platformě Soekris Net6501-70
- slouží také jako cíl pro měření malých sond
- 80 sond po světě, 3 v ČR

Uvnitř sondy Atlas Anchor



Služby sondy Atlas Anchor

Autoritativní DNS server

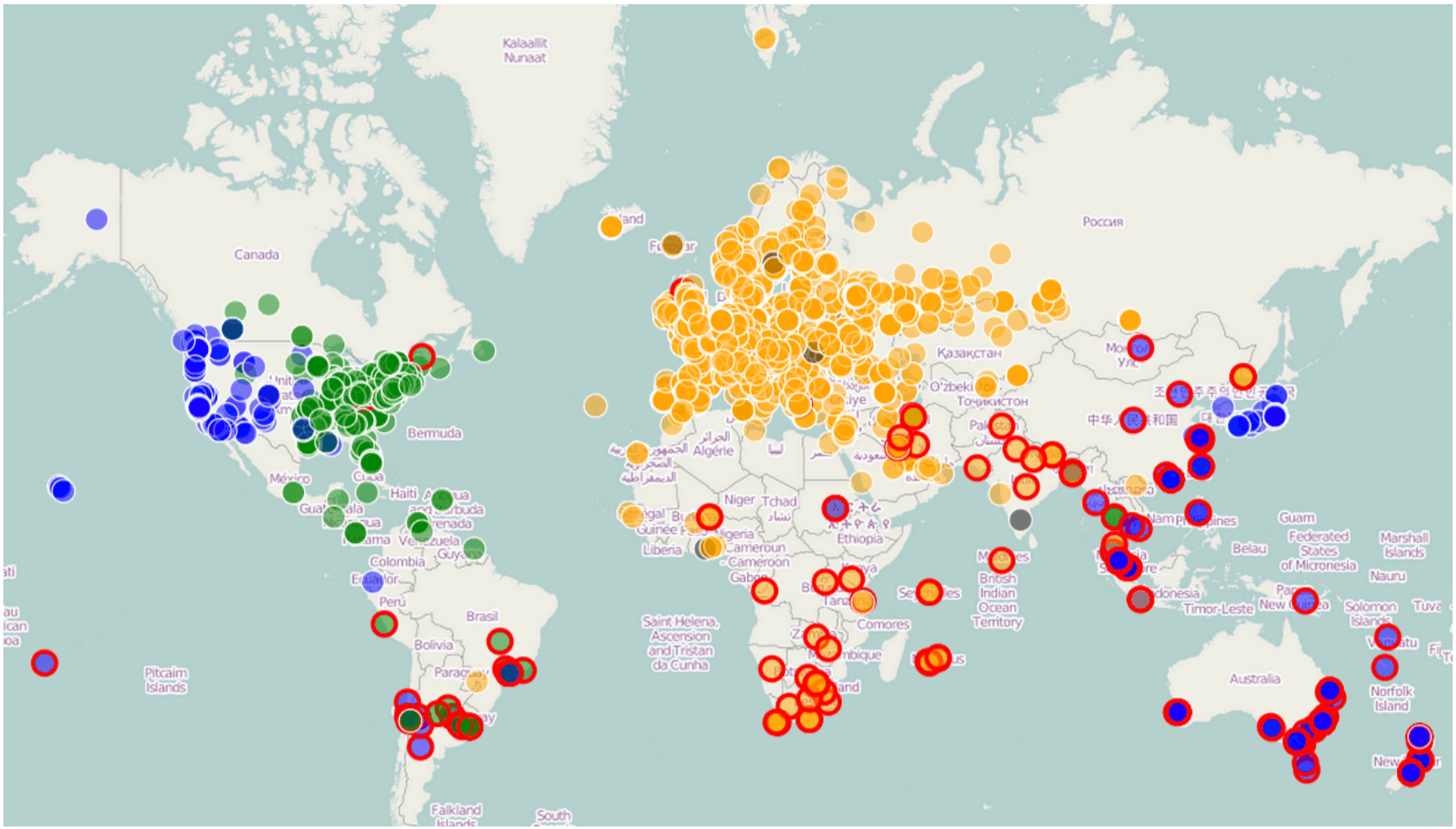
```
$ dig 512.4.dns.cz-prg-as2852.anchors.atlas.ripe.net txt
"XXXXXXXXXXXXXXXXXXXXXXXXXXXX…
…XXXXXXXXXXXXXXXXXXXXXXXXXXXX"
```

