Reverse DNS for Network Engineers

MMIX-MMNOG7

Champika Wijayatunga
Technical Engagement Sr. Manager – APAC

22 March 2025

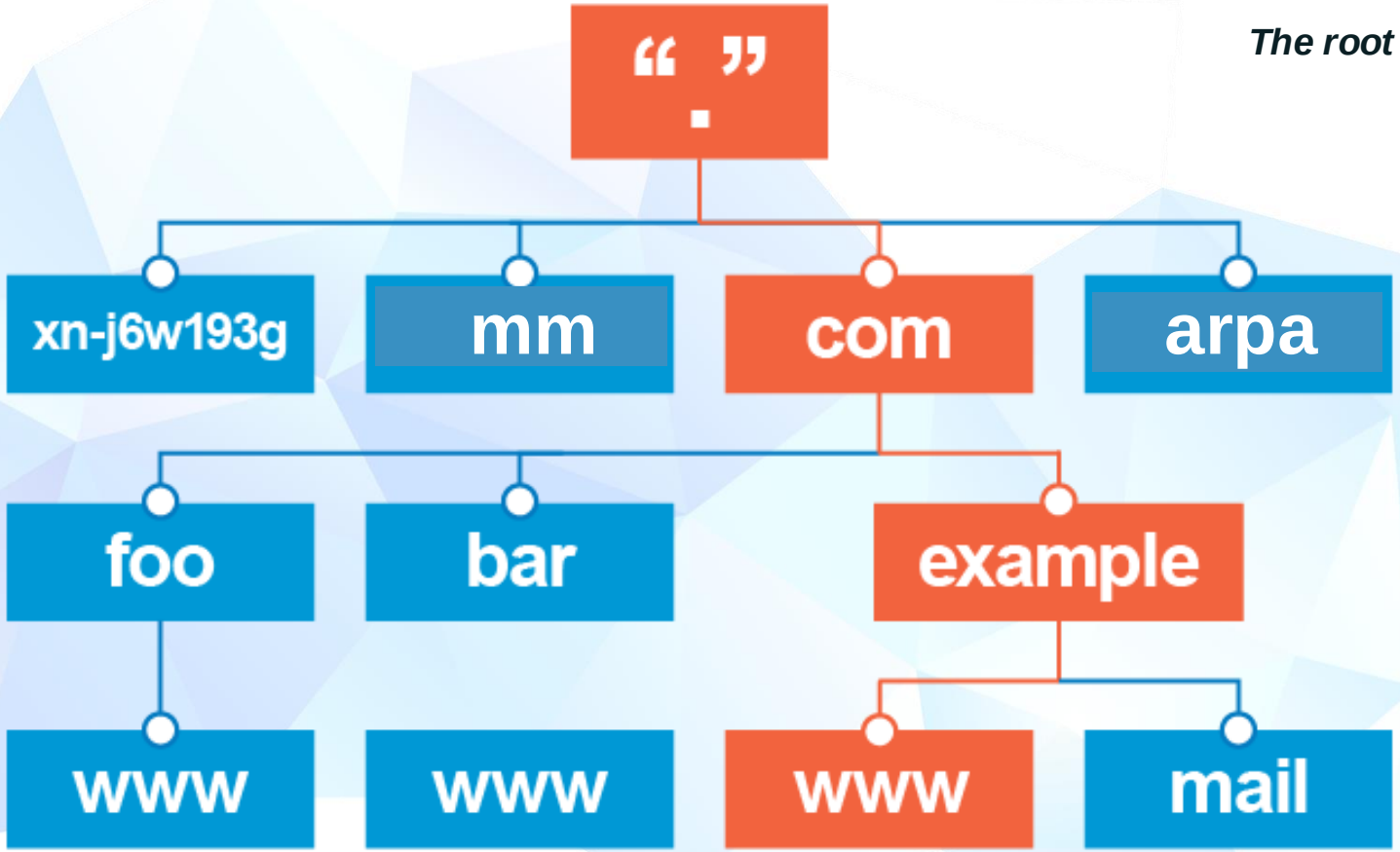
Introduction

What is Forward DNS?

