Root Management Update

San Francisco, USA
March 2011

Kim Davies
Manager, Root Zone Services

ICANN
Internet Corporation for
Assigned Names & Numbers

IANA NOI

Notice of Inquiry

- IANA Contract expires later in 2011
- US Government has issued a Notice of Inquiry, asking for feedback regarding how the IANA Contract should be stipulated.
- A good opportunity for ccTLDs to make known if you feel the IANA contract, and the requirements surrounding it prescribed by the USG, should change in nature.
- http://www.ntia.doc.gov/

Workflow automation

Workflow Automation

- Automation project has been a joint collaboration between ICANN, VeriSign and NTIA.
- We have been successfully running the automation system in “production shakeout” for a number of months, gaining confidence it works correctly for all use cases.
- A formal period of parallel evaluation is the last step to certifying the system for full production use.
- Watch this space.

DNSSEC Improvements

DNSSEC Improvements

- For testing if TLD’s DS records are valid, since day 1 we perform a “DS to DNSKEY” check.
  - Catches typos and other kinds of miscommunication
  - Does not catch common configuration errors relating to DNSSEC being misconfigured by the TLD operator.
- In order to help reduce the risk TLD operators list nameservers without proper DNSSEC support, propose to implement “RRSIG checks”.

RRSIG Checking

- Check that the domain is signed with valid RRSIG records, using one of the key-signing-keys listed within the top-level domain.
- As with most other tests, will result in a soft fail.
    - Will check with TLD operator, if they insist in proceeding, we can do so.
- Implementation into regular workflow in the next few weeks.

RRSIG Checking

```
$ ds-check xn--zckzah 56231 8 1 D2C46F1B7A4F83D99C5133671167D083243A3F48
Domain: xn--zckzah
Checking for DS record: 56231 8 1 d2c46f1b7a4f83d99c5133671167d083243a3f48
  computed DS: tag 56231 digest d2c46f1b7a4f83d99c5133671167d083243a3f48
Match found.
Test successful.

$ rrsig-check xn--zckzah a.iana-servers.net
3 DNSKEYs for xn--zckzah from a.iana-servers.net:
    1) (./8) AwEAAcdeWZYENiJJxT6s...0sEK7ETyZQsxjtfqGSe7
    2) (./8) AwEAAd4i2Kf2SrhuSVKJ...swt9Y2RvND8NdSiPMbRF
    3) (S/8) AwEAAaM6kV5YjIfdWIkW...aD2irDvCmHPyEK4DuTk=
1 RRSIGs:
    1) [X] WwgEPBLInvIcjVCE1N31...TGkIQyoJ/o6C3ILchA== (success with DNSKEY #3)
```

Country-wide Internet shutdowns

Country-wide Internet shutdowns

- In recent months, we’ve seen regulatory shutdowns of Internet in certain countries.
  - Relatively new phenomenon, but not entirely unprecedented
  - ICANN used to working in cases where it is clear restoration of service is a priority.

Egypt Case

- Internet traffic was blocked for a number of days.
- ccTLD registry was unreachable online.
- .EG continued to resolve
- .Masr (Egyptian IDN ccTLD) stopped functioning entirely
- Why?

