RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RIPE NCC DNS Update

Anand Buddhdev | 26 May 2016 | RIPE 72

K-root

Status

- Active at 39 sites
  - Five “core” sites - multi-server, high capacity
  - 34 “hosted” sites - single-server
- Fully up-to-date OS and name server software
- https://k.root-servers.org/
  - Updated with a new map and statistics
  - Integrated into www.ripe.net
- Seven /24 IPv4 prefixes returned

Routing policy changes

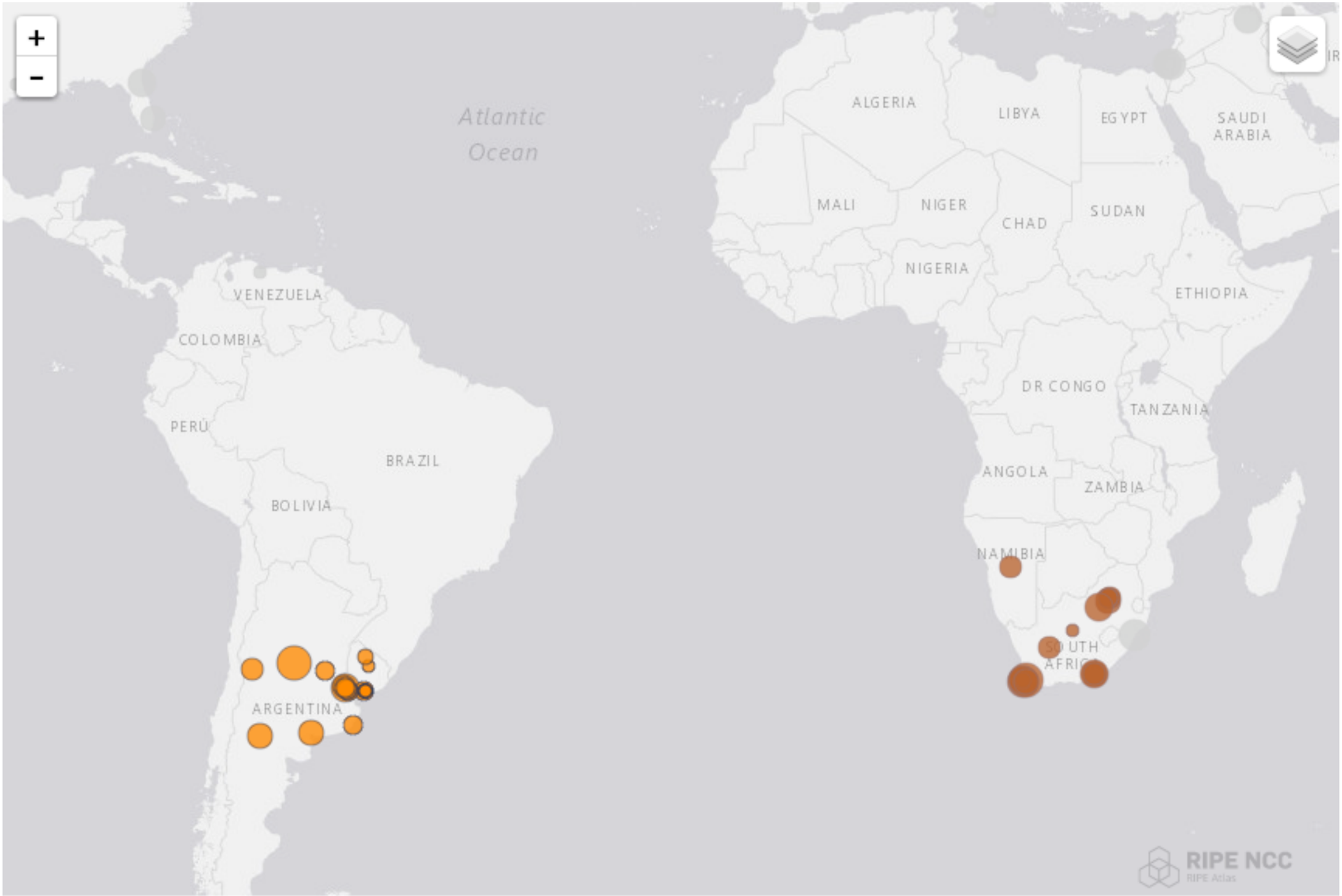
- No more “local” sites
  - Stopped using BGP NO_EXPORT community
- K-root hosts may choose how far to propagate prefixes
  - Based on host’s capacity and network policy
- Allows clients to have a better path to K-root
  - Avoids artificial black holes
  - Lets BGP do its job :)

