Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 4, 2009

M. Endo
H. Miyata
Yokogawa Electric Corp.

October 1, 2008

Translator Friendly DNS Proxy
draft-endo-v6ops-dnsproxy-01.txt

Status of this Memo

Abstract

This document describes the DNS Proxy that is separated from NAT-PT [RFC2766]. NAT-PT was designed to work with DNS Application Level Gateway. However [RFC4966] pointed out DNS related issues, and [RFC2766] was changed to historical state. This document attempts to DNS Proxy specification, removing dependency on NAT-PT as well as resolving problems pointed in [RFC4966].

Table of Contents

1. Introduction

Many IPv4-to-IPv6 translation technologies are proposed. The address mapping technology is one of the most important technologies to use IPv4-to-IPv6 translation technologies. Some IPv4-to-IPv6 translation technologies select a DNS Proxy as the address mapping technology.

NAT-PT [RFC2766], one of IPv4-to-IPv6 translation technologies, was designed. However NAT-PT had some issues that [RFC4966] describes. So, it was changed to historical state by [RFC4966].

Because DNS Proxy is located in NAT-PT, DNS Proxy related issues that [RFC4966] describes happened. In other words, if DNS Proxy is independent from NAT-PT, some issues will be solved.

This document proposes the DNS Proxy that is separated from NAT-PT. Proposed DNS Proxy isn't implemented in the host, but it co-exists with NAT-PT. There are some approaches that DNS Proxy is implemented in hosts. But, it is too hard to adopt DNS Proxy function, because many IPv6 and IPv4 hosts are already deployed. And it requires functionality discovering translators.

Proposed DNS Proxy requires a relationship with translators to map addresses dynamically. This document assumes a design to work with translators, which have an interface to collaborate with Application Level Gateways or Proxies.

The purpose of this document is to attempt a translator friendly DNS Proxy and to clear requirements for DNS Proxy.

2. Terminology

The majority of terms used in this document are borrowed almost as is from [SNATPT]. The following lists terms specific to this document.

2.1. Application Level Gateway (ALG)

Application Level Gateway (ALG) is an application specific agent that allows an IPv6 node to communicate with an IPv4 node and vice versa. Some applications carry network addresses in payloads. The translator such as NAT-PT is application unaware and doesn't snoop the payload. ALG could work in conjunction with NAT-PT to provide support for many such applications.

2.2. Dummy Prefix

The IPv6 Prefix to map IPv4 address to IPv6 address. And a length of the prefix is 96 bit. In this document, Dummy Prefix is represented as PREFIX or PREFIX::/96 when IPv6 address or prefix is described. The prefix PREFIX::/96 is advertised in an IPv6 network by the NAT-PT gateway, and packets addressed to this PREFIX will be routed to the NAT-PT gateway. This PREFIX is configured for each NAT-PT gateway, and DNS Proxy will use it during translating from A RR to AAAA RR.

2.3. Requirements Language

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [RFC2119].

3. Conceptual Model

This section describes the conceptual model for proposed DNS Proxy. Fig.3.1 shows a block diagram of proposed DNS Proxy. DNS Proxy has important components "Dummy Prefix List", "IPv4 Address Pool" and "Address Mapping Table". "Dummy Prefix List" and "IPv4 Address Pool" store addresses for mapping addresses. "Address Mapping Table" has entries of mapped addresses.

This document shows just an example. An implementation is not required to have them in the exact from described here, so long as its external behavior is consistent with that described in this document.

```
   +----------------------------------------------+
   | DNS Proxy                                    |
   |                      +-------------------+   |
   |           +--------->| Dummy Prefix List |   |
   |           |          +-------------------+   |
   |           |                                  |
   |           |          +-------------------+   |
   |           | +------->| IPv4 Address Pool |   |
   |           | |        +-------------------+   |
   |           | |                                |
   |   +------------+                             |  +------------+
   |   | Translator |<------------------------------>| Translator |
   |   | Dispatcher |                             |  | Interface  |
   |   +------------+                             |  +------------+
   |        ^    |                                |
   |        |    |    +-----------------------+   |
   |        |    +--->| Address Mapping Table |   |
   |        |         +-----------------------+   |
   |        |                                     |
   |        |                                     |
   |   +--------------------------------------+   |
   |   |         RR Translation Engine        |   |
   |   +--------------------------------------+   |
   |        ^ |                                   |
   +--------|-|-----------------------------------+
   +--------|-|-----------------------------------+
   |        | |     TCP/UDP Stack                 |
   +--------|-|-----------------------------------+
            | v
        DNS Messages
```

