Network Security and DNS/DNSSEC Worksho

SANOG 26 | Mumbai, India | 7-11 August 2015

Intros - Trainers

- Champika Wijayatunga (Champ) – ICANN
- Fakrul Alam (Pappu) – bdHUB
- Yoshinobu Matsuzaki (Maz) - IIJ

Agenda

- Internet Identifiers and DNS
- Cryptography and PKI (PGP, SSH)
- Network Security Best Practices
- Infrastructure and Device Security
- Security on Different Layers and Attack Mitigation
- Whois Databases (Names and Numbers)
- Route Filtering
- Virtual Private Networks and IPsec
- DNSSEC
- Tools (Wireshark, Snort)


Brief Overview of 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

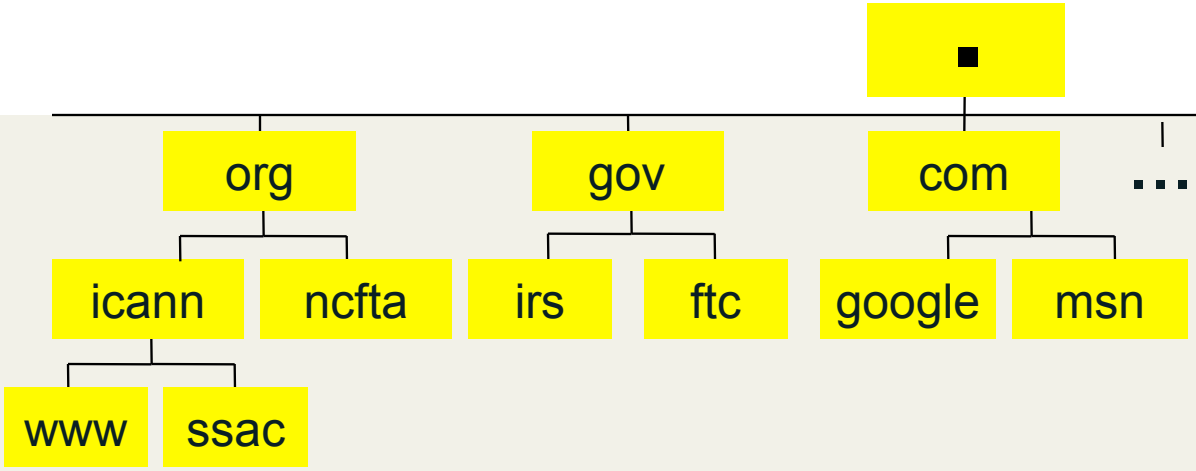
user-friendly name (www.example.com)

Why do we need a DNS?

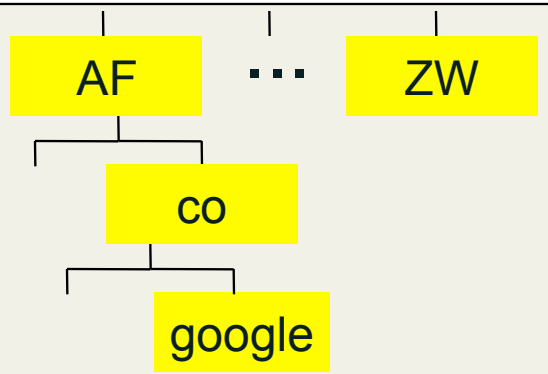
It's hard to remember lots of four decimal numbers and it's impossibly hard to remember hexadecimal ones

