DNS operations and ccTLD management

Champika Wijayatunga | SANOG28 Mumbai - India | 1-9 August 2016

The World's Network – the Domain Name System

- Internet Protocol numbers are unique addresses that allow computers to find one another
- The Domain Name System matches IP numbers with a name
- DNS is the underpinning of unified Internet
- DNS keeps Internet secure, stable and interoperable
- ICANN was formed in 1998 to coordinate DNS

History

1983 DNS was designed/invented by Paul Mockapetris (RFC882 & 883)

1984 Berkeley Internet Name Domain (BIND) Server developed
Original Seven Generic TLDs (.com, .edu, .gov, .int, .mil, .net, and .org)

1985 First country codes assigned .us, .uk, and .il
1986 .au, .de, .fi, .fr, .jp, .kr, .nl and .se
1987 RFC1034 (Considered the first full DNS Specification)

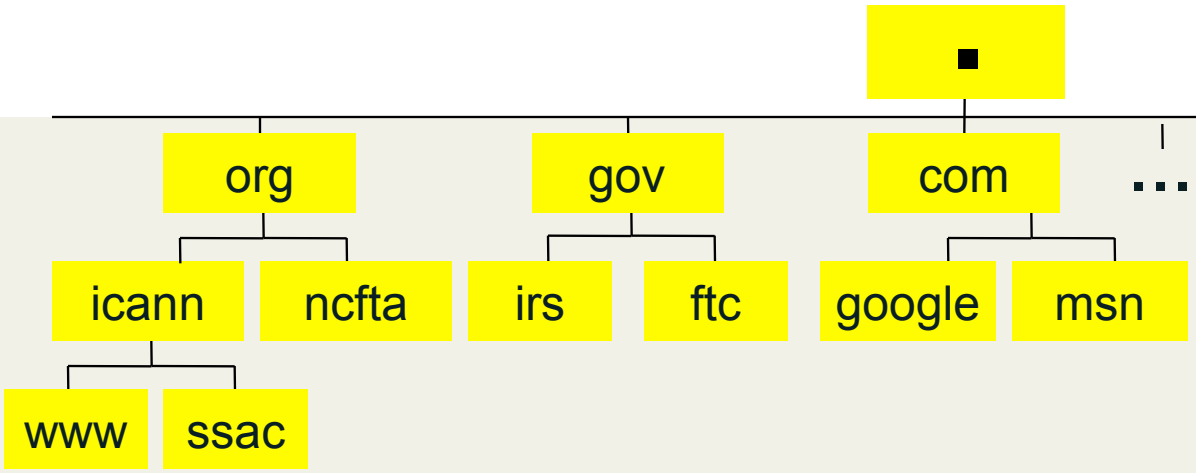
…….. Country Code TLDs continue to be added….

2000 Seven new TLDs added (.aero, .coop, .museum, .biz, .info, .name, and .pro)

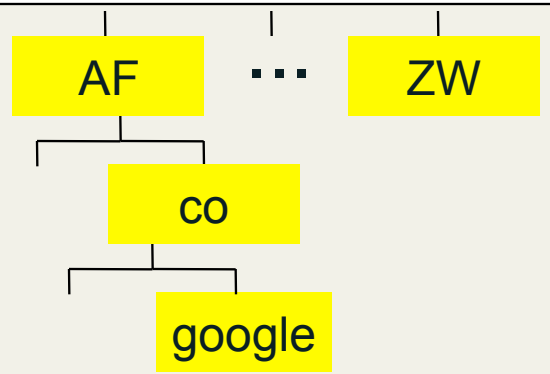
2012 New round of applications for gTLDs opened by ICANN

DNS Structure

- A **domain** is a node in the Internet name space
  - A domain includes all its descendants
- Domains have names
  - Top-level domain (TLD) names are generic or country-specific
  - TLD *registries* administer domains in the top-level
  - TLD registries *delegate* labels beneath their top level delegation



Names in generic Top Level Domains



Names in country-code TLDs


Root Server Operation

What do the Root-Server Operators do?

- Copy a very small database, the content of which is currently decided by IANA
- Put that database in the servers called ‘Root Servers.
- Make the data available to all Internet users
- Work stems from a common agreement about the technical basis
  - Everyone on the Internet should have equal access to the data
  - The entire root system should be as stable and responsive as possible

What do the Root-Server Operators do not do?

