DNS Security

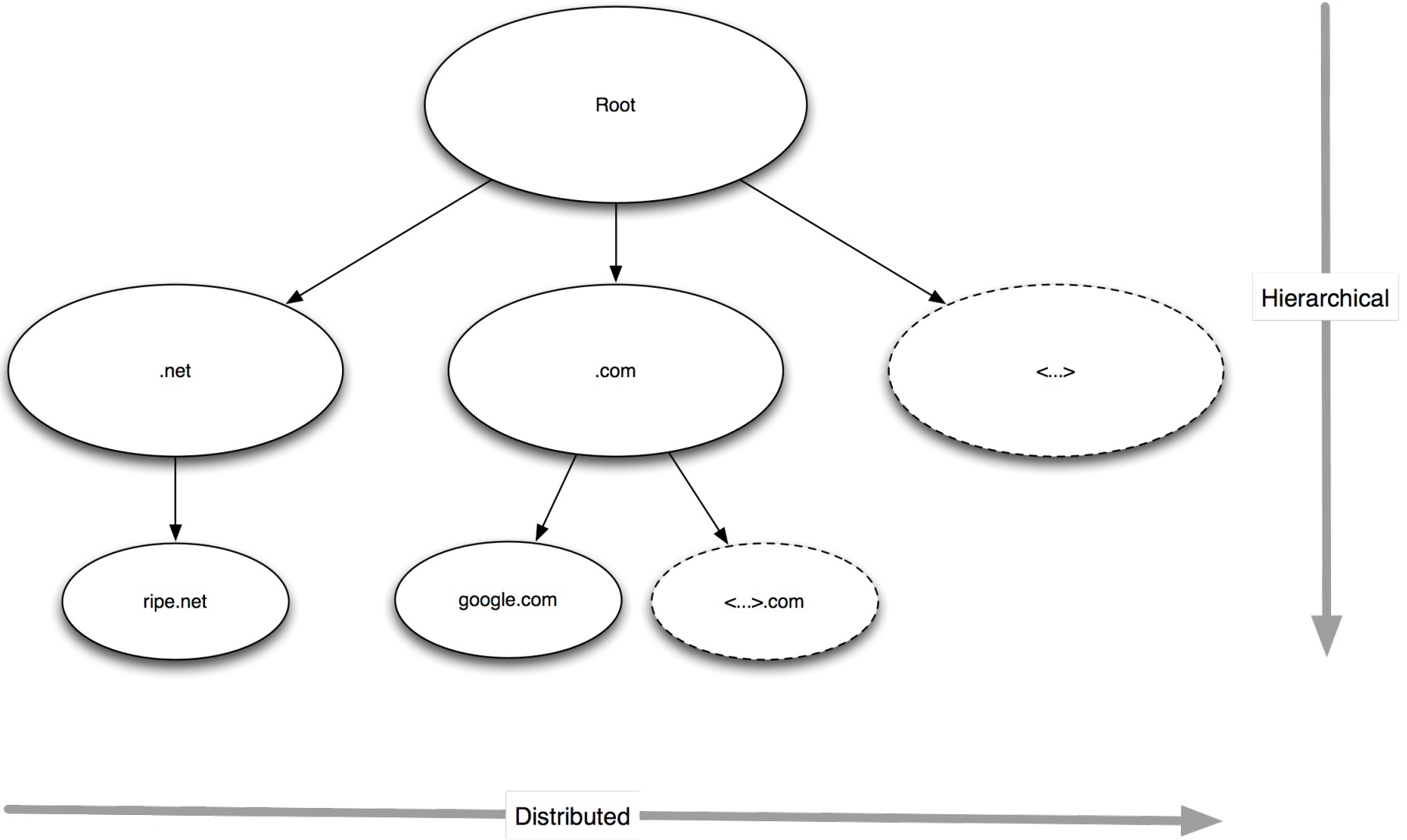
Wolfgang Nagele
Global Information Infrastructure Manager

RIPE NCC

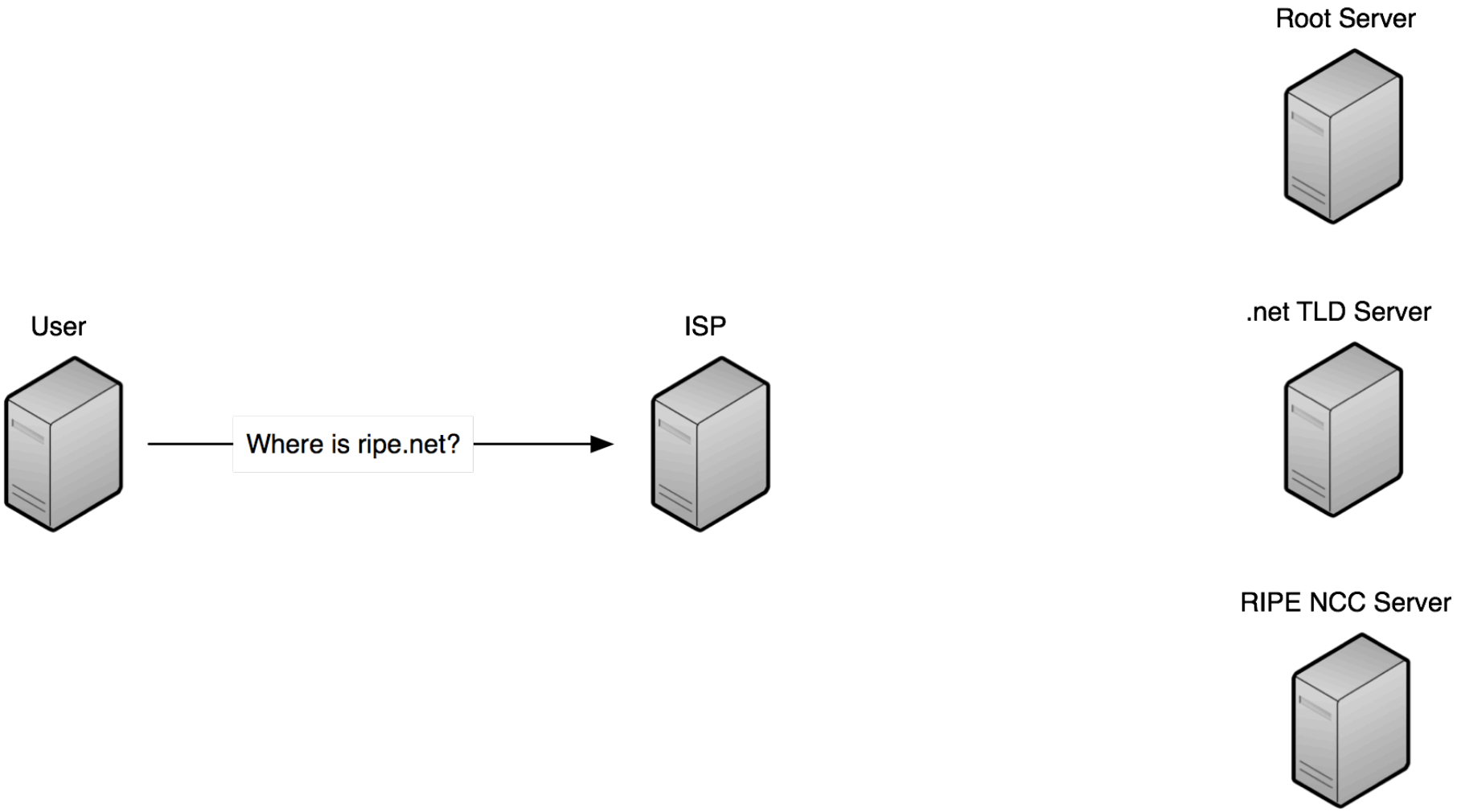
DNS: the Domain Name System

- Specified by Paul Mockapetris in 1983
- Distributed Hierarchical Database
  - Main purpose: Translate names to IP addresses
  - Since then: Extended to carry a multitude of information (such as SPF, DKIM)
- Critical Internet Infrastructure
  - Used by most systems (in the background)

