Use of ICMPv6 node information query for reverse DNS lookup

draft-itojun-ipv6-nodeinfo-revlookup-00.txt

Jun-ichiro itojun Hagino
`itojun@{iijlab,kame}.net`

Motivation

- **We will see more addresses without PTR records**
  - Stateless autoconfig
  - Temporary/privacy address

- **PTR does not work with scoped address**

- **DNS dynamic update deployment takes time**
  - TSIG key distribution issue

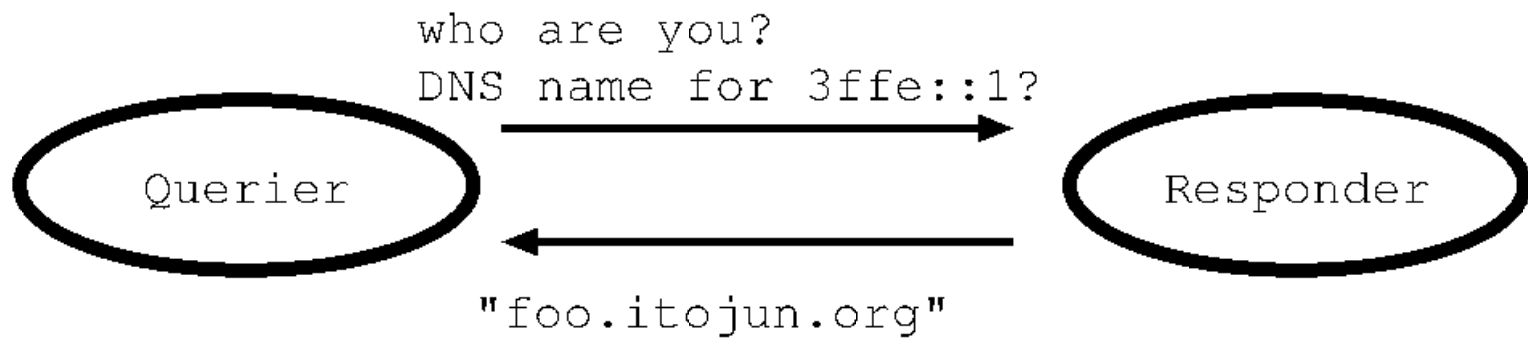- **So, why not propose an alternative way?**

Protocol

- **Querier -> Responder**
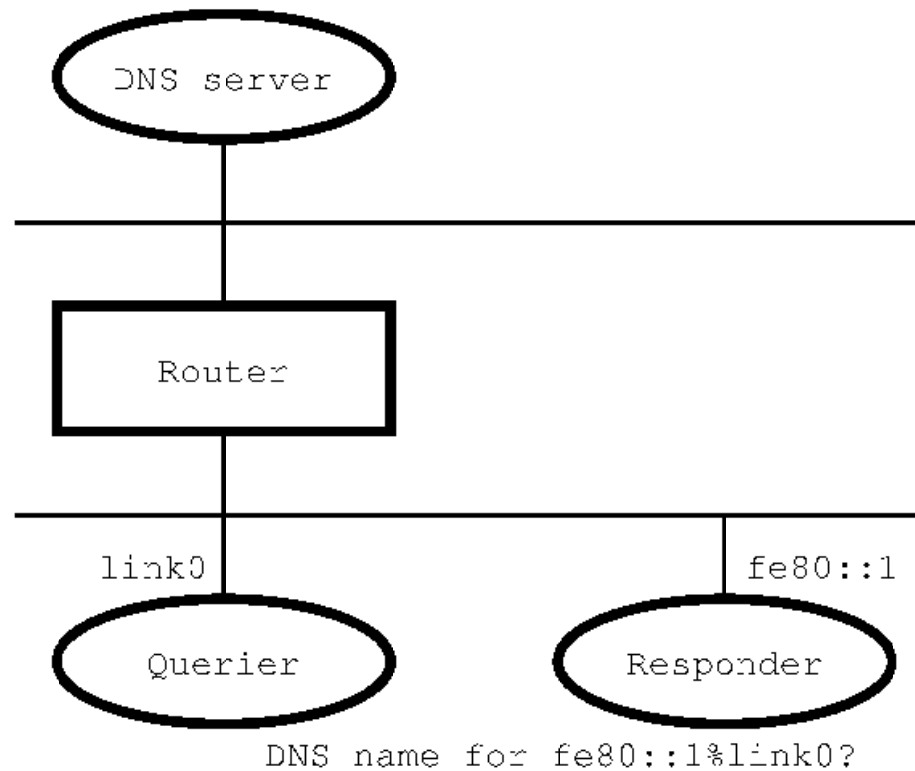 - ICMPv6 Node information query, Qtype = 2 (DNS name)
- **Responder -> Querier**
  - ICMPv6 Node information reply, with DNS name

```
              who are you?
              DNS name for 3ffe::1?
                ----------------->
   Querier                              Responder
                <-----------------
              "foo.itojun.org"
```

Scoped address

- ☐ **DNS: doesn't work**
  - ○ The view of scope zone differs
  - ○ DNS payload format does not handle scope zones
- ☐ **This approach: works okay**
  - ○ Querier is the node itself

```
              ┌─────────────┐
             (   DNS server  )
              └──────┬──────┘
        ───────────────────────────
              ┌──────┴──────┐
              │    Router    │
              └──────┬──────┘
        ───────────────────────────────
           link0│              │fe80::1
          ┌─────┴─────┐   ┌────┴─────┐
         ( Querier    ) ( Responder  )
          └───────────┘   └──────────┘
             DNS name for fe80::1%link0?
```

Differences w/ PTR

- ☐ **Is the DNS name really belong to the node?**
  - ○ (Reverse record w/o forward zone admins' knowing)
  - ○ Anyone can claim "www.ietf.org", same as PTR
- ☐ **Integrity between forward and reverse lookup**
  - ○ DNSSEC doesn't help, same as PTR
- ☐ **Malicious response injected from outsider**
  - ○ DNSSEC helps here, PTR has an advantage
  - ○ With ICMPv6, we need PKI infrastructure + IPsec

- ☐ **Admin diffs**
  - ○ PTR: DNS zone admin needs to configure single DNS server
  - ○ ICMPv6: every node has to be configured with a DNS name

Summary

- **An alternative way to perform reverse lookup**

- **Friendly with scoped addresses**
  - Works even for link-locals
  - Site-local - see the other discussion...

- **Some behavior differences with PTR**

- **Easy to implement**
  - Responder: KAME/USAGI kernel has it in ICMPv6 processing
  - Querier: KAME revlookupd, ping6 -w

- **Shouldn't trust reverse mapping too much anyways, btw**

  - draft-ietf-dnsop-inaddr-required-03.txt