- Interfere with the content of the database
  - E.g. run the printing presses, but don't write the book
- Make policy decisions
  - Who runs TLDs, or which domains are in them
  - What systems TLDs use, or how they are connected to the Internet

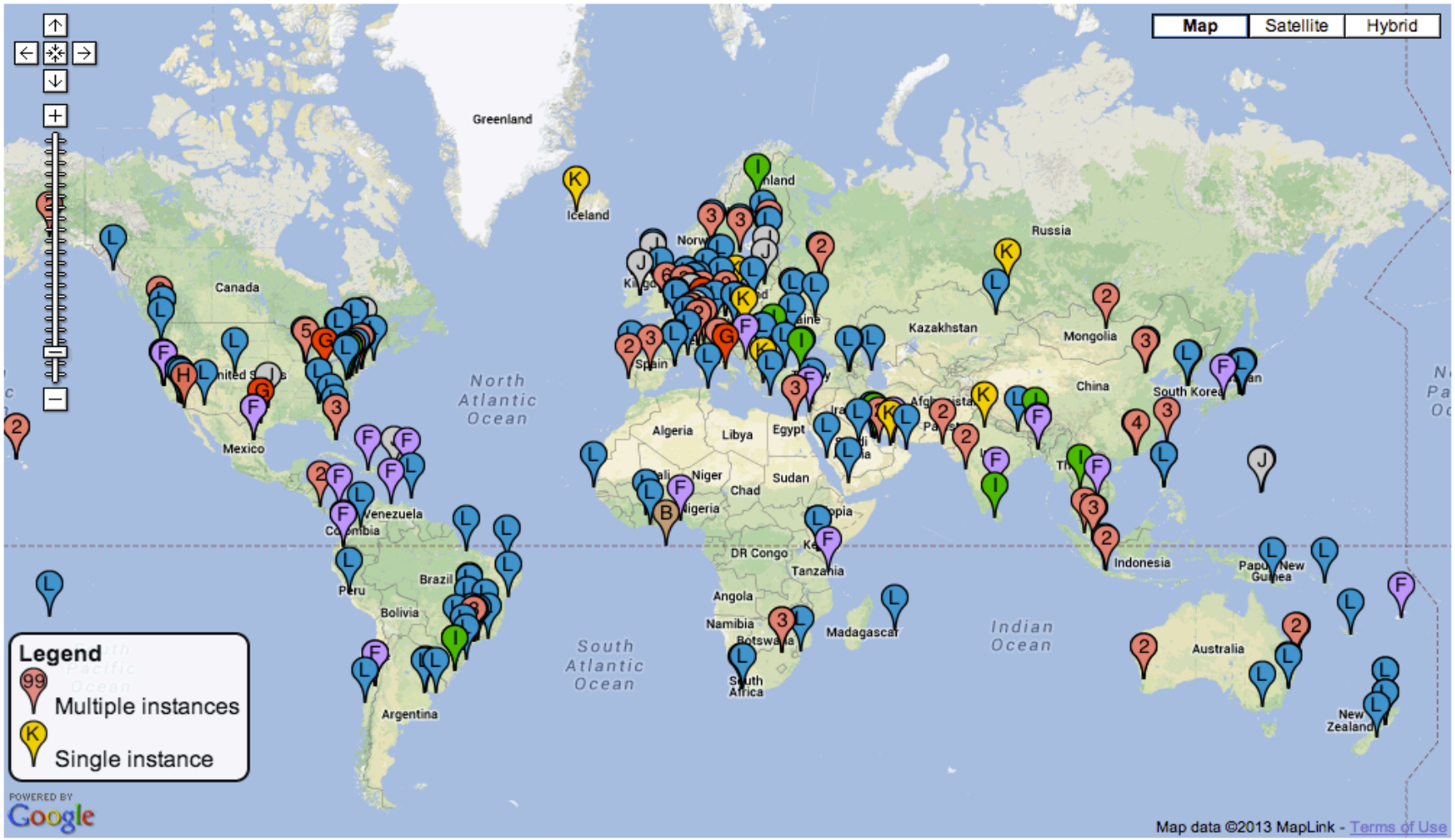
Who are the Root Server operators?

- Not "one group", 12 distinct operators
- Operational and technical cooperation
- Participate in RSSAC as advisory body to ICANN
- High level of trust among operators
  - Show up at many technical meetings, including IETF, ICANN, RIR meetings, NOG meetings, APRICOT etc.

How Secure are the Root Servers?

- Physically protected
- Tested operational procedures
- Experienced, professional, trusted staff
- Defense against major operational threat – i.e. DDoS.
  - Anycast
    - Setting up identical copies of existing servers
    - Same IP address
    - Exactly the same data.
    - Standard Internet routing will bring the queries to the nearest server
    - Provides better service to more users.

Root Servers



Avoiding Common Misconceptions

- Not all internet traffic goes through a root server
- Not every DNS query is handled by a root server
- Root servers are not managed by volunteers as a hobby
  - Professionally managed and well funded
- No single organization(neither commercial nor governmental) controls the entire system
- The "A" server is not special.
- Root Server Operators don't administrate the zone content
  - They publish the IANA-approved data

Root Server Operation @ICANN

- ICANN is the L-Root Operator
- L-Root nodes keep Internet traffic local and resolve queries faster
- Make it easier to isolate attacks
- Reduce congestion on international bandwidth
- Redundancy and load balancing with multiple instances

L-Root presence

L-Root presence

- Geographical diversity via Anycast
  - Around 160 dedicated servers
  - Presence on every continent
- On normal basis 15 ~ 25 kqps
  - That is app 2 billion DNS queries a day
- Interested in hosting a L-Root
  - Contact your ICANN Global Stakeholder Engagement Representative