Fig. 3.1 DNS Proxy Conceptual Model

3.1. Dummy Prefix List

Dummy Prefix List has dummy prefixes that are assigned to each translator. DNS Proxy selects a prefix from it, and DNS Proxy maps an IPv4 address to an IPv6 address with selected prefix.

The entry of this list MUST have following information.

IPv6 Prefix:
The IPv6 prefix assigned to one translator. This prefix is used to map an IPv4 address to an IPv6 address.

3.2. IPv4 Address Pool

IPv4 Address Pool stores IPv4 addresses that are assigned to each translator. DNS Proxy selects an IPv4 address from it, and DNS Proxy maps an IPv6 address to selected IPv4 address.

The entry of this pool MUST have following information.

IPv4 Address:
This IPv4 address is used to map to an IPv6 address.

Address Status:
This information indicates a status of this IPv4 address. The status has two condition "Un-Mapped" and "Mapped". If Un-mapped status, DNS Proxy can select this entry to map. Otherwise DNS Proxy cannot do it.

Un-mapped:
This IPv4 address is not mapped.
Mapped:
This IPv4 address is already mapped.

3.3. Address Mapping Table

Address Mapping Table has mapped addresses. When DNS Proxy maps an IPv5 address to an IPv6 address, DNS Proxy adds a new entry to Address Mapping Table. When DNS Proxy maps an IPv6 address to an IPv4 address, a new entry is not added because a mapped IPv6 address is globally unique.

The entry of this table MUST have following information.

IPv4 Address:
This IPv4 address is used to map to an IPv6 address.

IPv6 Address:
IPv6 address that is mapped to above IPv4 address.

Expire Time:
Lifetime for this entry. If it is expired, this entry will be released. Then an IPv4 address included in this entry will be re-used.

3.4. RR Translation Engine

Functionalities of RR Translation Engine are forwarding DNS messages and translating DNS messages.

Target types of resource records that RR Translation Engine can translate are A, AAAA and PTR resource record. Regarding A6 resource record type, because [RFC3363] changed to experimental status, translating A6 resource record isn't needed. Regarding PTR resource record type, RR Translation Engine only translates "IN-ADDR.ARPA" and "IP6.ARPA" domain. In other resource record types or other domains of PTR record case, RR Translation Engine SHOULD just forward DNS messages to DNS server or clients.

In translating resource records, RR Translation Engine sends DNS query to DNS server sequentially and sends only one DNS response to client. This behavior is already described by [RFC4966] section 4.1.

By default, DNS Proxy forwards unchanged DNS query to DNS server. Then if DNS server responds with no answer, DNS Proxy translates a query type and re-send DNS query to DNS server. Although DNS Proxy responds with real IPv6 addresses, client that are attached to an IPv6 network which has no global IPv6 connectivity cannot communicate. To support this case, RR Translation Engine SHOULD translate a query type when DNS Proxy forwards a first DNS query, and a behavior of RR Translation Engine SHOULD be configurable.

When RR Translation Engine decides to need to translate a resource record, it will make a request to Translator Dispatcher for mapping addresses. Translator Dispatcher selects the Dummy Prefix or IPv4 address. In case that translating from A to AAAA records, RR Translation Engine creates AAAA records with IPv6 address that is combined Translator Dispatcher selected Dummy Prefix and received A

record. In case that translating from AAAA to A records, RR Translation Engine creates A record with IPv4 address that Translator Dispatcher selected.

Especially in translating from AAAA to A records, RR Translation Engine must change TTL value for translated records to shorter. Because IPv4 address will be re-used, it avoids caching records in clients.

The DNS Proxy described by [RFC2766] is stateless DNS Proxy. According to [RFC4966] section 4.43, such a DNS Proxy can translate DNS response messages that need not be translated. So, proposed DNS Proxy MUST be stateful DNS Proxy. If RR Translation Engine received only DNS response message, RR Translation Engine MUST discard it.

