# DNS/DNSSEC Tutorial

*SANOG25 – Kandy, Sri Lanka*

*19 January 2015*

*Hosted by LEARN / IT Centre*

# Presenters

- Champika Wijayatunga
  - Security Engagement Manager (APAC) – ICANN

    champika@icann.org

- Sheryl Hermoso
  - Training Officer – APNIC

    shane@apnic.net

# Brief Overview of the DNS

# 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

# What is the Domain Name System?

A distributed database primarily used to obtain the

IP address, a number, e.g.,
192.168.23.1 or fe80::226:bbff:fe11:5b32

that is associated with a

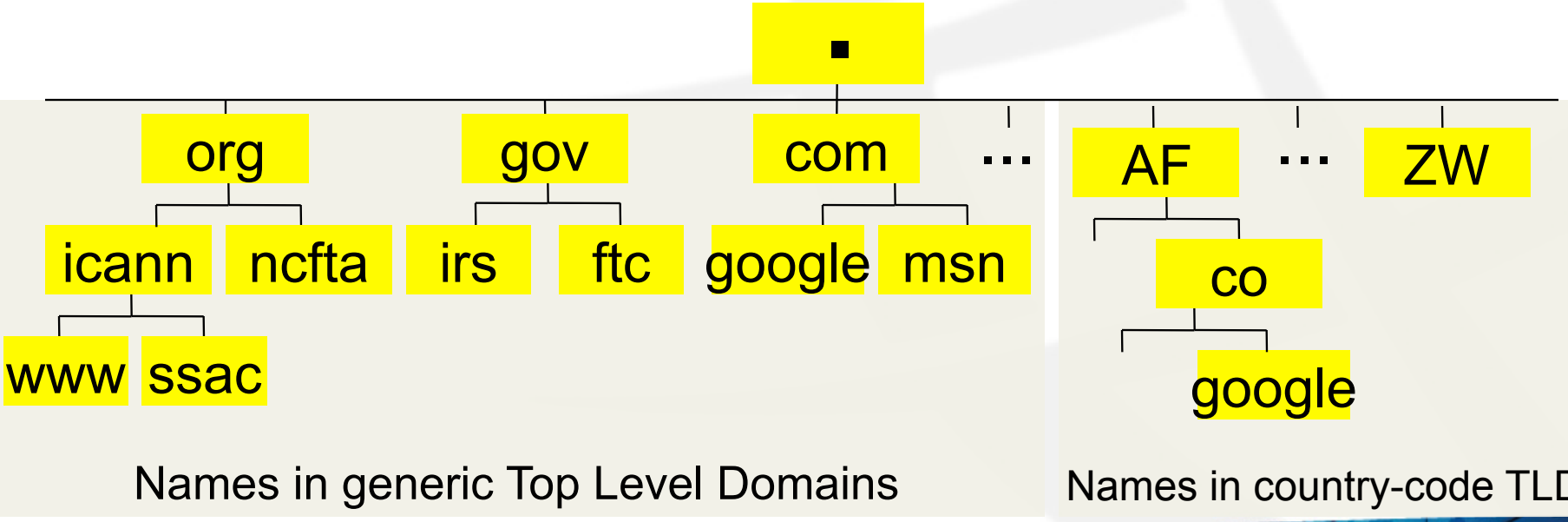
user-friendly name (www.example.com)

*Why do we need a DNS?*

*It's hard to remember lots of four decimal numbers and it's impossibly hard to remember hexadecimal ones*