HTTP(S) server

```
$ curl http://cz-prg-as2852.anchors.atlas.ripe.net/3
{
      "anchor": "cz-prg-as2852.anchors.atlas.ripe.net",
      "client": "2001:718:1:6::134:196",
      "payload": "AAA"
}
```

Zajímavé výsledky

Analýza CDN Wikipedie



Amsterdam Ashburn San Francisco

zdroj

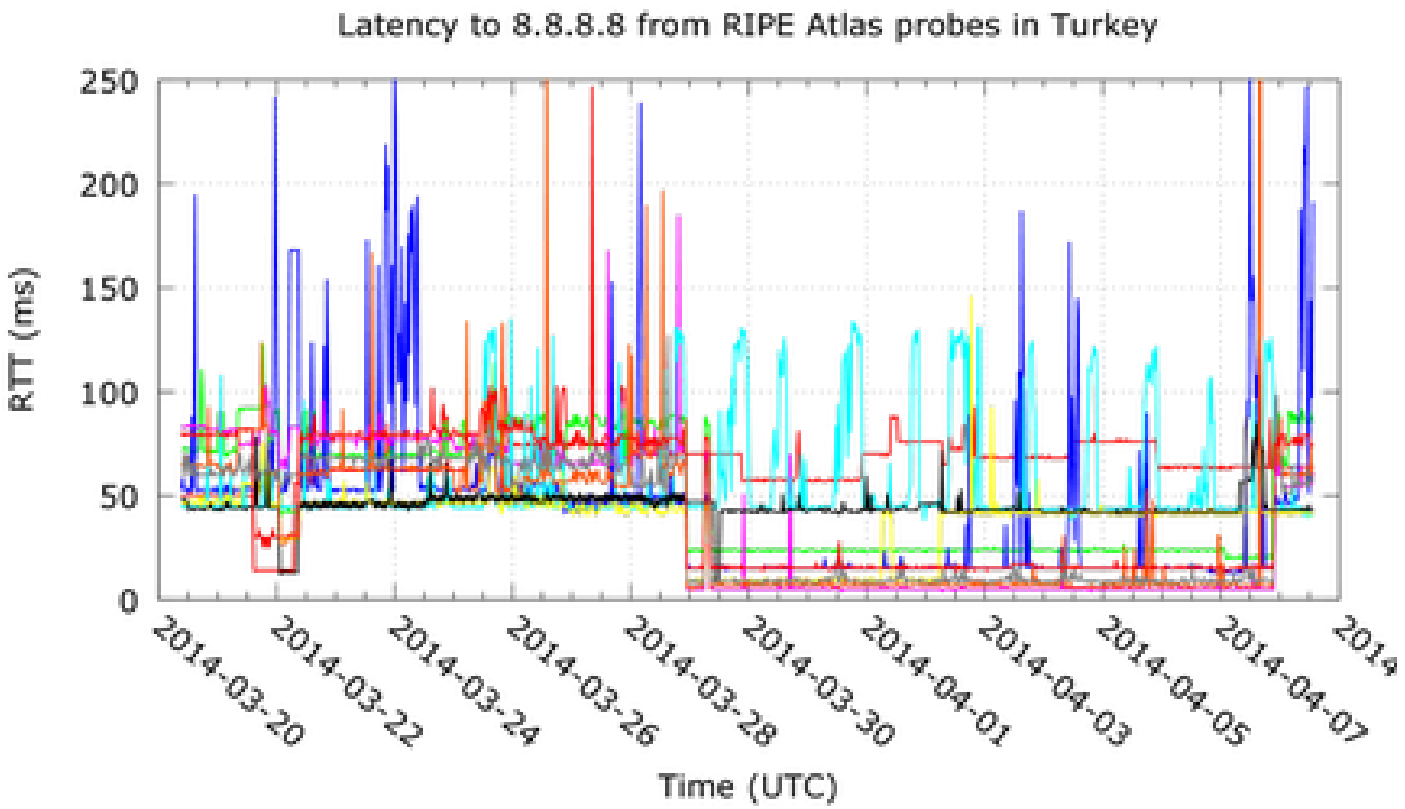
