Reverse DNS in IPv6 for ISPs

Chief Architect of BII Lab

Shane Kerr
Contents

- Introduction
- Reverse DNS in IPv4
  - What? Why? How?
- Reverse DNS in IPv6
  - What? Why? How... not.
  - NXDOMAIN
  - Wildcard
  - DDNS
  - Delegation
  - Dynamic Generation
Very Brief Introduction

Standard techniques for IPv4 reverse DNS mapping WILL NOT work in IPv6. Lee Howard's draft discusses this in detail. This presentation is an overview. https://.../draft-howard-isp-ip6rdns
Reverse DNS: IPv4 (1 of 2)

Simple mapping:
192.0.2.123 → 123.0.2.192.in-addr.arpa

DNS delegation is on octet boundaries:

```
... 0 1 255
```

```
arpa
in-addr
```
Reverse DNS: IPv4 (2 of 2)

Octet boundaries make delegation awkward:

<table>
<thead>
<tr>
<th>Octet boundaries</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.0.0.0/16</td>
<td>0.192.in-addr.arpa</td>
</tr>
<tr>
<td>192.0.0.0/17</td>
<td>0.0.192.in-addr.arpa</td>
</tr>
<tr>
<td>127.0.0.0/12</td>
<td>127.0.0.0/12</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Classful nature of reverse DNS motivated RFC 2137, a.k.a. “the CNAME hack”
Reverse DNS for ISP: IPv4

For infrastructure, hosted computers, and so on: manual or automated mapping from reverse to forward DNS names.

For “eyeball” computers:

143-245-128-083.dynamic.caiway.nl
D97B95C1.cm-3-4c.dynamic.ziggo.nl
84-245-31-233.dsl.cambrium.nl
ip5b403660.dynamic.kabel-deutschland.de
host223-178-dynamic.7-87-r.retail.telecomitalia.it
203.225.19.95.dynamic.jazztel.es
2-228-59-34.ip190.fastwebnet.it
Why Have Reverse DNS?

- Makes ping/traceroute more informative
- Helpful in log files
- SSH
  - Host name on login, with who/w, and so on
  - SSH host authentication
- (Helping) SMTP mail through spam filters
- Possibly security the DNS "last mile" in the future! https://tools.ietf.org/html/draft-osterweil-dane-ipsec-02
- RFC 1912 says:
  
  Thou shalt have a PTR to an A, and that A shall be the same PTR.
Reverse DNS: IPv6

Similar mapping to IPv4:
2001:db8::29 →
9.2.0.0.0 ... 8.b.d.0.1.0.0.2.ip6.arpa

Distressingly long. Don't forget to 0-pad!

DNS delegation is on nibble boundaries.

- At most 8 delegations for a net, not 128.
- A metric crapload of delegations possible.

IPv6 never had “classes”, so no RFC 2137.
The Problem

- Customers are given a /48 (or /56, or /64)
- You can't enumerate the possible hosts
  <insert pithy story about it taking longer than the age of the universe to finish>
- You can't know which IP addresses will actually be used, or how
  Especially with SLAAC
Option 1: NXDOMAIN

- “Fail fast”
  - Avoids timeouts
  - May cause SMTP to fail (perhaps a bug, perhaps a feature)

HOWTO:
- Set up IPv6 reverse delegations for parent (or child)
- An "empty" zone file is fine, after delegation from parent (probably RIPE NCC)
Option 2: *.Wildcard Match

- Documented in RFC 4472
- Labels like: *.8.b.d.0.1.0.0.2.ip6.arpa
- IPv6 address for every host gets the same PTR
  Forward doesn't match reverse

HOWTO:
- Set up IPv6 reverse delegations for parent (or child)
- A zone file with SOA, NS, and single wildcard PTR record should be fine
Option 3: Dynamic DNS

- Also documented in RFC 4472
- ISP holds customer DNS delegations
- Updated via DDNS
Sub-Options 3.[12]: meh

3.1: DDNS directly from hosts
  ▪ IP-based ACL for authentication
    BIND 9 has “tcp-self” update policy
  ▪ No client support

3.2: DDNS through Residential Gateways
  ▪ Either let clients know the ISP's DDNS server, or provide a proxy
  ▪ No client support
Sub-Options 3.[456]: meh

3.4: Match forward/reverse DDNS records
   - No client support

3.5: Use DHCPv6 information
   - Only for specific domains; no client support

3.6: Use RADIUS information
   - Only provides information about a single host
Sub-Option 3.3: Automatic DNS Delegations

- Customers get a forward domain as well as reverse
  - customer123.uithoorn.isp.example
- Devices get DHCPv6 Prefix Delegation (PD)
- Customers that have a gateway that provides DHCPv6 from prefix
- Doesn't name hosts that don't use DHCPv6 (like Android)

- May use DDNS to ISP's name server, or
- May act as hidden master for DNS to ISP, or
Option 4: Delegate DNS

- The Old Fashioned Way: Delegate the DNS
- General case of 3.3
- Possibly good for commercial customers
- Not good for many residential customers
Option 5: Dynamically-Generated PTR

- Generate PTR on query, with synthetic name
  Can also populate AAAA record at this time

- DNSSEC issues
  Unpredictable load if signatures generated on the fly
  Key material stored on each server

- HOWTO:
  PowerDNS can do this via Lua, or the "pipe" backend
  http://member.wide.ad.jp/~fujiwara/v6rev.html
  Net::DNS in Perl, dnspython in Python, Go dns library, ...
Speaker's Confession

- Tried to kill reverse DNS in IPv6
- Prefer something like RFC 4620 (IPv6 Node Information Queries)
- Would like "complete" solution, but realise that is a cost
- Good luck! :)