Effects of routing policy

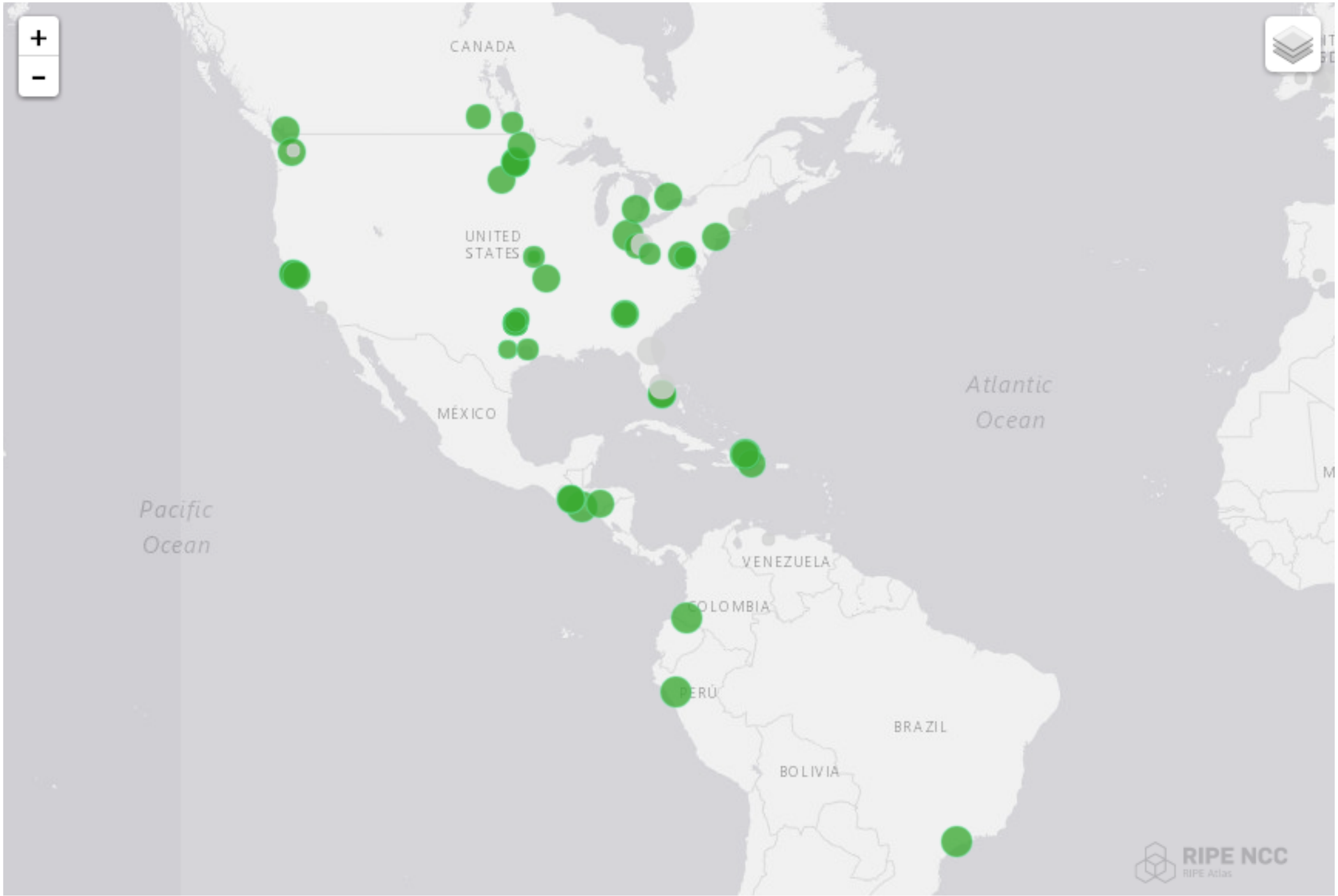
Athens


MONTENEGRO
BULGARIA
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
ALBANIA
GREECE
Gulf of Taranto
Ionian Sea
Aegean Sea
Sea of Crete
Mediterranean Sea
CYPRUS
RIPE NCC
RIPE Atlas