The behavior of DNS Proxy MUST NOT depend on transport or network protocol. DNS Proxy MUST decide own behavior according to the received DNS query.

3.5. Translator Dispatcher

Translator Dispatcher manages Address Mapping Table. With depend on the request from RR Translation Engine, Translator Dispatcher selects an address from Dummy Prefix List or IPv4 Address Mapping Pool and maps selected address.

To map an IPv4 address to an IPv6 address, Translator Dispatcher searches Address Mapping Table. If the table has entry that includes an IPv6 address which is mapped an IPv4 address, Translator Dispatcher answers the IPv4 address that the entry has. Otherwise Translator Dispatcher selects an IPv4 address from IPv4 Address Pool, maps selected IPv4 address and creates a new entry. If a new entry was created, Translator Dispatcher must inform a new mapping to a translator through Translator Interface. By doing that, dynamically address mapping is possible.

To map an IPv6 address to an IPv4 address, Translator Dispatcher selects a dummy prefix from Dummy Prefix List. Selected dummy prefix and an IPv4 address are combined. A translator like a [SNATPT] or TRT ([RFC3142]) can treat a packet destinated to dummy prefix as packet that is translate. So, informing a new mapping to a translator is not needed.

3.6. Translator Interface

The communication between DNS Proxies and translators is done through this interface. In this document, dynamic address mapping uses the interface.

The detail is TBD.

4. Benefits

4.1. Translator Independency

Proposed DNS Proxy does not depend on translators. So, this DNS Proxy can cooperate with not only [SNATPT] but also other translation technologies.

4.2. Transport Independency

The behavior of Proposed DNS Proxy does not depend on a transport or network protocol. Because the resolver of some client implementation can only support IPv4, in transition period, DNS Proxy must support such kind of clients. Because of transport independency, proposed DNS Proxy can be attached to any topology. And one more benefit is that the implementation will be simple.

4.3. Translation Mode

By translating query type at forwarding DNS query, DNS Proxy can control type of addresses that is returned to clients. For example, if DNS Proxy is attached to IPv6 only network, which has no IPv6 global connectivity, by DNS Proxy translate AAAA query type received from client to A query type forcibly, client can receive mapped IPv6 address. Because proposed DNS Proxy can change behavior of translating DNS query, proposed DNS Proxy can support various network.

4.4. Load Balancing of Translator

Translator Dispatcher selects an address arbitrary from Dummy Prefix List or IPv4 Address Pool to map an address. Addresses that are included in Dummy Prefix List or IPv4 Address Pool are assigned to translators. In other words, selecting an address means selecting a translator. So, proposed DNS Proxy can support load balancing for translators.

4.5. Dynamic Address Mapping Functionality

Proposed DNS Proxy can map an IPv4 address to an IPv6 address dynamically. It is very useful functionality for from IPv4 to IPv6 communication.

4.6. Host Implementation

This document requires no changes to host implementation.

4.7. Solution for RFC4966

Proposed DNS Proxy will be solutions following problems described by [RFC4966].

4.7.1. 3.1 Network Topology Constraints Implied by NAT-PT

Because proposed DNS Proxy is separated from NAT-PT, the problem that [RFC4966] describes will not happen.

4.7.2. 3.2 scalability and single point of failure

Because proposed DNS Proxy is separated from NAT-PT, the problem that [RFC4966] describes will not happen. But redundancy mechanism for DNS Proxy is needed.

4.7.3. 4.1 Address Selection Issues when Communicating with Dual-Stack End-Hosts

RFC4966 says

> If the query relates to a dual-stack host, the query will return both the native IPv6 address(es) and the translated IPv4 address(es) in AAAA RRs. Without additional information, the IPv6 host address selection may pick a translated IPv4 address instead of selecting the more appropriate native IPv6 address. Under some circumstances, the address selection algorithms [RFC3484] will always prefer the translated address over the native IPv6 address; this is obviously undesirable.

Proposed DNS Proxy does not reply both the real IPv6 addresses and the translated IPv4 addresses in one DNS response. So the problem will not happen.