DNS Servers

- DNS is a distributed database
- Types of DNS servers
  - DNS Authoritative
    - Primary (Master)
    - Secondary (Slaves)
  - DNS Resolver
    - Recursive
    - Cache
    - Stub resolver

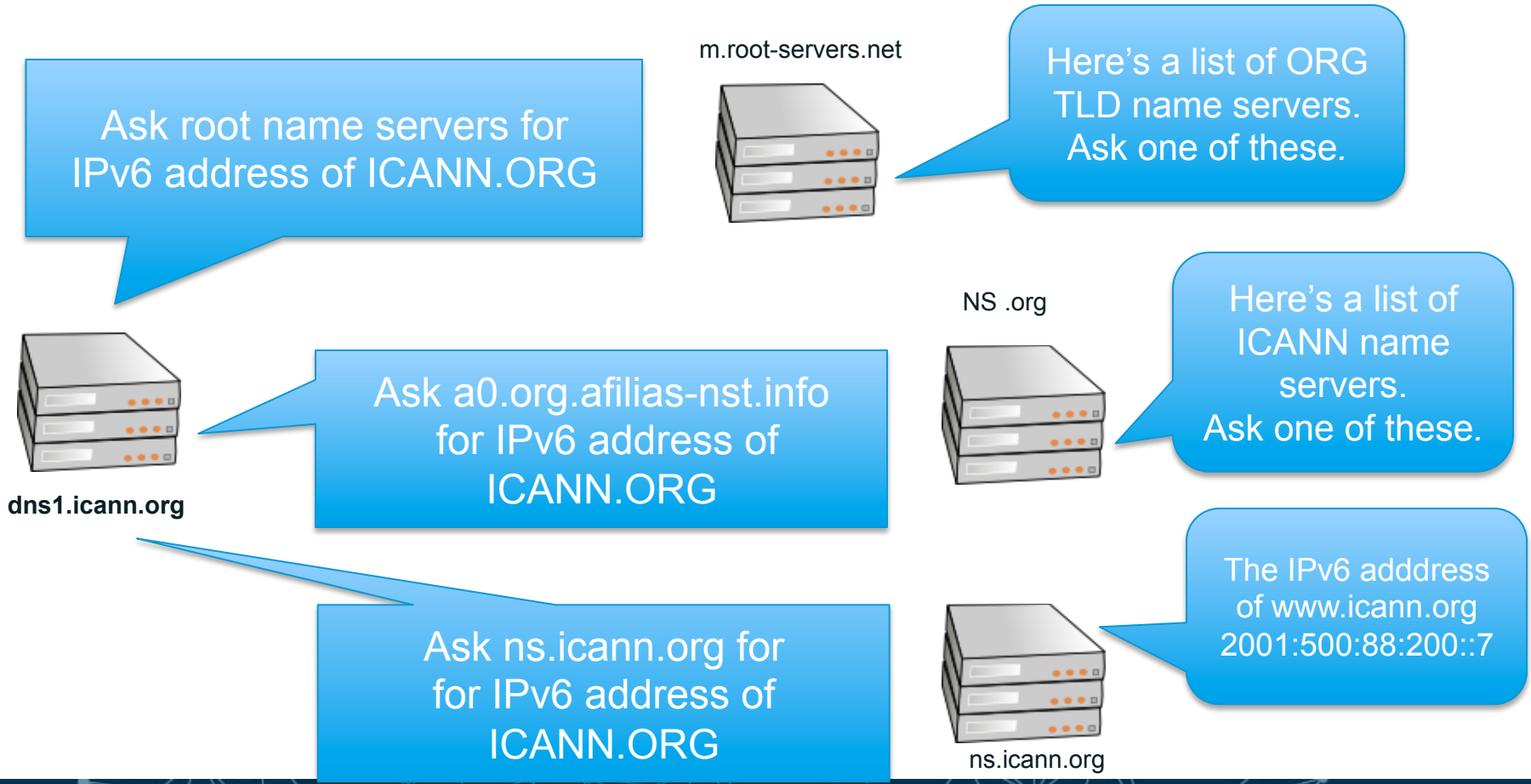
Operational elements of the DNS

- Authoritative Name Servers host zone data
  - The set of “DNS data” that the registrant publishes
- Recursive Name Resolvers (“resolvers”)
  - Systems that find answers to queries for DNS data
- Caching resolvers
  - Recursive resolvers that not only find answers but also store answers locally for “TTL” period of time
- Client or “stub” resolvers
  - Software in applications, mobile apps or operating systems that query the DNS and process responses

Domain name “directory assistance”

How does a resolver find the IP address of ICANN.ORG?