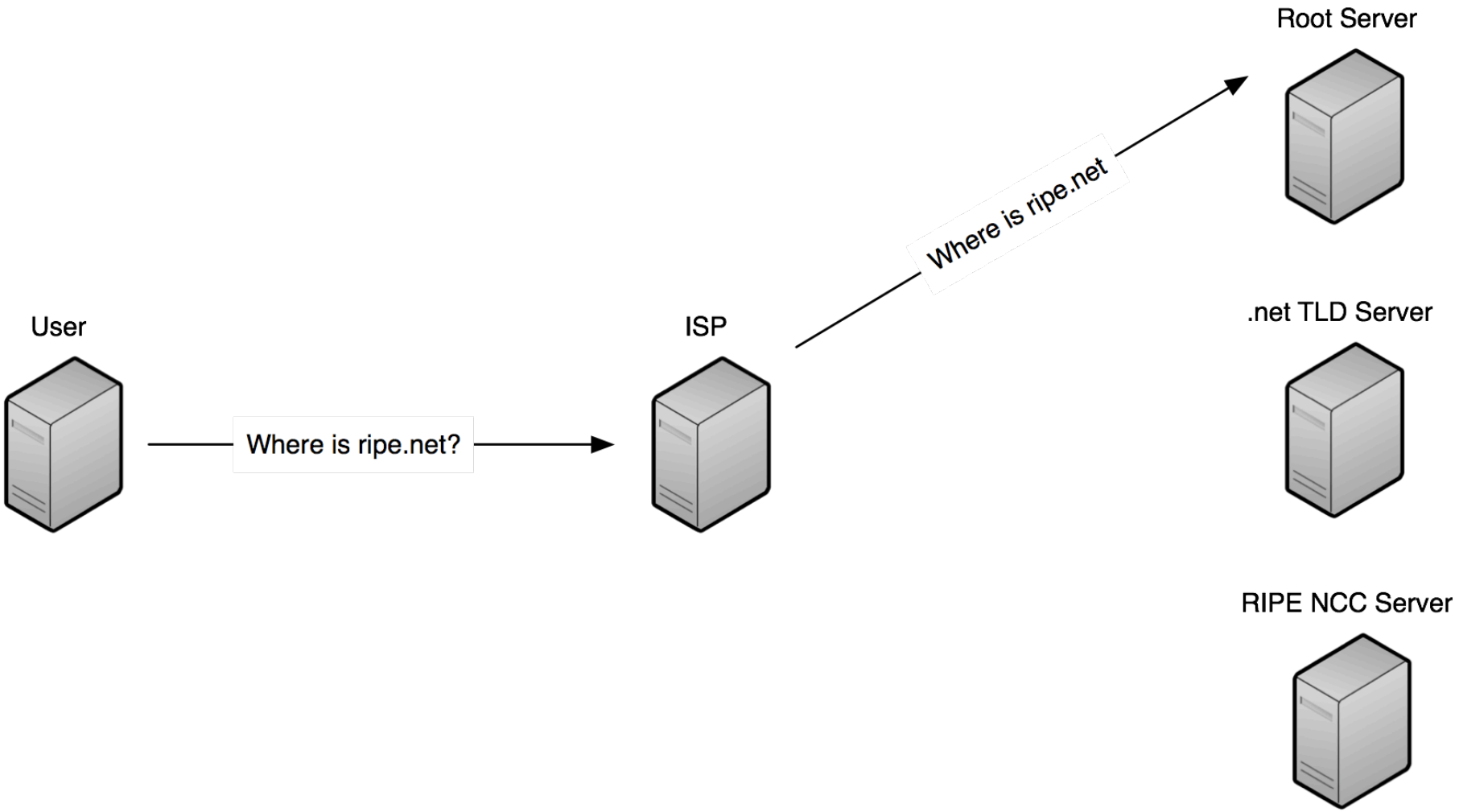
DNS Tree Structure



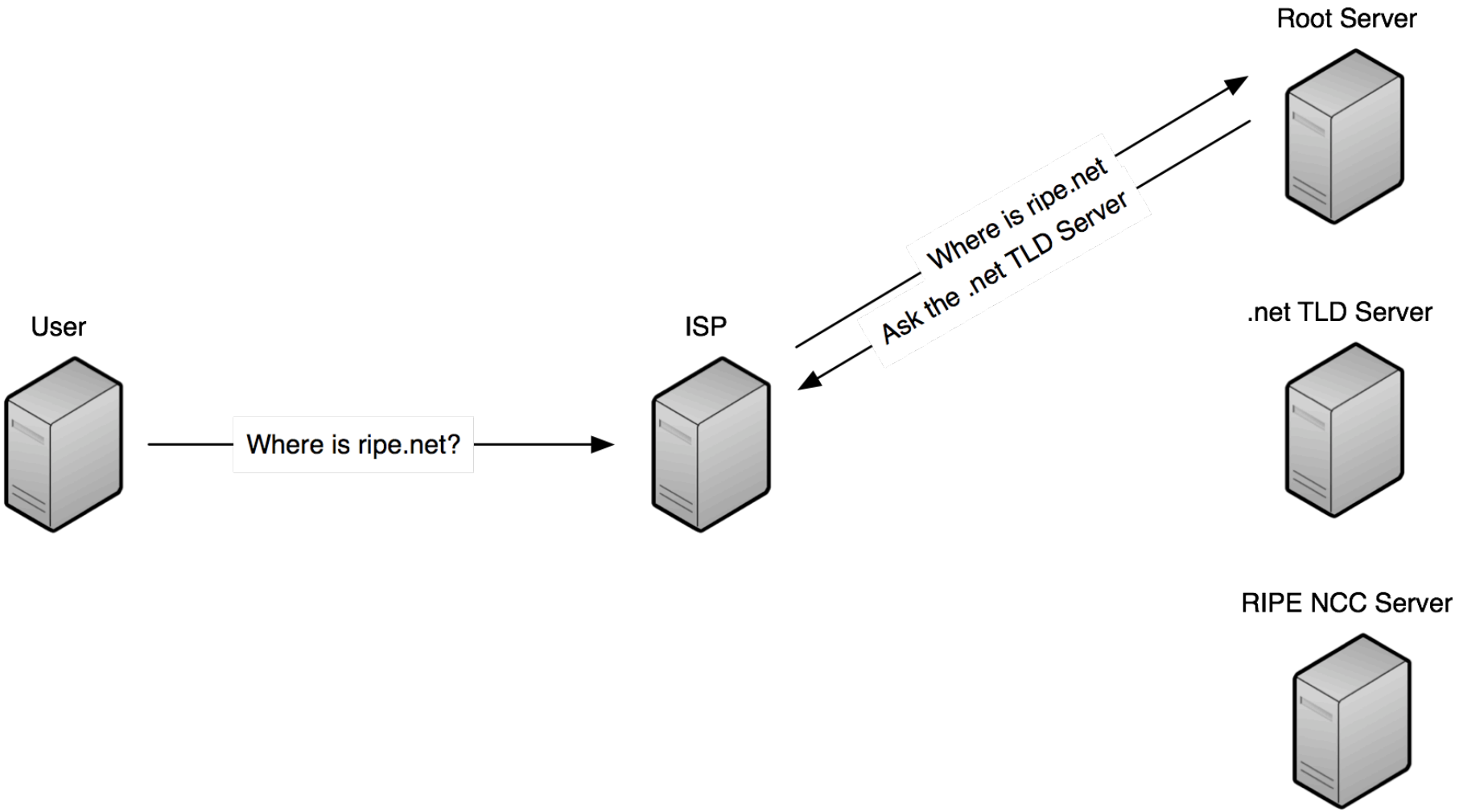
How does it work?



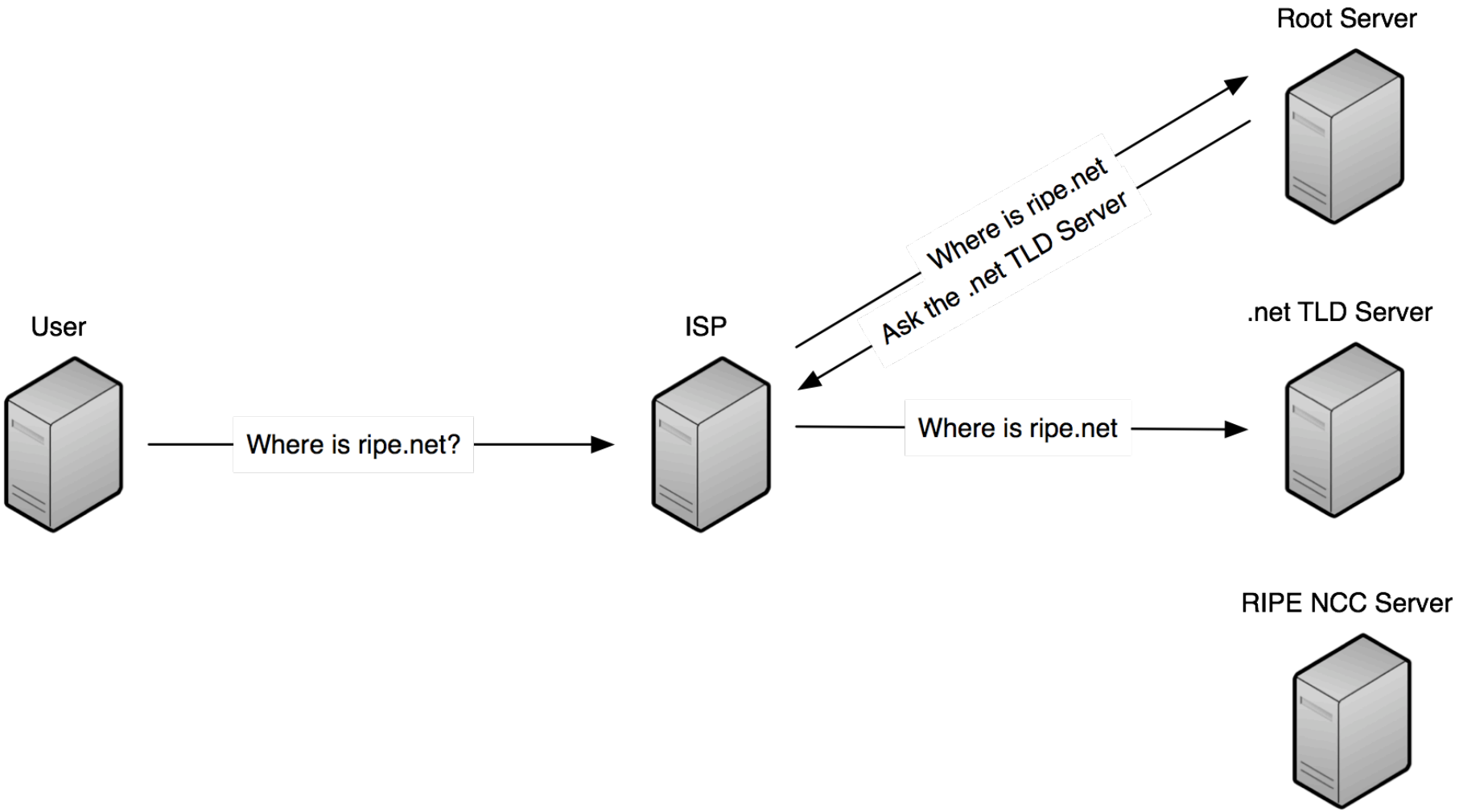
How does it work?