RFC4966 also says

o The DNS client may timeout the query if it doesn't receive a response in time. This is more likely than for queries not passing through a DNS ALG because the NAT-PT may have to make two separate, sequential queries of which the client is not aware. It may be possible to reduce the response time by sending the two queries in parallel and ignoring the result of the A query if the AAAA returns one or more addresses. However, it is still necessary to delay after receiving the first response to determine if a second is coming, which may still trigger the DNS client timeout.

The timeout may happen. However, actually, almost DNS resolutions

are not timeout. Furthermore, adopting DNS cache to DNS Proxy can reduce the timeout.

4.7.4. "4.3 Inappropriate Translation of Response to A Queries"

Because proposed DNS Proxy is stateful DNS Proxy, the problem will not happen.

5. RR Translation Behavior

Proposed DNS Proxy does not intercept any DNS messages. So, to use this DNS Proxy, this DNS Proxy MUST be specified as DNS resolver in client systems. Because proposed DNS Proxy is separated from the transport layer, there is no difference of processing a DNS AAAA query between from IPv6 network and from IPv4 network.

5.1. AAAA query processing

This section describes a behavior when DNS Proxy received AAAA query. There is assumption that DNS server to which DNS Proxy forwards DNS queries was pre-configured in DNS Proxy.

5.2. DNS server has AAAA resource records

This behavior is same as DNS Cache servers. If DNS server has native resource records which clients requested, DNS Proxy should just forward DNS messages.

There are host X and client in the IPv6 network. The IPv6 address of host X is registered in DNS server. If client want to communicate with host X, the client will send AAAA query to DNS Proxy. DNS Proxy will receive AAAA query from the client, then DNS Proxy will forward the query to DNS server without changing. DNS server will respond IPv6 address of X to DNS Proxy. The DNS response message that DNS Proxy received has IPv6 address for X, and then DNS Proxy will sends DNS response message to the client.

```
   Client                          DNS Proxy                    DNS Server
     |         AAAA query            |                             |
     |------------->-------------|  AAAA query (unchanged)     |
     |                           |-------------->-------------|
     |                           |                             |
     |                           |         AAAA reply          |
     |   AAAA reply (unchanged)  |--------------<-------------|
     |--------------<-------------|                             |
     |                           |                             |
```

5.3. DNS server has only A resource records

This is a basic behavior of proposed DNS Proxy. If DNS Proxy decides that DNS server does not have resource records which clients requested, DNS Proxy will translate DNS messages.

There is IPv4 only host Z and IPv6 client. The IPv4 address of host Z is registered in DNS server. If client want to communicate with

host Z using IPv6, the client will send AAAA query to DNS Proxy. DNS Proxy will receive AAAA query from the client, then DNS Proxy will forward the query to DNS server without changing. Because DNS server does not have IPv6 address for host Z, DNS server will send DNS response with no address. When DNS Proxy received DNS response without addresses, DNS Proxy will translate DNS query type to A record, and send translated DNS query(A) to DNS server. DNS server will respond IPv4 address of Z to DNS Proxy. The DNS response message that DNS Proxy received has IPv4 address for Z, and then DNS Proxy will translate IPv4 address that is contained DNS response message to IPv6 address. After translation, DNS Proxy will send translated DNS response message to the client.

Regarding address mapping, DNS Proxy selects the prefix from Dummy Prefix List, and appends IPv4 address that is included in DNS response message to last 32 bit of selected prefix. The information of address mapping does not needed to inform to translators, because translators can treat packets that destinated to Dummy Prefix as packets that will be translated.

```
Client                     DNS Proxy                  DNS Server
  |         AAAA query         |                            |
  |------------->--------------|  AAAA query (unchanged)    |
  |                            |-------------->-------------|
  |                            |                            |
  |                            |         AAAA reply         |
  |                            |--------------<-------------|
  |                            |                            |
  |                            |  A query (translated)      |
  |                            |-------------->-------------|
  |                            |                            |
  |                            |          A reply           |
  |                            |--------------<-------------|
  |   translated AAAA reply    |                            |
  |--------------<-------------|                            |
  |                            |                            |
```

NOTE:

The above described behavior is initially introduced by Jun-ichiro itojun HAGINO and Kazu Yamamoto at 47th IETF in 2000. And while being improved and extended the idea is widely deployed with not only with TRT [RFC3142] but also NAT-PT [RFC2766] like implementation introduced as [SNATPT].

