Monitoring the DNS

Gustavo Lozano | Event Name | XX XXXX 2015

Agenda

1

Components of the DNS

2

Monitoring gTLDs

3

Monitoring other components of the DNS

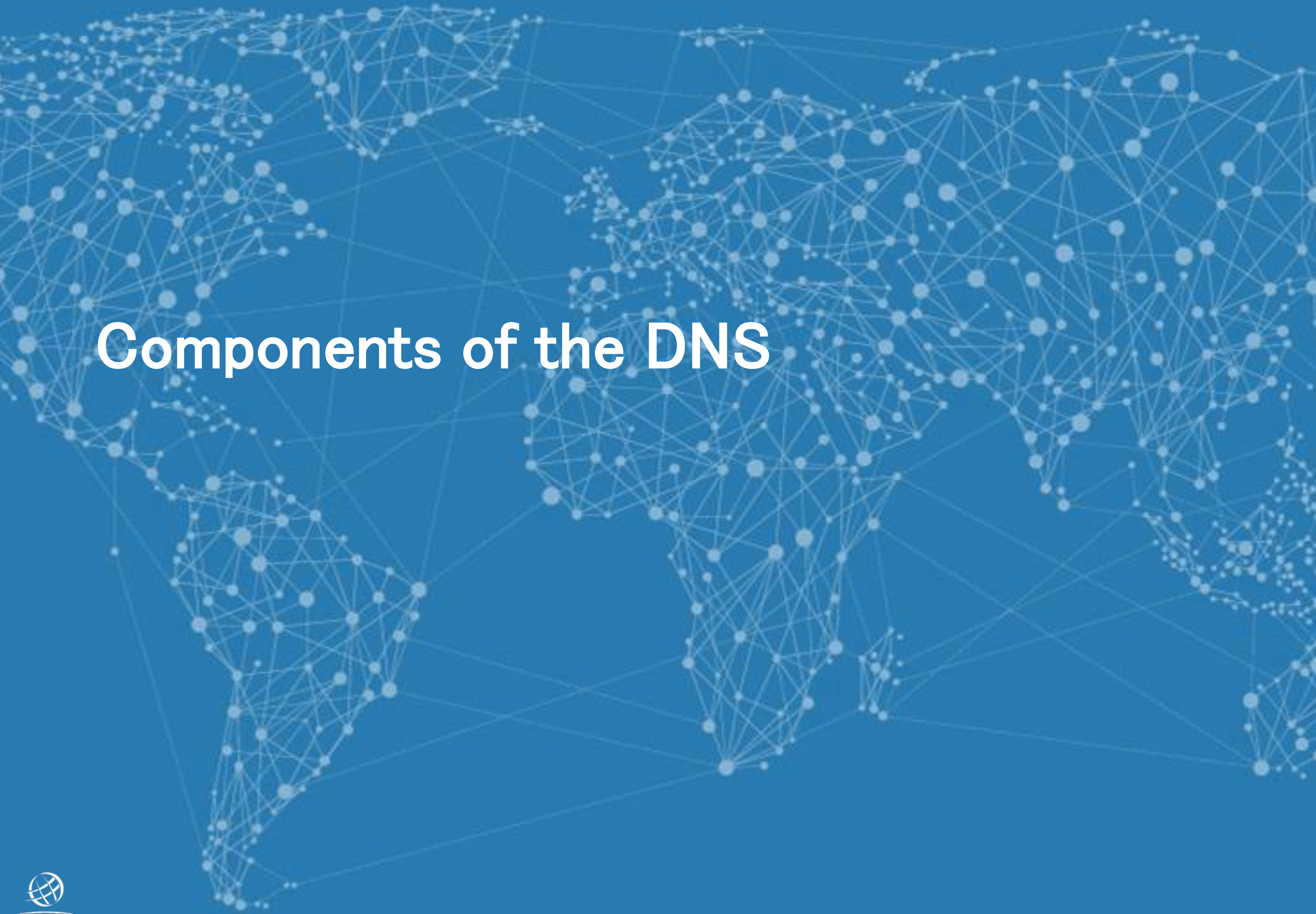
4

Monitoring system

5

Conclusion

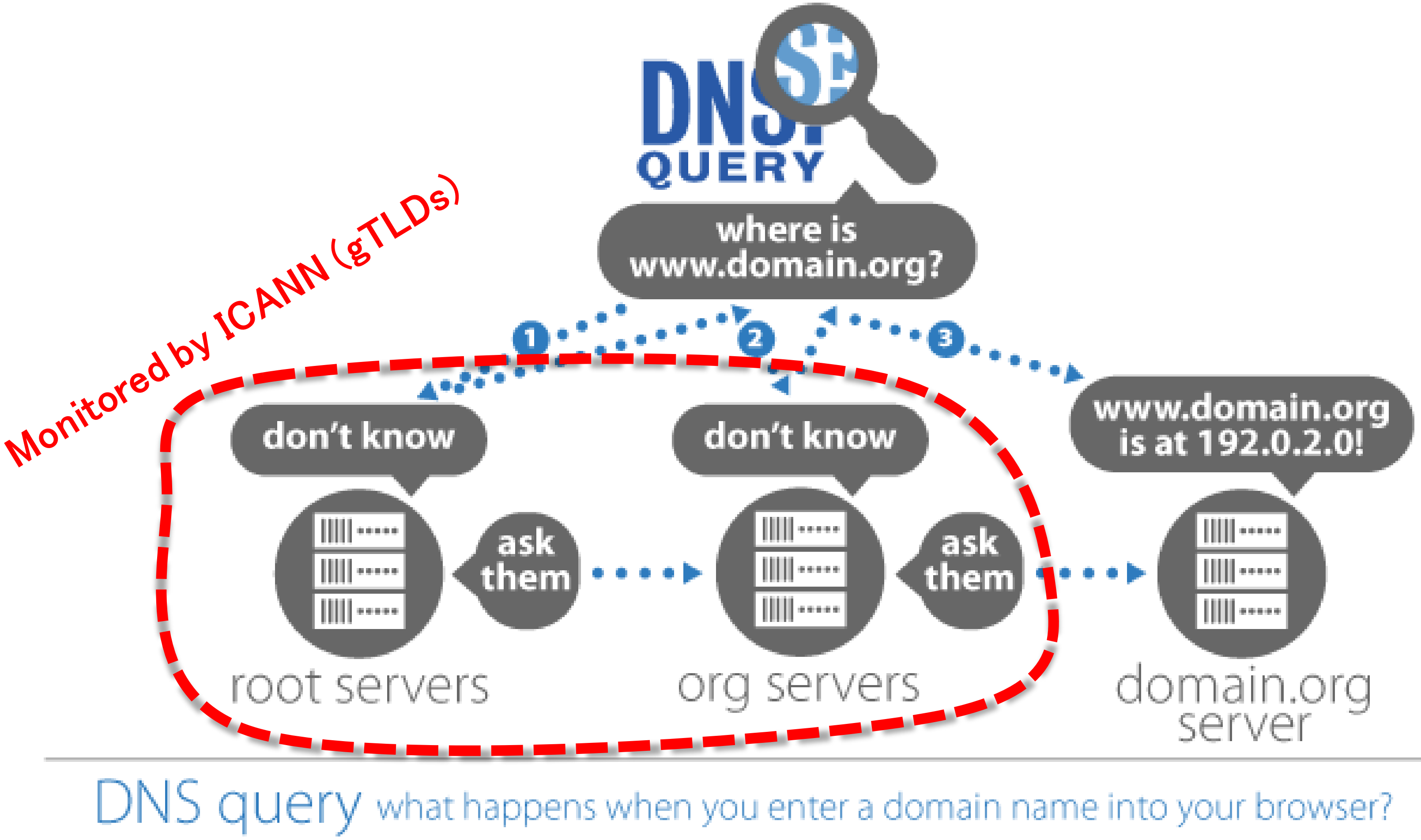
Components of the DNS



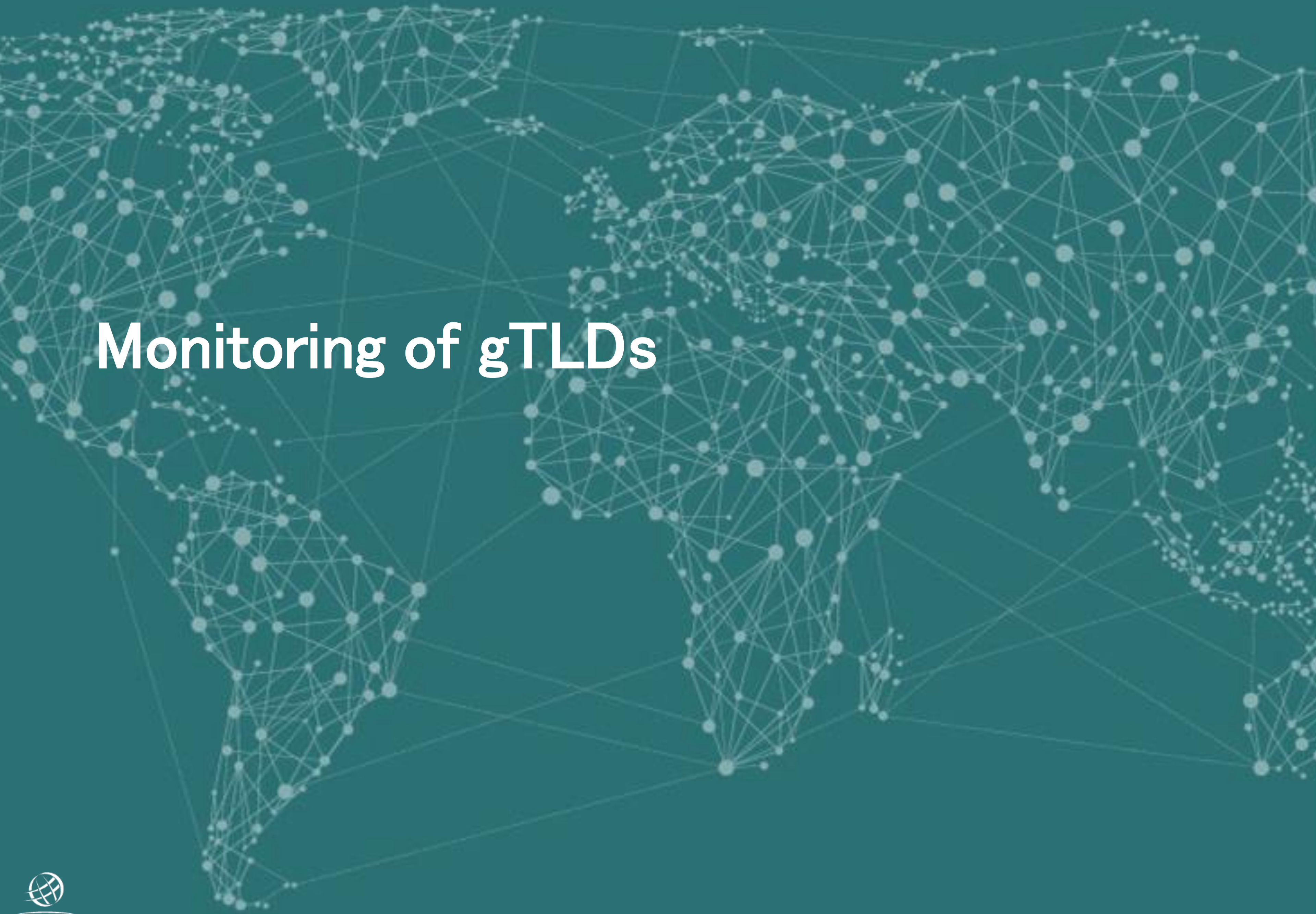
The DNS

- The DNS is made of several components that must work well, in order to have a system that performs optimally as a whole. The main components of the DNS are:
  - The root zone
  - Top Level Domains (TLDs)
  - Second Level Domains (SLDs)
  - Recursive DNS service
- Registries, registrars and DNS operators are also part of the equation, because they are the source for the majority of the information in the DNS.
- Most end-users don’t know about the DNS, but if the DNS is underperforming, the Internet is not working for them.

The DNS



DNS query what happens when you enter a domain name into your browser?



