Internet Engineering Task Force
INTERNET-DRAFT
Expires: December 20, 2002

Jun-ichiro itojun Hagino
IIJ Research Laboratory
June 20, 2002

Use of ICMPv6 node information query for reverse DNS lookup
draft-itojun-ipv6-nodeinfo-revlookup-00.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as ``work in progress.''

To view the list Internet-Draft Shadow Directories, see http://www.ietf.org/shadow.html.

Distribution of this memo is unlimited.

The internet-draft will expire in 6 months. The date of expiration will be December 20, 2002.

Abstract

The document proposes an alternative way to perform reverse DNS lookup, by using ICMPv6 node information query/reply [Crawford, 2002] . The proposed protocol works only with IPv6 (not with IPv4).

1. Motivation

As documented in [Senie, 2001] , even though many applications assume reverse address mapping to exist, DNS reverse address mapping table may not be present. With IPv4, automatically-generated reverse mapping table, like following, has been used.

```
123.123.123.123.in-addr.arpa. IN PTR 123-123-123-123.reverse.example.org.
```

However, it is difficult to provide such mapping for IPv6, due to the number of reverse mapping records needed. Therefore, with IPv6, it is more likely to see IPv6 addresses without reverse DNS mapping. While it may be possible to register reverse DNS records via dynamic DNS updates, it is still not widely practiced due to difficulties with authentication

(distribution of TSIG authentication keys). Also, reverse DNS lookup based on PTR record can cause more delay to applications than IPv4 case, as an IPv6 reverse DNS mapping requires much more of NS indirections (34 levels rather than 6 levels).

Another problem is that DNS PTR records do not support scoped IPv6 addresses well, as DNS infrastructure is global in nature and there is no way to differentiate between scope zones.

For this reason, this document discusses an alternative way to provide reverse DNS lookups. The approach uses ICMPv6 node information query/reply [Crawford, 2002] .

2. Protocol

There are two parties: querier and responder. The querier knows an IPv6 address of the responder, and is interested in getting fully-qualified DNS name for the responder,

Querier transmits the following ICMPv6 node information query packet to the reponder's address:

```
IPv6 source: one of querier's address (Q)
IPv6 destination: responder's address (R)
Code: 0 (Subject is an IPv6 address)
Qtype: 2 (DNS name)
Nonce: pseudo-random (N)
Data (Subject): responder's address
```

In response, the reponder transmits ICMPv6 node information reply with fully-qualified DNS name.

```
IPv6 source: one of responder's address
IPv6 destination: Q
Code: 0 (Successful)
Qtype: 2 (DNS name)
Flag: lowermost bit set (TTL is valid)
Nonce: N
Data: fully-qualified DNS name.
     TTL must be set based on R's address lifetime.
```

Note:

- The IPv6 source address of the reply need not be R; Nonce field should be used to match replies against a query.

- Fully-qualified DNS name must be sent on replies. If DNS name on the reply is a single-component name, the querier should ignore the response.

o Administrators are advised to provide consistent reverse mapping with forward DNS record, where possible.

Querier is allowed to retransmit query 3 times with 1 second interval.

Querier should implement cache mechanism, based on the TTL value sent from the responder. If TTL value is not present on replies, querier must not cache values on replies. If there is no response after 3 retransmissions, negative-cache entry with lifetime of 30 second should be installed.

Querier must ignore responses with a Nonce value unknown to the querier (it could be a malicious attempt to taint the cache).

Responder must rate-limit replies as documented in ICMPv6 node information query document [Crawford, 2002] .

3. Appicability

3.1. Is "DNS name" on the reply really a DNS name?

Responses returned on "DNS name" query can contain arbitrary string independent from deployed DNS infrastructure. For example, any node can respond with DNS name "foo.example.org" without example.org administrator's knowledge. This is also true for reverse DNS mapping based on PTR records.

3.2. Consistency with forward DNS records?

We cannot assume consistency with forward DNS records. It is the same as DNS PTR records.

With scoped IPv6 address, it is not possible to keep consistency between forward and reverse mapping (both with DNS PTR records and ICMPv6 node information queries), as it is discouraged to put scoped IPv6 address into global DNS database, and there is no DNS PTR delegation for scoped IPv6 addresses.

3.3. Number of configured elements?

With DNS PTR records, the reverse address mapping needs to be configured on DNS server. With ICMPv6 node information query, all nodes need to be configured with fully-qualified DNS name.

3.4. Interaction with scoped IPv6 addresses

DNS PTR records do not support scoped IPv6 addresses well, due to the following reasons:

o DNS database is a global database in nature, and does not fit well with scoped IPv6 address.

o ip6.arpa (or ip6.int) delegation structure does not deal with scoped

delegation.

- The view of scope zones differs from nodes to nodes. Therefore, if the querier node of DNS PTR record is different from the node holding DNS PTR database, they have different idea about/access to scope zones.

- There is no way to differentiate between scope zones, specifically from remote.

ICMPv6 node information query/reply handles scoped IPv6 address well, as the querier directly tries to obtain reverse name mapping (hence there is no difference in the view of scope zones).

Even with ICMPv6 node information query/reply, it is not possible to provide a consistent mapping between forward and reverse lookup for scoped IPv6 addresses, as DNS wire packet format (AAAA) does not have a way to identify scope zones.

4. Security consideration

4.1. Are there any possibility for forgery?

Yes. Intermediate nodes can intercept node information query/reply packet and throw in forged queries/replies. It is true for DNS query/reply too.

There are ongoing efforts in DNS arena for data integrity protection - DNSSEC. It is a bit hard to do similar thing for node information query. DNSSEC is possible because there is NS delegation tree in DNS. There is no obvious "structure" in node information query.

4.2. Use of reverse DNS mapping for authentication

As documented in [Senie, 2001] it is discouraged to use the existence of reverse DNS mapping as authentication.

References

Crawford, 2002.
Matt Crawford, "IPv6 Node Information Queries" in draft-ietf-ipngwg-icmp-name-lookups-09.txt (May 2002). work in progress material.

Senie, 2001.
Daniel Senie, "Requiring DNS IN-ADDR Mapping" in draft-ietf-dnsop-inaddr-required-02.txt (July 2001). work in progress material.

Change history

None.

Acknowledgements

(to be filled)

Author's address

Jun-ichiro itojun HAGINO
Research Laboratory, Internet Initiative Japan Inc.
Takebashi Yasuda Bldg.,
3-13 Kanda Nishiki-cho,
Chiyoda-ku,Tokyo 101-0054, JAPAN
Tel: +81-3-5259-6350
Fax: +81-3-5259-6351
Email: itojun@iijlab.net