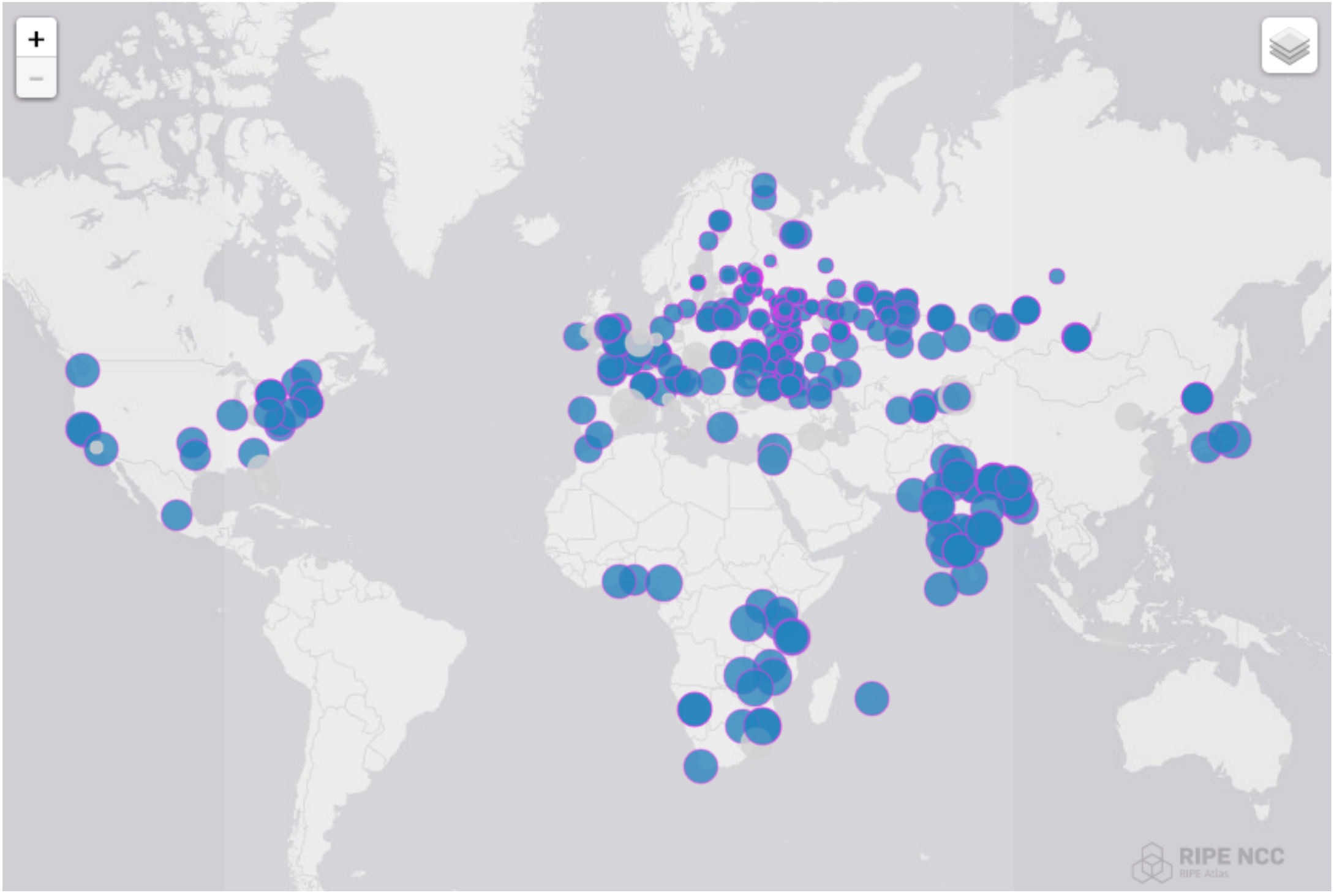
Johannesburg and Montevideo