Forward DNS is what most people are describing when they talk about "the DNS":

- **www.icann.org** is hosted at the IP address 192.0.32.7
- Humans do not want to have to memorize IP addresses
- The Domain Name System (DNS) maps semantic names (easily understood by humans) to these IP addresses

DNS Hierarchy



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

What is Reverse DNS

Reverse DNS is the opposite of forward DNS:

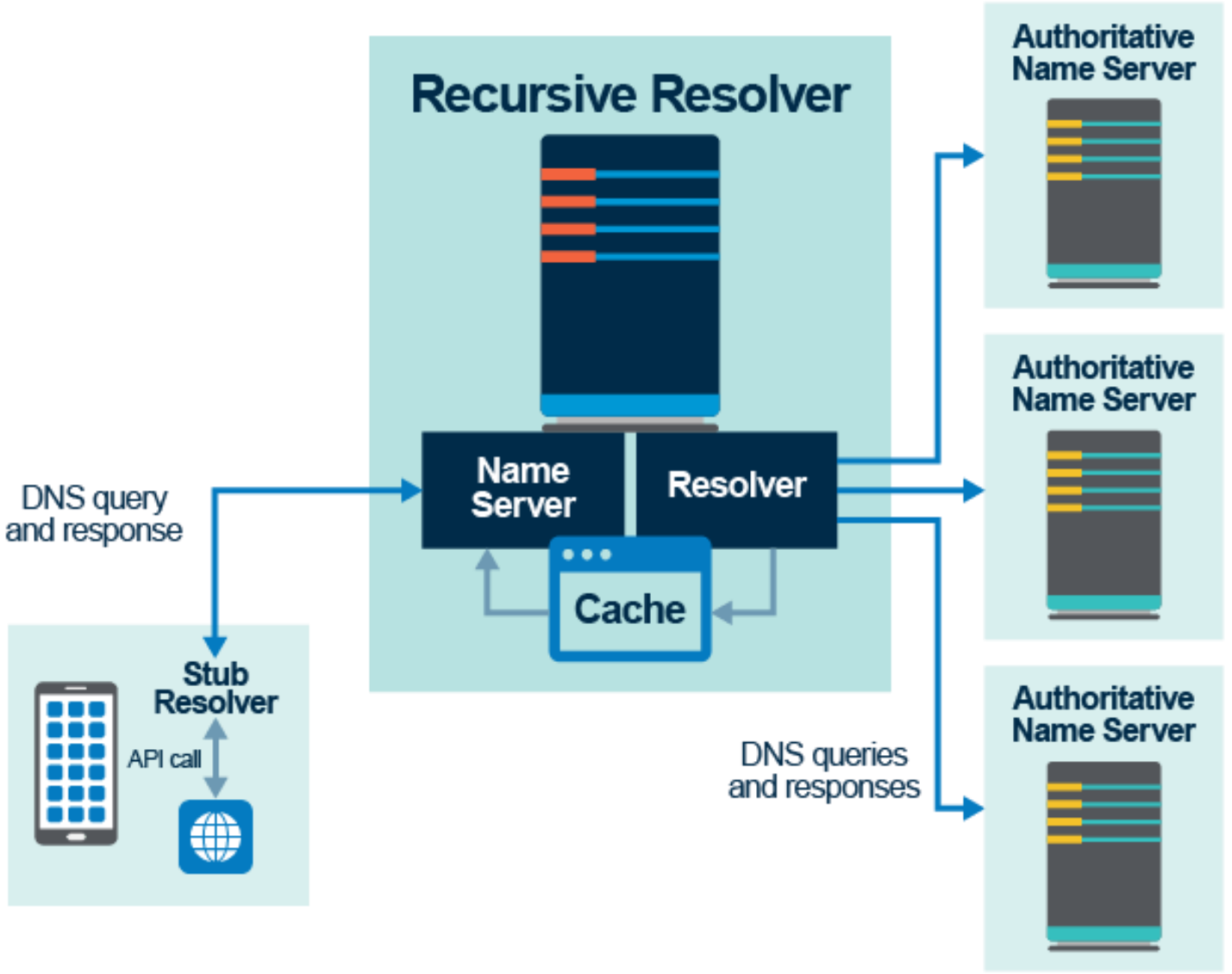
- 192.0.33.71 maps to ICANN's mail server **pechora1.icann.org.**

In operational networks, reverse DNS has two use cases relevant to network engineers:

- Authentication of mail server hostnames
- Marking network elements to make tools like traceroute more useful to humans

Resolving DNS Queries: Important Concepts

DNS Components and DNS Resolution



Resolving Reverse DNS Queries

A Practical Use of Reverse DNS: Mail Server Authentication

- ICANN's mail server is **pechora1.icann.org** and it is hosted on IP address:
  - **192.0.33.71**
- When mail is delivered via SMTP, the originating mail server presents its credentials to the destination mail server. ["Hi! I'm the mail server **pechora1.icann.org**!"]
- One of the useful mechanisms to combat spam is to authenticate those credentials, to ensure the mail server credentials are genuine (not forged)
- To authenticate the credentials, the destination mail server performs a reverse DNS lookup of the IP address of the originating mail server it is connected to. ["I know that the host **192.0.33.71** is connected to me and is trying to deliver mail to me. It claims it is the mail server **pechora1.icann.org**. Let me perform a reverse DNS lookup to see if these two statements reconcile."]