5.4. A query processing

This section describes a behavior when DNS Proxy received A query. The process of A query is similar process of AAAA query.

5.4.1. DNS server has A resource records

This behavior is same as that section 5.x.y described. The difference is a record type of DNS query requested.

There are host X and client in the IPv4 network. The IPv4 address of host X is registered in DNS server. If client want to communicate with host X, the client will send A query to DNS Proxy. DNS Proxy will receive A query from the client, and then DNS Proxy will forward the query to DNS server without changing. DNS server will respond IPv4 address of X to DNS Proxy. The DNS response message that DNS Proxy received has IPv4 address for X, and then DNS Proxy will sends DNS response message to the client.

```
   Client                     DNS Proxy                   DNS Server
     |            A query         |                            |
     |------------->--------------|     A query (unchanged)    |
     |                            |-------------->-------------|
     |                            |                            |
     |                            |            A reply         |
     |                            |--------------<-------------|
     |      A reply (unchanged)   |                            |
     |--------------<-------------|                            |
     |                            |                            |
```

5.4.2. DNS server has only AAAA resource records

This is a basic behavior of proposed DNS Proxy. If DNS Proxy decides that DNS server does not have resource records which clients requested, DNS Proxy will translate DNS messages.

There is IPv6 host Z and IPv4 client. The IPv6 address of host Z is registered in DNS server. If client want to communicate with host Z using IPv4, the client will send A query to DNS Proxy. DNS Proxy will receive A query from the client, and then DNS Proxy will forward the query to DNS server without changing. Because DNS server does not have IPv4 address for host Z, DNS server will send DNS response with no address. When DNS Proxy received DNS response without addresses, DNS Proxy will translate DNS query type to AAAA record, and send translated DNS query (AAAA) to DNS server. DNS server will respond IPv6 address of Z to DNS Proxy. The DNS response message that DNS Proxy received has IPv6 address for Z, and then DNS Proxy

will translate IPv6 address that is contained DNS response message to IPv4 address. After translation, DNS Proxy will send translated DNS response message to the client.

Regarding mapping addresses, DNS Proxy selects the IPv4 from IPv4 Address Pool, and maps IPv4 address to an IPv6 address that is included in DNS response message. After mapping addresses, DNS Proxy MUST inform pair of address to translator. After exchanging DNS messages, the client will send packets to the IPv4 address that DNS Proxy mapped. In that time, if translator does not known the mapping information, any packets that the client sent will not be translated by a translator.

```
   Client                     DNS Proxy                   DNS Server
     |            A query         |                            |
     |------------->--------------|     A query (unchanged)    |
     |                            |-------------->-------------|
     |                            |                            |
     |                            |            A reply         |
     |                            |--------------<-------------|
     |                            |                            |
     |                            |  AAAA query (translated)   |
     |                            |-------------->-------------|
     |                            |                            |
     |                            |       AAAA reply           |
     |                            |--------------<-------------|
     |     translated A reply     |                            |
     |--------------<-------------|                            |
     |                            |                            |
```

5.5. Translation Mode

By default, proposed DNS Proxy SHOULD just forward DNS query that DNS Proxy received first time in the DNS session. It avoids exhaustion of memory and address/port pool resources on the translators and the DNS Proxy. For example, there is an IPv6 network that does not have any global connectivity. In such case, if the client received native IPv6 address from DNS Proxy, the client cannot communicate. To solve them, the translation mode of DNS Proxy SHOULD be configurable. If a configuration is that DNS Proxy have priority to return mapped address, DNS Proxy will translate DNS AAAA query that the client sent to DNS A query, and forward DNS server.

```
   Client                     DNS Proxy                   DNS Server
     |         AAAA query          |                            |
     |------------->--------------|  A query (translated)      |
     |                            |-------------->-------------|
     |                            |                            |
     |                            |          A reply           |
     |                            |--------------<-------------|
     |   translated AAAA reply    |                            |
     |--------------<-------------|                            |
     |                            |                            |
```

5.6. PTR query (Optional)

The translation for PTR resource records is not mandate functionality. But, it is useful feature for network operations. Domains that Proposed DNS Proxy supports are IP6.ARPA and IN-ADDR.ARPA domains. If DNS Proxy receive PTR query that has other domain, DNS Proxy SHOULD forward it without changing.