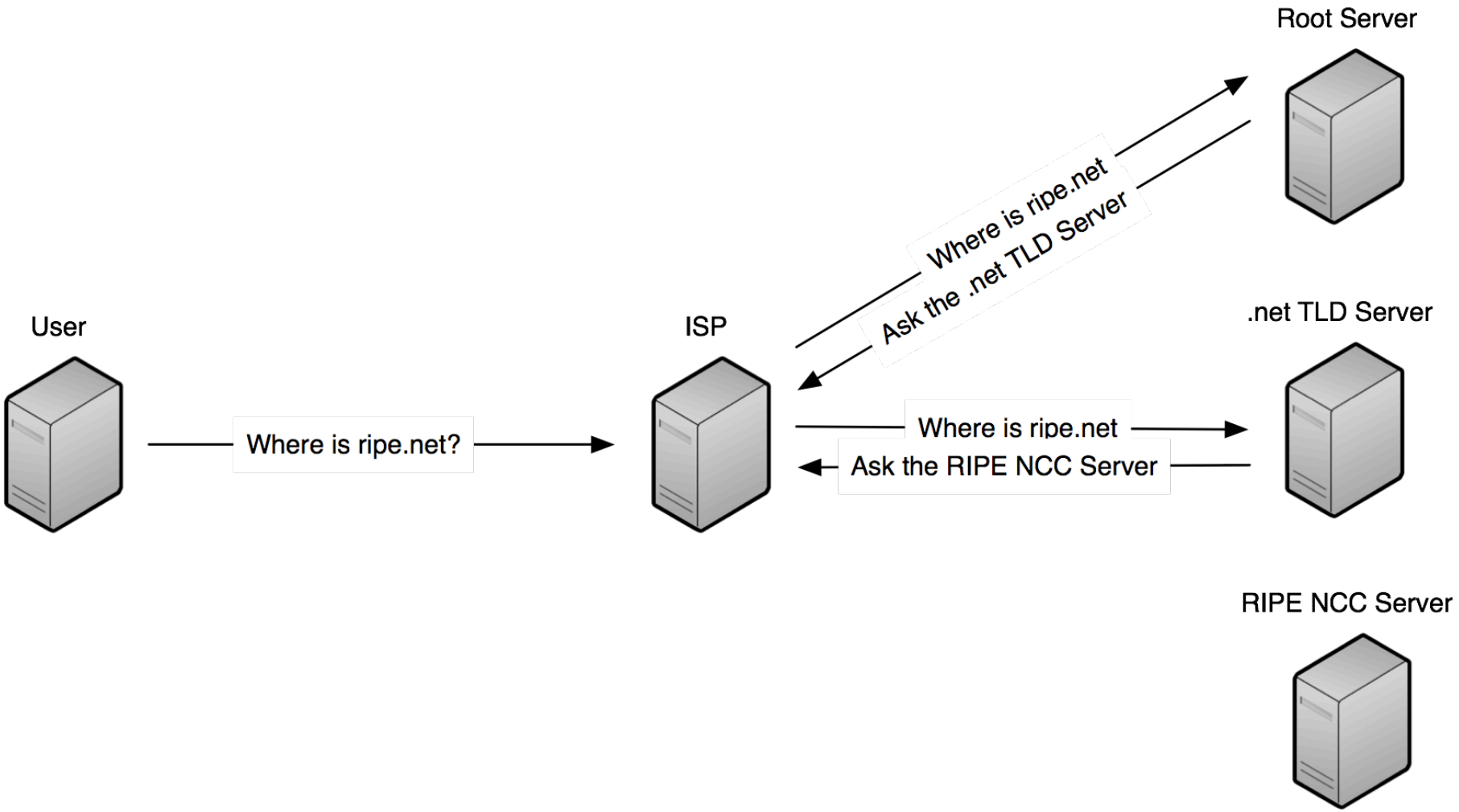
How does it work?



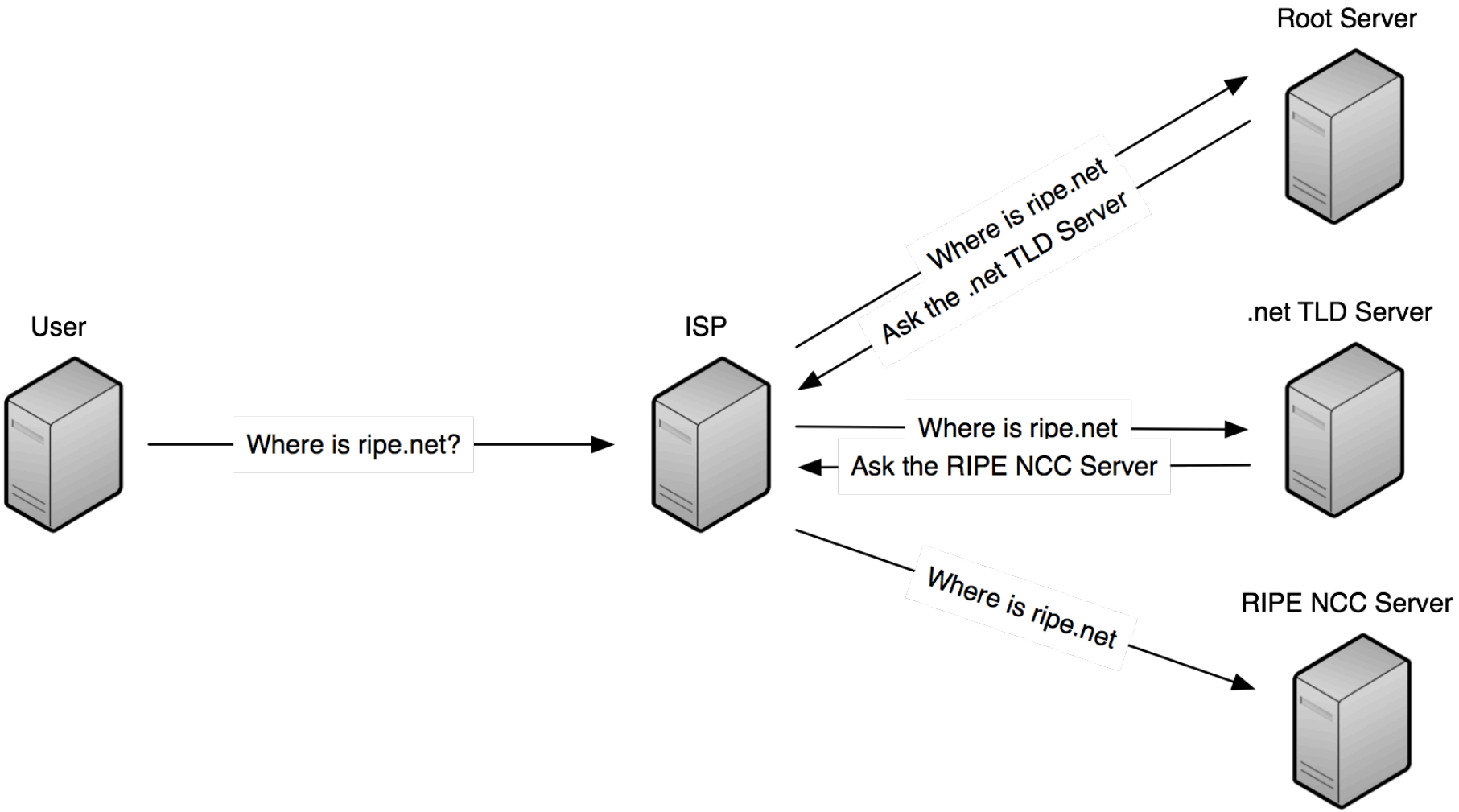
How does it work?