Únos DNS v Turecku ①

21. 3. 2014 zablokován Twitter na DNS serverech ISP
25. 3. 2014 zablokován přístup k Google Public DNS a podobným
28. 3. 2014 nainstalován falešný DNS server na 8.8.8.8

Únos DNS v Turecku ②

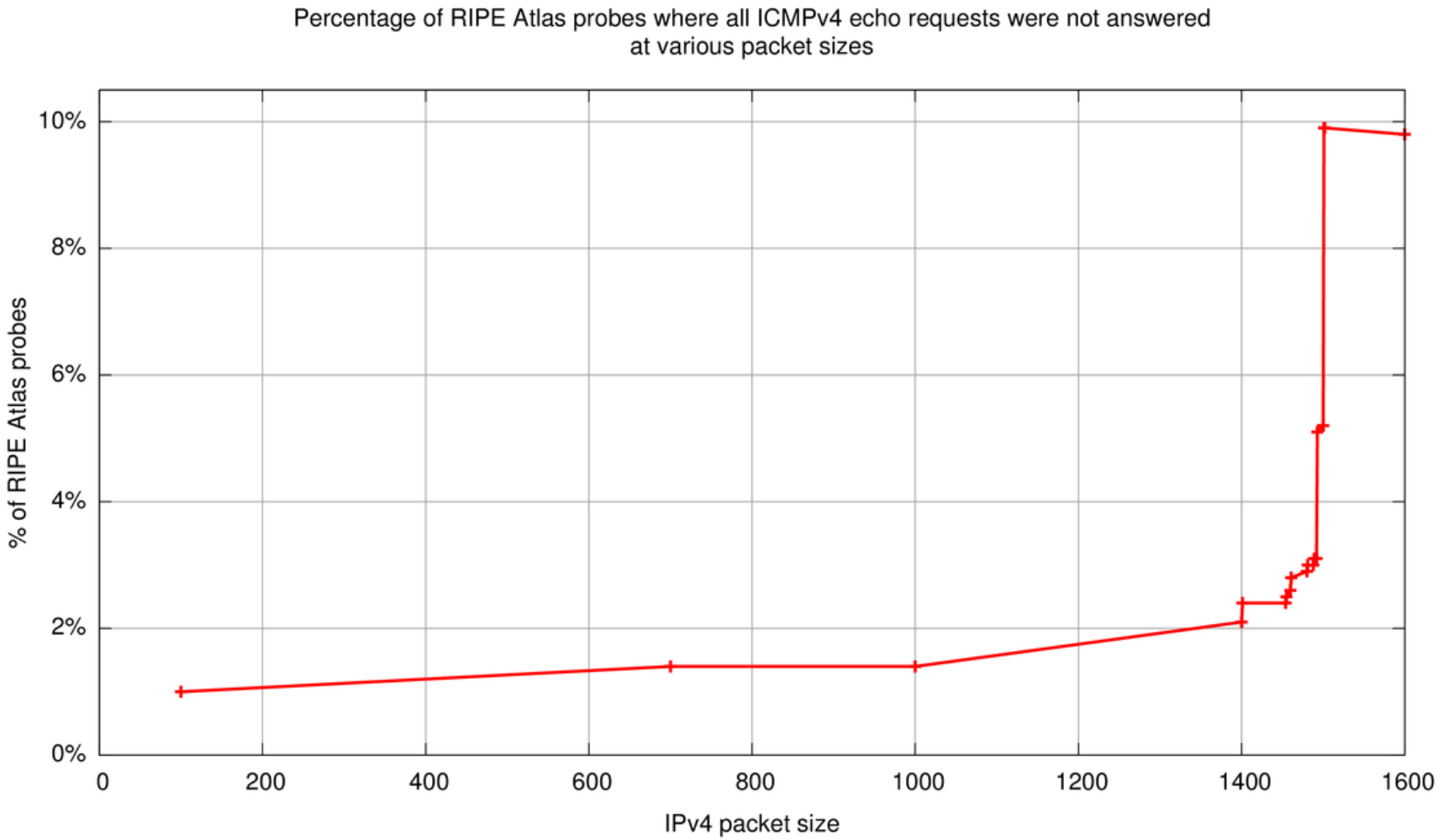
4. 4. 2014 ukončeno lhaní o Twitteru a Youtube
7. 4. 2014 ukončen únos DNS serverů