Monitoring of gTLDs

Monitoring of gTLDs

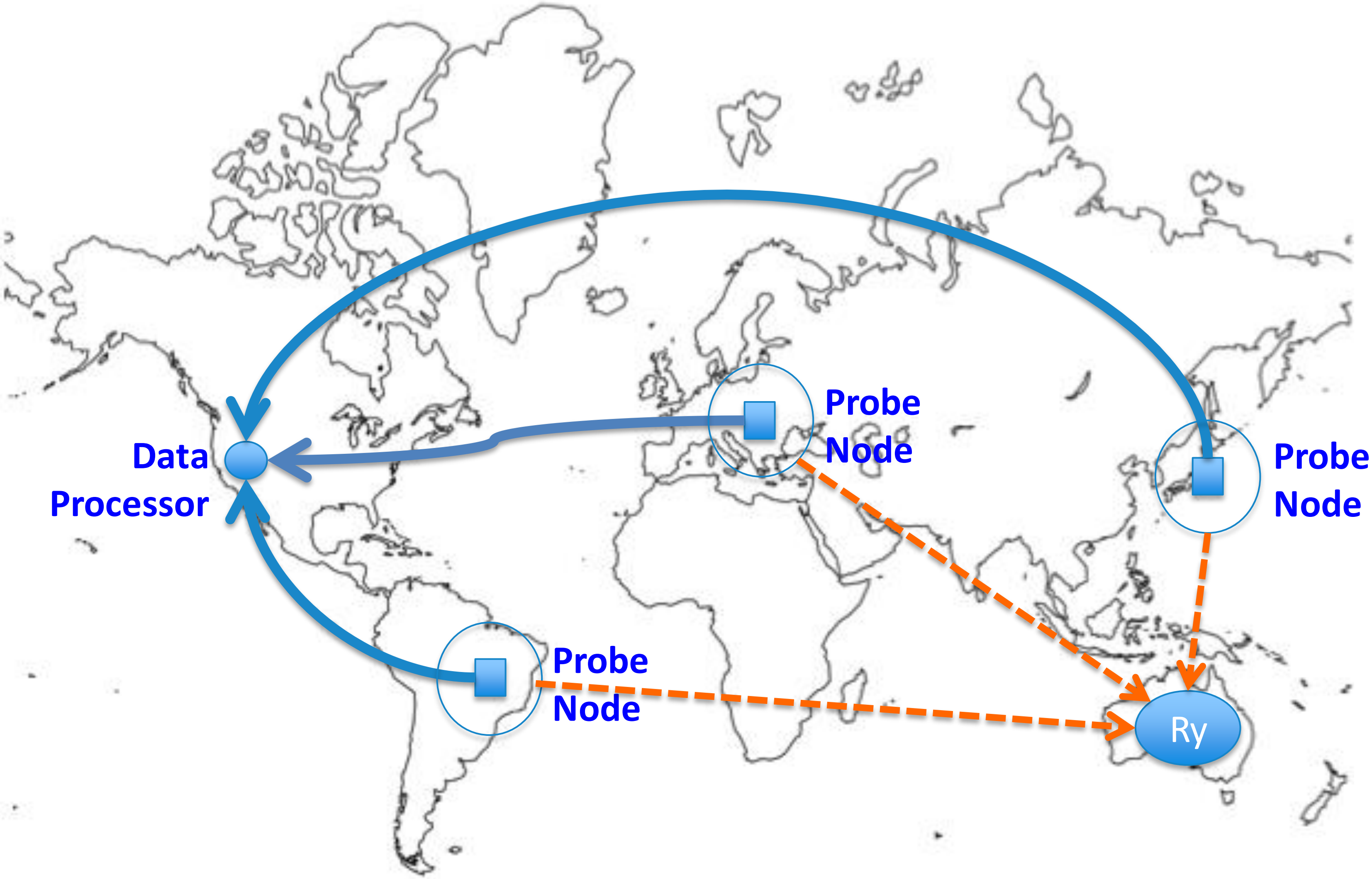
- The new gTLD program redefined ICANN's responsibilities regarding monitoring the performance of the DNS, DNSSEC, WHOIS and EPP services (critical services).

- The new gTLD program also redefined the Service Level Requirements for Registries regarding these critical functions.

- The specific details about the Service Level Agreement and ICANN's responsibilities regarding monitoring could be found in Specification 10 of the new gTLD base registry agreement:

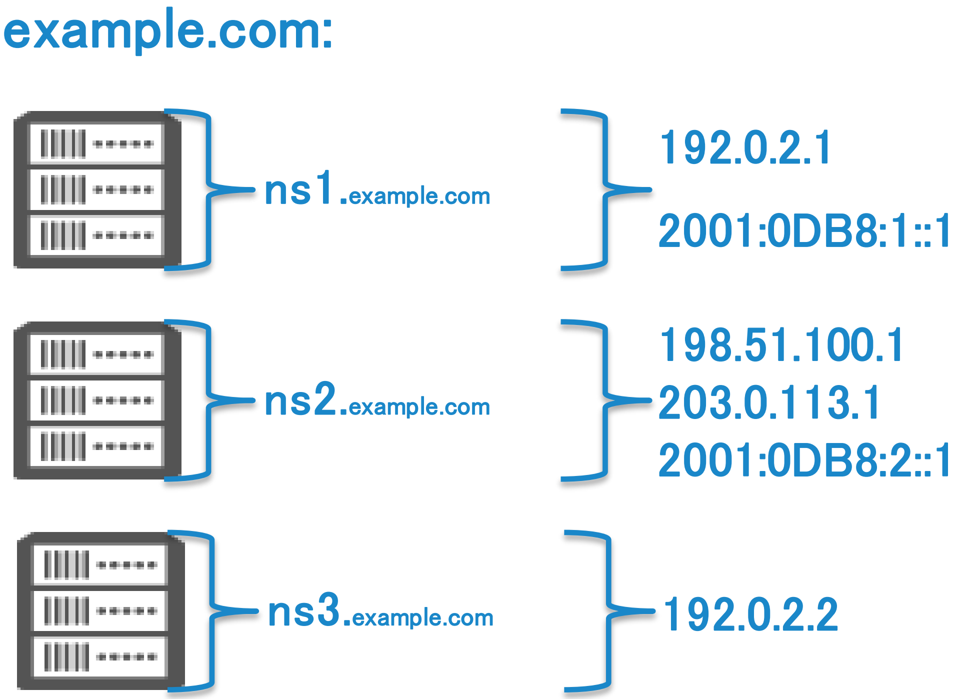
https://www.icann.org/resources/pages/registries/registries-agreements-en

How does ICANN monitor gTLDs?



Anatomy of the DNS service (authoritative)

- An authoritative server provides authoritative information about a DNS zone.



Service Level Agreement

- **DNS SLA:**

Parameter	SLR (monthly basis)
DNS service availability	0 min downtime (100% availability)
DNS name server availability	£ 432 min of downtime (» 99%)
TCP DNS resolution RTT	£ 1500 ms, for at least 95% of the queries
UDP DNS resolution RTT	£ 500 ms, for at least 95% of the queries
DNS update time	£ 60 min, for at least 95% of the probes

DNS Monitoring

The probe node network consists of approximately 45 probe nodes around the world.

If 51% or more of the DNS testing probes see the service as unavailable during a given time, the DNS service will be considered unavailable.