5.6.1. IP6.ARPA domain

When DNS Proxy received PTR query for IP6.ARPA domain, DNS Proxy will search own Dummy Prefix List. If the prefix included in IP6.ARPA domain is not exist in Dummy Prefix List, DNS Proxy will just forward the query to DNS server. If exist, DNS Proxy will translate QNAME field to IN-ADDR.ARPA domain, and send translated query to DNS server. When DNS Proxy received DNS response that DNS server responded, DNS Proxy would restore QNAME field to IP6.ARPA domain, and send DNS response to the client.

```
   Client                     DNS Proxy                   DNS Server
     |[translated IPv6].IP6.ARPA  |                            |
     |         PTR query          |                            |
     |------------->--------------| <IPv4>.IN-ADDR.ARPA        |
     |                            |   PTR query (translated)   |
     |                            |-------------->-------------|
     |                            |                            |
     |                            | <IPv4>.IN-ADDR.ARPA PTR    |
     |                            |       Z.example.com reply  |
     |                            |--------------<-------------|
     |[translated IPv6].IP6.ARPA  |                            |
     |   PTR Z.example.com reply  |                            |
     |--------------<-------------|                            |
     |                            |                            |
```

5.6.2. IN-ADDR.ARPA domain

When DNS Proxy received PTR query for IN-ADDR.ARPA domain, DNS Proxy will search own Address Mapping Table. If the IPv4 address included in IN-ADDR.ARPA domain is not exist in Address Mapping Table, DNS Proxy will just forward the query to DNS server. If exist, DNS Proxy will translate QNAME field to IP6.ARPA domain for IPv6 address that entry of Address Mapping Table has, and send translated query to DNS server. When DNS Proxy received DNS response that DNS server responded, DNS Proxy would restore QNAME field to IN-ADDR.ARPA domain, and send DNS response to the client.

```
   Client                     DNS Proxy                   DNS Server
     |[mapped IPv4].IN-ADDR.ARPA  |                            |
     |         PTR query          |                            |
     |------------->--------------| <IPv6>.IP6.ARPA            |
     |                            |   PTR query (translated)   |
     |                            |-------------->-------------|
     |                            |                            |
     |                            | <IPv6>.IP6.ARPA PTR        |
     |                            |       Y.example.com reply  |
     |                            |--------------<-------------|
     |[mapped IPv4].IN-ADDR.ARPA  |                            |
     |   PTR Y.example.com reply  |                            |
     |--------------<-------------|                            |
     |                            |                            |
```

5.7. Other Resource Record Types

If DNS Proxy received queries for resource record types that this document does not described, DNS Proxy SHOULD forward queries to DNS server.

6. Limitation

There are some limitations when DNS Proxy maps an IPv4 address to an IPv6 address dynamically.

When DNS Proxy will map an IPv4 address dynamically, DNS Proxy MUST inform the pair of addresses. And timing of releasing the mapping should be concerned. Because DNS Proxy only manages DNS exchange, DNS Proxy cannot care about communications. It is require exchanging information of sessions that translators operate. The detail of relationship between DNS Proxy and translator is out of scope of this document.

Another limitation is TTL of resource record. DNS Proxy SHOULD change the TTL value for translated resource records to shorter. IPv4 addresses that contained in IPv4 Address Pool will re-used, because address space of IPv4 is less than IPv6's one. So it avoids to cache translated record in clients.

7. Security Considerations

7.1. DNSSEC

This DNS Proxy translates resource records, so that nodes implementing DNSSEC may ignore the translated records. Due to avoid this issue, there are two solutions. One is that the DNS Proxy behaves like a secure DNS server. The DNS proxy, which behaves like a secure DNS server, is same as a Man-in-the-Middle model. It requires a verifying method for the DNS Proxy. Another one is that clients, which initiate a DNS communication, validate responses by themselves. This solution requires modification for DNSSEC implementation of clients. In this document proposes the 2nd solution. We need more discussion about this issue, because other drafts like a [NAT64] propose alternative solutions.

