DNS/DNSSEC

In conjunction with APRICOT2020

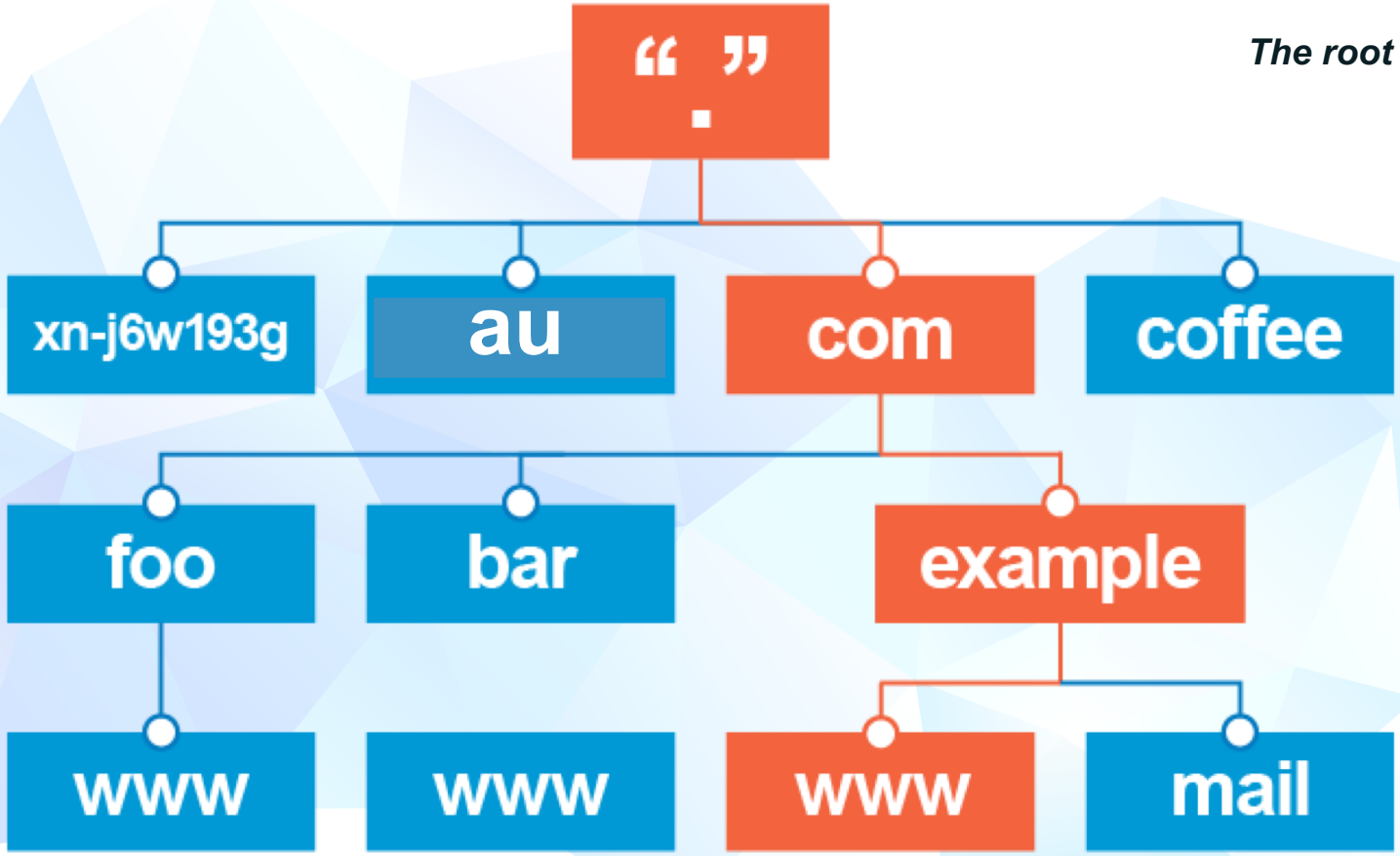
Champika Wijayatunga
Regional Technical Engagement Manager – Asia Pacific

12-16 Feb 2020, Melbourne – Australia

Agenda

- DNS Recap
- Setting up Authoritative and Recursive Servers
- DNS Security concepts
- DNS Security Extensions (DNSSEC)
- DNSSEC Key Management

The Domain Name System (DNS)



