APNIC eLearning:
Reverse DNS Delegation

Contact: training@apnic.net

APNIC

Overview

- What is Reverse DNS?

- Principles of DNS Tree

- Creating Reverse Zones

- PTR Records

- Reverse Delegation

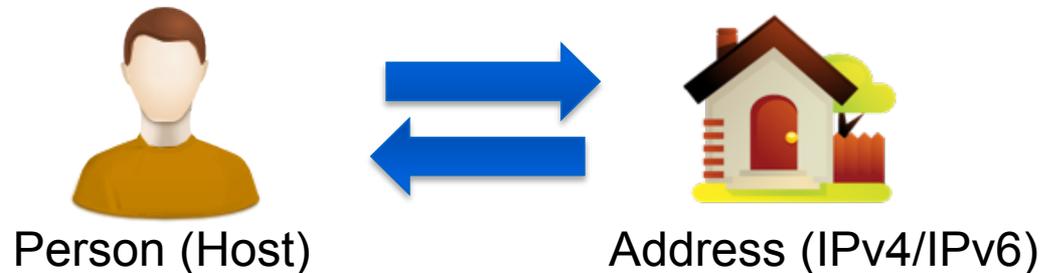- Whois Domain Objects

What is 'Reverse DNS'?

- 'Forward DNS' maps names to numbers

  svc00.apnic.net ➜ 202.12.28.131
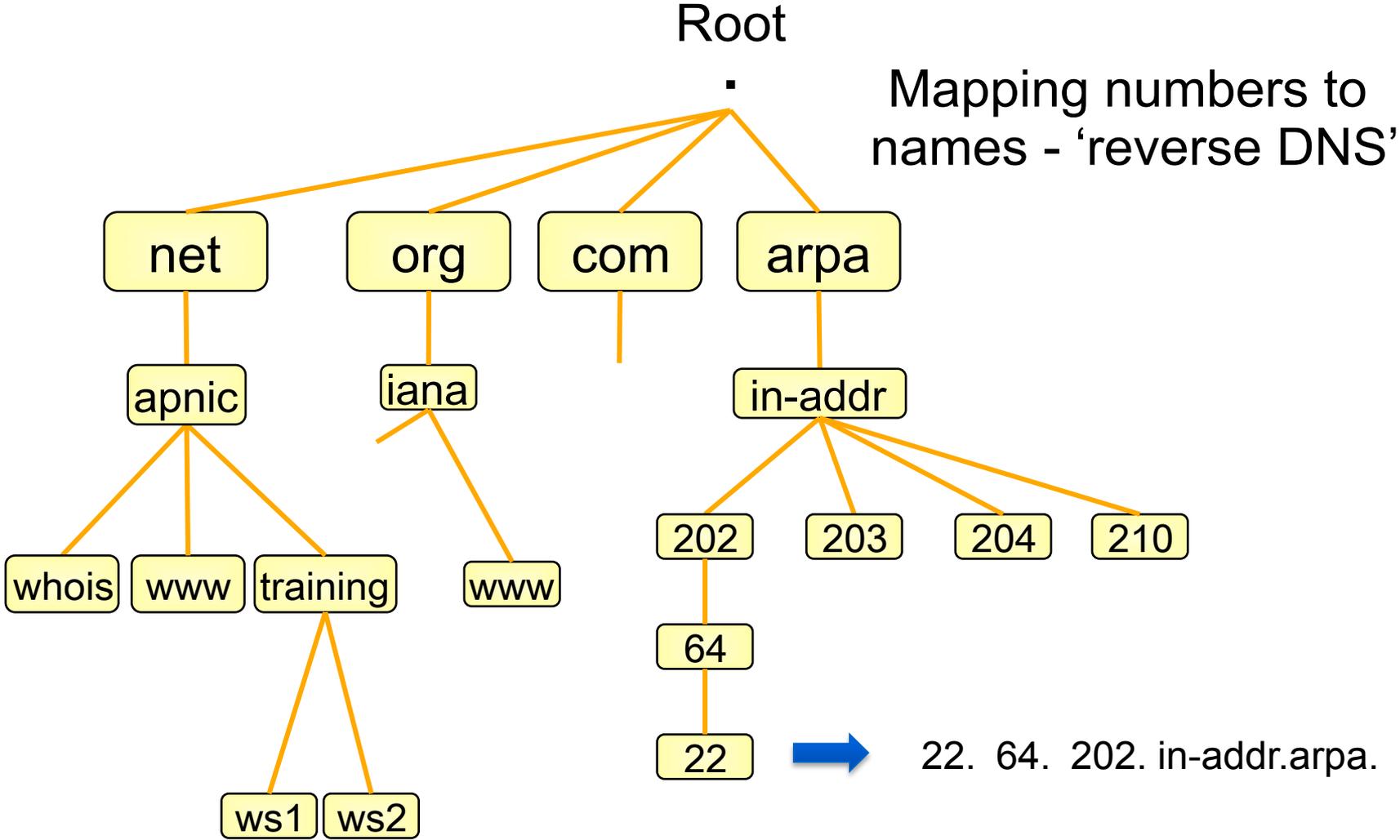

- 'Reverse DNS' maps numbers to names

  202.12.28.131 ➜ svc00.apnic.net

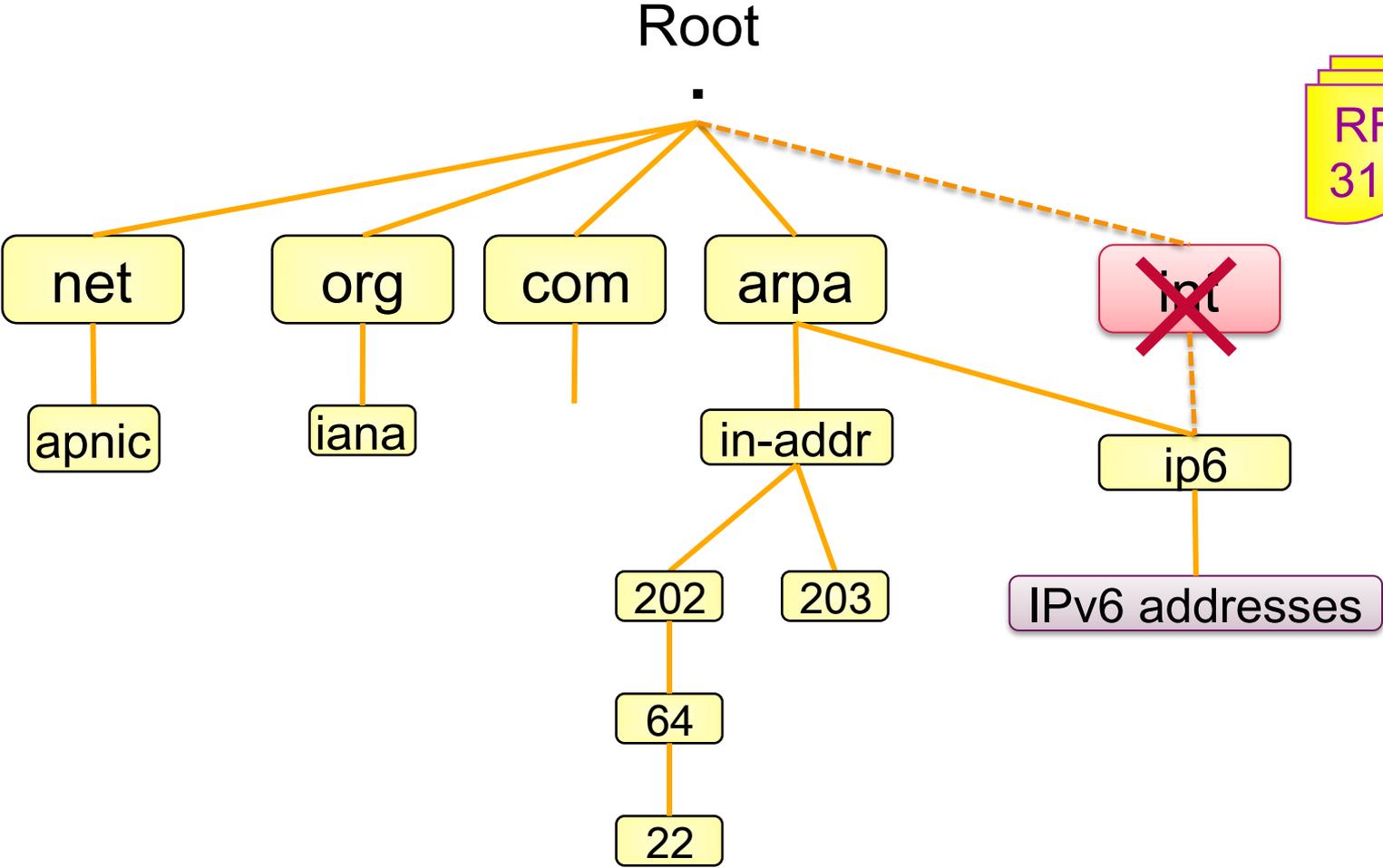Person (Host)   Address (IPv4/IPv6)

Reverse DNS - Why bother?