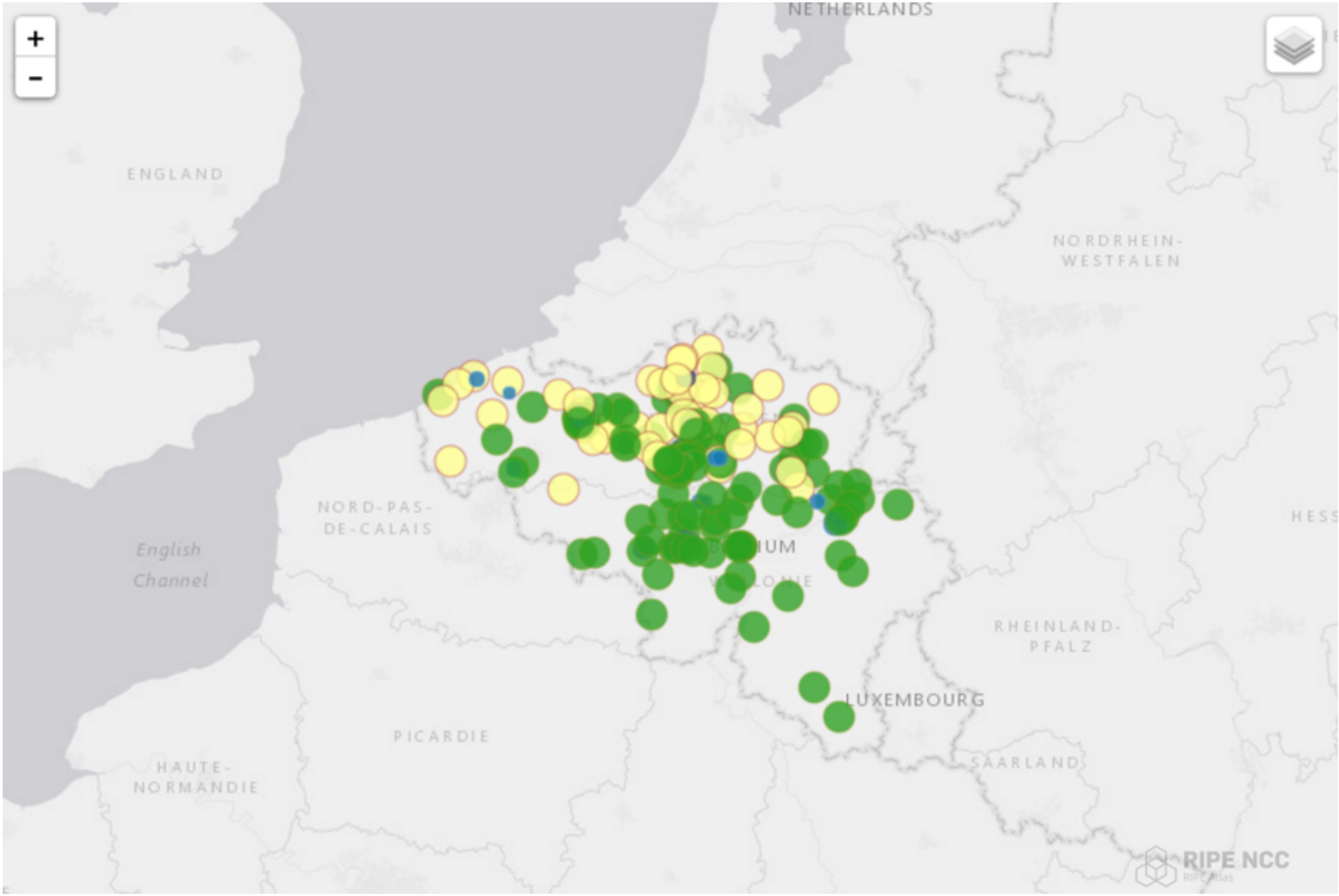
Kansas City (MO)