The root

Top-level nodes

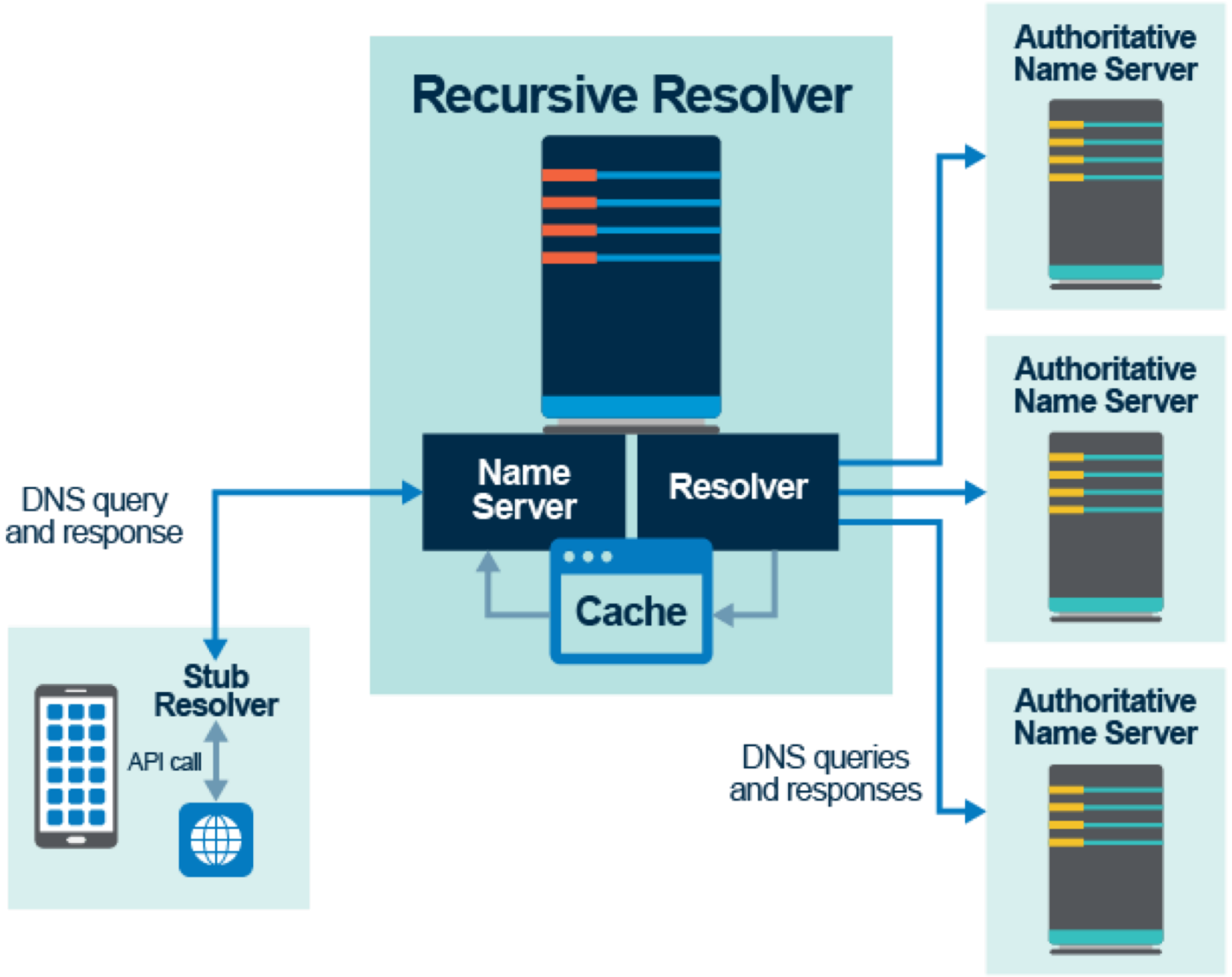
Second-level nodes

Third-level nodes

Root
Top-level
Second level
www.example.com.