Two Factors

1. Expiry period in SOA field
2. Geographically diverse name servers

❶ Expiry period

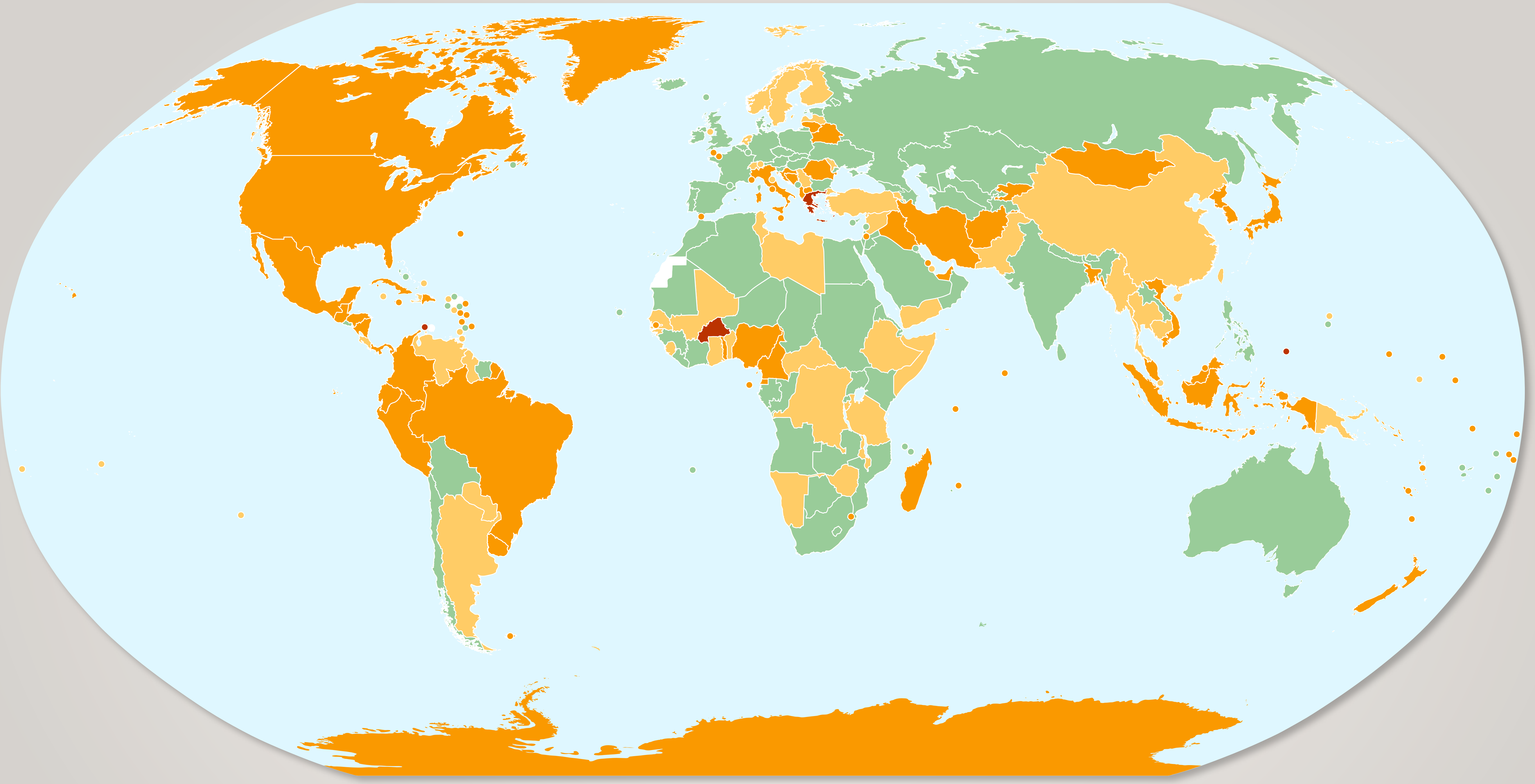
- Expiry field in the SOA tells secondary authorities how long they can keep serving data until they consider it stale and throw it away.

- Long expiry period helped the .EG domain stay online globally while Internet connectivity was severed to the registry.

- Once expire period lapses, the domain is offline unless there is some external intervention.

What expiry period do TLDs use?