St. Petersburg



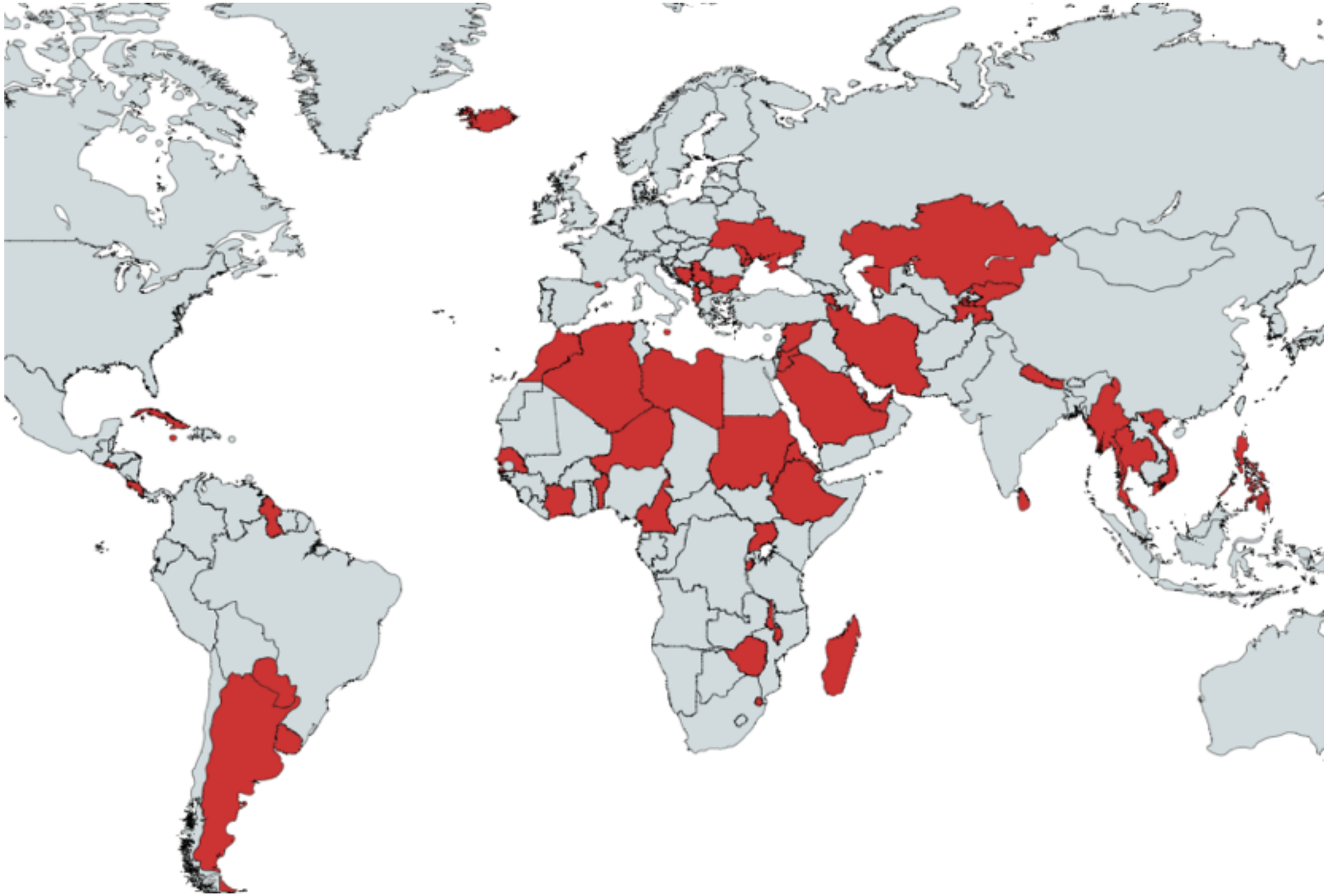
Poorly served regions



ccTLDs

Secondary DNS

77 ccTLDs with RIPE NCC DNS



Status

- RIPE-663 published in December 2015
- We are evaluating all ccTLDs
  - Some ccTLDs will stop receiving service
  - One ccTLD has pre-emptively migrated away

Authoritative DNS

dig ripe.net ns +short

manus.authdns.ripe.net.

sns-pb.isc.org.

sec3.apnic.net.

tinnie.arin.net.

c1.authdns.ripe.net

c2.authdns.ripe.net

Resilience for ripe.net

- DDoS attacks are increasing
  - RIPE NCC services affected when ripe.net name servers are unavailable
- We increased resiliency
  - Added CloudFlare name servers to our NS RRset
  - CloudFlare has many POPs around the world and can absorb many gigabits/s of inbound traffic
  - Short-term arrangement
  - After RIPE 72, we will do a request for proposals, for long-term secondary DNS for ripe.net