FQDN = **F**ully **Q**ualified **D**omain **N**ame

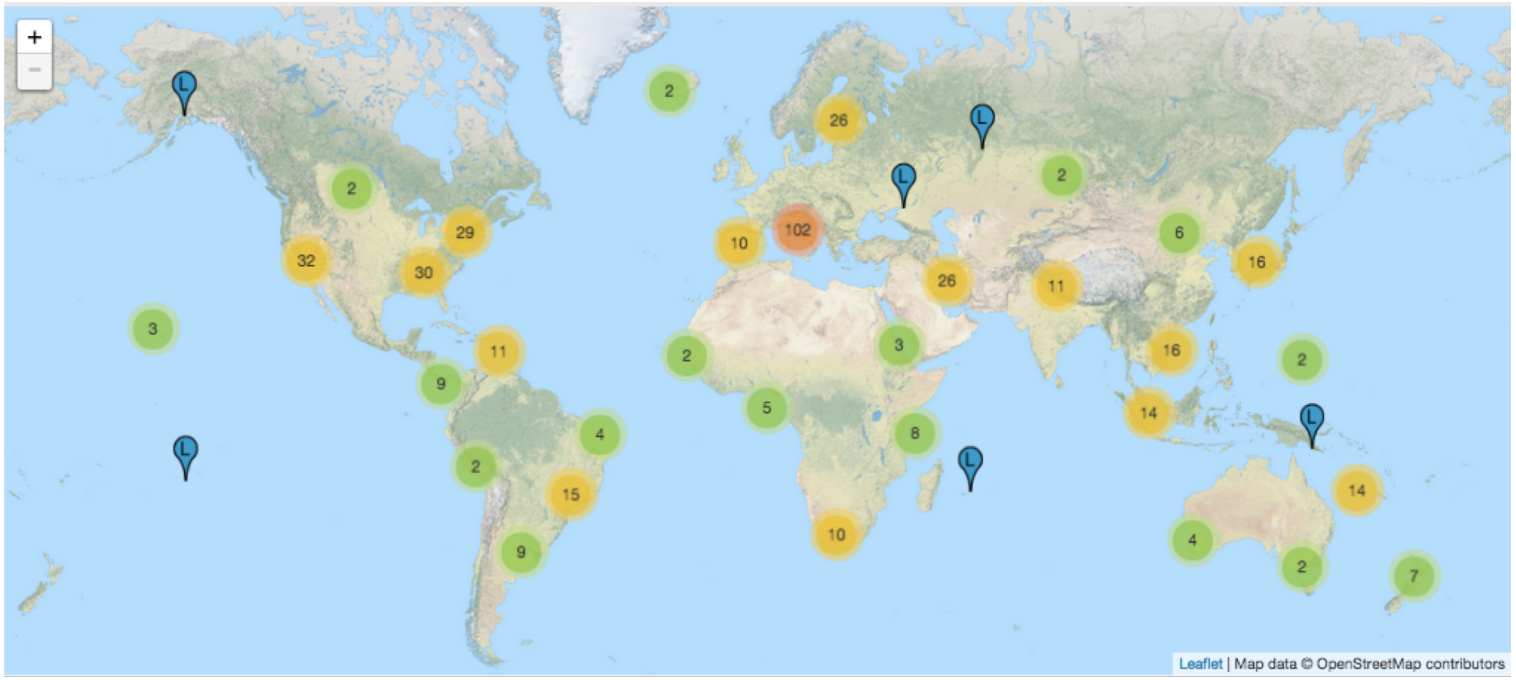
DNS Components at a Glance



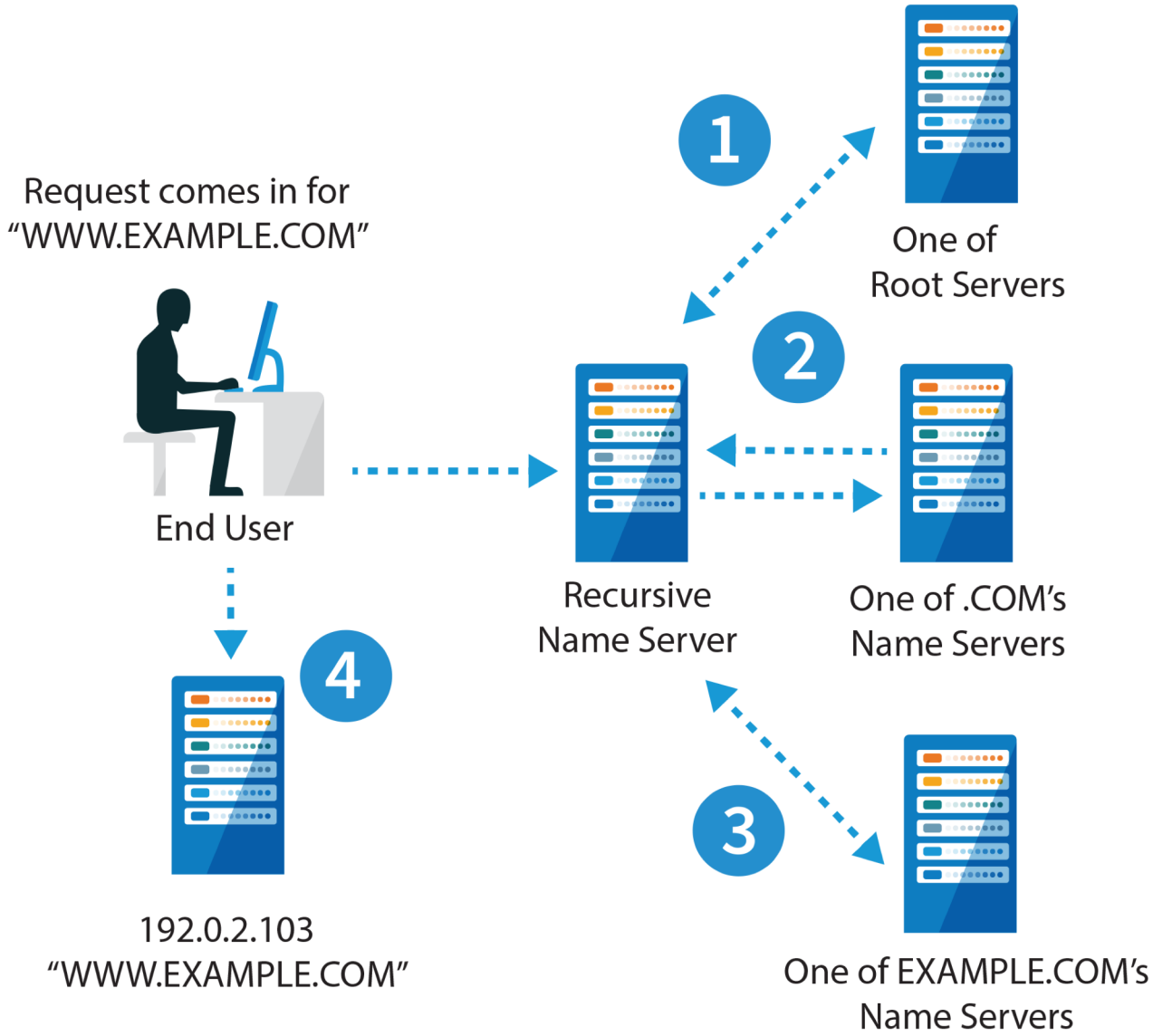
DNS Servers

- Authoritative Servers
  - Root Servers
  - Primary
  - Secondary

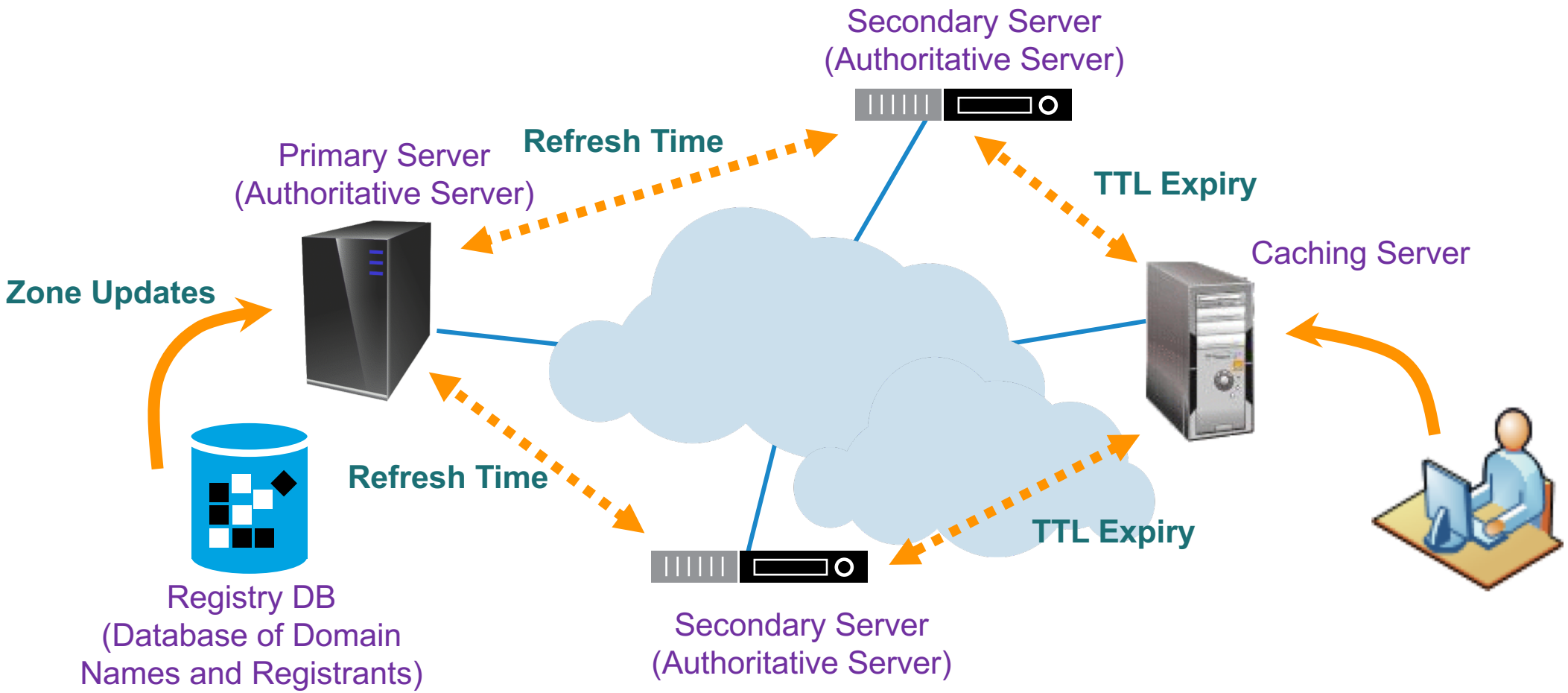
- Recursive Servers
  - Or Recursive Resolvers
  - Or Caching Servers



How DNS Works



Propagation of DNS Data



Zone Data and Resource Records (RR)

- Consists of resource mappings

Label	TTL	Class	Type	RData
www	3600	IN	A	192.168.0.1

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

Resource Record	Function
Label	Name substitution for FQDN
TTL	Timing parameter, an expiration limit
Class	IN for Internet, CH for Chaos
Type	RR Type (A, AAAA, MX, PTR) for different purposes
RDATA	Anything after the Type identifier; Payload of the record

Zone Files

```
$TTL 86400        ; 24 hours could have been written as 24h or 1d
$ORIGIN example.com.