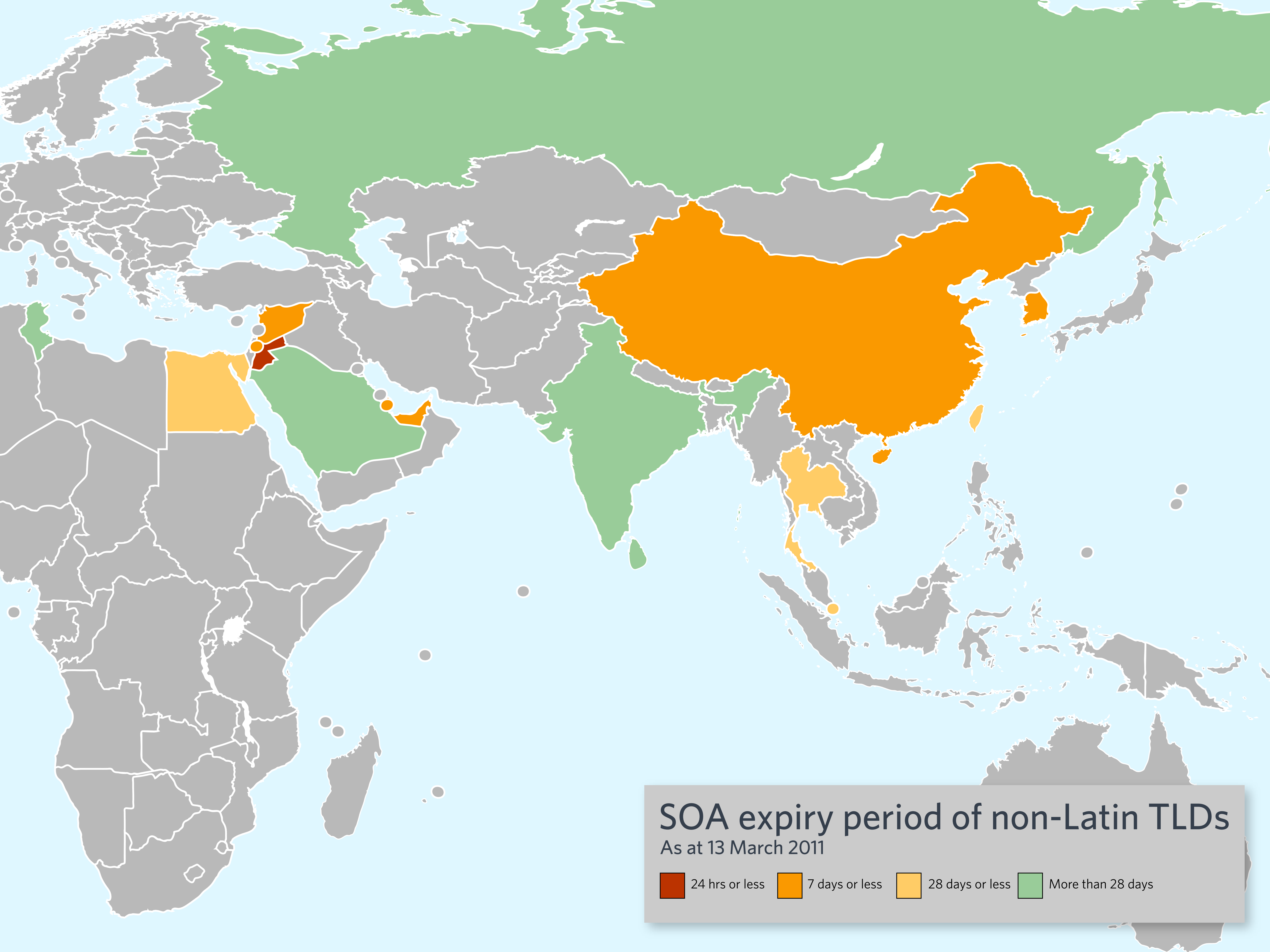
3 hours	1
12 hours	1
16 hours, 48 mins	1
1 day	2
5 days	2
7 days	106
8 days, 1 hour	1
10 days	2
12.1 days	1
14 days	33
15 days	8
16 days	1
18 days, 13h, 46m, 40s	1
19 days, 6h, 13m, 20s	1
20 days	4
21 days	1
21 days, 33m, 20s	1
27 days, 18h, 40m	4
28 days	27
30 days	50
35 days, 5 hrs	2
41 days, 16 hrs	43
42 days	1
49 days	1
56 days	3
60 days	1
63 days	1
70 days	3
140 days	1
182 days	1
210 days, 7 seconds	1