So how do we do that?

Reverse DNS Resolution: ARPA

- The reverse DNS TLD is in the **.ARPA** TLD
- It has an IPv4 version: **in-addr.arpa**
- It has an IPv6 version: **ip6.arpa**
- The reverse domain is appended to the IP address:
  - **71.33.0.192.in-addr.arpa.**
  - But why???

… Because it's Just Like Forward DNS

- Forward DNS resolution goes from right to left:
  - **www.example.com.**
- Conceptually, note that it is also going from least specific to more specific
  - "." encompasses the entire name space
  - .com represents the entire .com TLD
  - example.com covers the entire example domain
  - www.example.com is a specific host

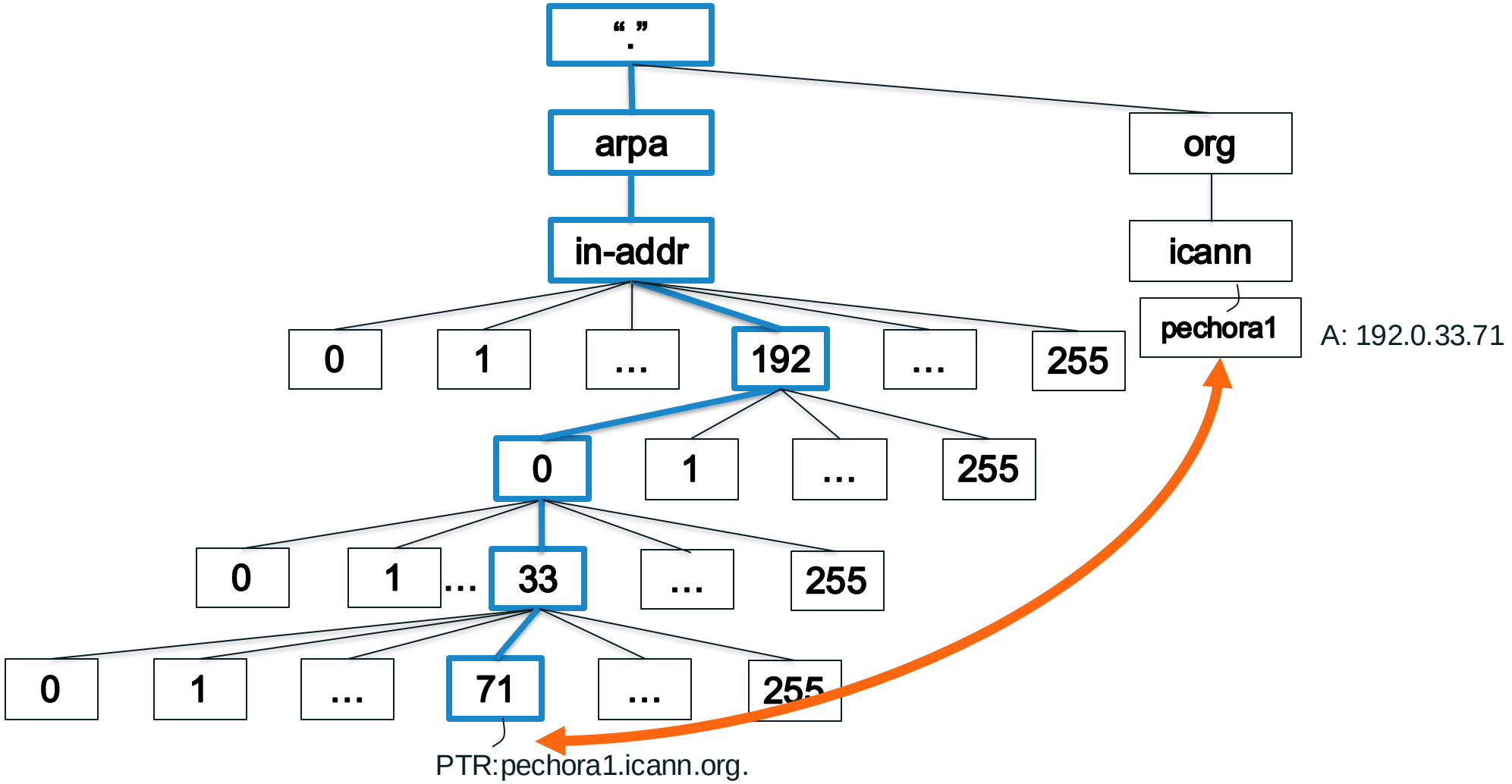
Reverse DNS from Least to Most Specific: IPv4