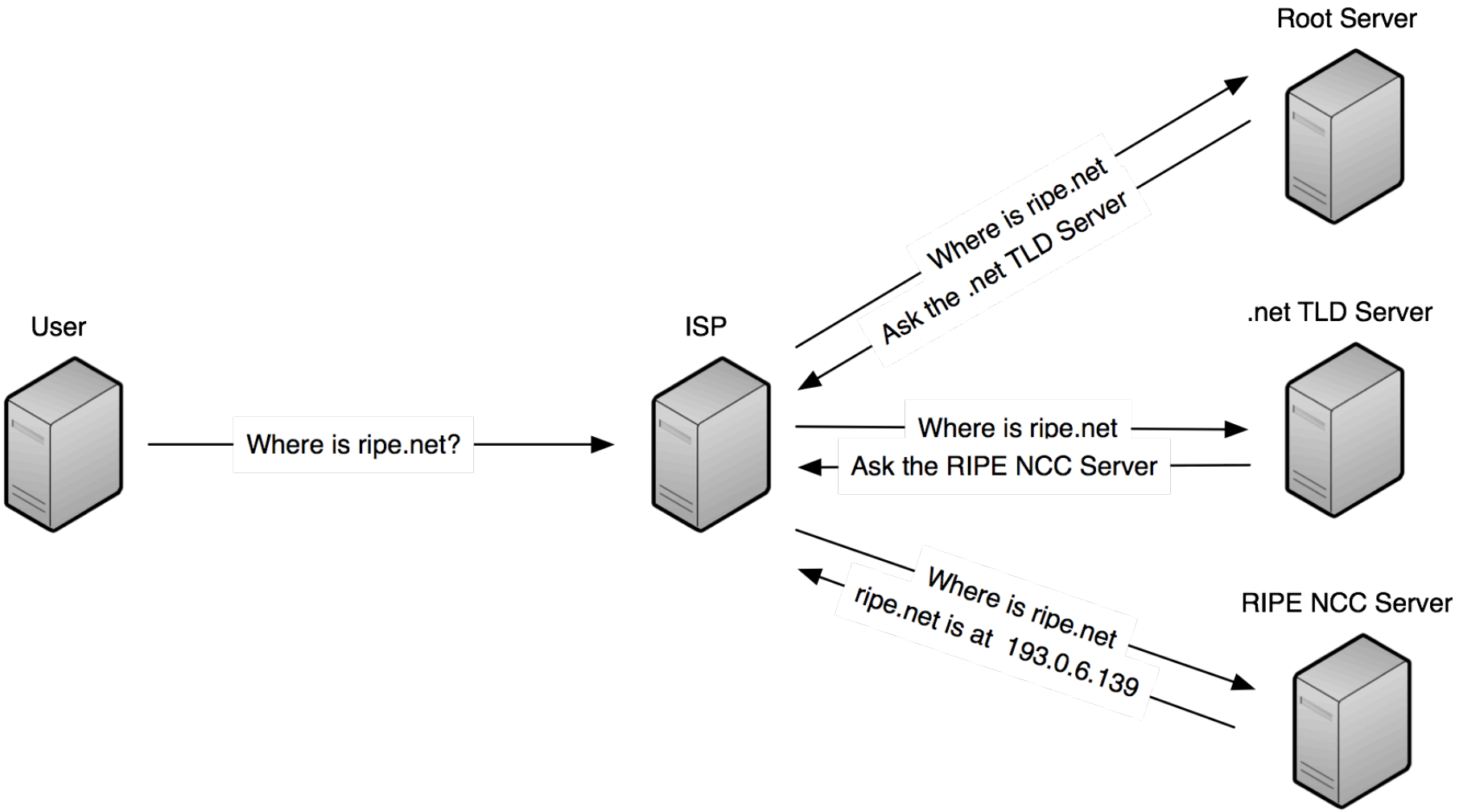
How does it work?



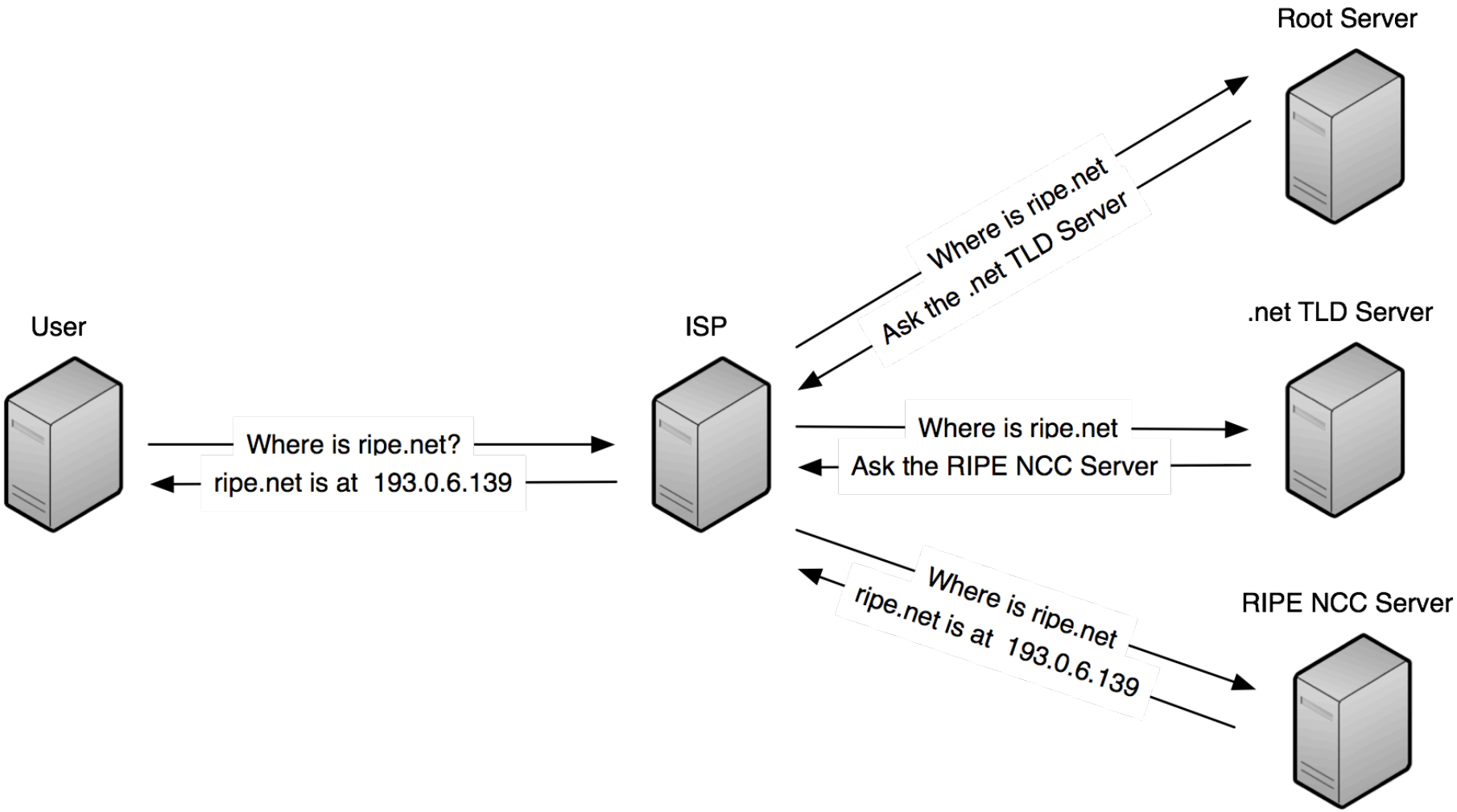
How does it work?



How does it work?



How does it work?



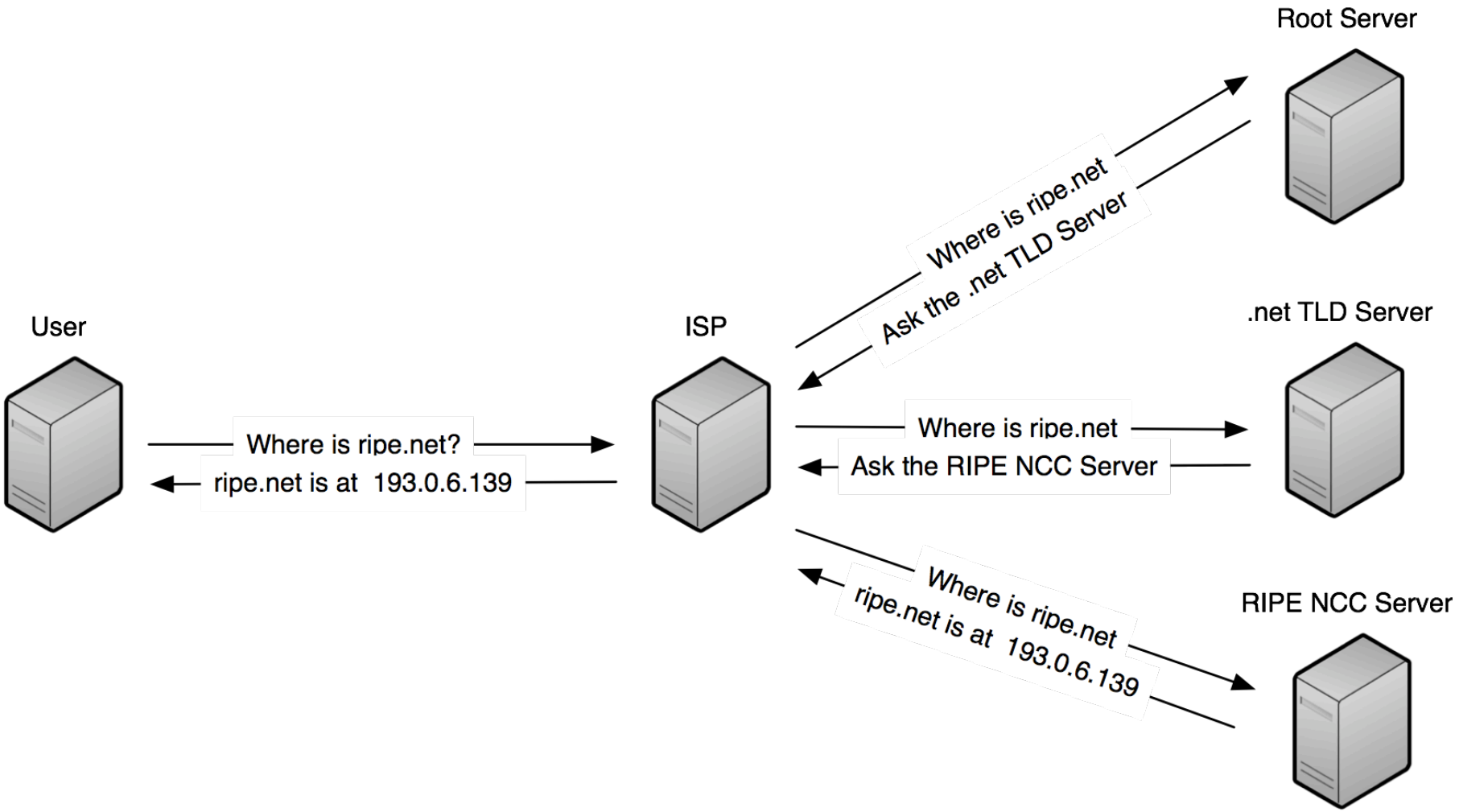
What is the problem?