# What is a domain?

- 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



# Root Servers

# L-Root

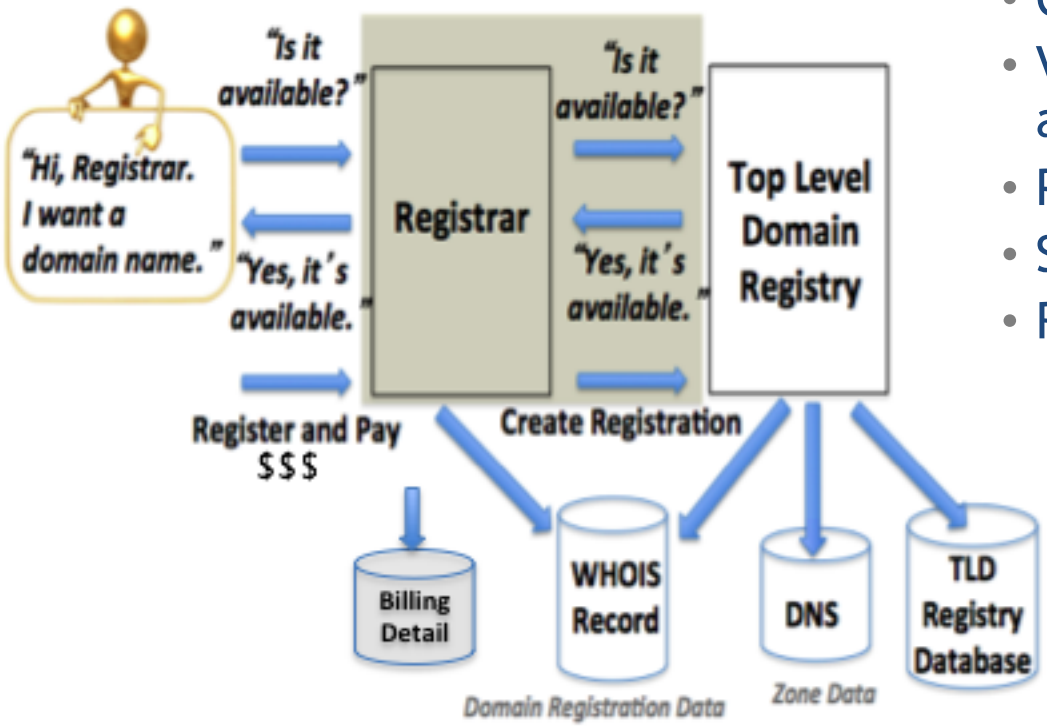
- Geographical diversity via Anycast
  - Around 160 dedicated servers
  - Presence on every continent
- On normal basis 15 ~ 25 kqps
  - That is app 2 billion DNS queries a day

# L-Root presence

# What is the New gTLD Program?

| | |
|---|---|
| **largest-ever expansion** of the domain name system | global restructuring |
| **Internationalized Domain Names** and non Latin-based characters | innovation |
| Managed by ICANN = **multistakeholder input** | security and stability |