- The least specific zone in an IPv4 name space is a **/8 zone**:
  192.in-addr.arpa covers all reverse DNS zones for addresses in 192.0.0.0/8
- The next least specific zone in an IPv4 name space is a **/16 zone**:
  0.192.in-addr.arpa covers all reverse DNS zones for addresses in 192.0.0.0/16
- As expected, the next zone boundary in IPv4 is for the **/24 zone**:
  33.0.192.in-addr.arpa covers all reverse DNS zones for addresses in 192.0.33.0/24

***By the way …* notice that we left out all leading .0 octets in our zone names**

- 0.0.0.192.in-addr.arpa is incorrect
- 192.in-addr.arpa is correct

Reverse Mapping



Zone Boundaries in IPv6

- In IPv6 reverse DNS, zone boundaries are defined on the *nibble boundary*
  - In classical computer science, a “nibble” is any four-bit aggregation
  - IPv6 lends itself nicely to nibble boundaries, because it is represented as eight 16-bit quartets:

    _ _ _ _: _ _ _ _: _ _ _ _: _ _ _ _: _ _ _ _: _ _ _ _: _ _ _ _: _ _ _ _
  - Each underscore represents 4-bits:

    2 0 0 1: D B 8 0: 0 0 0 0: 0 0 0 0: 0 0 0 0: 0 0 0 0: 0 0 0 0: 0 0 0 0
  - Each number, therefore, is a nibble boundary, so each number signifies a zone boundary for reverse DNS
  - Similar to IPv4, we reverse the numbers when defining reverse DNS zones.

    0.8.b.d.1.0.0.2.ip6.arpa is the reverse zone for 2001:db8::/32

- Leading zeros are important, because the reverse zone’s domain must mathematically match the number of bits it represents

IPv6 Reverse DNS in Practice

- Under the current allocation practices agreed upon by IANA and the RIRs, the IANA delegates /12 blocks to each RIR as needed
- In 2006, IANA delegated 2400::/12 for APNIC to issue to its customers
- APNIC is therefore responsible for the delegation of reverse DNS at the **/12 boundary**:

  0.4.2.ip6.arpa covers all reverse DNS zones for addresses in 2400::/12
- APNIC often issues /32s to customers
- A customer is delegated reverse DNS at the **/32 boundary**:

  0.8.b.7.0.0.4.2.ip6.arpa covers all reverse DNS zones for addresses in 2400:7b8::/32

Reverse DNS Resolution: the PTR Record

- When discussing forward DNS, we were resolving A records and AAAA records, which resolve a domain name to an IP address
- In reverse DNS, the RR type is PTR:
  - “Pointer” record
  - Resolves a domain name that ends in in-addr.arpa or ip6.arpa that represents an IP address into a fully-qualified domain name
  - (It requires a FQDN, so the trailing dot is necessary in the zone file!)

More About Zone Delegations

Your Delegations and Your RIR

Reminder:

- In IPv4, zones are delegated at either the /8, the /16, or the /24 boundary
- In IPv6, zones are delegated on the nibble boundary