- UDP transport can be spoofed
  - Anybody can pretend to originate a response
- If a response is modified the user will connect to a possibly malicious system

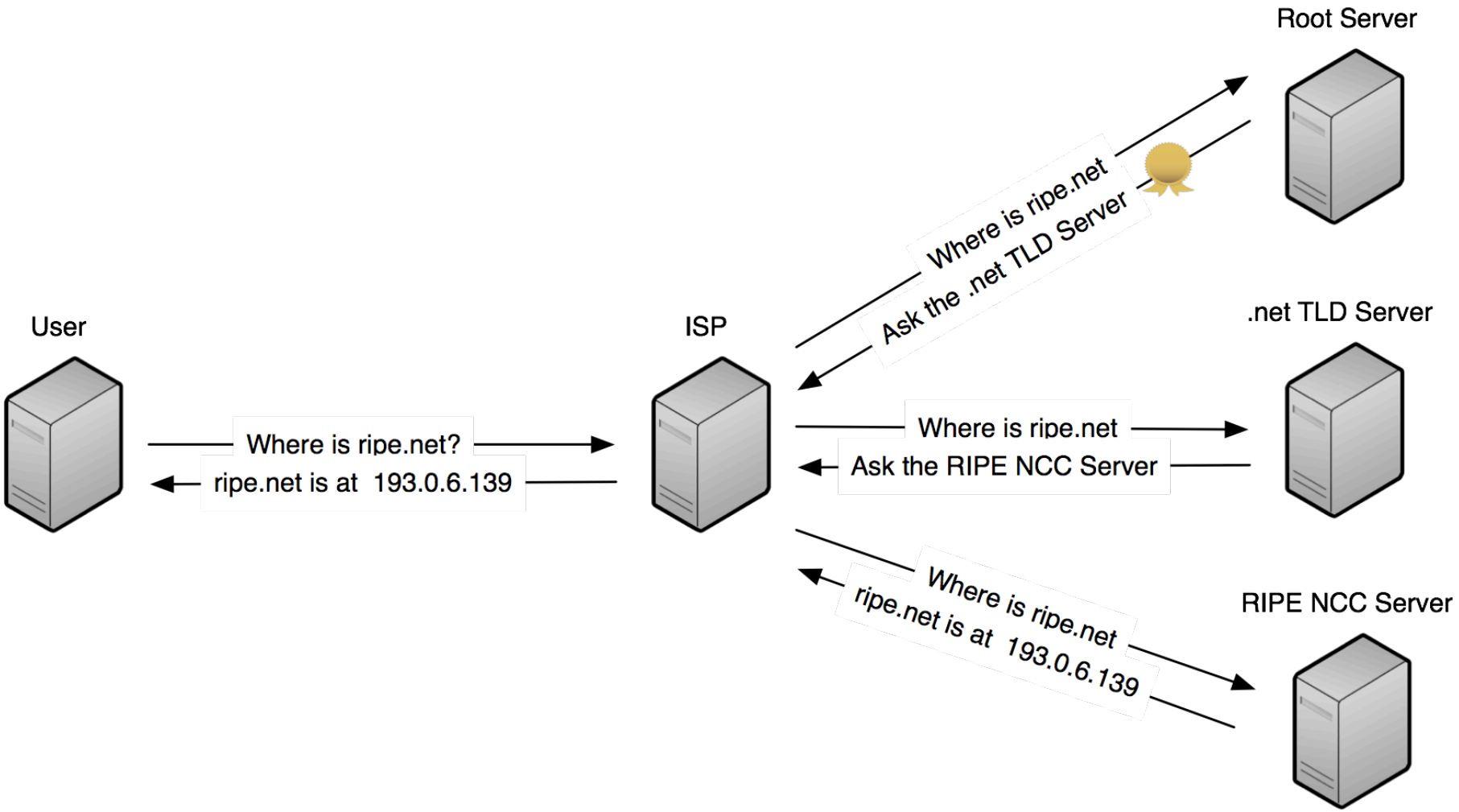
The Solution

- Make the responses verifiable
  - Cryptographic signatures
- Hierarchy exists so a Public Key Infrastructure is the logical choice
  - Same concept as used in eGovernment infrastructures

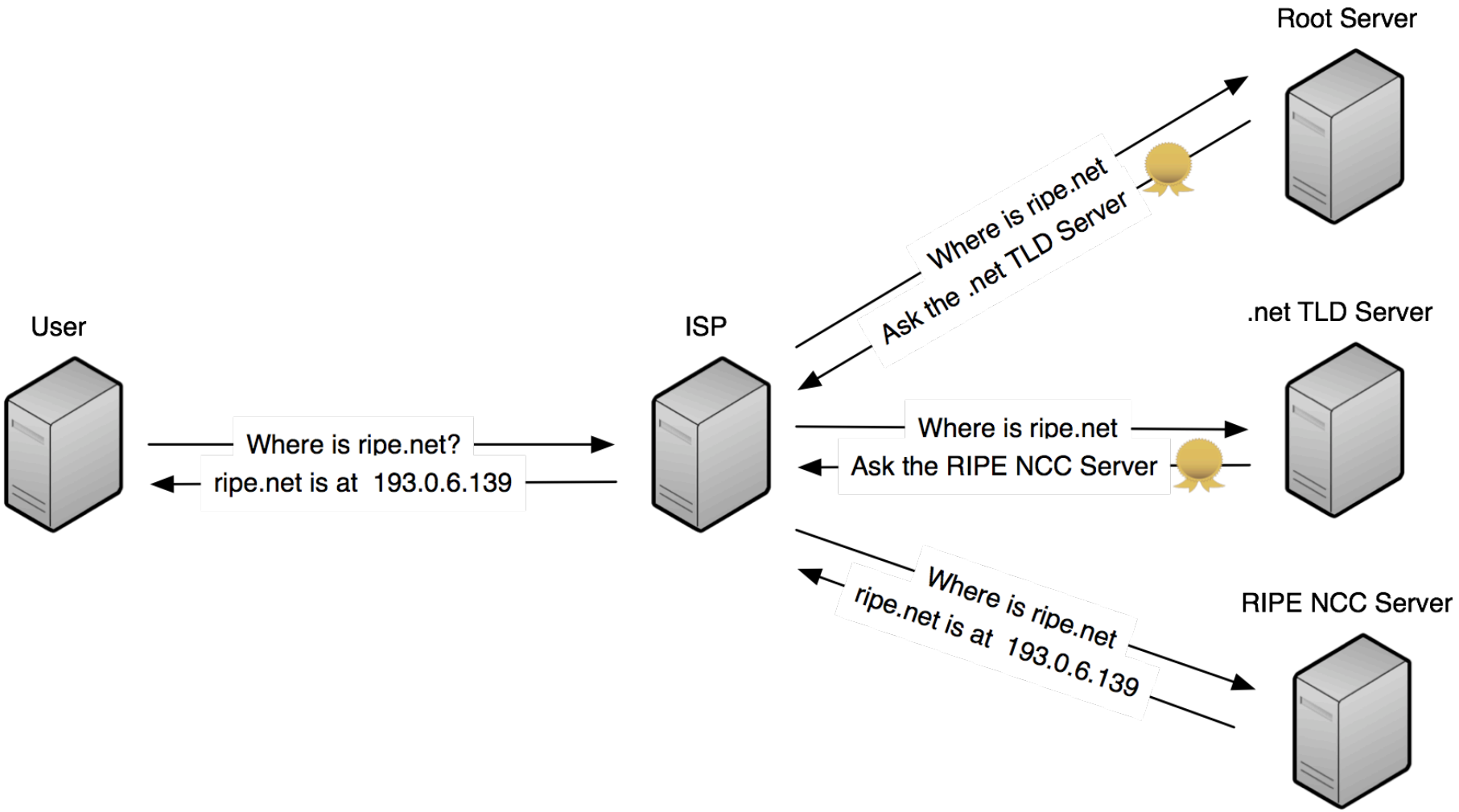
How does it work with DNSSEC?