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

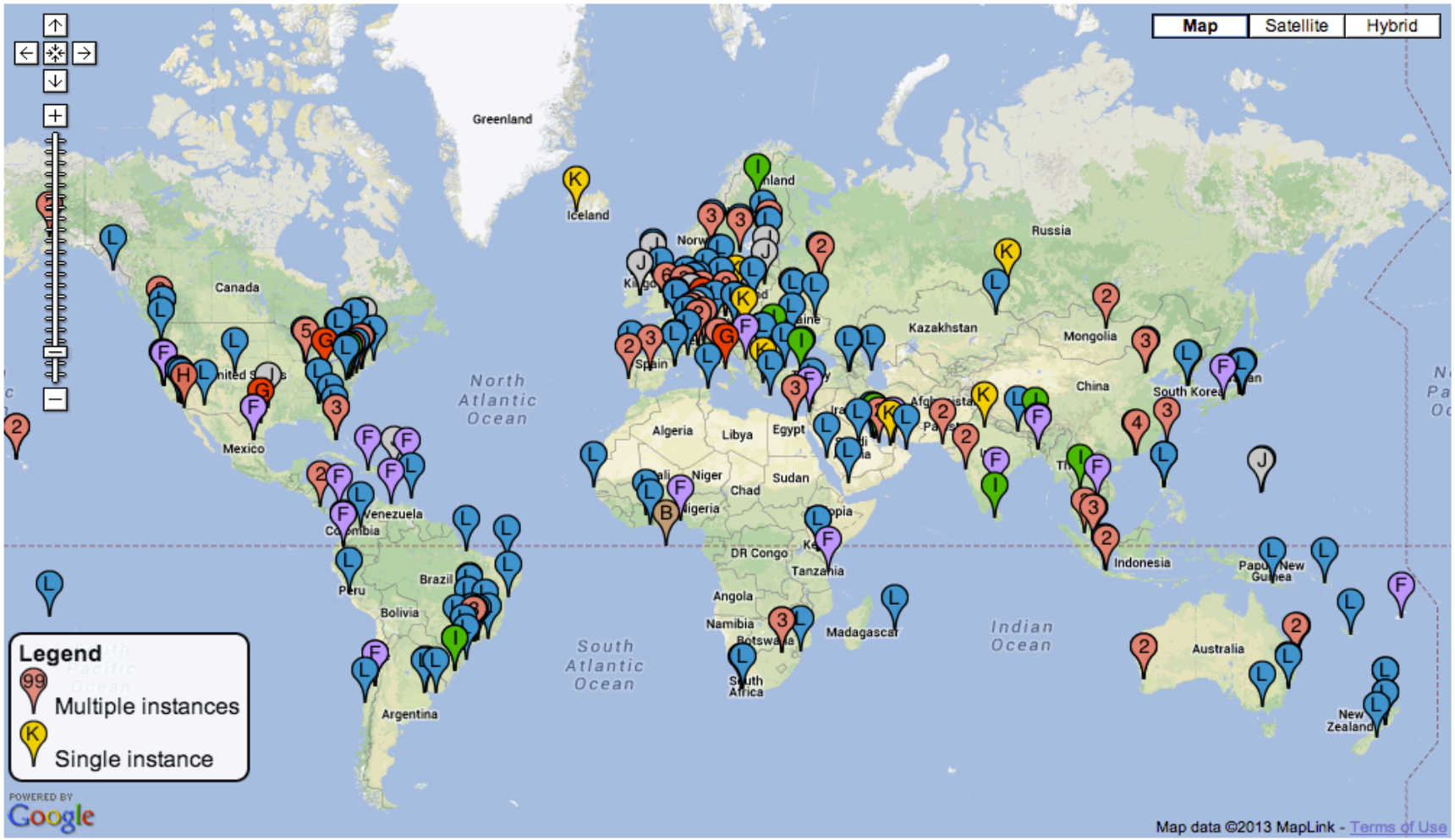
Who are the Root Server operators?