nikdo se k incidentu nevyjádřil



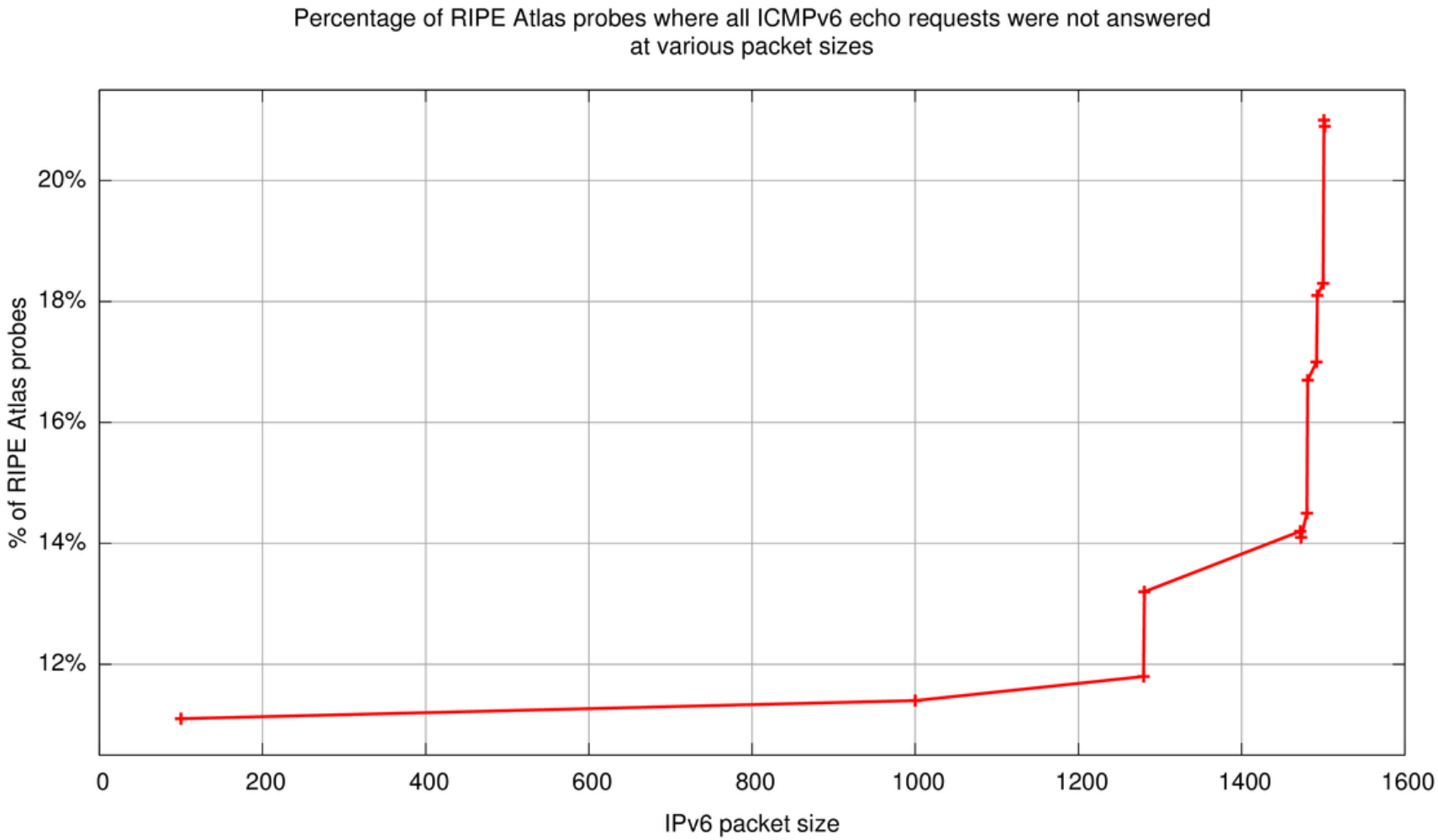
zdroj

Problémy s MTU na IPv4



zdroj

Problémy s MTU na IPv6



zdroj

Jsou si všechny IP adresy rovny?

- dědictví pro classfull routingu
- adresy končící `.0` nebo `.255` jsou mylně považovány za adresy sítě/broadcastu
- 2 – 4 % sond není schopno pingnout adresu `.0`
- výrazně vyšší zastoupení u adres z bývalé třídy C (`192.* – 223.*`)

Příklad

Síť: `192.0.2.0/23, (192.0.2.0 – 192.0.3.255)`
Problémové adresy: `192.0.2.255` a `192.0.3.0`

