

Network Working Group
Internet-Draft
Expires: April 19, 2014

M. Andrews
ISC
October 16, 2013

Automatic Delegation of IP6.ARPA reverse zones with PD
draft-andrews-dnsop-pd-reverse-00

Abstract

This document describes a method to automate the delegation of IPv6.ARPA reverse zones when performing Prefix Delegations.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on April 19, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Internet-Draft

customer reverse zones

October 2013

Table of Contents

1.

Introduction

.

2.

Method

.

3.

IANA Considerations

.

4.

Security Considerations

.

5.

Normative References

.

Author's Address

.

[3](#)

[3](#)

[3](#)

[4](#)

[4](#)

[4](#)

Internet-Draft

customer reverse zones

October 2013

[1.](#) Introduction

This document describes a method to automate the delegation of IPv6.ARPA reverse zones when performing Prefix Delegations.

This will allow home users and small businesses to have IPv6.ARPA zones without manual intervention on the part of the ISP.

[2.](#) Method

CPE generates a RSA key pair and stores this in non-volatile memory.

CPE generates DHCPv6 Prefix Delegation [[RFC3633](#)] request which includes a KEY-RDATA option (code point TBA) which contains a the rdata of a DNS KEY record containing a RSASHA256 key using the public components of the previously generated RSA key pair.

DHCP server updates DNS server based on the prefix it is delegating and the KEY-RDATA using TSIG [[RFC2845](#)] for authentication and responds with prefix. If this is a new prefix delegation it will clear out all the old DNS records as part of the delegation process. If there are multiple prefixes being delegated the ISP's DNS server will be updated for all of them.

The CPE device configures the nameserver built in to it to server the reverse of the delegated prefixes. Alternatively it may configure other nameservers to server these zones however the method to do that is out of scope for this document.

CPE device generates DNS UPDATE [[RFC2136](#)] which delegates the reverse name space to itself and others if they have been configured. The CPE uses SIG(0) [[RFC2931](#)] to sign the request with owner name matching the reverse of the delegated prefix.

The ISP's DNS server is configured to accept self signed requests

(the owner name used in the SIG(0) signature matches the owner name of the data to be updated). It examines the request. Looks at the KEY record added by the DHCPv6 server and decides the request is valid.

[3.](#) IANA Considerations

Allocate a DHCPv6 code point for KEY-RDATA.

Andrews

Expires April 19, 2014

[Page 3]

Internet-Draft

customer reverse zones

October 2013

[4.](#) Security Considerations

The UPDATE requests are all signed. This is a proven method for securing UPDATE requests in the DNS.

As a RSA key is being used there is no issue with the key material being in the clear.

Only the CPE device and the ISP itself is capable of creating, updating or destroying the delegation.

[5.](#) Normative References

- [RFC2136] Vixie, P., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", [RFC 2136](#), April 1997.
- [RFC2845] Vixie, P., Gudmundsson, O., Eastlake, D., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", [RFC 2845](#), May 2000.
- [RFC2931] Eastlake, D., "Secret Key Transaction Authentication for DNS (TSIG)", [RFC 2931](#), September 2000.
- [RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", [RFC 3633](#), December 2003.

Author's Address

M. Andrews
Internet Systems Consortium
950 Charter Street
Redwood City, CA 94063
US

Email: marka@isc.org