- 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

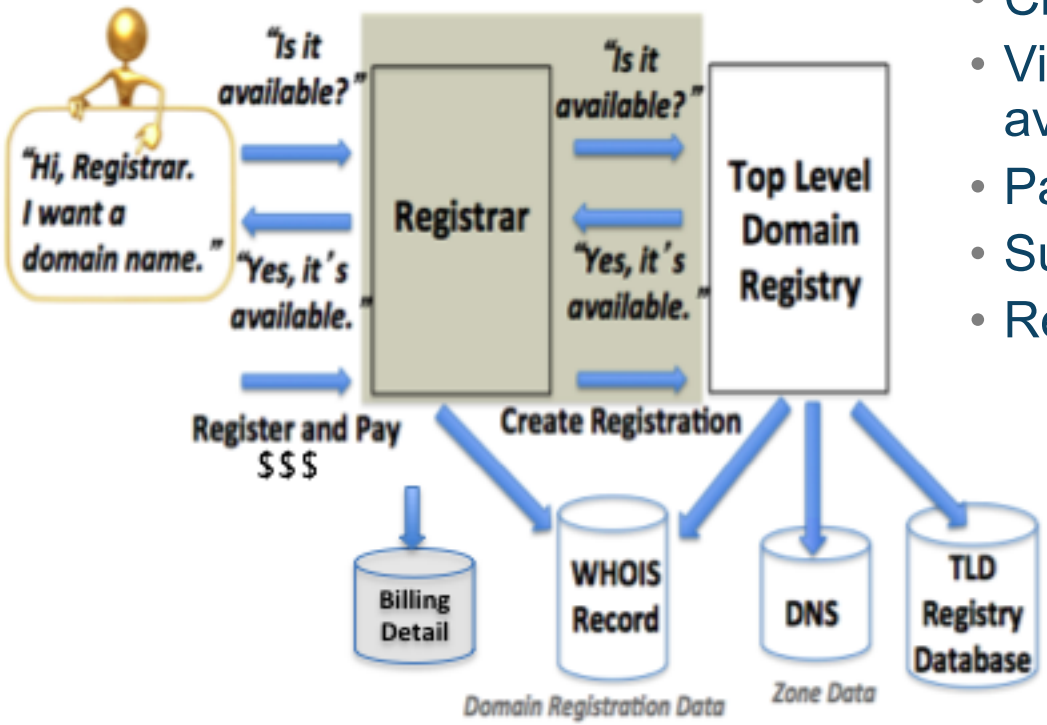
DNS Servers

- 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 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

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*

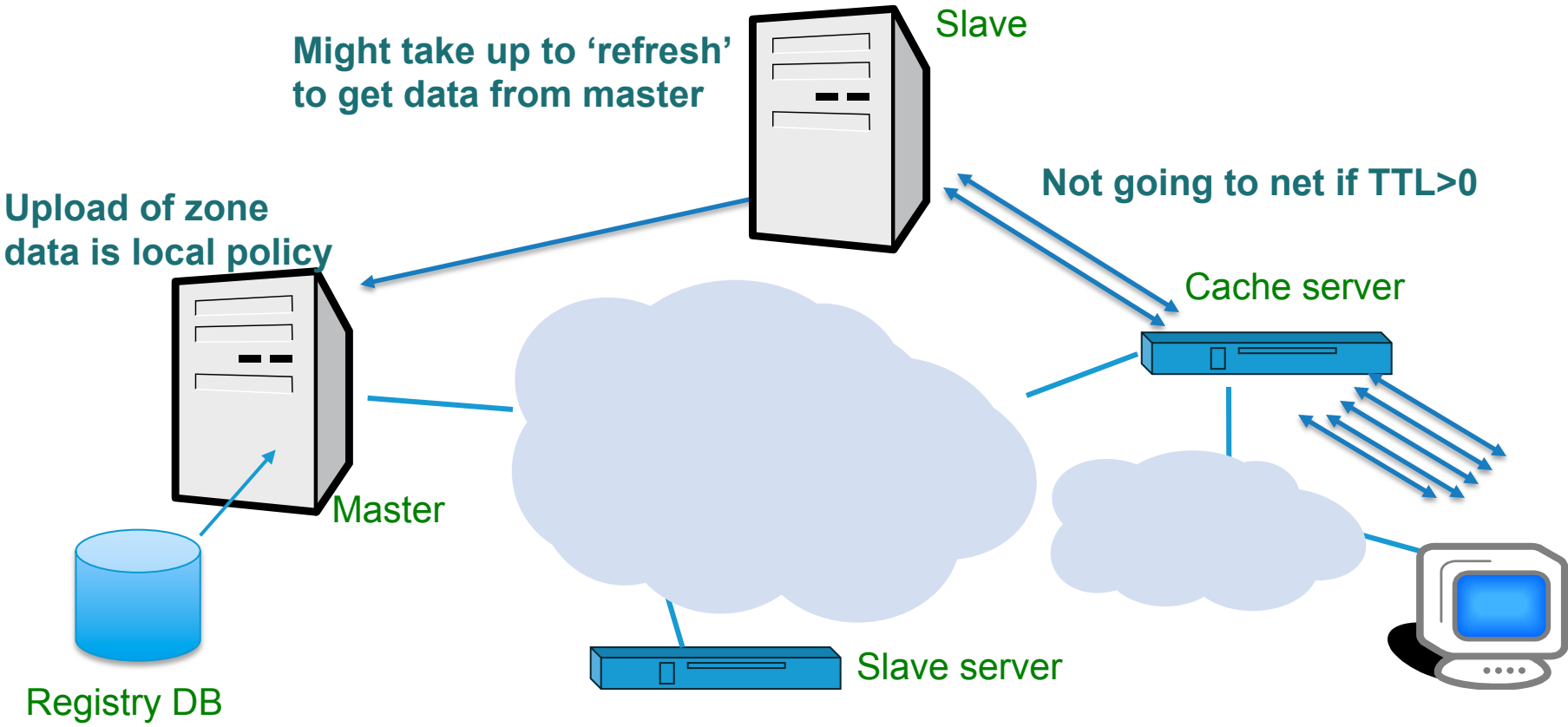
IPv4 address (192.168.0.2)