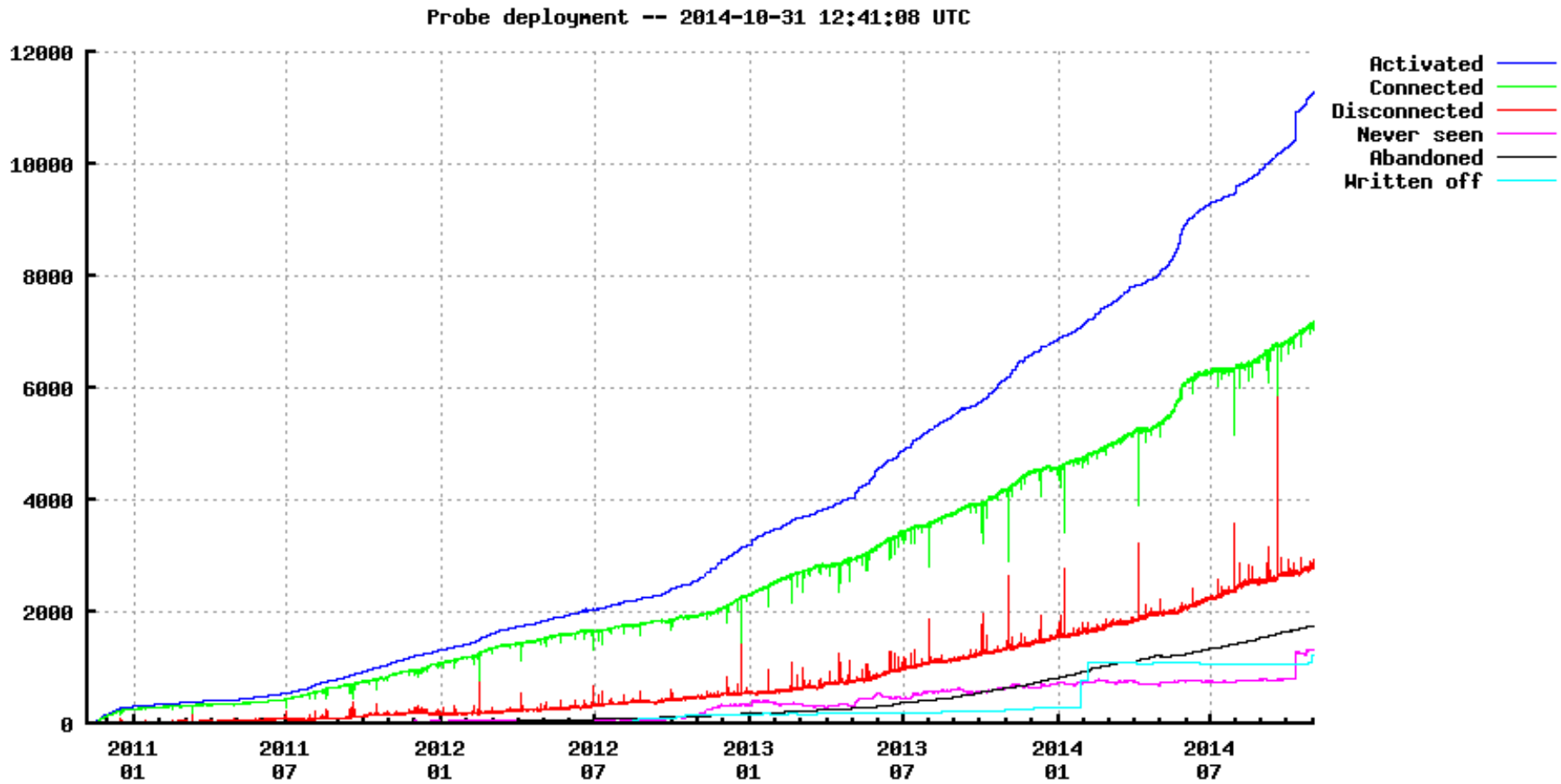
zdroj

Jak se zapojit

Pokrytí sondami Atlas Anchor

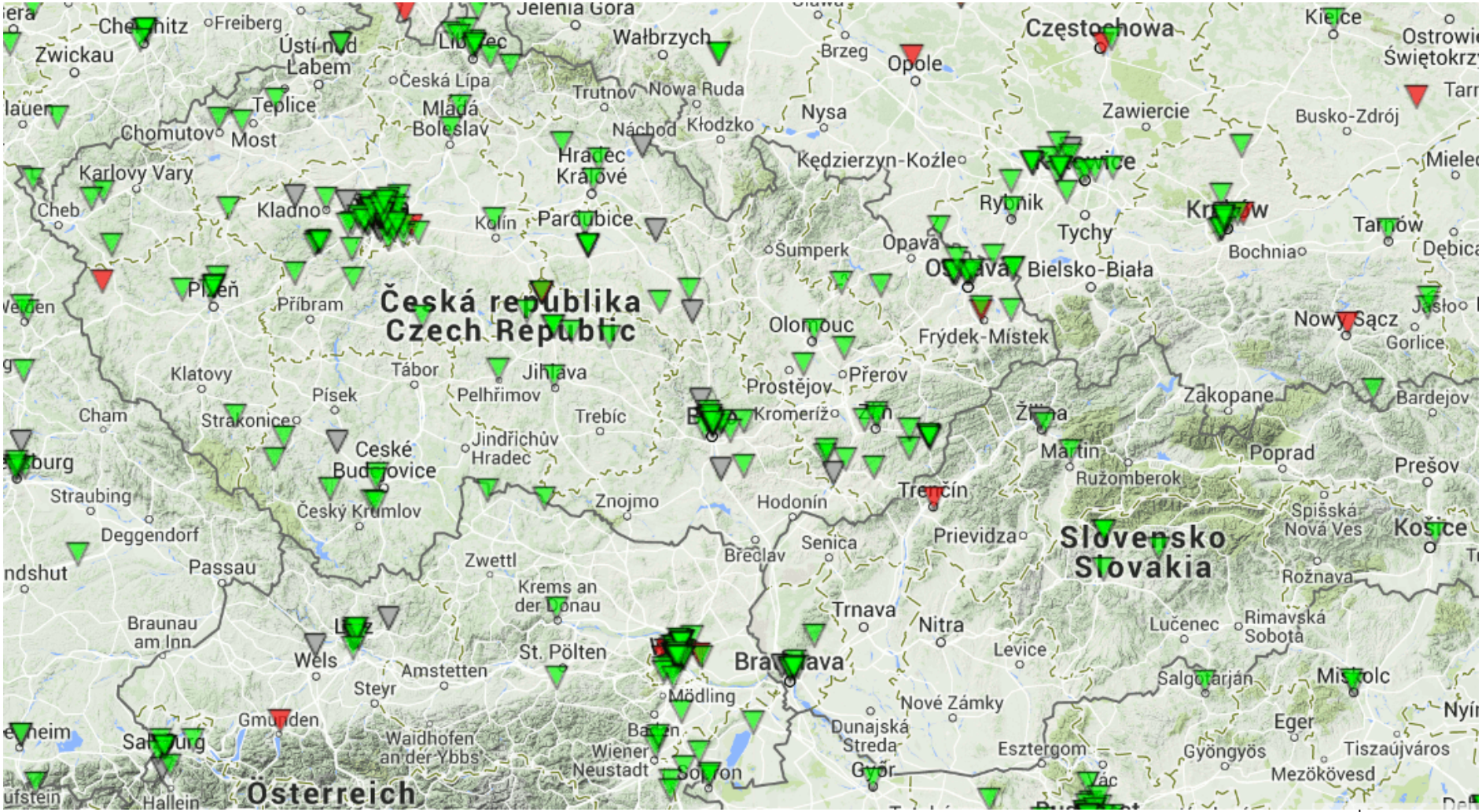
zdroj

Aktuální počet sond



zdroj

Aktuální pokrytí regionu



zdroj

Jak se zapojit

- hostujte sondu
  - zejména bydlíte-li mimo velká města
  - nebo není-li v aut. systému vašeho ISP dostatek sond `https://stat.ripe.net/widget/atlas-probes`
- měřte a zpracovávejte
  - kredit je možné získat od jiných uživatelů (třeba ode mě)
  - pro větší projekty stačí požádat s námětem přímo RIPE NCC, rádi poskytnou kredit, případně odstraní některá omezení