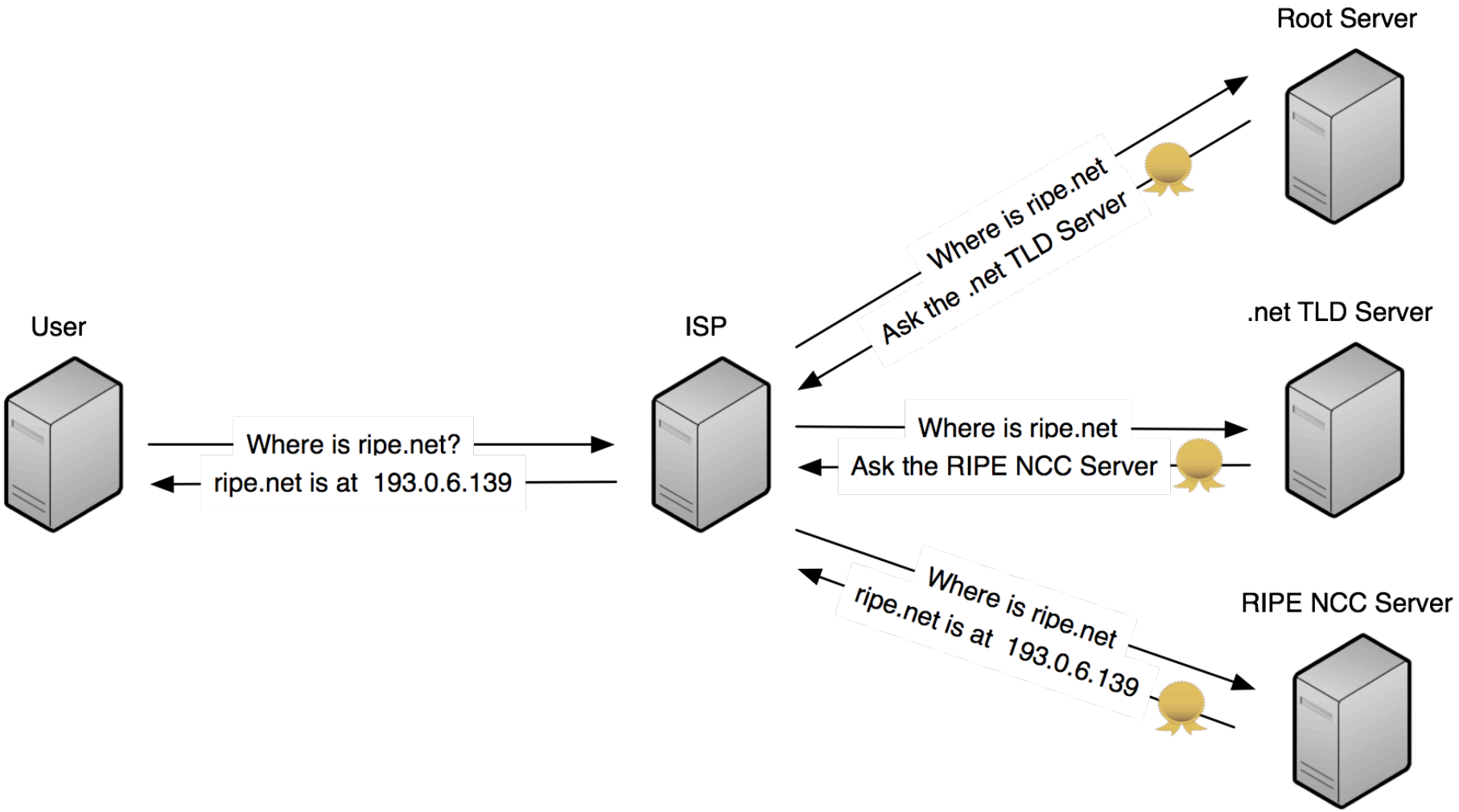
How does it work with DNSSEC?



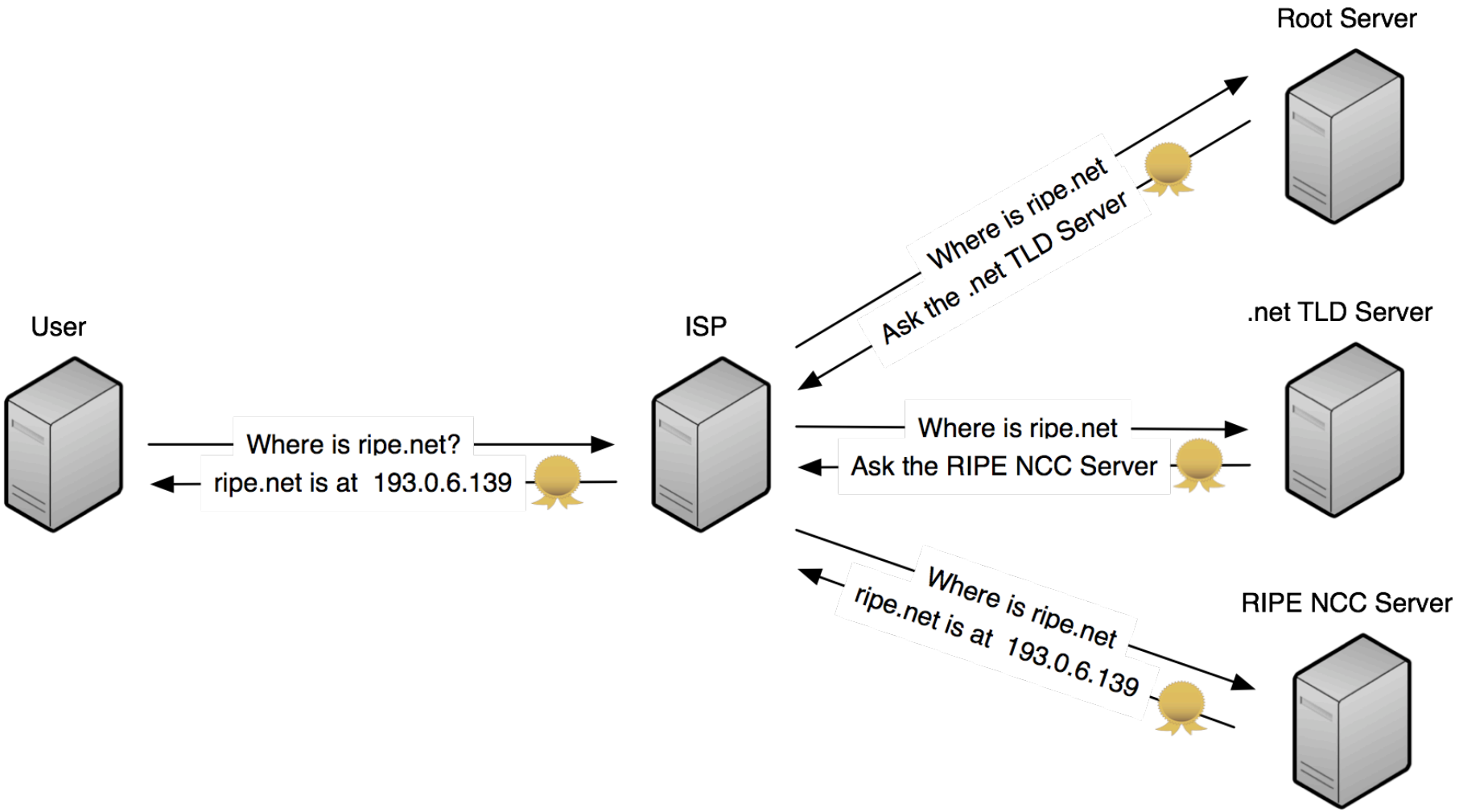
How does it work with DNSSEC?



How does it work with DNSSEC?



How does it work with DNSSEC?



DNS Security Extensions: A Long Story

- 1990: Theoretical problem discovered (Bellovin)
- 1995: Work on DNSSEC started
- 1999: First support for DNSSEC in BIND
- 2005: Standard is redesigned to better meet operational needs

  RIPE NCC along with .SE among the first to deploy it in their zones

DNS Security Extensions

- 2005 - 2008: Stalled deployments due to the lack of a signed root zone
- 2008: D. Kaminsky shows the practical use of the protocol weakness

  Focus comes back to DNSSEC
- July 2010: Root Zone signed with DNSSEC
- Oct 2011: 72/306 signed TLDs