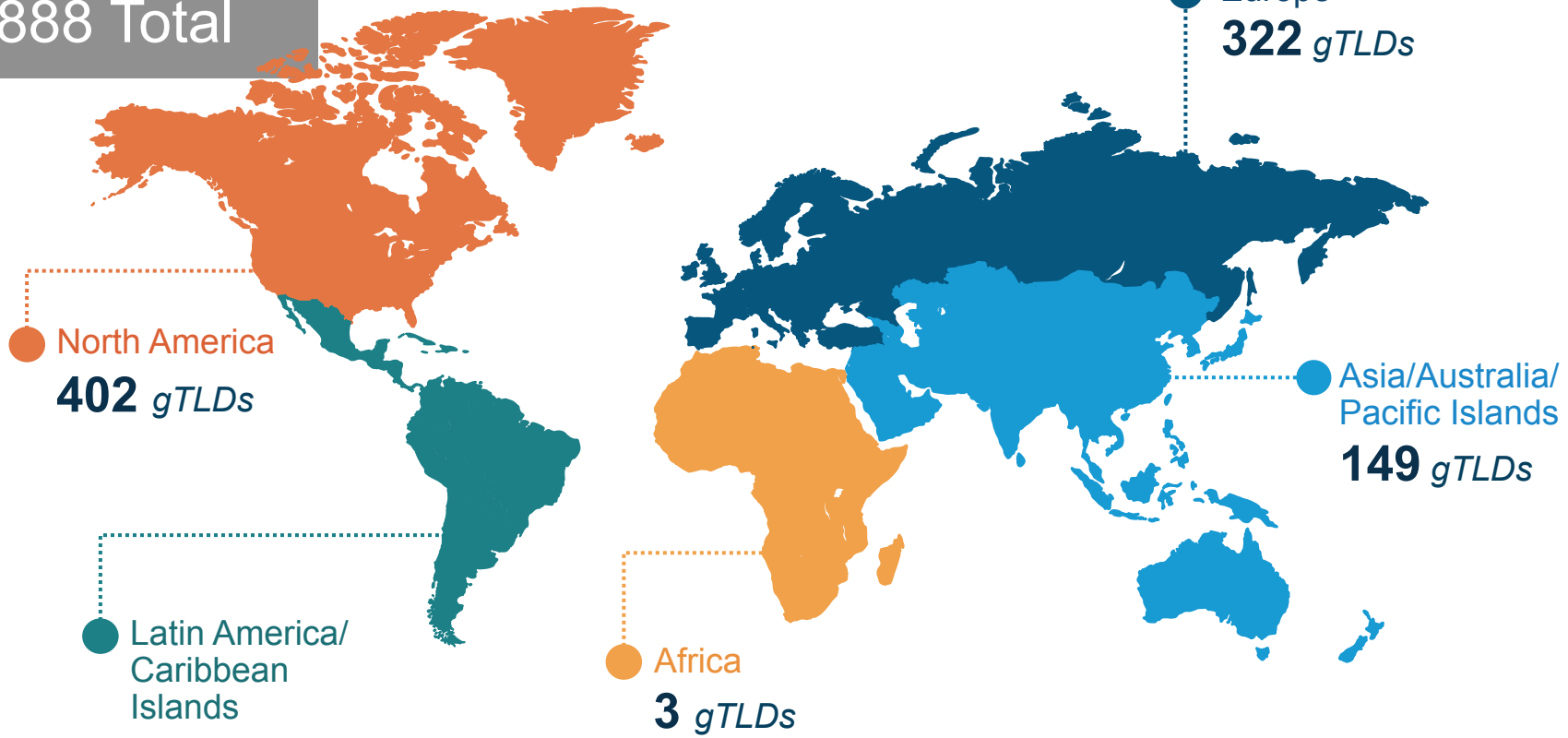
- Resolvers find answers by asking questions *iteratively*