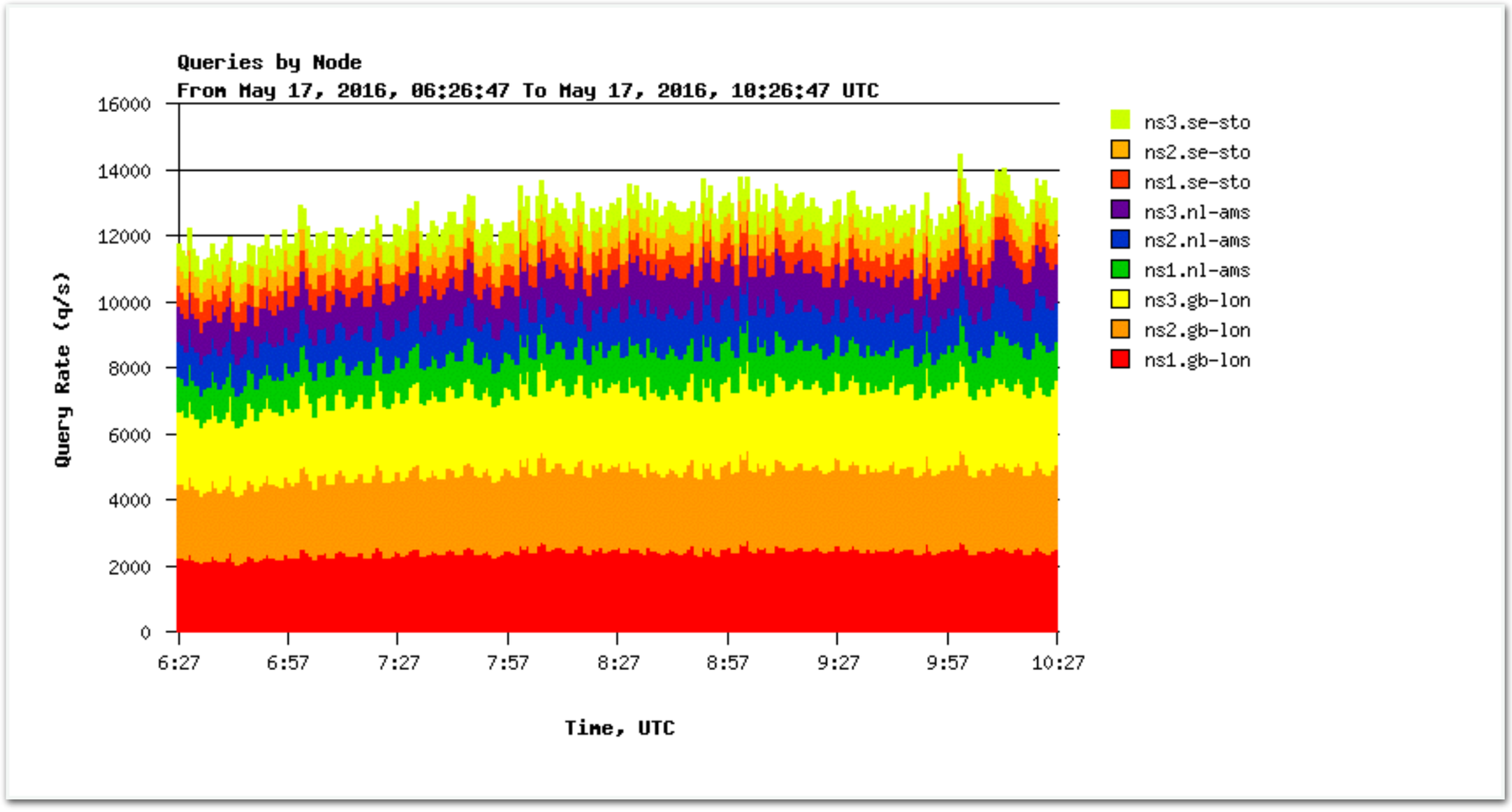
Secondary DNS for LIRs

domain: X.Y.in-addr.arpa
descr: example
admin-c: example
tech-c: example
zone-c: example
nserver: ns1.example.com
nserver: ns2.example.com
nserver: ns.ripe.net