  - možno prezentovat své výsledky před RIPE komunitou `http://www.ripe.net/ripe/raci`

FAQ k sondám ①

Musí být sonda v provozu 24 hodin denně?

Měla by být. Každé úmyslné odpojení sondy poškodí měření, která na ní běží.

Může být za NATem/firewallem?

Za NATem ano, za firewallem jen takovým, který neblokuje pokusy o spojení z vnitřní sítě a reakce na ně.

Nebude sonda odposlouchávat provoz?

Nebude; je ale doporučeno zapojit ji tak, aby ani nemohla (např. samostatná VLAN).

Potřebuje sonda DHCP server?

Je možná i ruční konfigurace, ale nastavení IP adresy se provádí prostřednictvím www stránek `https://atlas.ripe.net`

FAQ k sondám ②

Proč není sonda k dispozici jako virtuální appliance?

Virtualizované sondy byly vyhodnoceny jako nevyhovující kvůli nedeterministickým změnám latence.

Dokáže sonda měřit přenosovou rychlost?

Ne, taková měření nemají velký praktický význam a jsou potenciálně nebezpečné z hlediska DoS. Možná hledáte projekt SamKnows.

K čemu je na sondě přepínač?

Jedná se o dědictví po původním účelu routeru, pro RIPE Atlas sondu nemá žádný význam.

Závěr

Děkuji za pozornost

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