File server address record

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

Places where DNS data lives

Changes do not propagate instantly



Delegating a Zone

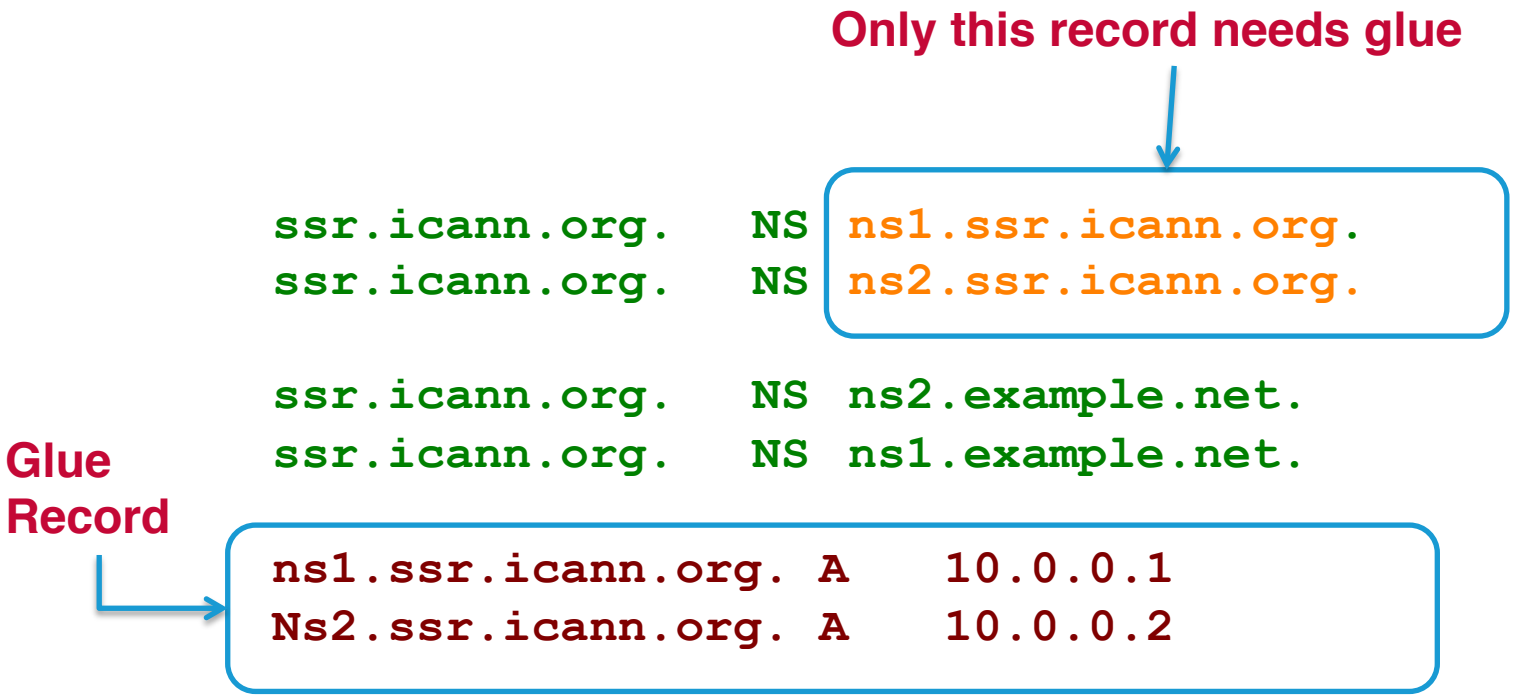
- Delegation is passing of authority for a subdomain to another party
- Delegation is done by adding NS records
  - Ex: if icann.org wants to delegate ssr.icann.org

```
ssr.icann.org.    NS ns1.ssr.icann.org.
ssr.icann.org.    NS ns2.ssr.icann.org.
```

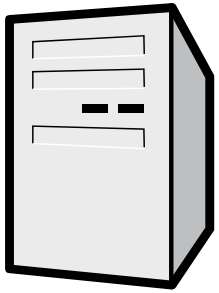
- Now how can we go to ns1 and ns2?
  - We must add a **Glue Record**

Glue Record

- Glue is a ‘non-authoritative’ data
- Don’t include glue for servers that are not in the sub zones

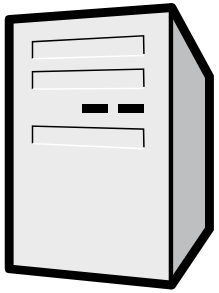


Delegating ssr.icann.org. from icann.org.