Registry, Registrar Model

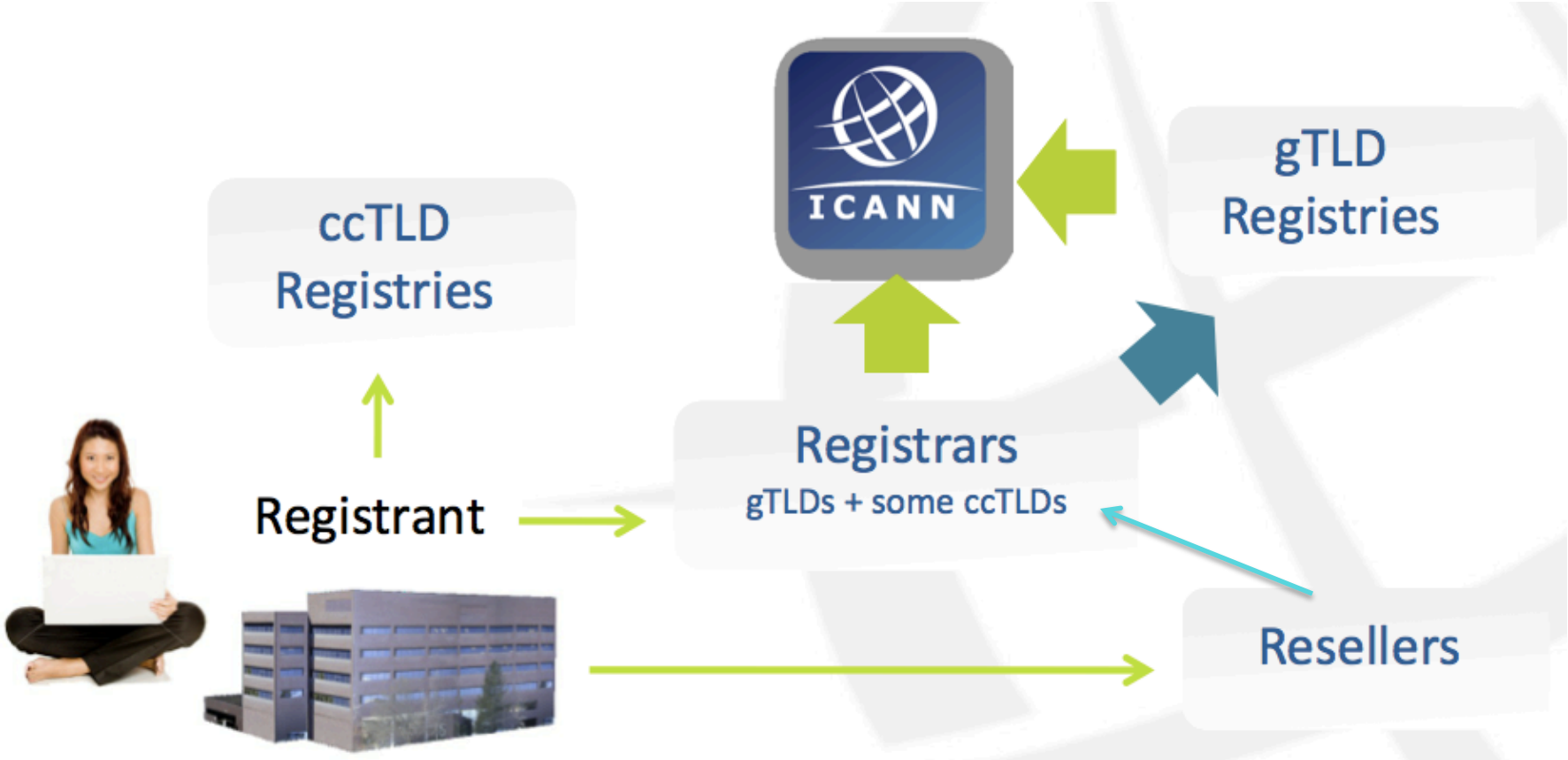
Regional Distribution of Delegated gTLDs

888 Total

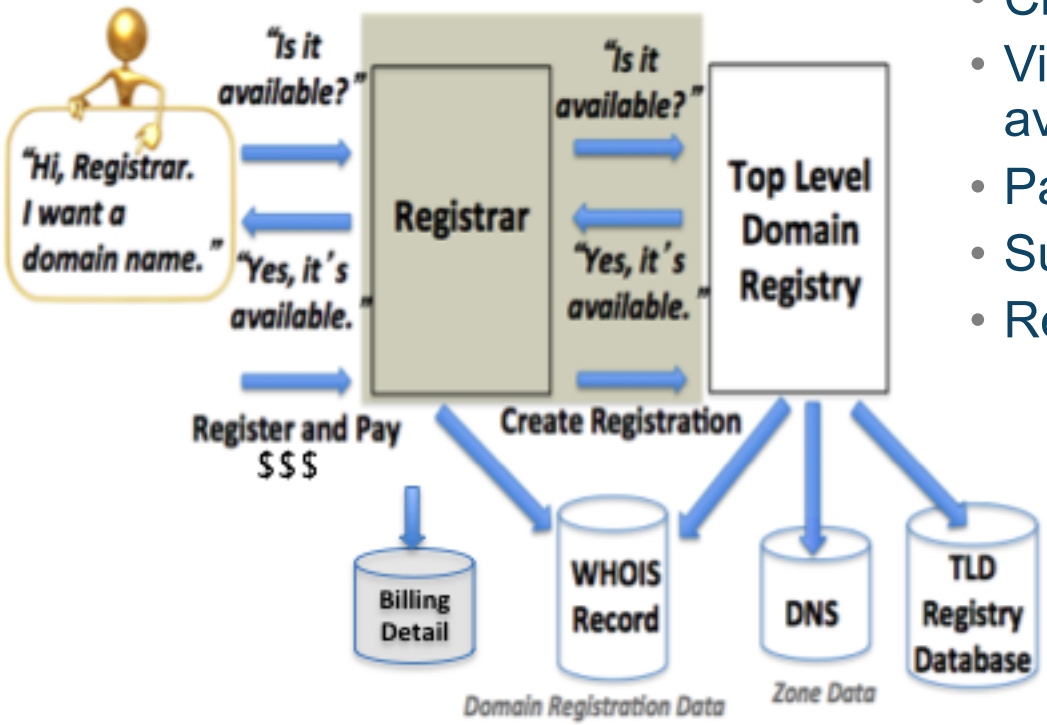


Data as of January 2016
Categorized by ICANN region

The Registry/Registrar Ecosystem



Domain Name Registration



How to register a domain:

- Choose a string e.g., `example`
- Visit a registrar to check string availability in a TLD
- Pay a fee to register the name
- Submit registration information
- Registrar and registries manage:
  - "string" + TLD (managed in registry DB)
  - Contacts, DNS (managed in Whois)
  - DNS, status (managed in Whois DBs)
  - Payment information


Managing Zones

DNS Resource Records (RR)

- Unit of data in the Domain Name System
- Define attributes for a domain name

Label	TTL	Class	Type	RData
www	3600	IN	A	192.168.0.1

- Most common types of RR
  - A
  - AAAA
  - NS
  - SOA
  - MX
  - CNAME

What is a DNS zone *data*?

- DNS zone data are hosted at an *authoritative name server*
  - Each “cut” has zone data (root, TLD, delegations)
- DNS zones contain *resource records that* describe
  - name servers,
  - IP addresses,
  - Hosts,
  - Services
  - Cryptographic keys & signatures…

```
$TTL    86400 ; 24 hours could have been written as 24h or 1d
; $TTL used for all RRs without explicit TTL value
$ORIGIN example.com.
@  1D          IN  SOA ns1.example.com. hostmaster.example.com. (
                       2002022401 ; serial
                       3H ; refresh
                       15 ; retry
                       1w ; expire
                       3h ; minimum
                       )
               IN  NS     ns1.example.com.    ; NS in the domain bailiwick
               IN  NS     ns2.smokeyjoe.com.  ; NS external to domain
               IN  MX  10 mail.another.com.   ; external mail provider
;
; Sender policy framework with hard fail
; Use A and MX resource records for verification and google too
;
example.com. IN TXT "v=spf1 a mx include:google.com ~all"
;
; server host definitions
;
ns1            IN  A      192.168.0.1        ;name server definition
www            IN  A      192.168.0.2        ;web server definition
;
; web and ftp server on same address
;
ftp            IN  CNAME  www.example.com.   ;ftp server definition
;
; endpoint or non server domain hosts
;
mikeslaptop    IN  A      192.168.0.3
fredsipad      IN  A      192.168.0.4
```

Only US ASCII-7 letters, digits, and hyphens can be used as zone data.

In a zone, IDNs strings begin with XN--

Common DNS Resource Records

```
$TTL    86400 ; 24 hours could have been written as 24h or 1d
; $TTL used for all RRs without explicit TTL value
$ORIGIN example.com.
@  1D          IN  SOA ns1.example.com. hostmaster.example.com. (
                       2002022401 ; serial
                       3H ; refresh
                       15 ; retry
                       1w ; expire
                       3h ; minimum
                       )
               IN  NS     ns1.example.com.    ; NS in the domain bailiwick
               IN  NS     ns2.smokeyjoe.com.  ; NS external to domain
               IN  MX  10 mail.another.com.   ; external mail provider
;
; Sender policy framework with hard fail
; Use A and MX resource records for verification and google too
;
example.com. IN TXT "v=spf1 a mx include:google.com ~all"
;
; server host definitions
;
ns1            IN  A      192.168.0.1        ;name server definition
www            IN  A      192.168.0.2        ;web server definition
;
; web and ftp server on same address
;
ftp            IN  CNAME  www.example.com.   ;ftp server definition
;
; endpoint or non server domain hosts
;
mikeslaptop    IN  A      192.168.0.3
fredsipad      IN  A      192.168.0.4
```

Time to live (TTL)

- *How long RRs are accurate*

Start of Authority (SOA) RR

- *Source: zone created here*
- *Administrator's email*
- *Revision number of zone file*

Name Server (NS)

- *IN (Internet)*
- *Name of authoritative server*

Mail Server (MX)

- *IN (Internet)*
- *Name of mail server*

Sender Policy Framework (TXT)

- *Authorized mail senders*

Common DNS Resource Records

```
$TTL    86400 ; 24 hours could have been written as 24h or 1d
; $TTL used for all RRs without explicit TTL value
$ORIGIN example.com.
@  1D          IN  SOA ns1.example.com. hostmaster.example.com. (
                       2002022401 ; serial
                       3H ; refresh
                       15 ; retry
                       1w ; expire
                       3h ; minimum
                       )
               IN  NS     ns1.example.com.    ; NS in the domain bailiwick
               IN  NS     ns2.smokeyjoe.com.  ; NS external to domain
               IN  MX  10 mail.another.com.   ; external mail provider
;
; Sender policy framework with hard fail
; Use A and MX resource records for verification and google too
;
example.com. IN TXT "v=spf1 a mx include:google.com ~all"
;
; server host definitions
;
ns1            IN  A      192.168.0.1        ;name server definition
www            IN  A      192.168.0.2        ;web server definition
;
; web and ftp server on same address
;
ftp            IN  CNAME  www.example.com.   ;ftp server definition
;
; endpoint or non server domain hosts
;
mikeslaptop    IN  A      192.168.0.3
fredsipad      IN  A      192.168.0.4
```