# Domain name registration 101




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

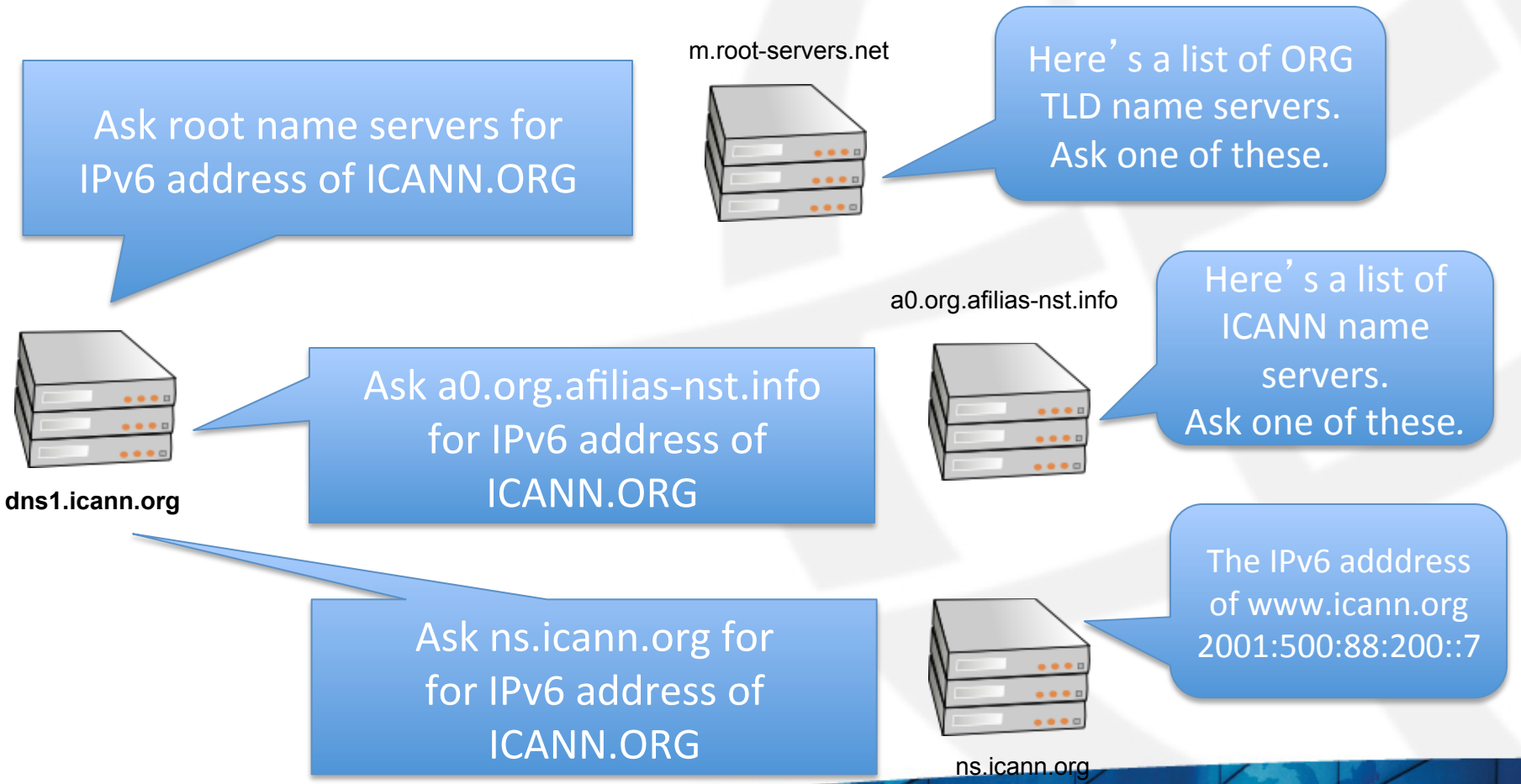
# Operational elements of the DNS

- 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*



# DNS Resource Records (RR)

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

| Label | TTL | Class | Type | Data |
|---|---|---|---|---|
| www | 3600 | IN | A | 192.168.0.1 |

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

# DNS Resource Record Sets

- Multiple RR with same LABEL and TYPE are grouped into Resource Record Sets (RRsets)

```
www       A   192.168.0.1
www       A   192.168.10.10
```
} RRset

```
mail      MX 5 server1.zone.
mail      MX 5 server1.zone.
```
} RRset

```
server2   A   10.20.30.40
```
} RRset

```
server1   AAAA  2001:123:456::1
server2   AAAA  2001:123:456::2
```
} RRset