7.1.1. The EDNS Original Resource Record option

EDNS [RFC2671] defines a mechanism to add option to the DNS [RFC1035] protocol. This secsion defines the Original Resource Record (ORR) option that indicate the answer section includes translated RRs.

The format of the ORR option is:

```
   0   1   2   3   4   5   6   7   8   9  10  11  12  13  14  15
 +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
 |                          OPTION-CODE                          |
 +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
 |                         OPTION-LENGTH                         |
 +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
 |                                                               |
 /                          OPTION-DATA                          /
 |                                                               |
 +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

The fields are defined as follows:

- OPTION-CODE: (Assigned by IANA.)

- OPTION-LENGTH: Size (in octets) of OPTIONS-DATA.

- OPTION-DATA: This field includes the original resource record which the DNS Proxy would translate from.

7.1.2. Usage of the ORR option

The ORR option can carries original RRs. So that the client can verify RRs at receiving first response from the DNS Proxy, if the response has translated RR in its answer secDNS tion. This section describes the usage of ORR option.

```
Client                     DNS Proxy                    DNS Server
  |         AAAA query         |                             |
  |------------->--------------|  AAAA query (unchanged)     |
  |                            |-------------->-------------|
  |                            |                             |
  |                            |         AAAA reply          |
  |                            |--------------<-------------|
  |                            |                             |
  |                            |  A query (translated)       |
  |                            |-------------->-------------|
  |                            |                             |
  |                            |  A reply (authorized)       |
  |                            |--------------<-------------|
  |   translated AAAA reply    |                             |
  |   and
  |   authorized A reply (ORR) |                             |
  |--------------<-------------|                             |
  |                            |                             |
```

1. A client send an AAAA query to the DNS Proxy.

2. The DNS Proxy received above query and forwards it to a DNS server.

3. A DNS server replies with no answer.

4. The DNS Proxy sends a query, which is translated to an A query by the DNS Proxy.

5. A DNS server sends an A response, which has an authenticated answer.

6. The DNS Proxy receives an authenticated response. The DNS Proxy MUST keep SIG RR and adopt ORR option with RR, which is included in an authenticated response. And The DNS Proxy translates RR from A to AAAA.

7. When the client receives a response which has ORR option, the client decide that the response has translated RRs. Then, the client verifies answer section using RR, which was included in

ORR option.

8. IANA Considerations

The option type Original Resource Record option, as defined in section 7 is new EDNS option. A code number for new EDNS option should be assigned by IANA.

9. References

9.1. Normative References

[RFC2119] Bradner, S. and E. Davies, "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, BCP 14, March 1997.

[RFC3142] Hagino, J. and K. Yamamoto, "An IPv6-to-IPv4 Transpot Relay Translator", RFC 3142, June 2001.

[RFC3363] Bush, R., Durand, A., Fink, B., Gudmundsson, O., and T. Hain, "Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS)", RFC 3363, August 2002.

[RFC4966] Aoun, C. and E. Davies, "Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status", RFC 4966, July 2007.

[SNATPT] Miyata, H. and M. Endo, "Simplified Network Address Translation - Protocol Translation", Work in Progress draft-miyata-v6ops-snatpt-01, September 2008.

9.2. Informative References

[NAT64] Bagnulo, M. and P. Matthews, "NAT64/DNS64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", Work in Progress draft-bagnulo-behave-nat64-01, September 2008.

[RFC1035] Mockapetris, P., "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION", RFC 1035, November 1987.

[RFC2671] Vixie, P., "Extension Mechanisms for DNS (EDNS0)", RFC 2671, August 1999.

[RFC2766] Tsirtsis, G. and P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766, February 2000.

Authors' Addresses

Masahito Endo
Yokogawa Electric Corporation
2-9-32 Nakacho
Musashino-shi, Tokyo 180-8750
JAPAN

Email: masahito.endou@jp.yokogawa.com

Hiroshi Miyata
Yokogawa Electric Corporation
2-9-32 Nakacho
Musashino-shi, Tokyo 180-8750
JAPAN

Email: h.miyata@jp.yokogawa.com

Full Copyright Statement

Intellectual Property