SPEC10: *Probes for measuring DNS parameters shall be placed as near as possible to the DNS resolvers on the networks with the most users.*

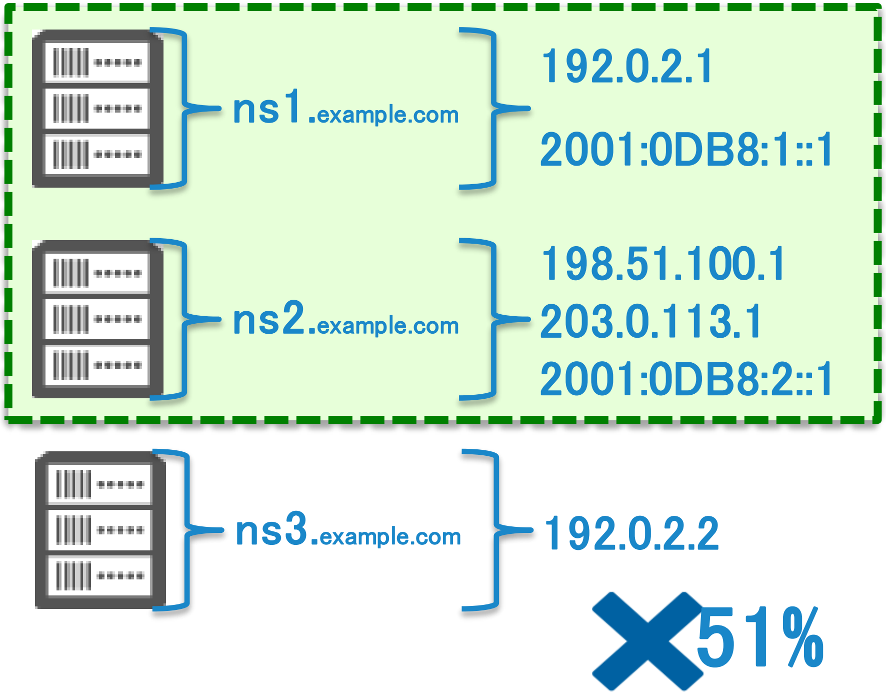
DNS service availability

Parameter	SLR (monthly basis)
DNS service availability	0 min downtime (100% availability)
DNS name server availability	£ 432 min of downtime (» 99%)
TCP DNS resolution RTT	£ 1500 ms, for at least 95% of the queries
UDP DNS resolution RTT	£ 500 ms, for at least 95% of the queries
DNS update time	£ 60 min, for at least 95% of the probes

- **DNS service availability:**

SPEC10: *For the service to be considered available at a particular moment, at least, two of the delegated name servers registered in the DNS must have successful results from “**DNS tests**” to each of their public-DNS registered “**IP addresses**” to which the name server resolves.*

example.com:



ns1.example.com

192.0.2.1

2001:0DB8:1::1

ns2.example.com

198.51.100.1

203.0.113.1

2001:0DB8:2::1

ns3.example.com

192.0.2.2

51%

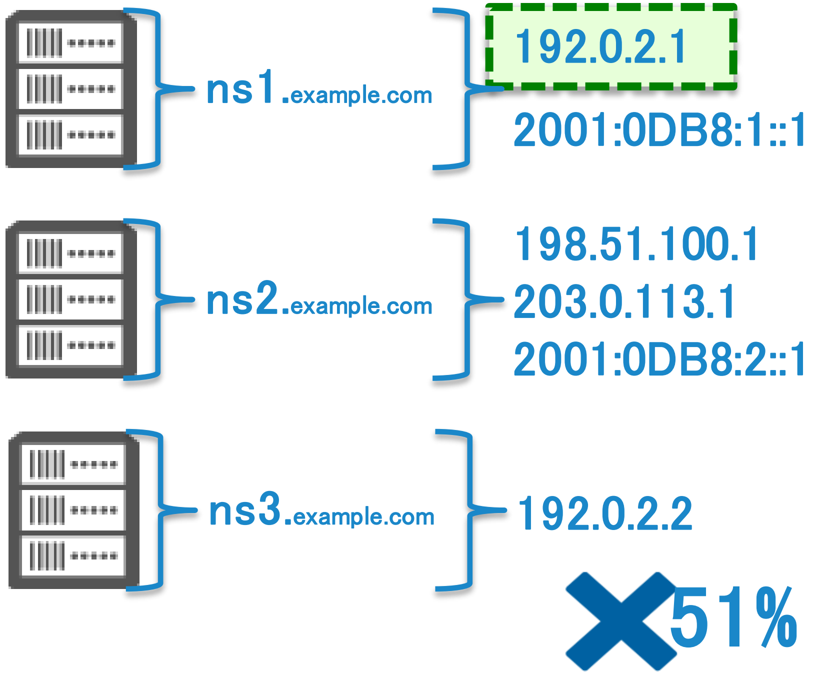
DNS name server availability

Parameter	SLR (monthly basis)
DNS service availability	0 min downtime (100% availability)
DNS name server availability	£ 432 min of downtime (» 99%)
TCP DNS resolution RTT	£ 1500 ms, for at least 95% of the queries
UDP DNS resolution RTT	£ 500 ms, for at least 95% of the queries
DNS update time	£ 60 min, for at least 95% of the probes

- **DNS NS availability:**

SPEC10: *Refers to the ability of a public-DNS registered **“IP address”** of a particular name server listed as authoritative for a domain name, to answer DNS queries from an Internet user.*

example.com:



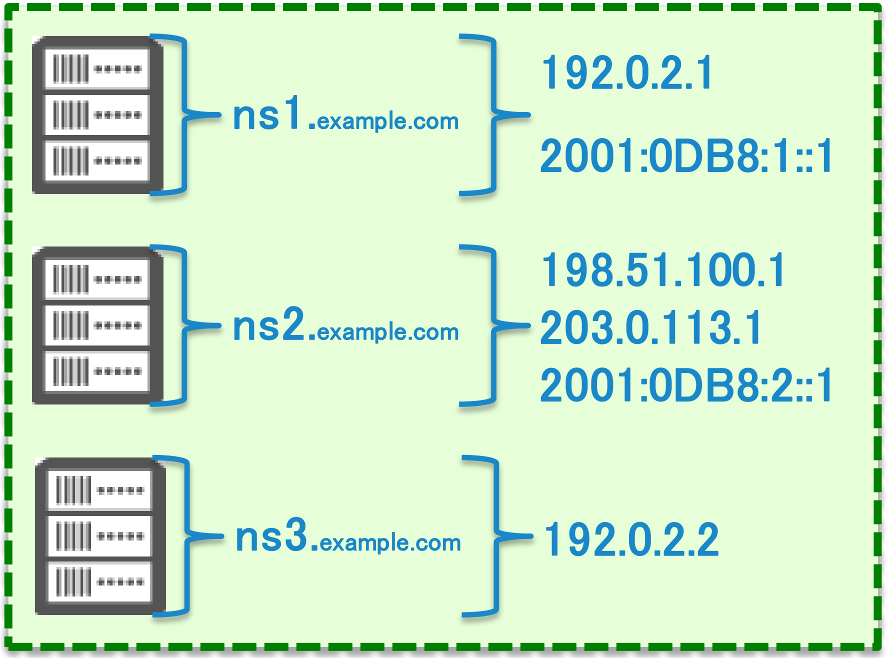
UDP/TCP DNS resolution RTT

- **TCP DNS resolution RTT**

SPEC10: *Refers to the RTT (Round-Trip Time) of the sequence of packets from the start of the TCP connection to its end, including the reception of the DNS response for only one DNS query. If the RTT is 5 times greater than the time specified in the relevant SLR, the RTT will be considered undefined.*

Parameter	SLR (monthly basis)
DNS service availability	0 min downtime (100% availability)
DNS name server availability	£ 432 min of downtime (» 99%)
TCP DNS resolution RTT	£ 1500 ms, for at least 95% of the queries
UDP DNS resolution RTT	£ 500 ms, for at least 95% of the queries
DNS update time	£ 60 min, for at least 95% of the probes

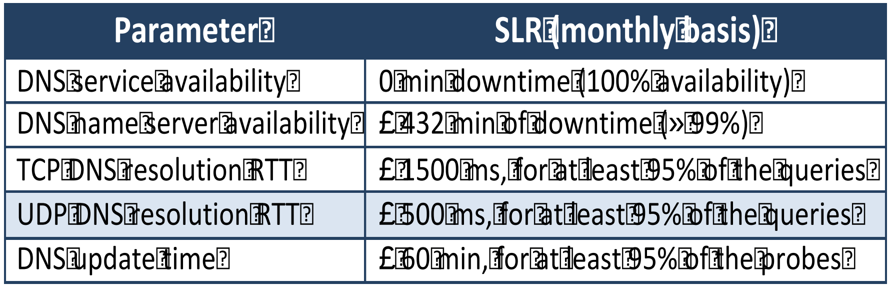
example.com:



UDP/TCP DNS resolution RTT

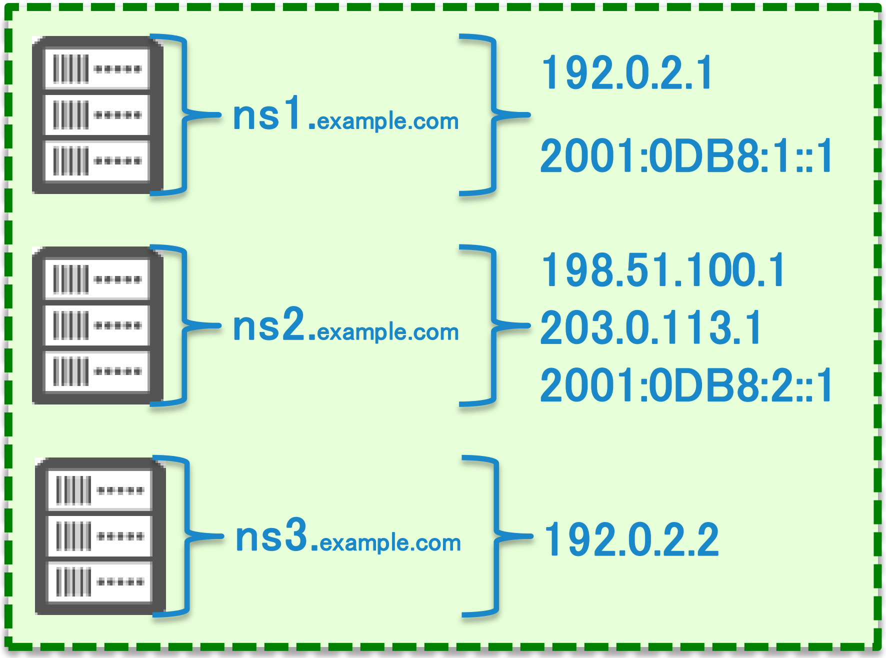
⊙ UDP DNS resolution RTT

SPEC10: *Refers to the RTT (Round-Trip Time) of the sequence of two packets, the UDP DNS query and the corresponding UDP DNS response. If the RTT is 5 times greater than the time specified in the relevant SLR, the RTT will be considered undefined.*



Parameter	SLR (monthly basis)
DNS service availability	0 min downtime (100% availability)
DNS name server availability	£ 432 min of downtime (» 99%)
TCP DNS resolution RTT	£ 1500 ms, for at least 95% of the queries
UDP DNS resolution RTT	£ 500 ms, for at least 95% of the queries
DNS update time	£ 60 min, for at least 95% of the probes

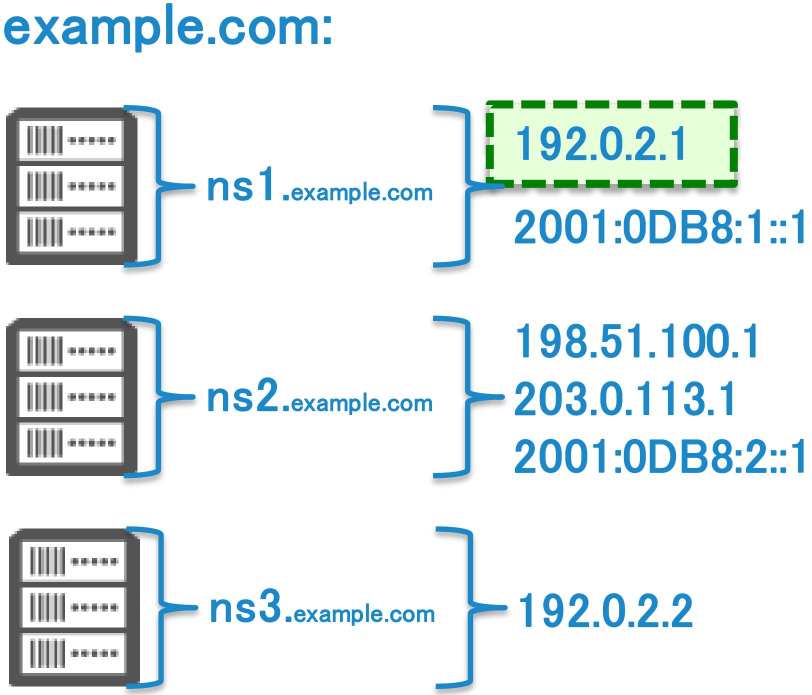
example.com:



DNS test

- **DNS test:**

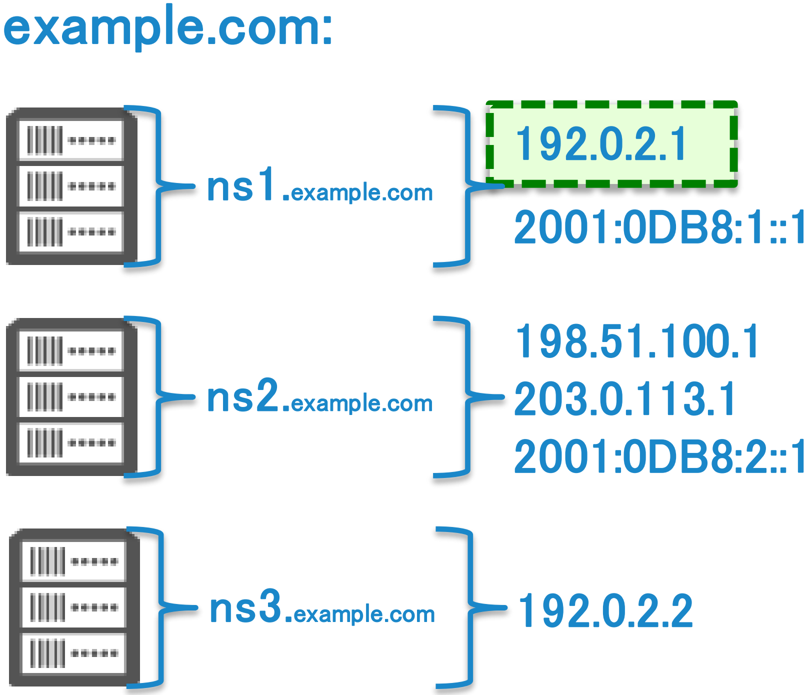
SPEC10: *Means one non-recursive DNS query sent to a particular **"IP address"** (via UDP or TCP). A query with a "DNS resolution RTT" 5 times higher than the corresponding SLR, will be considered unanswered.*



DNSSEC

- **DNSSEC:**

SPEC10: *For a query to be considered answered, the signatures must be positively verified against a corresponding DS record published in the parent zone.*



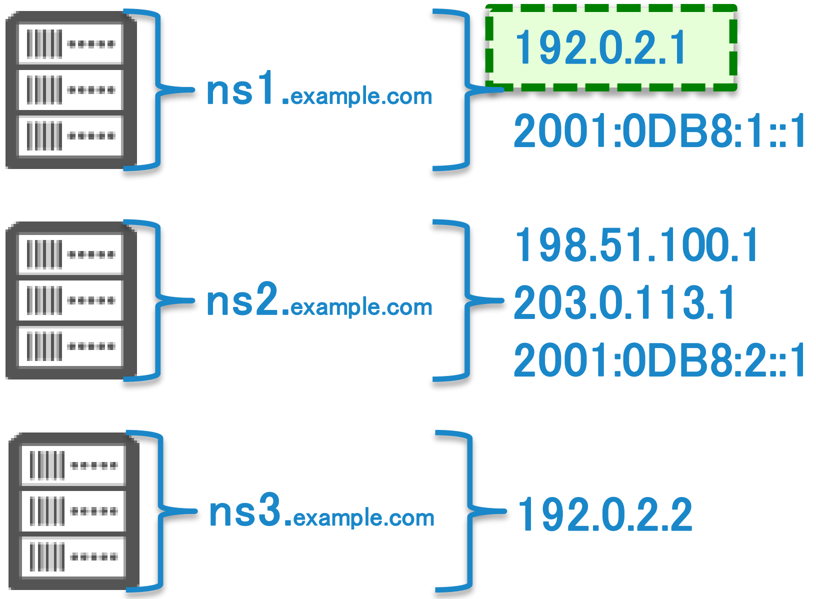
DNS update time

⊙ **DNS update time:**

SPEC10: *Refers to the time measured from the reception of an EPP confirmation to a transform command on a domain name, until the name servers of the parent domain name answer “**DNS queries**” with data consistent with the change made.*

Parameter	SLR (monthly basis)
DNS service availability	0 min downtime (100% availability)
DNS name server availability	£ 432 min of downtime (» 99%)
TCP DNS resolution RTT	£ 1500 ms, for at least 95% of the queries
UDP DNS resolution RTT	£ 500 ms, for at least 95% of the queries
DNS update time	£ 60 min, for at least 95% of the probes

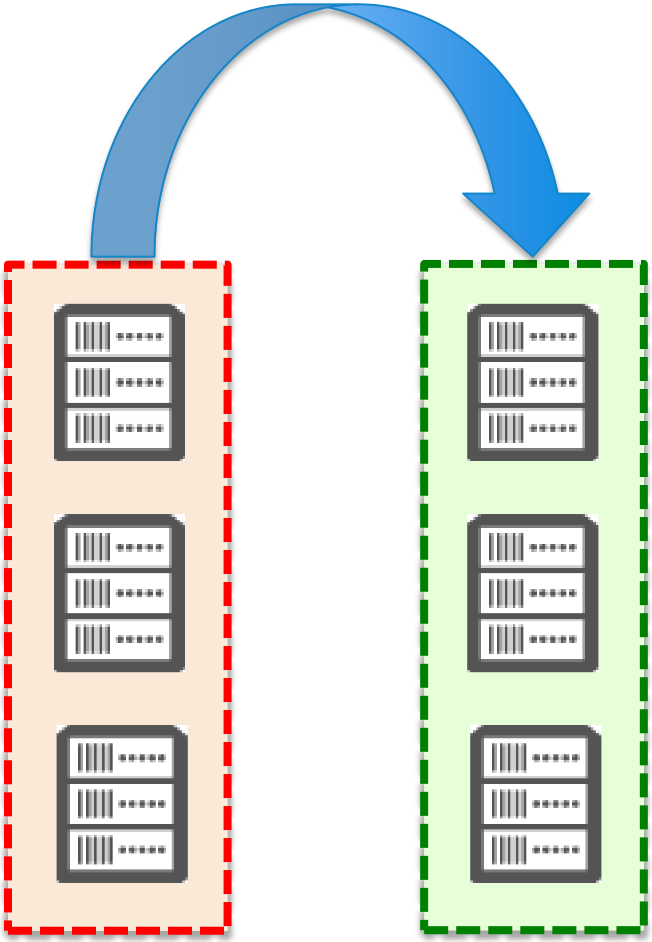
example.com:

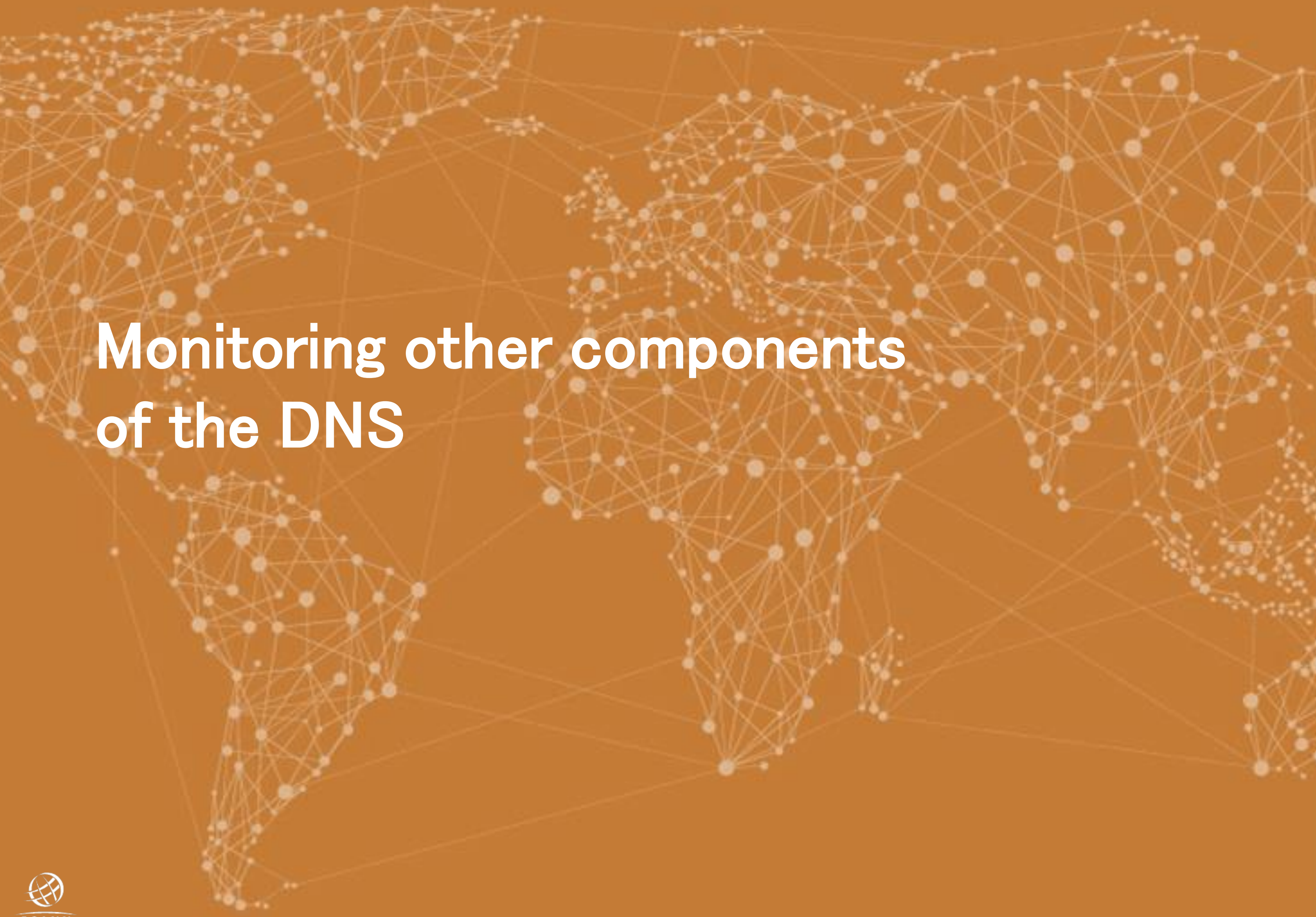


EBERO

- **EBERO:**

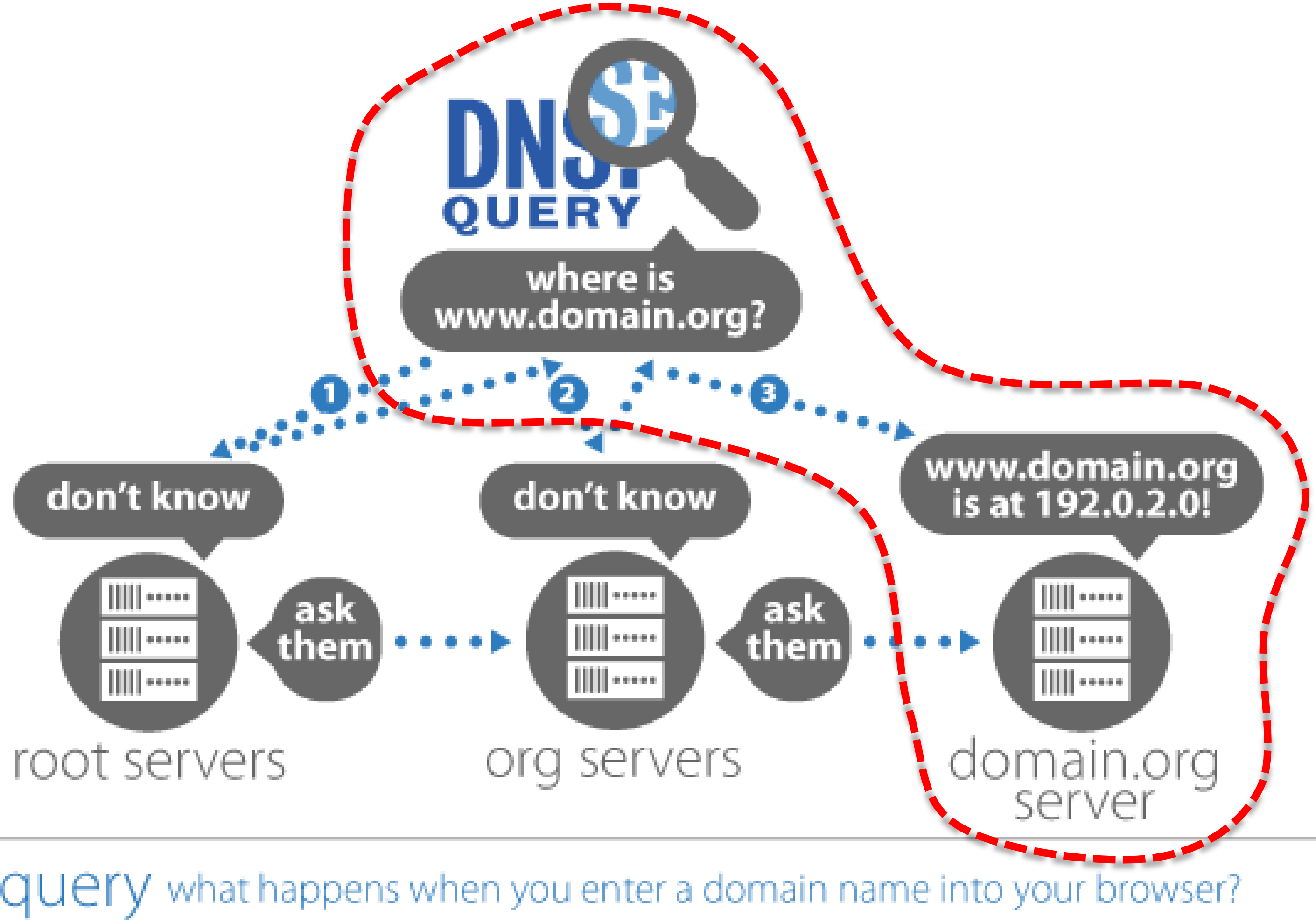
If the DNS service of a TLD fails for more than 4 hours on a rolling week basis, ICANN may appoint an Emergency Back-end Registry Operator (EBERO) to maintain the correct operation of the TLD.