# 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

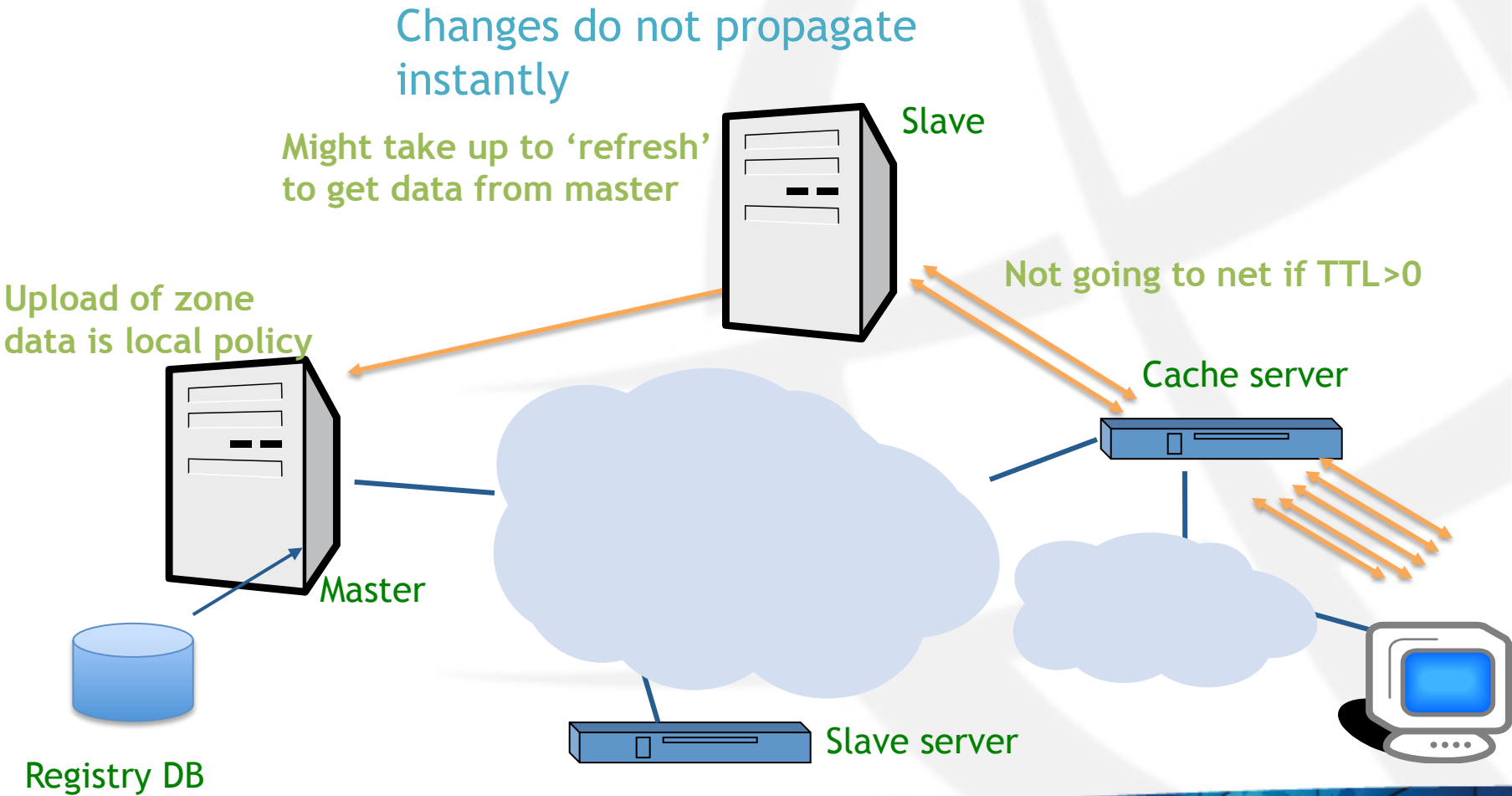
- *www (world wide web)*
- *IN (Internet)*
- *A (IPv4)  * AAAA is IPv6*

*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”*

# Places where DNS data lives



# Registration Data Directory Services

## Whois

Databases containing records of registrations

- Domain Whois
  - Sponsoring Registrar
  - Domain Name Servers
  - Domain Status
  - Creation/Expiry dates
  - Point of Contact
  - DNSSEC data
- Address Whois
  - Regional Internet Registry
  - IPv4/v6 address allocation
  - ASN allocation
  - Creation/Expiry dates
  - Point of Contact

# Questions?