🟥 24 hrs or less 🟧 7 days or less 🟨 28 days or less 🟩 More than 28 days

SOA expiry period of ASCII TLDs

As at 13 March 2011



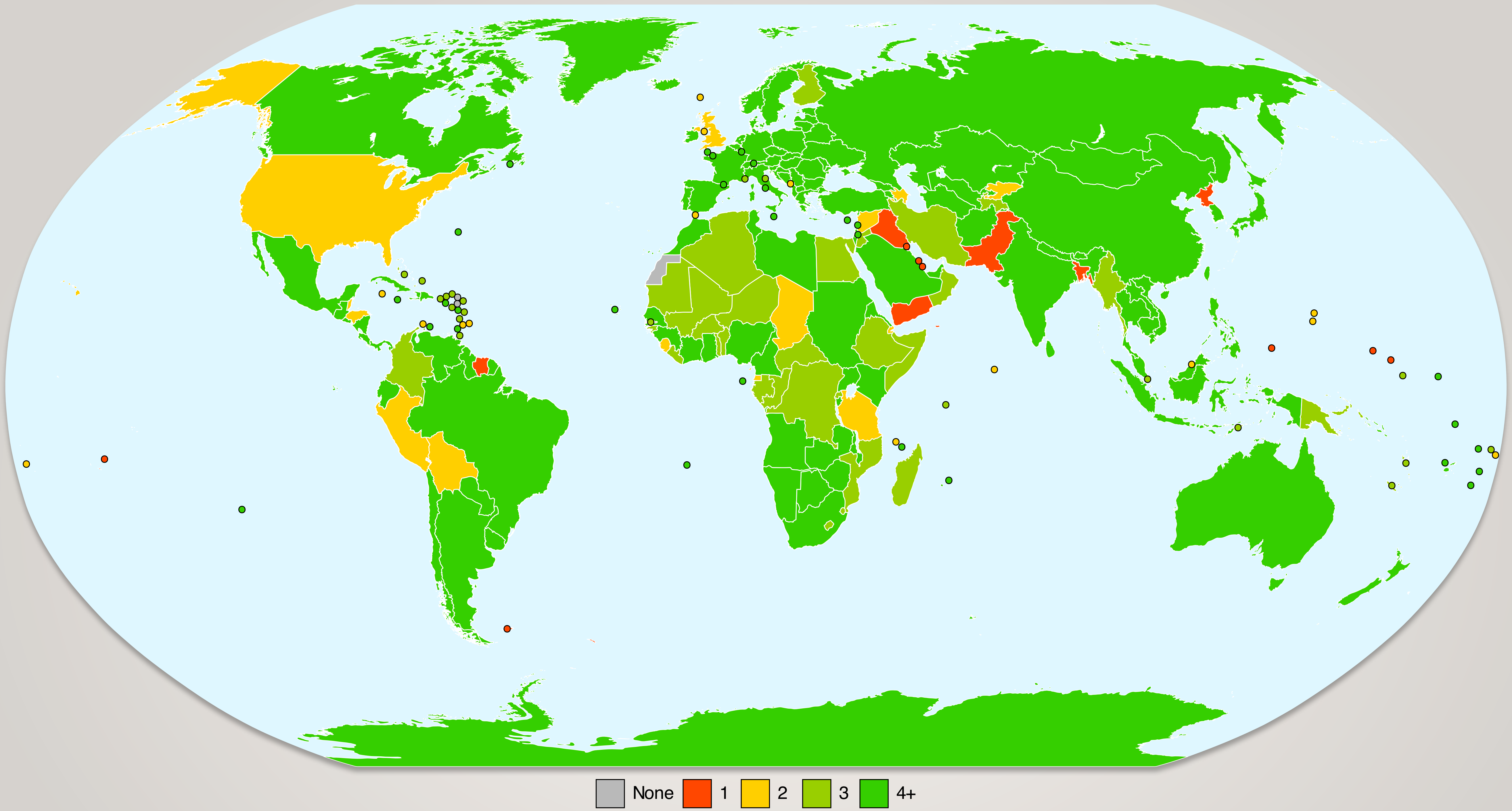
SOA expiry period of non-Latin TLDs

As at 13 March 2011

🟥 24 hrs or less 🟧 7 days or less 🟨 28 days or less 🟩 More than 28 days

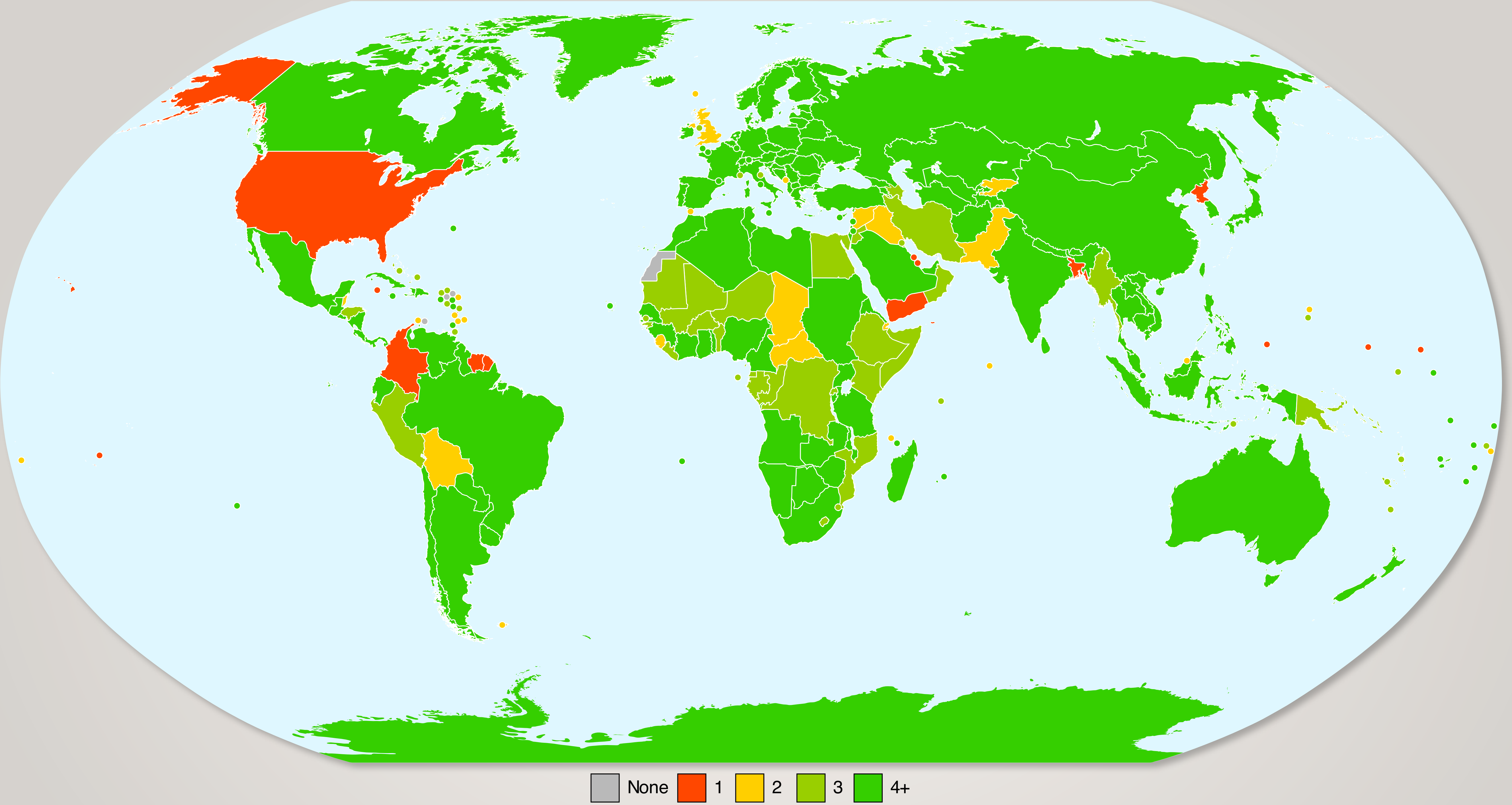
❷ Nameserver diversity

- IANA “requirement” that nameservers be on two separate topologically diverse networks, measured by unique origin AS
  - Not a guarantee there is not a single point of failure, but a reasonable best effort
  - Definitely no guarantee they are in multiple countries
  - ccTLD operators, as with many technical tests we do, can waive the requirement and proceed regardless.



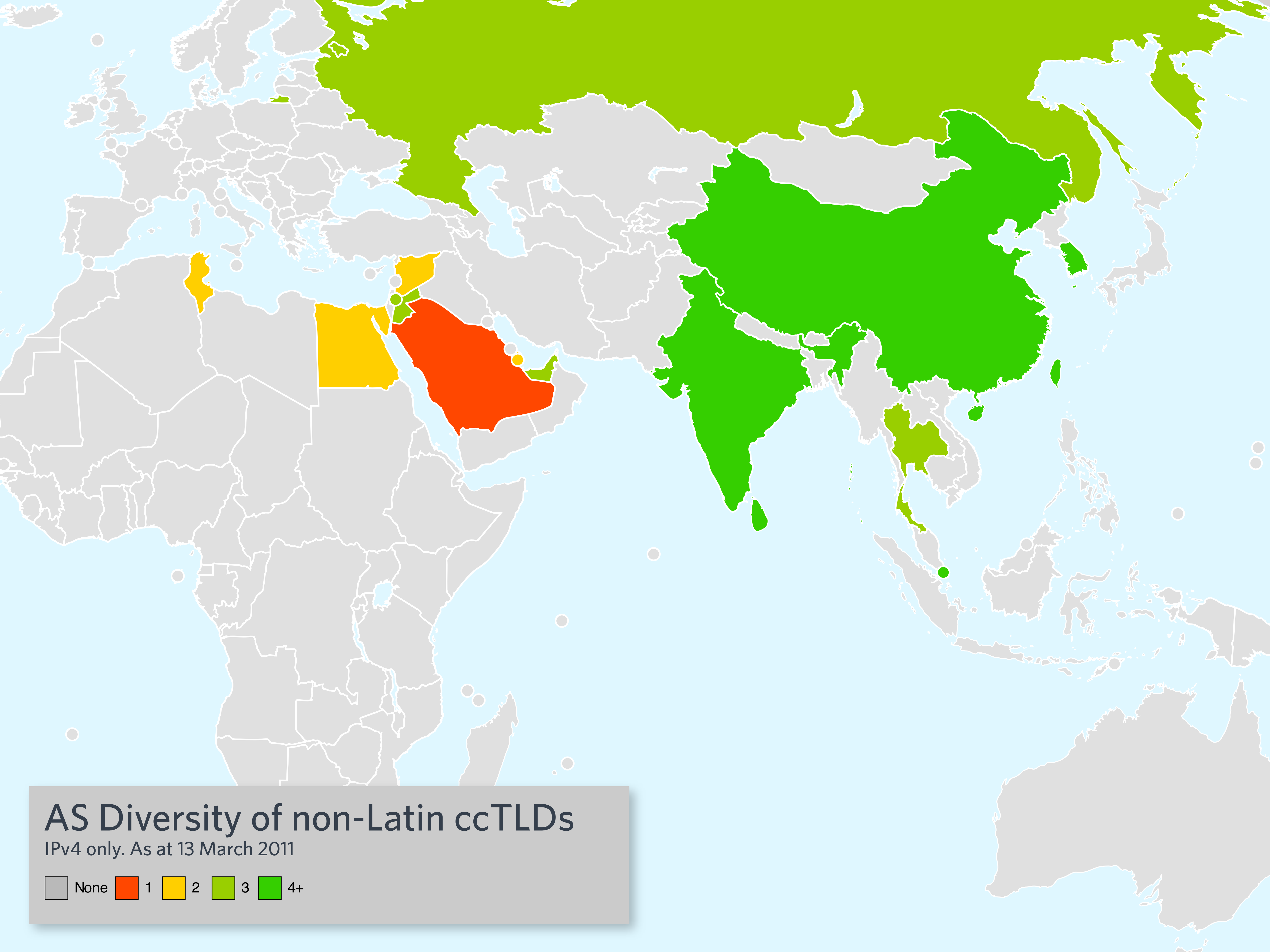
ccTLDs with AS diversity

IPv4 only. As at 1 March 2009



ccTLDs with AS diversity

IPv4 only. As at 13 March 2011



AS Diversity of non-Latin ccTLDs

IPv4 only. As at 13 March 2011

⬜ None 🟥 1 🟨 2 🟩 3 🟩 4+

Conclusion

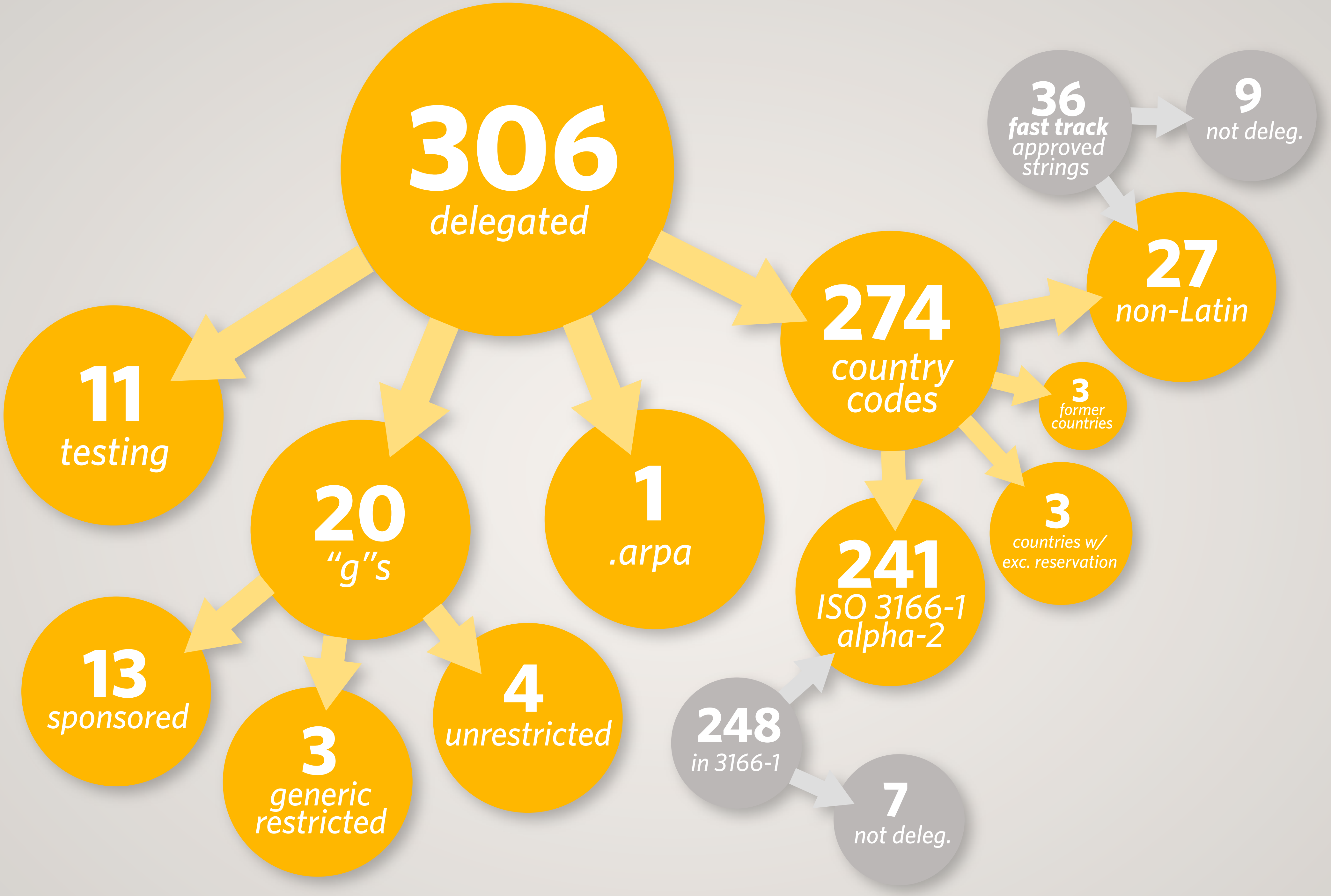
- A combination of long expiry periods; and geographically and topologically diverse name servers; will help protect against these kinds of incidents, whether man-made or natural disasters.
    - Note that long expiries are not without other consequences, consider the trade-offs carefully.
- In recent cases, the registry was collateral damage. If someone of authority was serious they could still shut down a TLD no matter what (e.g. having the authority publish an empty zone).
- ICANN's ability to act depends on what the ccTLD operator wants us to do.
- Primary responsibility for contingency planning in the event of disaster belongs to the ccTLD operator. Secondary domain operators should rely ccTLD operators for instruction, ICANN involvement is a last result.

Staffing update

Root Management Staffing

- Naela Sarras has been promoted to responsibility of the IDN Fast Track process (string selection, etc.)
    - Recruiting for a new root management staff member
- Other internal restructures in IANA dept.

Over 300 TLDs...



306 delegated

11 testing

20 “g”s

13 sponsored

3 generic restricted

4 unrestricted

1 .arpa

274 country codes

27 non-Latin

36 fast track approved strings

9 not deleg.

3 former countries

3 countries w/ exc. reservation

241 ISO 3166-1 alpha-2

248 in 3166-1

7 not deleg.

kim.davies@icann.org