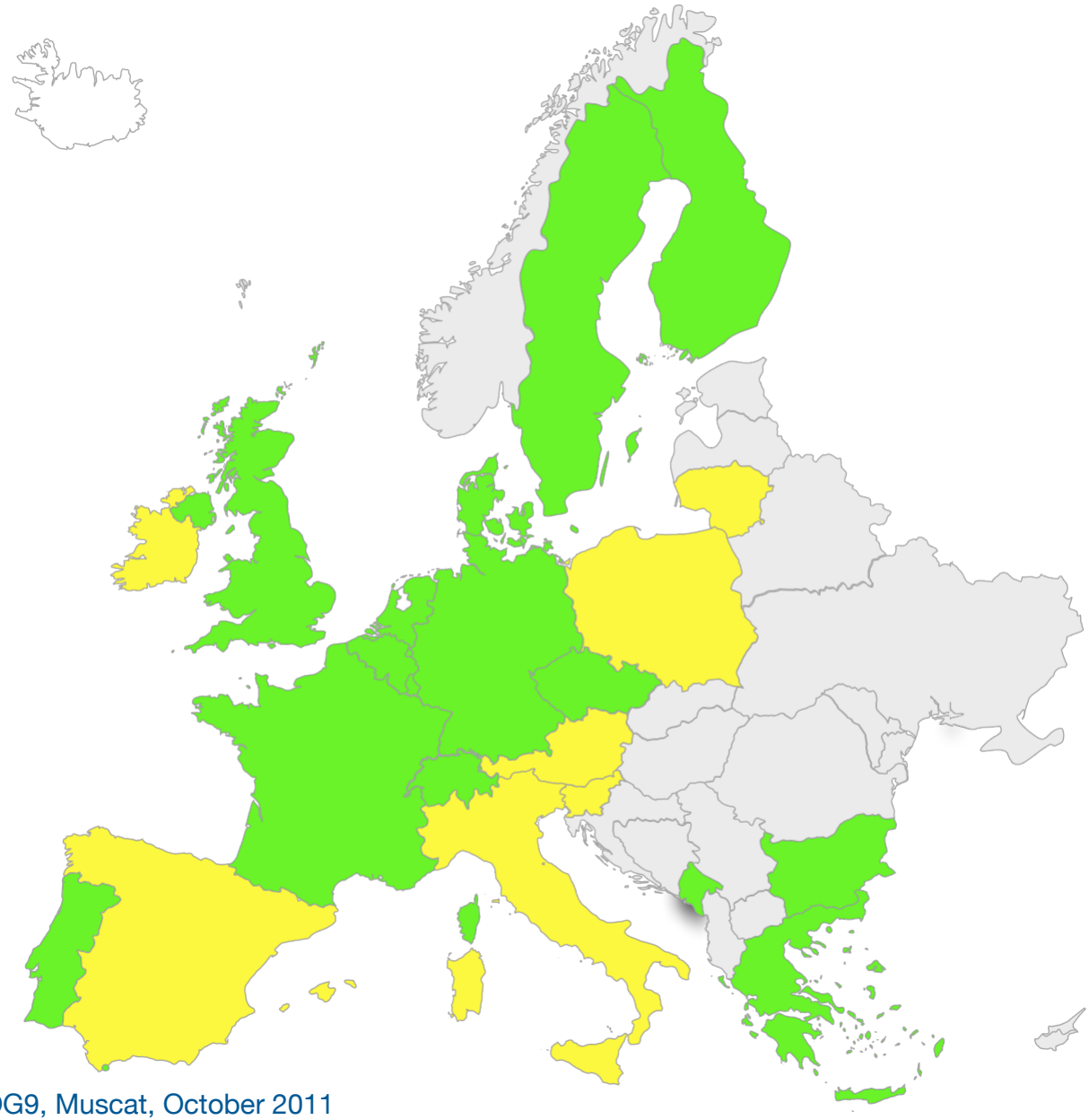
DNSSEC and the RIPE NCC

- Sponsor development of NSD DNS software
- Participated in the “Deployment of Internet Security Infrastructure” project
  - Signed all our DNS zones
    - IPv4 & IPv6 reverse space
    - E164.arpa
    - ripe.net
- K-root server readiness for a signed root zone

Singing of the Root Zone

- Shared custody by Root Zone maintainers
  - Currently: U.S. DoC NTIA, IANA/ICANN, VeriSign
- Split key among 21 Trusted Community Representatives
- In production since July 2010

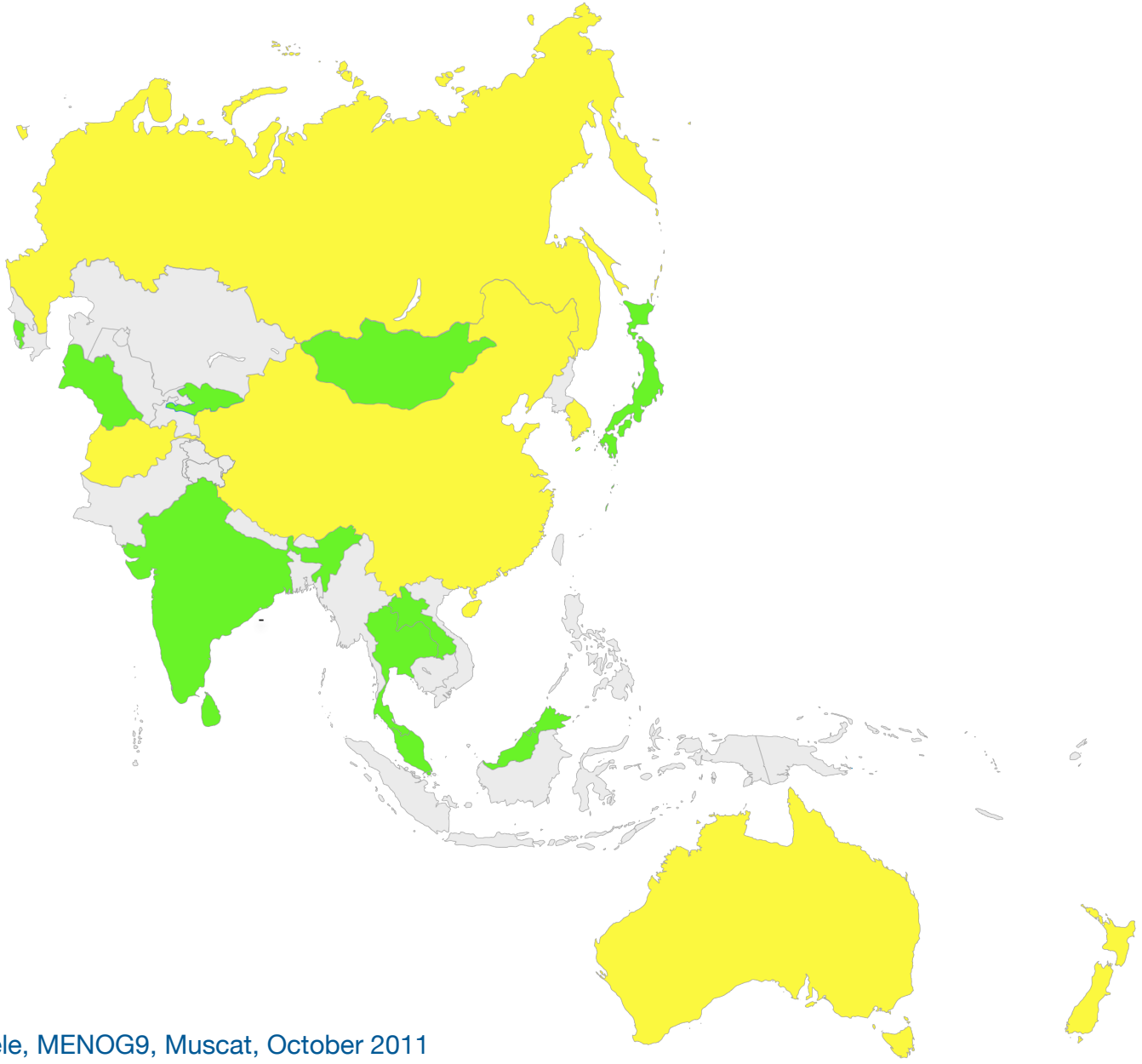
Deployment in ccTLDs: Europe



Deployment in ccTLDs: Middle East

OH NO!