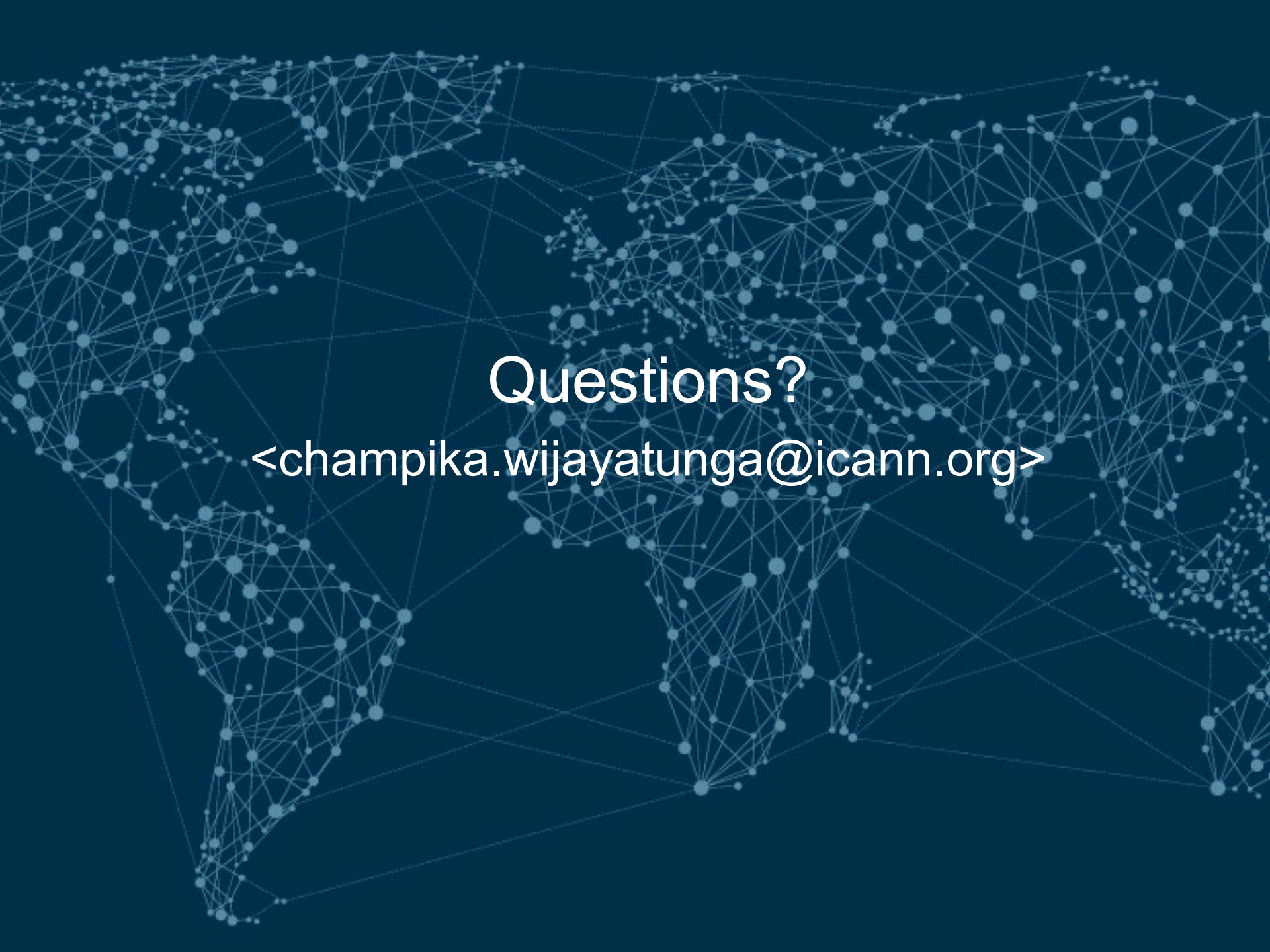
ns.icann.org

1. Add NS records and glue
2. Make sure there is no other data from the ssr.icann.org. zone in the zone file



ns.ssr.icann.org

1. Setup minimum two servers
2. Create zone file with NS records
3. Add all ssr.icann.org data


Questions?
<champika.wijayatunga@icann.org>