Name server address record

- *NS1 (name server name)*
- *IN (Internet)*
- *A (IPv4) * AAAA is IPv6*
- *IPv4 address (192.168.0.1)*

Web server address record

- *www (world wide web)*
- *IN (Internet)*
- *A (IPv4) * AAAA is IPv6*

IPv4 address (192.168.0.2)

File server address record

- *FTP (file transfer protocol)*
- *IN (Internet)*
- *CNAME means “same address spaces and numbers as www”*


Best practices in
ccTLD Management

Designation of codes

- ccTLDs are given a DNS string based on the Alpha-2 codes within ISO-3166

http://www.iso.org/iso/home/standards/country_codes.htm

Standard: ISO 3166 — Codes for the representation of names of countries and their subdivisions

Committee: ISO/TC 46 ICS: 01.140.30

Alpha-2 code	IN
Short name	INDIA
Short name lower case	India
Full name	the Republic of India
Alpha-3 code	IND
Numeric code	356
Remarks	
Independent	Yes
Territory name	Andaman Islands, Laccadive Islands , Minicoy Island, Nicobar Islands, Amindivi Islands
Status	Officially assigned
Remark part 1	Includes: Amindivi Islands, Andaman Islands, Laccadive Islands, Minicoy Island, Nicobar Islands.
Remark part 2	Remark: the forms used in the list are English-language forms provided by India.
Remark part 3	Sikkim (SK, SKM, --) is now part of the entry for India.

This code is part of collection(s)
Online collection : Country codes

ccTLD as a Public Trust

- ccTLDs are designated to operators who would operate them in the best interests of the local communities they served

- Operators should strive to tailor operations to best serve the users:
  - Ensure minimum technical standards are met
  - Strive to meet best practices
  - Operate with policy that suits local requirements

Who Currently Operate ccTLDs

- Many of the ccTLDs were assigned in the 1980's.
- They tended to be assigned to whoever was involved in building the Internet in a specific country
- Some changed hands over the years

What types of organisations?

- Universities
- ISPs/Telcos
- Regulators
- Dedicated entities

http://www.iana.org/domains/root/db

What do I mean by “ccTLD policies”

- Anything that defines how and by whom names can be registered.
- Typically ccTLDs have no contract with ICANN and are bound by local rather than ICANN policies
- Can participate in global discussion through ICANN’s ccNSO
  - http://ccnso.icann.org

There is no ONE model for ccTLDs

- Different models work well in different environments.
- This is driven by many things including operational considerations on the ground, local business practices and local culture.
- Policy and operations of a ccTLDs are often built over time and reflect the local environment.

Who should decide the policies

- Whoever has the role of Sponsoring organisation has the role of ensuring that policies are developed and implemented.
- Many ccTLDs have a model that follow a multi-stakeholder Solution.
- This can take many forms from formal “Policy boards” to processes for gathering public input.
- Often inclusive of Government, Industry and Civil Society as well as registrants

Some discussions

- Which model?

Direct registration

- No middle man - easier to control most aspects of Registration

Registry-registrar model

- Requires an interface between registry and registrar
- Offloads end-user interface from registry

Both

Some discussions

- Scope of Registrations?

  Local or Global?

  There are examples of ccTLDs of both types decide which best serves the community

  - Consider that the legal implications are different
  - Consider that the risks are different

Some discussions

- Dispute Resolution:

  Ensure that local law prevails?

  You don't want to be arguing in foreign courts

  Alternate Dispute Resolution (ADR)?

  Design to be lightweight!

  UDRP is often used as a base model

  http://www.icann.org/udrp/udrp.htm

Some discussions

- Who runs the technical operations?

  This is really a business decision.

  Policy can define the type of organisation but business decisions should guide the actual choice.

- Technology choices

  These are generally operational matters.

  The important factor to ensure that the “operator” is bound by the policies created and that choices they make meet those requirements.

Outsourcing

- There are an increasing number of companies that will provide services to TLD managers.
  - Whole registry back-end providers
  - Authoritative name server providers
- ccTLD managers should understand the basics of how to run the services themselves before they outsource them.
  - Allows you to manage and monitor performance of suppliers
  - Have a back-up strategy! What if your supplier fails?


Operational Decisions
What does it take to run a TLD?

Technical Requirements for a TLD

- Networks and Servers (redundant)
- Back office systems.
- Physical and Electronic Security
- Quality of Service (24/ 7 availability!)
- Name Servers
- DNS software (BIND, NSD, etc.)
- Registry software
- Diagnostic tools (ping, traceroute, zonecheck, dig)
- Registry Registrar Protocol

Name Server Considerations

- Support technical standards
- Handle load multiple times the measured peak
- Diverse bandwidth to support above
- Must answer authoritatively
- Turn off recursion!
- Should “NOT” block access from a valid Internet hosts

Secondary name server choice

Diversity, diversity and diversity!

- Don’t place all on the same LAN/building/segment
- Network diversity
- Geographical diversity
- Institutional diversity
- Software and hardware diversity

Security, Stability & Resliency Considerations

- Physical security
  - Deploy stringent access controls
  - Fire detection and retardation
  - Other environmental sensors (Flood, Humidity etc.)
  - Power continuity for 48 hours (or more)

- Backups
  - Multiple secure copies locally and offsite
  - Test, test and test!!

Separations of Services

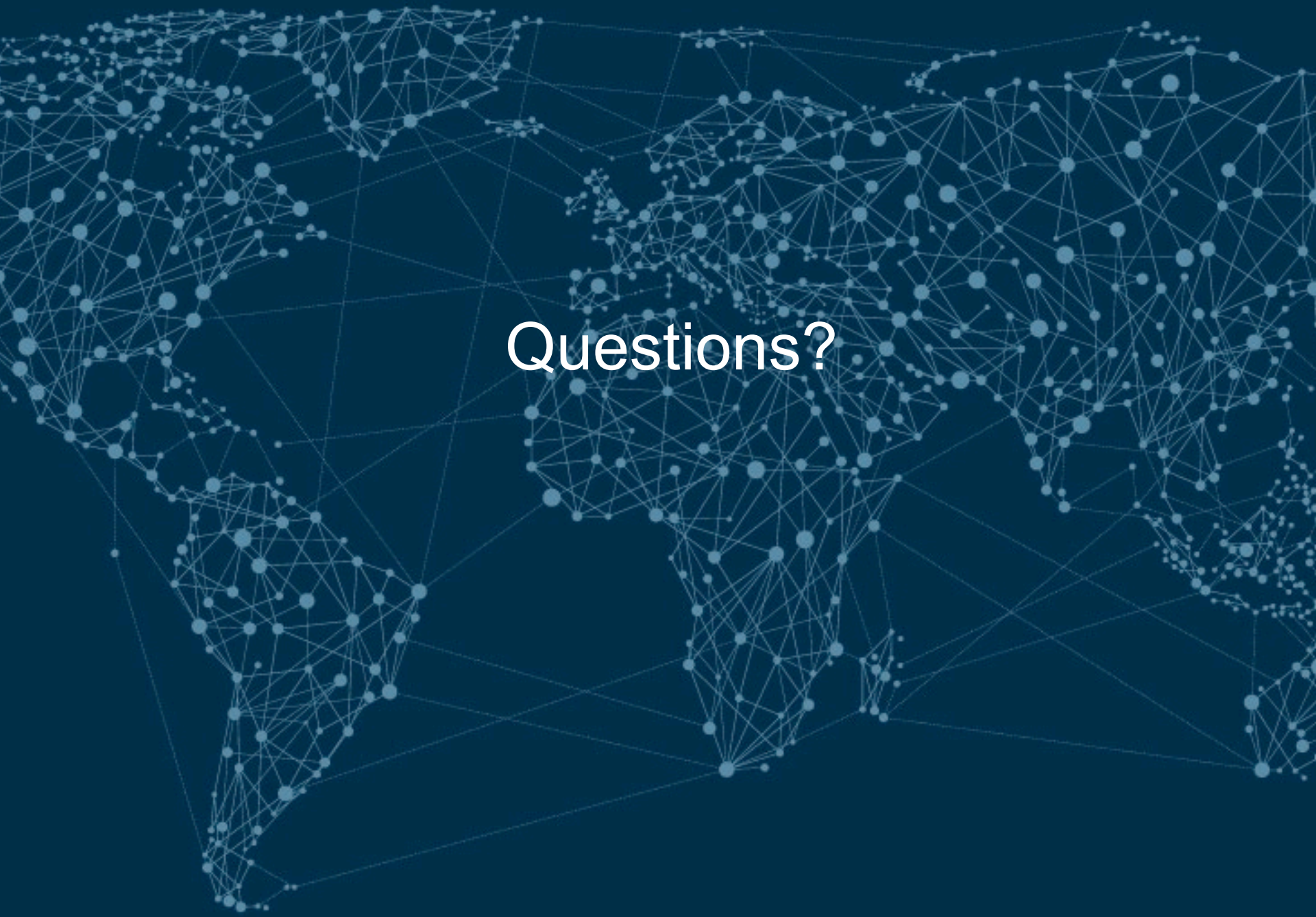
- Registries generally start small and evolve
- Separation of services means separating the logical functions and elements of the registry
- Two key benefits:
  - SECURITY: Clear separation of services is a manner in which to create logical security zones
  - SCALABILITY: You can scale only the services that need to grow as they need to grow

Know your SLAs

- Functioning name servers are the most critical/visible service
- All other services also need to be considered
  - Billing
  - Whois server, webservers
  - Registrar APIs
- Consider your service level targets and how you will meet them
- DNS servers always on, other systems mostly on?

When it all goes wrong

- DNS is a known target for hackers.
- You will be targeted at some point!
- Have plans in place to deal with attacks, failures and disasters.
- Test those plans regularly!


Questions?


Thank You!
<champika.wijayatunga at icann.org>