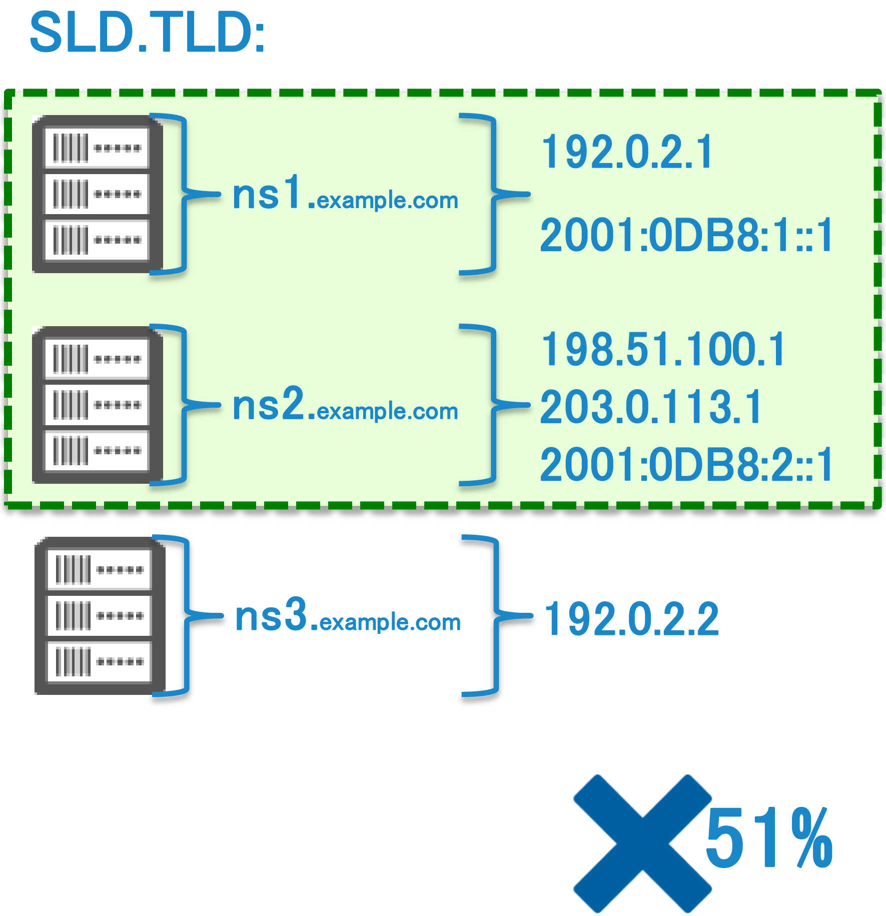
Monitoring other components of the DNS

Monitoring other components of the DNS



Monitoring other components of the DNS

- ISPs and DNS Operators should monitor the authoritative servers for their SLDs.
- ISPs and DNS Operators may use the same methodology used by ICANN to monitor new gTLDs.



Monitoring recursive DNS servers

- The recursive DNS service plays an important role in the perception of a healthy Internet service for end-users.

- ISPs and DNS Operators may monitor the recursive DNS service using the same methodology that ICANN uses for gTLDs with some differences:

  1. The probe nodes should be placed close to the end-users of the recursive name servers.

Monitoring recursive DNS servers

2. A domain name hosted on authoritative servers outside of the internal network may be used to monitor the recursive DNS servers. Preferably, the domain name used to monitor should be registered by the ISP or DNS Operator.

3. The cache of the recursive DNS server should be considered when monitoring a recursive DNS server. For example, the domain name used to monitor could be configured with a low TTL in order to force the recursive DNS server to execute the resolution process for the domain name.

Monitoring recursive DNS servers

4. If DNSSEC is supported by the recursive DNS server, the domain name used to monitor should be signed with DNSSEC.

5. Negative testing in the case of DNSSEC should be performed. A domain name with failing DNSSEC signatures should be used for negative testing.

Monitoring system

Monitoring system

- The monitoring system used by ICANN is operated in-house.
- The monitoring system is actively developed by Zabbix SIA, and it is based on the Zabbix monitoring platform.
- All code is open source, and published under the same license as the Zabbix monitoring platform.

Alerting

- The monitoring system sends email alerts to the registry operators.
- The monitoring system escalates the alerts via voice (phone call) to the registry operators.
- In addition to the threshold of 51% probe nodes detecting a problem, the monitoring system creates an incident after 3 consecutive failing test cycles (test cycle is calculated every minute).

Conclusion

Conclusion

- The health of the DNS system requires that several components operated by different actors are performing optimally.

- ICANN monitors and proactively works with the gTLD operators when DNS issues are detected.

- ISPs and DNS Operators may use the same methodology to monitor the other components of the DNS (i.e. recursive servers and authoritative severs for SLDs).

Thank You and Questions

ICANN

Thank You and Questions

Reach us at:
Email: gustavo.lozano@icann.org
Website: icann.org

- twitter.com/icann
- facebook.com/icannorg
- linkedin.com/company/icann
- youtube.com/user/icannnews
- gplus.to/icann
- weibo.com/ICANNorg
- flickr.com/photos/icann
- slideshare.net/icannpresentations