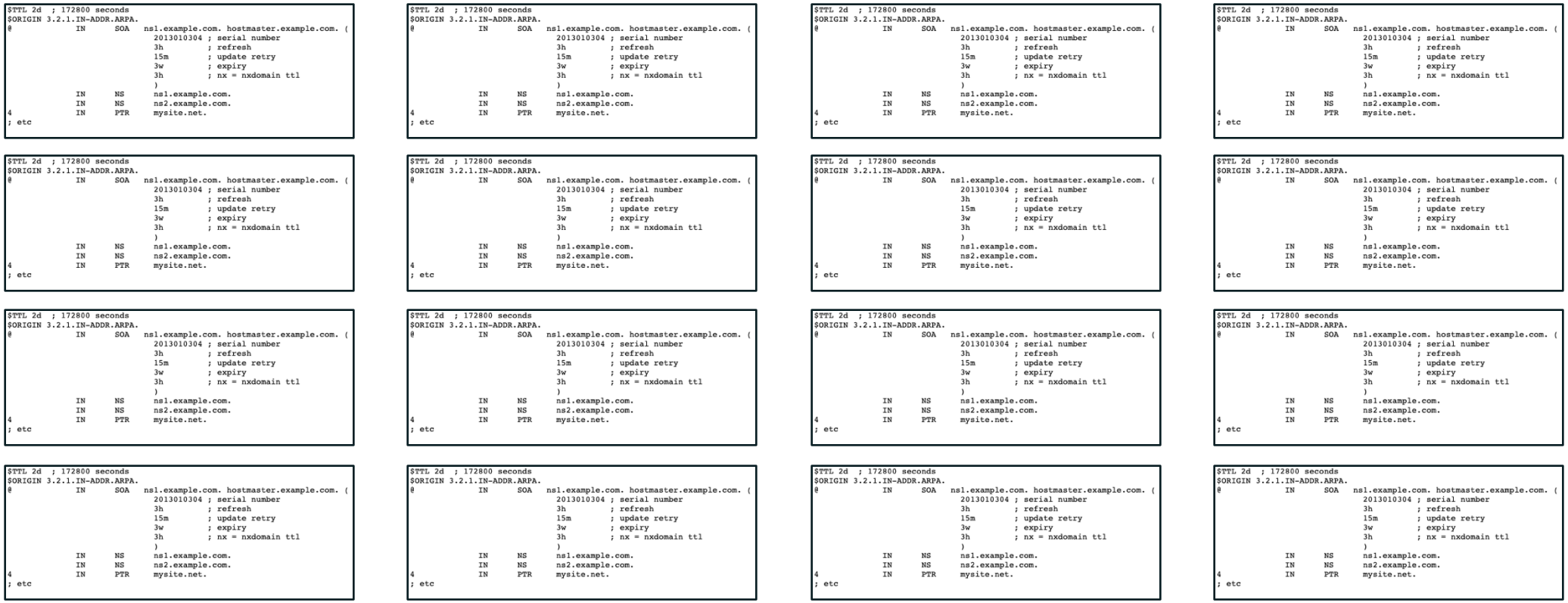
You are the Registrant of a /24

- If you have a /24, you configure a reverse domain in your zone files for the /24

```
$TTL 2d  ; 172800 seconds
$ORIGIN 3.2.1.IN-ADDR.ARPA.
@               IN      SOA     ns1.example.com. hostmaster.example.com. (
                                  2013010304 ; serial number
                                  3h         ; refresh
                                  15m        ; update retry
                                  3w         ; expiry
                                  3h         ; nx = nxdomain ttl
                                  )
                IN      NS      ns1.example.com.
                IN      NS      ns2.example.com.
4               IN      PTR     mysite.net.
; etc
```

You are the Registrant of a /20

- If you have a /20, you configure sixteen reverse domains – one for each /24 - in your zone files



Delegations Smaller than a /16

- /24 = 1 reverse domain
- /23 = 2 reverse domains
- /22 = 4 reverse domains
- [. . .]
- /18 = 64 reverse domains
- /17 = 128 reverse domains

Your Delegation of a /16 (or larger)

- If you are the registrant of a /16, simply insert a new level of hierarchy:
  - Configure a /16 reverse domain with authoritative NSes
- Then configure the individual /24 reverse domain zone files
- If you are the registrant of a /15, configure two /16 reverse domains, and then configure two sets of 256 /24 reverse domain zone files

IPv6 Delegations

- A /32 is the default size for LIRs. It acts just like a /16 in IPv4. You answer for the /32, then define individual reverse domains as necessary – respecting the nibble boundaries.
- If you have a /48 or something smaller, the RIR will respond to the /32, and delegate the individual /48s or /44s (etc.) to your name servers

CNAMES and Really Small Zones

- Delegation boundaries are easy to respect as an LIR. But what about your customers who need reverse DNS for small address blocks (e.g. a /28 in IPv4)?
- There can only be one delegation by the RIR for each /24
- To overcome this restriction, we use the **CANONICAL NAME** (CNAME) RR type
  - “An alias name for a host. Causes redirection for a single RR at the owner-name.”
- In reverse DNS, **RFC2317** was written to define how to use CNAME RRs in reverse DNS zone files to handle address blocks smaller than a /24

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