@       IN      SOA         ns1.example.com.    hostmaster.example.com.     (
                                2017092701 ; serial number
                                3H         ; refresh
                                15         ; retry
                                1w         ; expire
                                3h         ; nxdomain TTL              )

        IN      NS      ns1.example.com.            ; in the domain
        IN      NS      ns2.anotherexample.net.     ; external to domain
        IN      MX  10  mail.someotherexample.com.  ; external mail provider
ns1     IN      A       192.168.0.1                 ; name server definition
www     IN      A       192.168.0.2                 ; web server definition
ftp     IN      CNAME   www.example.com.           ; ftp server definition
host    IN      A       192.168.0.3                 ; host definition
```

Delegating a Zone

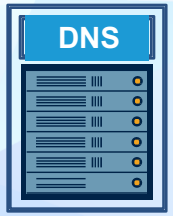
- Delegation is done by adding NS records
  - Ex: if example.com wants to delegate training.example.com to another party,

```
training.example.com.   NS ns1.training.example.com.
training.example.com.   NS ns2.training.example.com.
```

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

Delegating a Child Zone from a Parent Zone

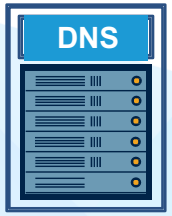
example.com (Parent Zone)



ns.example.com

1. Add NS records and glue
2. Make sure there is no other data from the training.example.com. zone in the zone file

training.example.com (Child Zone)



ns.training.example.com

1. Setup minimum two servers
2. Create zone file with NS records
3. Add all training.example.com data

Labs
Configuring Recursive Servers
Configuring Authoritative Servers

Engage with ICANN – Thank You and Questions

One World, One Internet

Visit us at **icann.org**

Email: champika.wijayatunga@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann