Reverse DNS

Champika Wijayatunga <champika@icann.org>

What is ‘Reverse DNS’?

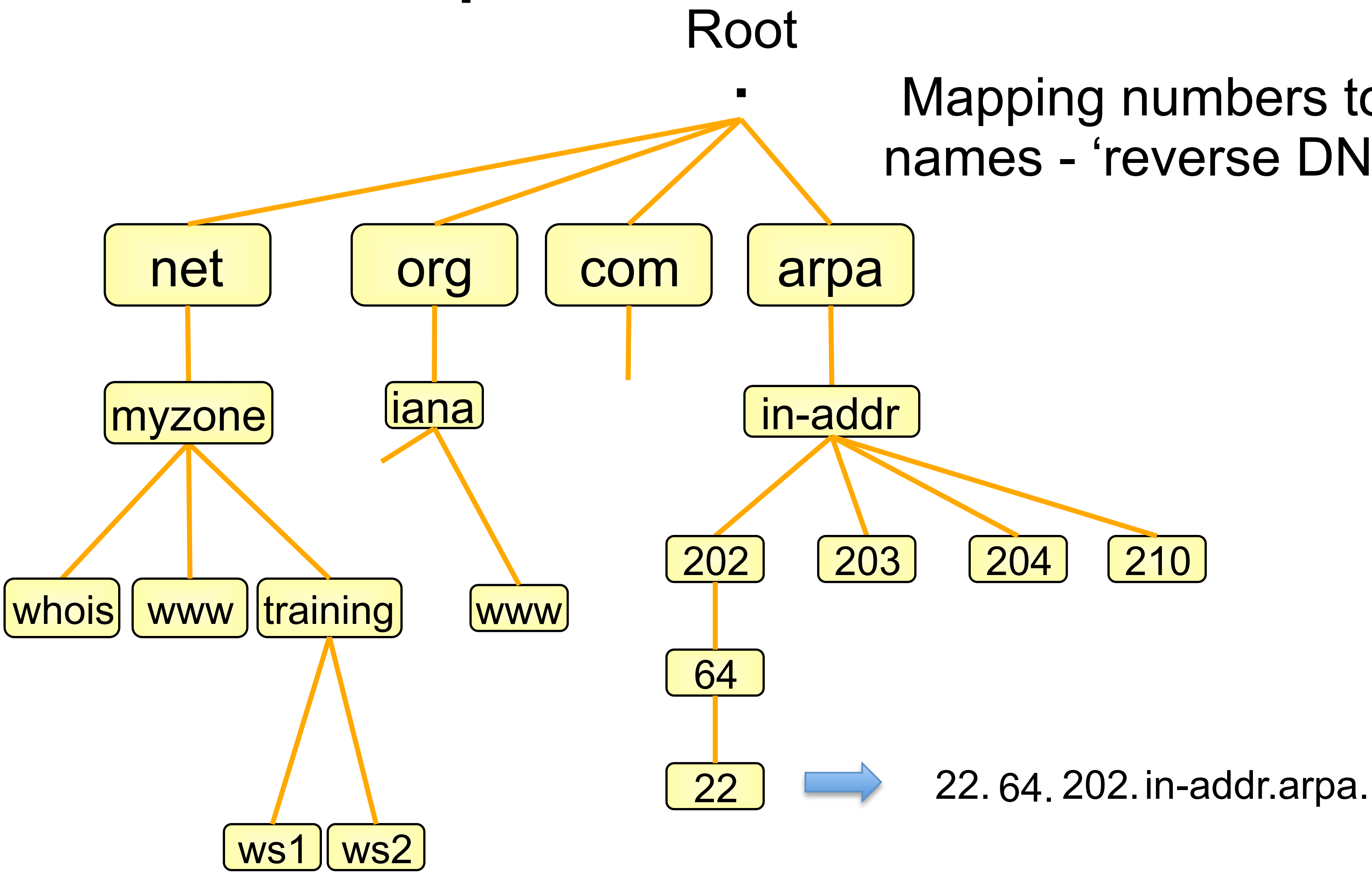
- ‘Forward DNS’ maps names to numbers
  - www.icann.org ➔192.0.32.7

- ‘Reverse DNS’ maps numbers to names
  - 192.0.32.7 ➔ www.icann.org

Reverse DNS - why bother?

- Service denial
  - only allow access when fully reverse delegated
  - Example: anonymous ftp
- Diagnostics
  - Assisting in trace routes etc
- SPAM identifications
  - Failed reverse lookup results in a spam penalty score

Principles – DNS Tree



Mapping numbers to names - ‘reverse DNS’

22. 64. 202. in-addr.arpa.

Creating Reverse Zones

- Same as creating a forward zone file
  - SOA and initial NS records are the same as normal zone
- Main difference
  - need to create additional PTR records
- Can use BIND or other DNS software to create and manage reverse zones
  - Details can be different
- In addition to the forward zone files, you need the reverse zone files
  - Ex: for a reverse zone on a 192.168.1.0/24 block, create a zone file and name it as “db.192.168.1” (make it descriptive)

Start of Authority (SOA) record

```
Domain_name. CLASS  SOA  hostname.domain.name. mailbox.domain.name (
      Serial Number
                              Refresh
                              Retry
                              Expire
                              Minimum TTL )
```

- **Serial Number** – must be updated if any changes are made in the zone file
- **Refresh** – how often a secondary will poll the primary server to see if the serial number for the zone has increased
- **Retry** - If a secondary was unable to contact the primary at the last refresh, wait the retry value before trying again
- **Expire** - How long a secondary will still treat its copy of the zone data as valid if it can't contact the primary.
- **Minimum TTL** - The default TTL (time-to-live) for resource records

Pointer (PTR) Records

- Create pointer (PTR) records for each IP address

```
7.32.0.192.in-addr.arpa. IN PTR www.icann.org.
```

```
7         IN     PTR       www.icann.org.
```

Reverse Zone Example

```
$ORIGIN 1.168.192.in-addr.arpa.
@  3600  IN SOA test.company.org. (
          sys\.admin.company.org.
          2015022401   ; serial
          1h           ; refresh
          30M          ; retry
          1W           ; expiry
          3600 )       ; neg. answ. ttl

   NS  ns1.company.org.
   NS  ns2.company.org.

1  PTR    gw.company.org.
          router.company.org.

2  PTR    ns.company.org.
```

Reverse Delegation Requirements

- /24 Delegations
  - Address blocks should be assigned/allocated
  - At least two name servers
- /16 Delegations
  - Same as /24 delegations
  - RIR delegates entire zone to member
- < /24 Delegations
  - Read “Classless IN-ADDR.ARPA delegation” (RFC 2317)