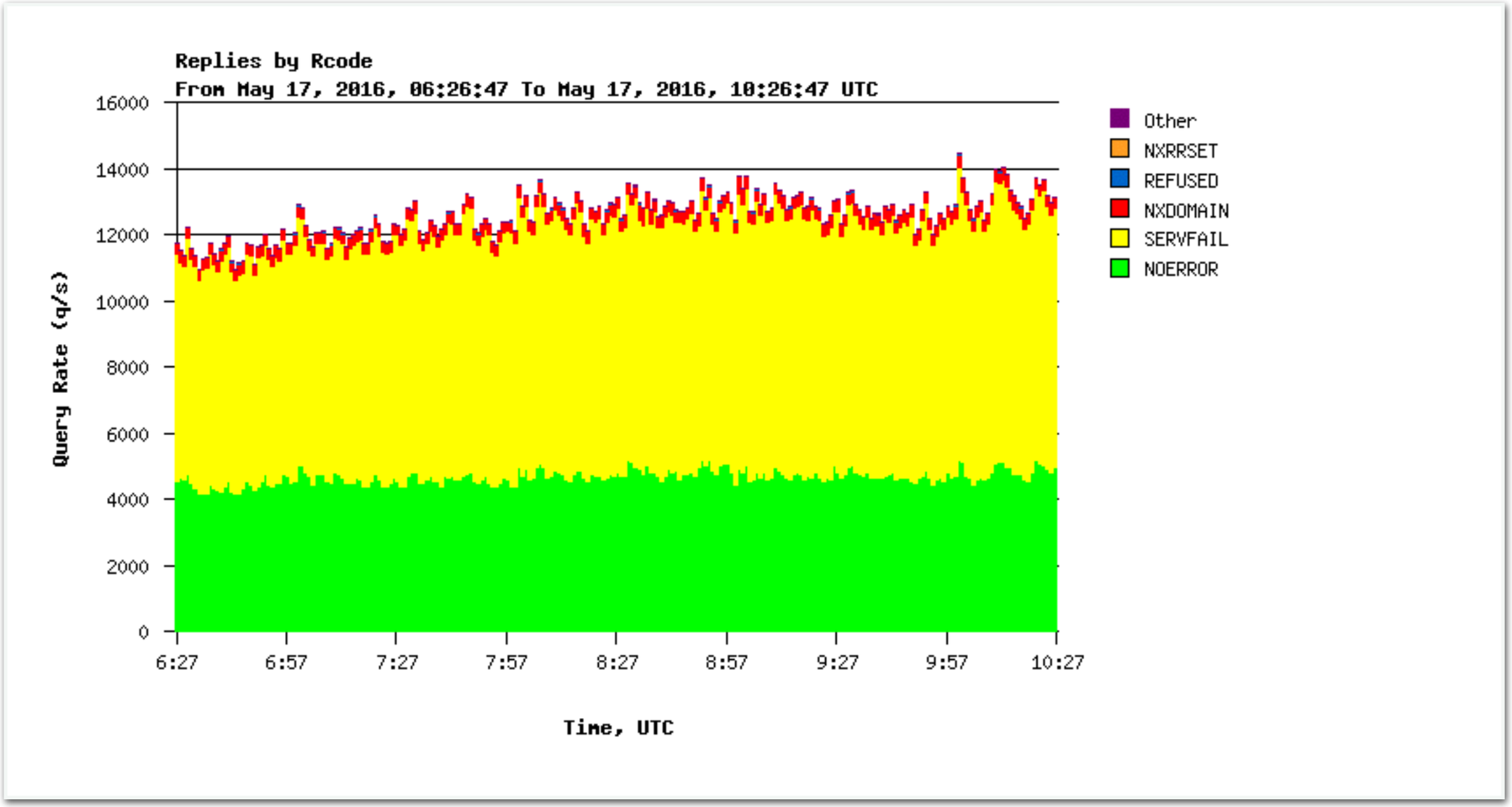
Provisioning on ns.ripe.net

- Only allowed for /16 IPv4 or /32 IPv6 reverse DNS zones
- DNS pre-delegation checker skips ns.ripe.net
  - No easy way to do pre-delegation checks for this setup
- After **domain** object creation or modification, hidden masters and ns.ripe.net are configured
- Often, the zone cannot be transferred

Query rate at ns.ripe.net



RCODE rate at ns.ripe.net



ns.ripe.net numbers

- 4,069 zones configured
- 1,946 zones expired (47%)
- 14,000 q/s, peaking at 25,000 q/s
- 38% responses have rcode SERVFAIL

Problems with ns.ripe.net service

- Refreshing expired zones perpetually is a burden
- Two distribution servers and nine publication servers leads to many failed AXFR attempts
  - Exposed bugs in name server implementations :)
  - A problem, nevertheless
- Users don’t understand that ns.ripe.net is anycasted, and uses hidden masters for XFR

Future of ns.ripe.net service

- Retire the service - most operators now have good DNS infrastructure, or
- Move configuration of the service into LIR portal
  - Allows proper pre-delegation checks
  - Users could specify alternative master servers, and optionally ports and TSIG keys

DNScheck -> Zonemaster

- DNScheck used for pre-delegation checks for reverse DNS delegations
  - Development has stopped - no features or bug fixes
- Zonemaster is its successor
  - New code all tests properly defined
  - More modular architecture
  - Well-defined API for submitting checks and getting results
- We plan to switch to Zonemaster later in 2016

DNSSEC

DNSSEC algorithm roll-over

- We announced plans to do algorithm roll-over at RIPE 71
- Successfully achieved in November 2015
- All RIPE NCC zones signed with SHA256
- Interesting lessons learnt; experiences in RIPE Labs article:
  - https://labs.ripe.net/Members/anandb/dnssec-algorithm-roll-over

Questions

anandb@ripe.net
@aabdnn