DNSOPS
Internet-Draft
Intended status: Informational
Expires: May 15, 2018

T. Saraj, Ed.
Riphah Institute of Systems Engineering (RISE)
M. Yousaf, Ed.
Riphah Institute of Systems Engineering
A. Qayyum, Ed.
Capital University of Science and Technology

November 11, 2017

IVIPTR: Resource Record for DNS
draft-tariq-dnsop-iviptr-00.txt

Abstract

This document propose a new DNS Resource Record IVIPTR which provides the capability to resolve the IPv4 address to IPv6 address and IPv6 address to IPv4 address. This document assumes that the reader is familiar with all the concepts and details discussed in Domain Names Concepts and Facilities [RFC1034] , Domain Names - Implementation and Specification [RFC1035]

Status of This Memo

This Internet-Draft will expire on May 15, 2018.

Copyright Notice

1. Introduction

The current DNS standard does not support to resolve IPv4 address to IPv6 address and IPv6 address to IPv4 address. For example, when querying for AAAA against a known A record of a resource, the response code (RCODE) for such query is normally Non-Existent Domain (3). Using the current DNS standard, this requirement can be fulfilled by the following process if one of the address (i.e. IPv4 or IPv6) is known:

The stub-resolver send a query request to the locally configured recursive name server to resolve a domain name against an A record

The recursive name server respond with a PTR record in query response if there exists a domain name on corresponding authoritative name server.

The stub-resolver then further request the recursive name server to resolve the AAAA record against the corresponding domain name

The recursive name server respond with an AAAA record if it exists in the authoritative name server zone file.

Here, the bottleneck in this process is that now a days, mostly domains has different PTR records for a corresponding AAAA or A record in which case the aforementioned process is not suitable. Also, this process requires to make changes to the stub-resolver functionality to pursue the aforementioned process. Even, if the stub-resolver functionality is modified it will work only if a single domain name is used for both A and AAAA record. The proposed solution is that when the stub-resolver send a query to the locally configured recursive name server for resolving AAAA record against an A record and vice versa, it will respond with the desired resource record (RR) without depending upon a Fully Qualified Domain Name FQDN knowledge on stub-resolver. The term IVI in the proposed IVIPTR resource record is borrowed from one of the IPv4/IPv6 transition mechanisms address translation algorithm [RFC6219].

2. Motivation

In network security components such as firewall or proxy firewall, mostly traffic monitoring rules are configured based on IPv4 or IPv6 addresses. A network running on IPv4 may enable IPv6 for certain reason such as testing a newly developed application, performance and compatibility testing of application with IPv6 or the organization has decided to keep their network from onwards as a dual stack etc. The administrator responsible for network security has to maintain dual security rules for both Inbound and Outbound network traffic. This can be done by manually configuring the security rules in all network security components for the newly enabled Internet protocol. Mistakenly, configuring any security rule can result in an undesired consequences. To automate such services in a network there is a need to resolve addresses for the newly enabled Internet protocol using the already configured one. Currently, there is no such mechanism that can return IPv6 address of a domain if IPv4 address is known or vice versa. The IVIPTR Resource Record conceived as a solution to the problem for resolving IPv6 address if IPv4 address is known or IPv4 address if IPv6 address is known. There may exist IPv4/IPv6 address in network security components rules set which does not belong to any fully qualified domain name (FQDN) and thus, are out of the scope of this work. The IVIPTR RR can have a number of use cases other than just security rules based on preconfigured IPv4 or IPv6 addresses as target. The presence of this Resource Record in the reverse zone file of a domain Name server can result in automating a number of service for enabling them to reconfigure their security rules for the newly enabled address family protocol i.e. IPv4 or IPv6.

3. The IVIPTR Resource Record

The IVIPTR RR has mnemonic IVIPTR and type code TBA (decimal). The IVIPTR RR has the following format: <OWNER> <TTL> <CLASS> IVIPTR <IVI target > The OWNER is the unqualified or fully qualified domain name depending upon the configuration of reverse zone file optional directive $ORIGIN. The TTL and CLASS fields are the same as for all other PTR records in the reverse zone file. Keeping the use case of IVIPTR RR usage, it is to be believed that this resource record will not be required to access frequently or in some cases just once so one can set a smaller TTL value for this resource record to facilitate the recursive name server cache unnecessary increase. IVIPTR is the new RR type that points to a fully qualified domain name (FQDN) i.e. IVI target in a reverse zone file. The <IVI target> from onwards for simplicity written as <target> SHOULD be a fully qualified domain name (FQDN). The presence of <IVIPTR RR> in a reverse zone can be elaborate by considering the domain example.com. Realistically, most of the time the target domain labels for an A and AAAA PTR records are different. The RRs in zone files for both forward zone and reverse zone would be as: ; zone file for example.com foo.example.com IN CNAME a.x.foo.example.com. a.x.foo.example.com. IN A 192.168.0.1 a.x6.foo.example.com. IN AAAA 2001:DB8:0::1 ; reverse zone file for example.com A record

