RIPE NCC DNS Update

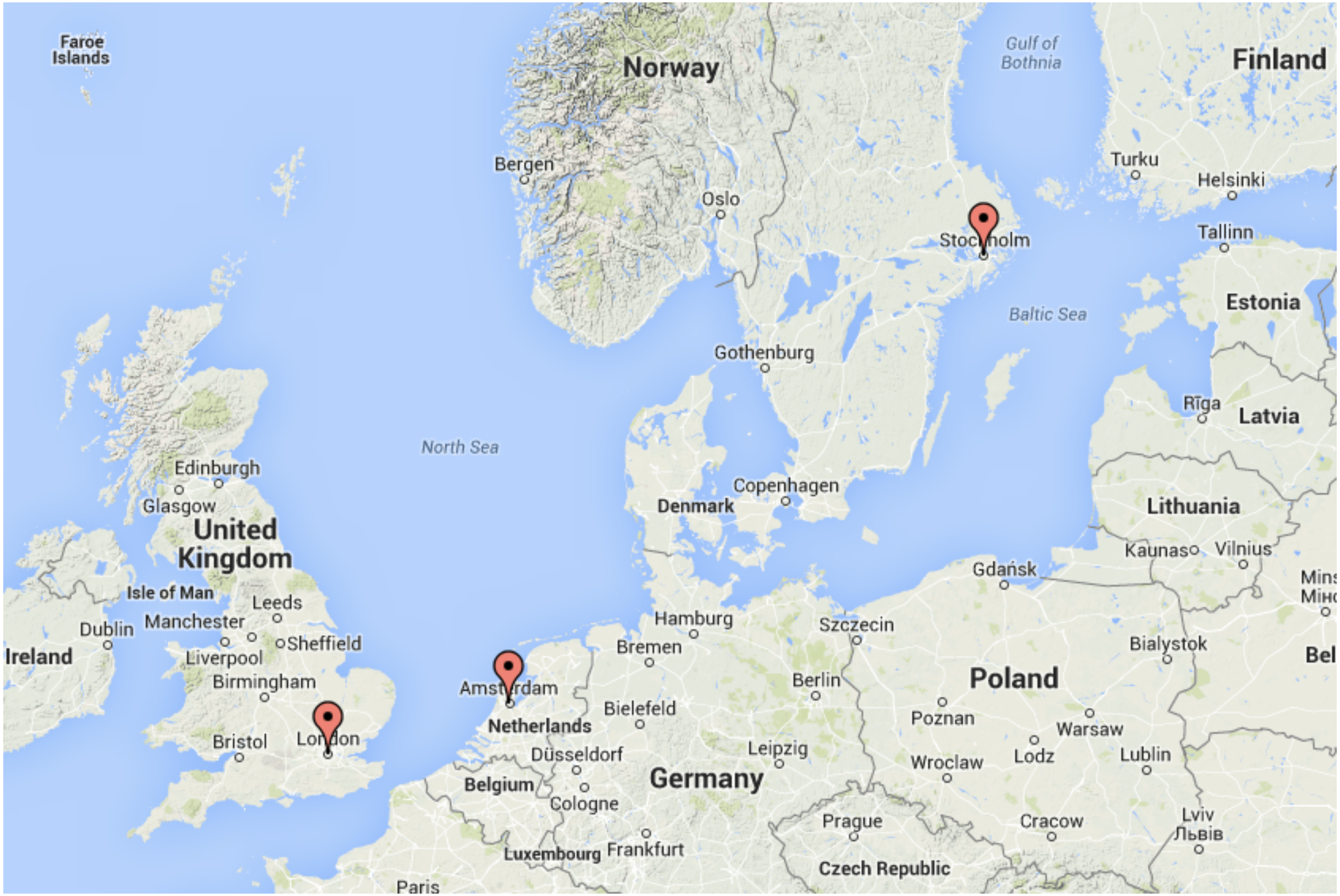
Anand Buddhdev

RIPE 69 | London - UK | 6 Nov 2014

K-root

- Renewal of hardware at all existing global instances
- Upgrade to NSD 4
  - Introduction of BIND and Knot
- Single-server setups when renewing local instances
- Proposal for experiment on RIPE Labs
  - Lower latency and hop count
  - Improve coverage in less well-served areas

Authoritative DNS



Authoritative DNS

- Stockholm active since June 2014
  - 9 servers (3 per site)
- Network equipment diversity
  - Juniper and Cisco routers
- Name server diversity
  - 4 x BIND 9.10.1
  - 3 x Knot 1.6.0
  - 2 x NSD 4.1.0
- 100,000 q/s

Provisioning resiliency

- Two new servers in Amsterdam and Stockholm
- Slave zones update independently on each server
- Manually maintained master zones
    - Synchronise git repositories
- Dynamically updated zones
    - Update forwarding
    - Master-master replication
    - AMQP with two consumers
- Challenges
    - Synchronising zone serial numbers

DNSSEC algorithm roll-over

- RIPE NCC zones signed with SHA-1 since 2005
  - In 2005, only SHA-1 was defined for DNSSEC
- In 2009, SHA-2 was defined (RFC 5702)
  - Root zone is signed with RSASHA256 in 2010
  - Resolvers must support SHA-2 for validating the root zone
- We should upgrade to SHA-2 for RIPE NCC zones
  - Current best practice
  - SHA-1 has known collisions and may be deprecated soon

DNSSEC algorithm roll-over issues

- Signatures required with keys of both algorithms
  - CZNIC’s report from OARC fall 2010 workshop
  - RFC 4035 section 2.2
  - Accurate timing required when adding keys and signatures
- Sign simultaneously with SHA-1 and SHA-2 keys
  - Secure64 signer does not support this
  - Need to go through an insecure phase
- Should we do an algorithm upgrade?

Open issues

- ccTLD secondary agreement
- DNSMON
  - Visualisation delay
  - Criteria for adding new zones