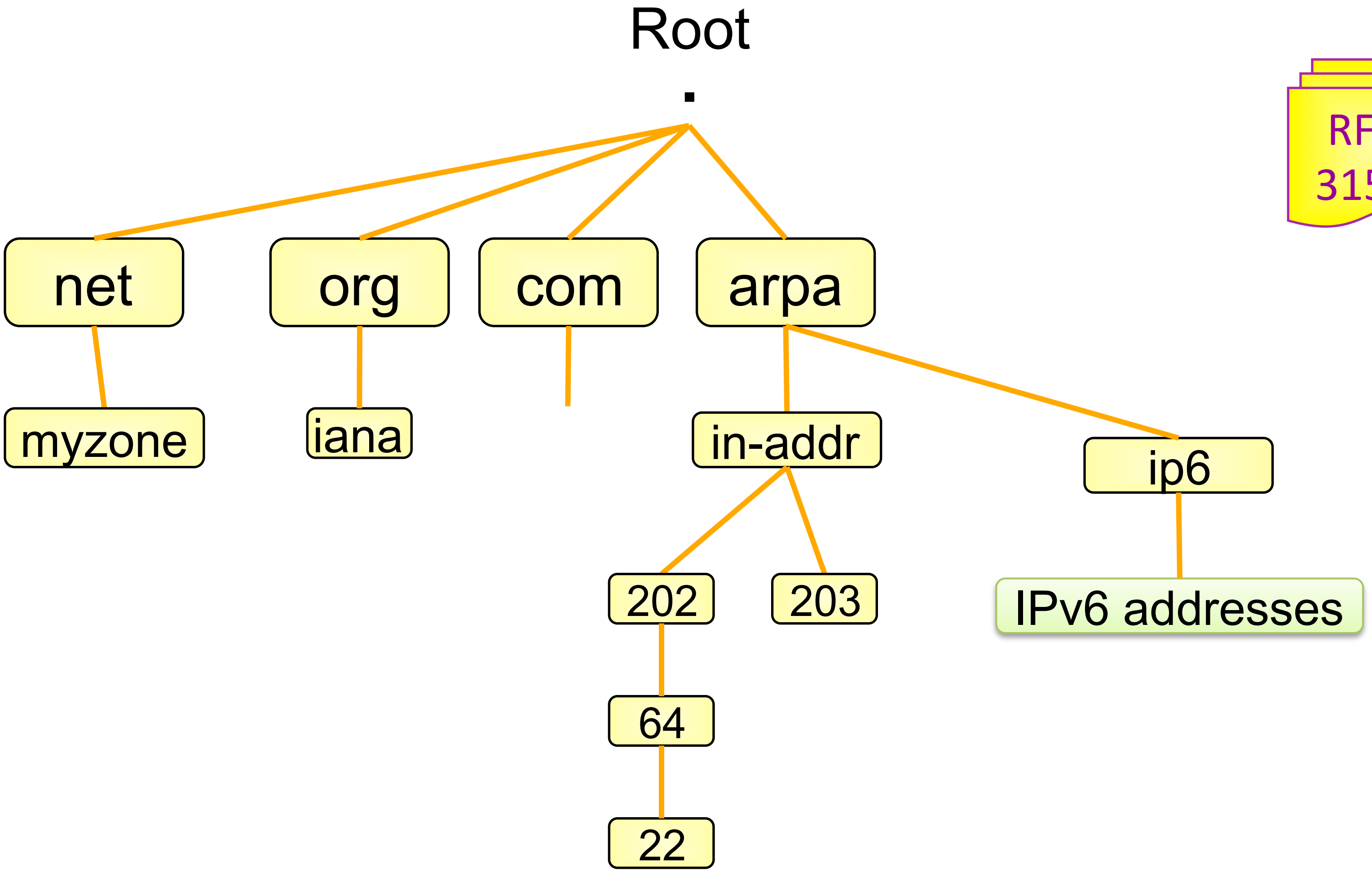
RFC
2317

Your responsibilities

- Be familiar with RIR Reverse DNS procedures
- Ensure that addresses are reverse-mapped
- Maintain nameservers for allocations
- Minimise pollution of DNS

IPv6 Reverse Delegations

Reverse DNS Tree – with IPv6



RFC 3152

IPv6 Representation in the DNS

- Forward lookup support: Multiple RR records for name to number
  - AAAA (Similar to A RR for IPv4)
- Reverse lookup support:
  - Reverse nibble format for zone ip6.arpa

IPv6 Reverse Lookups – PTR records

- Similar to the IPv4 reverse record

```
b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.ip6.arpa.
   IN     PTR  test.ip6.example.com.
```

- Example: The reverse name lookup for a host with address `3ffe:8050:201:1860:42::1`

```
$ORIGIN 0.6.8.1.1.0.2.0.0.5.0.8.e.f.f.
3.ip6.arpa.

1.0.0.0.0.0.0.0.0.0.0.0.2.4.0.0  14400  IN
PTR host.example.com.
```

IPv6 forward and reverse mappings

- Existing A record will not accommodate the 128 bit addresses for IPv6
- BIND expects an A record's record-specific data to be a 32-bit address (in dotted-octet format)
- An address record
  - AAAA (RFC 1886)
- A reverse-mapping domain
  - ip6.arpa

IPv6 forward lookups

- Multiple addresses possible for any given name
- Can assign A records and AAAA records to a given name/domain
- Can also assign separate domains for IPv6 and IPv4

Sample forward lookup file

```
;; domain.edu
$TTL          86400
@    IN      SOA     ns1.domain.org. root.domain.org. (
       20150224  ; serial - YYYYMMDDXX
       21600     ; refresh - 6 hours
       1200      ; retry - 20 minutes
       3600000   ; expire - long time
       86400)    ; minimum TTL - 24 hours
;; Nameservers
       IN NS ns1.domain.org.
       IN NS ns2.domain.org.

;; Hosts with just A records
host1     IN A  1.0.0.1

;; Hosts with both A and AAAA records
host2     IN A  1.0.0.2
          IN AAAA   2001:468:100::2
```

Sample reverse lookup file

```
;; 0.0.0.0.0.0.1.0.8.6.4.0.1.0.0.2.rev
;; These are reverses for 2001:468:100::/64)
;; File can be used for both ip6.arpa
$TTL          86400
@    IN      SOA     ns1.domain.org. root.domain.org. (
             2002093000       ; serial - YYYYMMDDXX
             21600            ; refresh - 6 hours
             1200             ; retry - 20 minutes
             3600000          ; expire - long time
             86400)           ; minimum TTL - 24 hours
;; Nameservers
         IN   NS   ns1.domain.edu.
         IN   NS   ns2.domain.edu.
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0   IN   PTR host1.ip6.domain.org
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0   IN   PTR host2.domain.org
;;
;; Can delegate to other nameservers in the usual way
;;
```