1.0.168.192.IN-ADDR.APRPA. IN PTR a.foo.example.com. 1.0.168.192.IN-ADDR.ARPA. IN IVIPTR a.x6.foo.example.com. ; reverse zone file for example.com AAAA record 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.IP6.ARPA. IN PTR a.x6.foo.example.com. 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.IP6.ARPA. IN IVIPTR a.x.foo.example.com. The target a.x.foo.example.com. in the reverse zone file is a target in the forward zone file in CNAME. Thus, IVIPTR MUST follow the rule of robustness principle discussed in section 3.6.2 of RFC 1034 [RFC1034] to avoid extra indirections in accessing information.

4. Query Processing

The IVIPTR follow the top level RR format and semantics as defined in the section 3.2.1 of RFC 1035 [RFC1035].

```
                                       1  1  1  1  1  1
         0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5
       +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
       |                                               |
       /                                               /
       /     NAME = A.IN-ADDR.ARPA. OR AAAA.IP6.ARPA.  /
       |                                               |
       +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
       |                      TYPE = IVIPTR            |
       +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
       |                     CLASS = IN                |
       +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
       |                      TTL                      |
       |                                               |
       +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
       |                   RDLENGTH                    |
       +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--|
       /                     RDATA                     /
       /                                               /
       +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

Figure 1

Where: b" NAME: the owner name, same as in any reverse lookup query. b" TYPE: the two octets field containing the IVIPTR RR TYPE code. b" CLASS: two octets containing the RR IN CLASS code value 1. b" TTL: the time interval in seconds that the resource record may be cached before the source of the information again to be contacted. b" RDLENGTH: specifies the length of RDATA field. b" RDATA: A variable length string of octets that represents the <IVI target> resource. The resource depends on the owner in the NAME field of the query. The query processing is same as any other DNS query except that when the recursive name server receives the response for the IVIPTR RR, first it will cache the response like any other RR and then it will form a new query in such a way that: Case-01: If the original query NAME field is A.IN-ADDR.ARPA. and TYPE field is IVIPTR then upon receiving the response at the recursive name server the NAME field of the new query should be mapped appropriately in the desired format to the RDATA resource and the TYPE field should be AAAA. Case-02: If the original query NAME field is AAAA.IP6.ARPA. and TYPE field is IVIPTR then upon receiving the response at the recursive name server the NAME field of the new query should be mapped appropriately in the desired format to the RDATA resource and the TYPE field should be A. This query will be resolved by properly following the hierarchy just like any other forward lookup query request resolution process. Upon receiving the response RR the recursive name server after caching, the answer section will be modified such that the owner NAME will be replaced with the owner NAME in the original query request and the TYPE value instead of A or AAAA should be IVIPTR. The IVIPTR RRs cause no additional section processing. In case of failure or any error the standard error response will be send back to the stub-resolver against the original query request.

5. Security considerations

Security issues are not discussed in this memo. It is expected that the new IVIPTR resource record will be treated the same way as any other PTR RR on the security aware name server.

6. Acknowledgement

7. Informative References

[RFC1034] "Domian Concepts and Facilities", November 1987, <https://www.ietf.org/rfc/rfc1034.txt>.

[RFC1035] "Domian Implementation and Specification", November 1987, <https://www.ietf.org/rfc/rfc1035.txt>.

[RFC6219] The China Educaiton and Research Network (CERNET), "IVI Translation Design and Deployment for the IPv4/IPv6 Coexistence and Transition", MAY 2011, <https://www.ietf.org/rfc/rfc6219.txt>.

Authors’ Addresses

Tariq Saraj (editor)
Riphah Institute of Systems Engineering (RISE)
Agha Khan Road Evacuee Trust
Islamabad, Federal Capital 44000
Pakistan

Phone: +923345755556
Email: tariqsaraj@gmail.com

Muhammad Yousaf (editor)
Riphah Institute of Systems Engineering
Agha Khan Road, Evacuee Trust
Islamabad, Federal Capital 44000
Pakistan

Amir Qayyum (editor)
Capital University of Science and Technology
Main Sihala Road
Islamabad, Federal Capital 44000
Pakistan