- Service denial
  - only allow access when fully reverse delegated
  - Example: anonymous ftp

- Diagnostics
  - Assisting in trace routes

- SPAM identifications

- Registration responsibilities

Principles – DNS Tree

Root

Mapping numbers to names - 'reverse DNS'

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

APNIC

Reverse DNS Tree – with IPv6

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 PTR records

- Can use BIND or other DNS software to create and manage reverse zones
  - Details can be different

Creating Reverse Zones (continued)

- Files involved
  - Forward zone files
    - `db.domain.net`
  - Reverse zone files
    - `db.192.168.254`
  - Configuration files
    - `named.conf`
  - Hints File
    - `Root.hints, db.cache, named.cache`

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

APNIC

TTL Time Values

- The right value depends on your domain

- Recommended time values for TLD (based on RFC 1912)

Refresh	86400 (24h)
Retry	7200 (2h)
Expire	2592000 (30d)
Min TTL	345600 (4d)

- For other servers – optimize the values based on
  - Frequency of changes
  - Required speed of propagation
  - Reachability of the primary server
  - (and many others)

Pointer (PTR) records

- Create pointer (PTR) records for each IP address

```
131.28.12.202.in-addr.arpa. IN PTR svc00.apnic.net.
```

or

```
131            IN    PTR           svc00.apnic.net.
```

IPv6 Reverse Lookups – PTR records

- Similar to the IPv4 reverse record

```
b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.1.2.3.4.ip6.arpa.

        IN      PTR   test.ip6.example.com.
```

- Example: 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.


1.0.0.0.0.0.0.0.0.0.0.0.0.2.4.0.0  14400   IN PTR host.example.com.
```

Reverse Zone Example

```
$ORIGIN 1.168.192.in-addr.arpa.
@       3600  IN SOA test.company.org. (
                      sys\.admin.company.org.
                      2002021301    ; serial
                      1h            ; refresh
                      30M           ; retry
                      1W            ; expiry
                      3600 )        ; neg. answ. ttl


        NS      ns.company.org.
        NS      ns2.company.org.

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

2       PTR     ns.company.org.
;auto generate:  65 PTR host65.company.org
$GENERATE 65-127 $ PTR host$.company.org.
```

Reverse Delegation Requirements

- /24 Delegations
  - Address blocks should be assigned/allocated
  - At least two name servers

- /16 Delegations
  - Same as /24 delegations
  - APNIC delegates entire zone to member
  - Recommend APNIC secondary zone

- < /24 Delegations
  - Read "Classless IN-ADDR.ARPA delegation" (RFC 2317)

RFC
2317

APNIC & ISPs Responsibilities

- APNIC
  - Manage reverse delegations of address block distributed by APNIC
  - Process organisations requests for reverse delegations of network allocations

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

Reverse Delegation Procedures

- Standard APNIC database object,
  - can be updated through myAPNIC

- Nameserver/domain set up verified before being submitted to the database.

- Protection by maintainer object
  - (current auths: CRYPT-PW, PGP).

- Any queries
  - Contact helpdesk@apnic.net

APNIC

Reverse Delegation Procedures

Whois domain object

```
domain:      28.12.202.in-addr.arpa
Descr:       in-addr.arpa zone for 28.12.202.in-addr.arpa
admin-c:     NO4-AP
tech-c:      AIC1-AP
zone-c:      NO4-AP
nserver:     cumin.apnic.net
nserver:     tinnie.apnic.net
nserver:     tinnie.arin.net
mnt-by:      MAINT-APNIC-AP
mnt-lower: MAINT-AP-DNS
changed:     inaddr@apnic.net 20021023
changed:     inaddr@apnic.net 20040109
changed:     hm-changed@apnic.net 20091007
changed:     hm-changed@apnic.net 20111208
source:      APNIC
```

Reverse Zone

Contacts

Nameservers

Maintainers

APNIC

Questions

- Please remember to fill out the feedback form
  - \<survey-link\>

- Slide handouts will be available after completing the survey

APNIC Helpdesk Chat

Thank you!

End of Session

APNIC