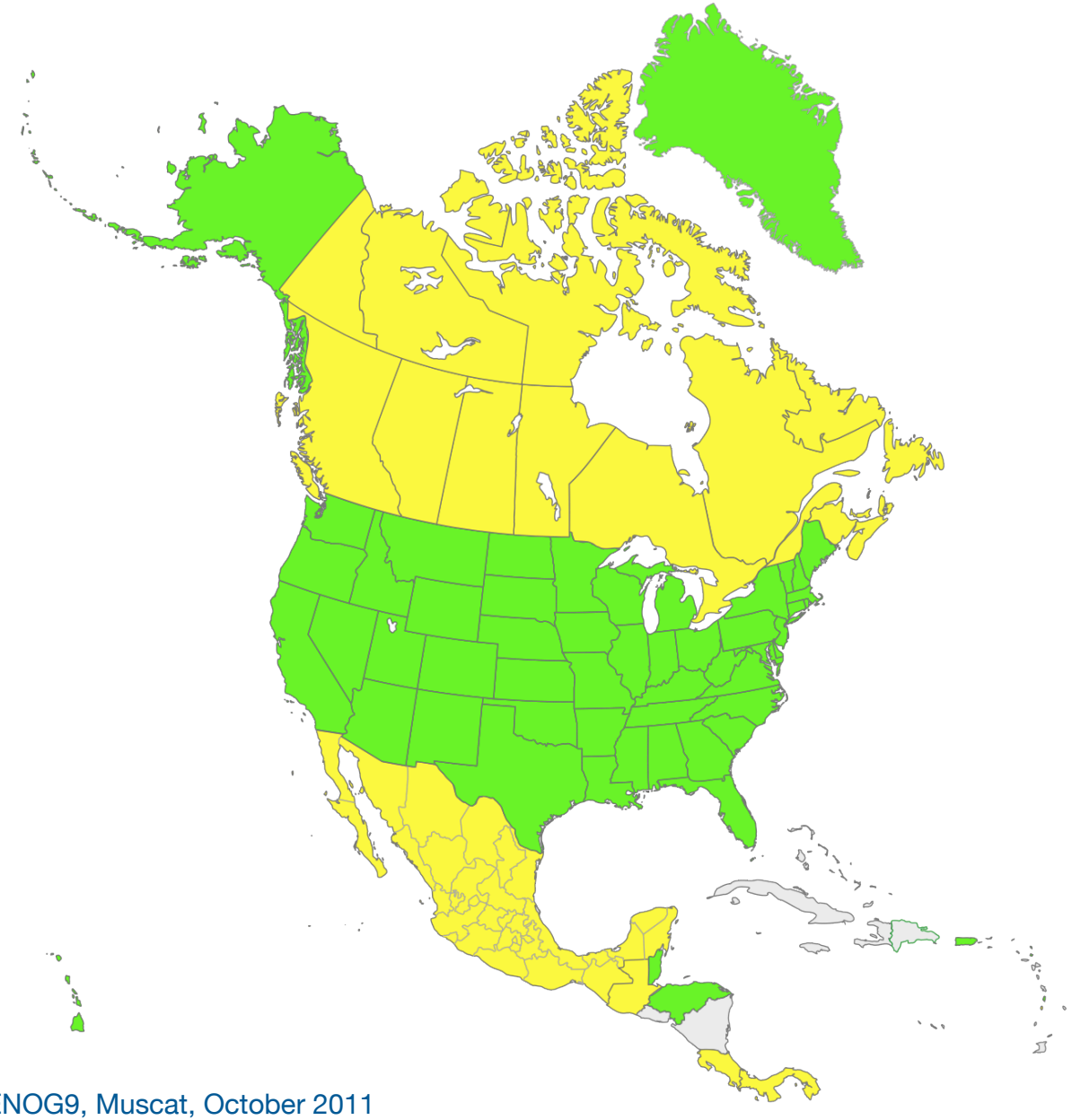
Deployment in ccTLDs: Asia Pacfic



Deployment in ccTLDs

Deployment in ccTLDs

Deployment in ccTLDs



Deployment in gTLDs

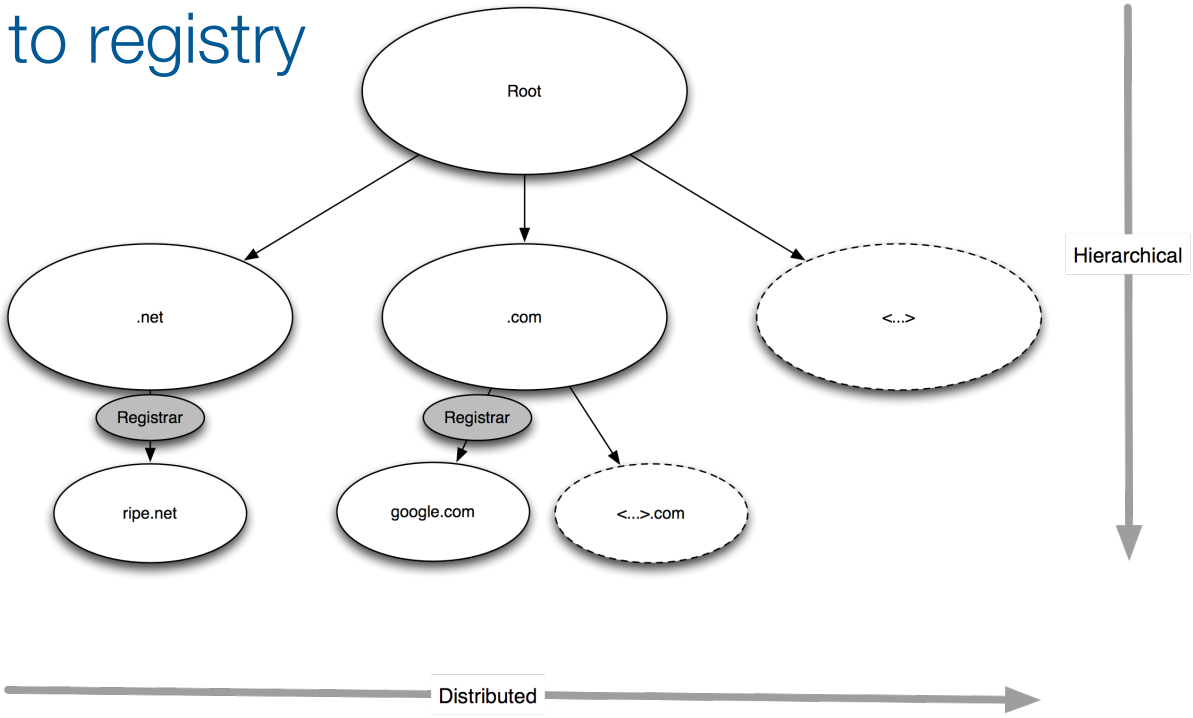
- .com/.net/.org (57% of world wide total domains)
- .asia
- .cat
- .biz
- .edu
- .gov
- .info
- .museum
- .mobi (Planned)

Deployment in Infrastructure TLD .arpa

- E164.arpa
  - ENUM number mapping
  - signed by the RIPE NCC
- in-addr.arpa
  - Reverse DNS for IPv4
- ip6.arpa
  - Reverse DNS for IPv6

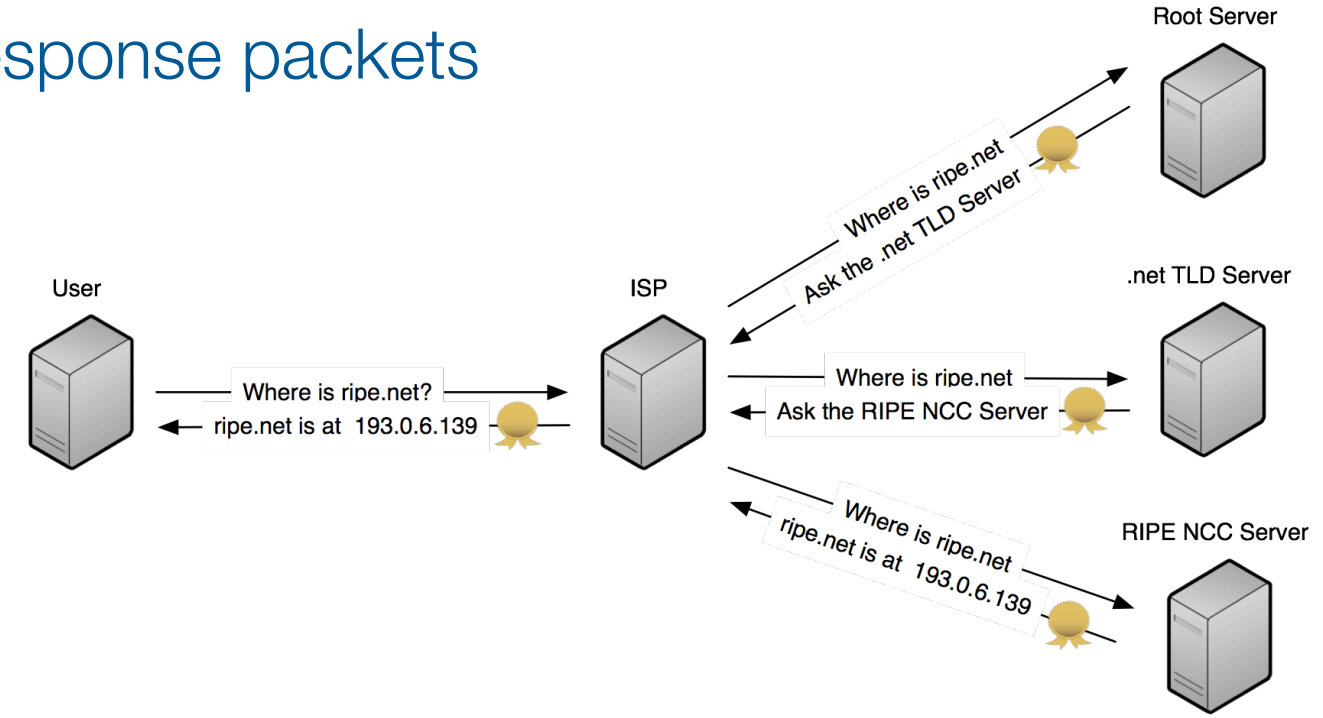
Are We Done?

- Signed TLD is not the same as a signed domain
  - Thick registry model (Registry-Registrar-Registrant)
  - Registrars need to enable their customers to provide public key data to registry



Are We Done?

- Ultimately responses should be verified by the end user
  - Home routers need to support DNS specifications with large response packets



Leverage Infrastructure

- DNS is a cross organisational data directory
- DNSSEC adds trust to this infrastructure
  - Anybody can verify data published under ripe.net was originated by the domain holder
  - Could be used to make DKIM and SPF widely used and trusted
  - SSL certificates can be trusted through the DNS
  - More ideas to come …

What about SSL/TLS?

- SSL as a transport is well established
- CA system currently in use is inherently broken
  - Any Certificate Authority delivered with a browser to date can issue a certificate for any domain
    - 100 and more shipped in every Browser
  - If any one of them fails - security fails with it
    - Recent incident with Comodo & Digitnotar CA is one example
- DANE working group at IETF
  - Supported in Chrome 14 browser

DNSSEC and the Middle East

- ccTLDs need to get signed
- ISPs need to enable validation on their resolvers

- What keeps you from deploying?

Questions?

wnagele@ripe.net

RIPE NCC