DNS/DNSSEC Workshop

In conjunction with LKNOG8

13-16 August 2024

ICANN

Introductions – Trainers

Champika Wijayatunga - *ICANN*
Sampath Hennayake – *LK Domain Registry*
Chamara Disanayake - *NSBM*
Pasan Ravinatha – *University of Moratuwa*

Zone File Management

Zone Files

- A zone consists of multiple resource records
- All the resource records for a zone are stored in a ***zone file***
- Every zone has (at least) one zone file
- Resource records from multiple zones are never mixed in the same file

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

Start of Authority (SOA)

- Contains administrative information about the zone.
- Every domain must have a Start of Authority record at the cutover point where the domain is delegated from its parent domain.
- SOA indicates that a name server is authoritative for a domain. If we do not receive a SOA RR in a query response from a server, that indicates the server is not authoritative for that domain.
- DNS name servers are normally set up in clusters (*master* and *secondaries*). The database for each cluster is synchronized through zone transfers. The data in a SOA record for a zone is used to control the zone transfer.

Start of Authority (SOA)

```
example.com.        SOA   ns1.example.com. John\.doe.example.com. (
                           2020031615      ; serial
                           86400           ; refresh (1 day)
                           7200            ; retry (2 hours)
                           3600000         ; expire (1000 hours)
                           172800 )        ; minimum (2 days)
```

CANNONICAL NAME (CNAME)

- The canonical name (CNAME) is normally used to alias one name to another (but do not confuse it with an ALIAS). In the case of CNAME there should be no other records on the same name.
- As an example suppose we want to have both *example.com* and *www.example.com* pointing at the same server *example.com*, the record should be:

```
www.example.com.   CNAME example.com.
```

- Note that a CNAME always points to a name (not an IP address).
- So somewhere else there should be a record like:

```
example.com.         A      192.0.2.7
```

AAAA

- IPv6 uses ‘AAAA’ records (or Quad-A records)
- E.g. if you receive a /32 prefix 2001:db8::/32
  - And your nameserver (ns1.example.com) IP address is 2001:db8::1/128 then you need to create a Quad-A record as below.

```
ns1.example.com.   IN   AAAA   2001:db8::1
```

- In IPv6, the loopback address is ::1
- E.g. if you want to configure the localhost,

```
localhost.         IN   AAAA   ::1
```

Mail Exchange (MX)

- Specifies a mail server and a preference for a mail destination

```
example.com.   MX   10 mail.example.com.
example.com.   MX   20 mail-backup.example.com.
```

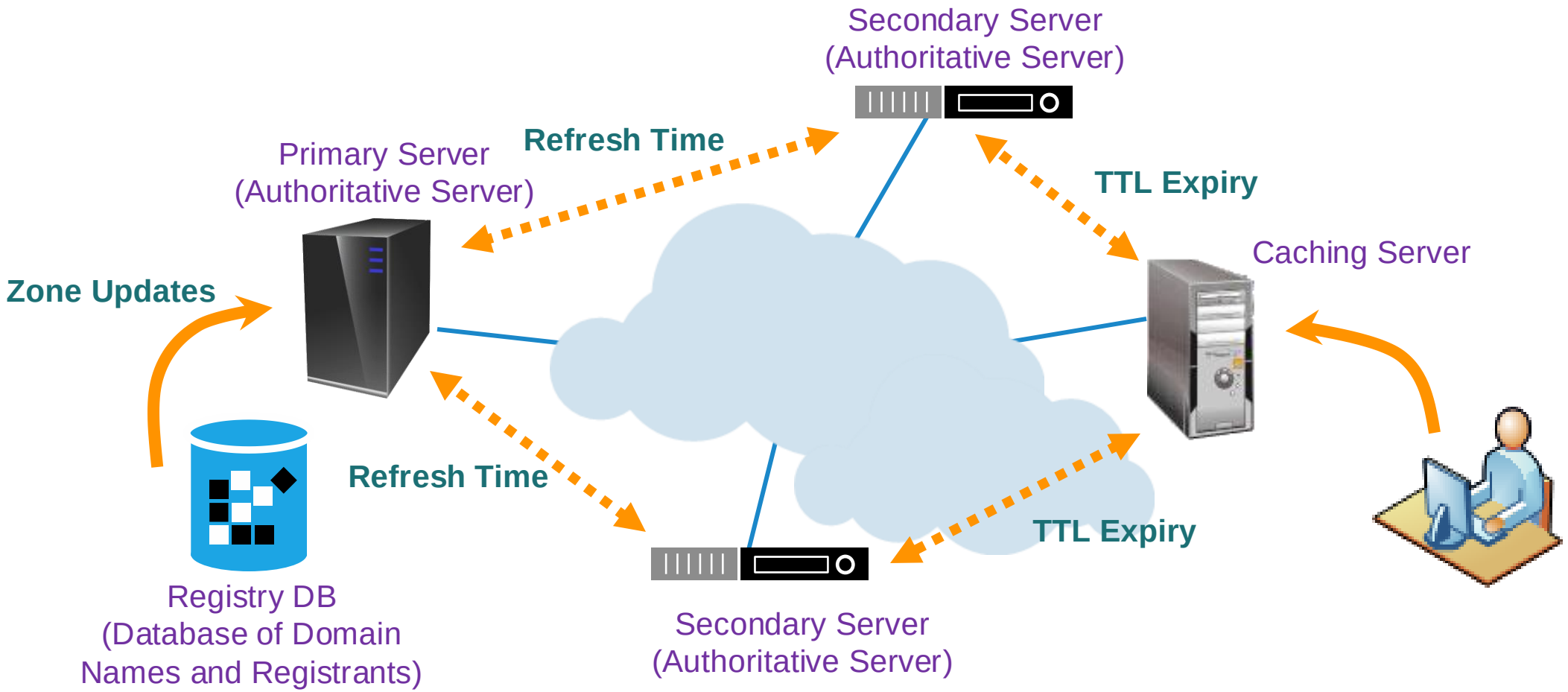
- Owner name corresponds to the domain name in an email address, i.e., to the right of the “@”
- The number is a preference, lower is more desirable
- Rightmost field is the domain name of a mail server that accepts mail for the domain in the owner name

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
```

Propagation of DNS Data



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