

Network Working Group
Internet-Draft
Intended status: Informational
Expires: February 16, 2014

J. Abley
TekSavvy Solutions, Inc.
August 15, 2013

Resource Records for EUI-48 and EUI-64 Addresses in the DNS
draft-jabley-dnsexst-eui48-eui64-rrtypes-07

Abstract

48-bit Extended Unique Identifiers (EUI-48) and 64-bit Extended Unique Identifiers (EUI-64) are address formats specified by the IEEE for use in various layer-2 networks, e.g. Ethernet.

This document describes two new DNS resource record types, EUI48 and EUI64, for encoding Ethernet addresses in the DNS.

This document describes potentially severe privacy implications resulting from indiscriminate publication of link-layer addresses in the DNS. EUI-48 or EUI-64 addresses SHOULD NOT be published in the public DNS. This document specifies an interoperable encoding of these address types for use in private DNS namespaces, where the privacy concerns can be constrained and mitigated.

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 February 16, 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.

Table of Contents

1.	Introduction	3
2.	Terminology	4
3.	The EUI48 Resource Record	5
3.1.	EUI48 RDATA Wire Format	5
3.2.	EUI48 RR Presentation Format	5
3.3.	Example	5
4.	The EUI64 Resource Record	6
4.1.	EUI64 RDATA Wire Format	6
4.2.	EUI64 RR Presentation Format	6
4.3.	Example	6
5.	Example Use-Case: IP Address Tracking in DOCSIS Networks . . .	7
6.	DNS Protocol Considerations	8
7.	IANA Considerations	9
8.	Security Considerations	10
9.	Acknowledgements	11
10.	References	12
10.1.	Normative References	12
10.2.	Informative References	12
10.3.	Informative References	12
Appendix A.	Editorial Notes	13
A.1.	RRType Parameter Allocation Template	13
A.2.	Change History	14
	Author's Address	16

1. Introduction

The Domain Name System (DNS) is described in [[RFC1034](#)] and [[RFC1035](#)]. This base specification defines many Resource Record Types (RRTypes), and subsequent specifications have defined others. Each defined RRType provides a means of encoding particular data in the DNS.

48-bit Extended Unique Identifiers (EUI-48) [[EUI48](#)] and 64-bit Extended Unique Identifiers (EUI-64) [[EUI64](#)] are address formats specified by the IEEE for use in various layer-2 networks, e.g. Ethernet.

This document defines two new RRTypes, EUI48 and EUI64 for encoding EUI-48 and EUI-64 addresses in the DNS.

There are potentially severe privacy implications resulting from the indiscriminate publication of link-layer addresses in the DNS (see [Section 8](#)). This document recommends that EUI-48 or EUI-64 addresses SHOULD NOT be published in the public DNS. This document specifies an interoperable encoding of these address types for use in private DNS namespaces, where the privacy implications can be constrained and mitigated.

[2.](#) Terminology

This document uses capitalised keywords such as MUST and MAY to describe the requirements for using the registered RRTypes. The intended meaning of those keywords in this document are the same as those described in [[RFC2119](#)]. Although these keywords are often used to specify normative requirements in IETF Standards, their use in this document does not imply that this document is a standard of any kind.

3. The EUI48 Resource Record

The EUI48 Resource Record (RR) is used to store a single EUI-48 address in the DNS.

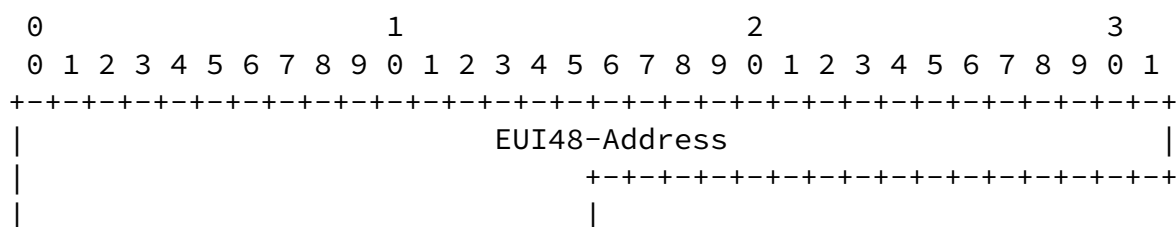
The Type value for the EUI48 RRTYPE is 108 (decimal).

The EUI48 RR is class-independent.

The EUI48 RR has no special Time-to-Live (TTL) requirements.

3.1. EUI48 RDATA Wire Format

The RDATA for an EUI48 RR consists of a single, 6-octet EUI48-Address field, encoded in network (big-endian) order.



+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+

[3.2.](#) EUI48 RR Presentation Format

The Address field MUST be represented as six two-digit hexadecimal numbers separated by hyphens. The hexadecimal digits "A" through "F" MAY be represented in either upper or lower case.

[3.3.](#) Example

The following EUI48 RR stores the EUI-48 unicast address 00-00-5e-00-53-2a.

```
host.example. 86400 IN EUI48 00-00-5e-00-53-2a
```

[4.](#) The EUI64 Resource Record

The EUI64 RR is used to store a single EUI-64 address in the DNS.

The Type value for the EUI64 RR is 109 (decimal).

The EUI64 RR is class-independent.

The EUI64 RR has no special TTL requirements.

[4.1.](#) EUI64 RDATA Wire Format

The RDATA for an EUI64 RR consists of a single, 8-octet Address field, encoded in network (big-endian) order.

to the subscriber, but has no direct knowledge of the IP addresses assigned. In order for the reseller to be able to map the IP address assigned to a subscriber to that EUI-48 address (and hence to the subscriber identity), the cable company can make available information from the DHCP server which provides that (EUI-48, IP) address mapping.

Cable companies in Canada are required [[NTRE038D](#)] to make this address mapping available using the DNS. Zones containing the relevant information are published on DNS servers, access to which is restricted to the resellers corresponding to particular sets of subscribers. Subscriber address information is not published in the public DNS.

Existing DNS schemas for the representation of (EUI-48, IP) mapping used by Canadian cable companies are varied and inefficient; in the absence of a RRType for direct encoding of EUI-48 addresses, addresses are variously encoded into owner names or are published in TXT records.

The specification in this document facilitates a more efficient, consistent and reliable representation of (EUI-48, IP) mapping than was previously available.

The specification of the new RRTypes in this document has no effect on the address resolution behaviour of any previously existing network processes or protocols. Proposals or specifications to modify or augment address resolution processes or protocols by making use of these RRTypes should specify how any address conflicts or use of multiple EUI48/EUI64 RRs are handled.

[7.](#) IANA Considerations

IANA has assigned the RRType value 108 (decimal) for EUI48 and 109 (decimal) for EUI64. This document directs the IANA to confirm that the corresponding entries in the "Resource Record (RR) TYPEs" sub-registry match the following data:

Type	Value	Meaning	Reference
EUI48	108	an EUI-48 address	this document
EUI64	109	an EUI-64 address	this document

8. Security Considerations

There are privacy concerns with the publication of link-layer addresses in the DNS. EUI-48 and EUI-64 addresses with the Local/Global bit zero [[RFC5342](#)] (referred to in [[RFC4291](#)] as the universal/local bit) are intended to represent unique identifiers for network connected equipment, notwithstanding many observed cases of duplication due to manufacturing errors, unauthorised use of OUIs, and address spoofing through configuration of network interfaces. Publication of EUI-48 or EUI-64 addresses in the DNS may result in privacy issues in the form of unique trackable identities that in some cases may be permanent.

For example, although IP addresses and DNS names for network devices typically change over time, EUI-48 and EUI-64 addresses configured on the same devices are normally far more stable (in many cases, effectively invariant). Publication of EUI-48 addresses associated with user devices in a way that could be mapped to assigned IP addresses would allow the behaviour of those users to be tracked by third parties, regardless of where and how the user's device is connected to the Internet. This might well result in a loss of privacy for the user.

The publication of EUI-48 or EUI-64 addresses associated with deployed equipment, using the mechanism described in this document or any other mechanism, has the potential to facilitate MAC cloning -- that is, facilitate link-layer attacks against deployed devices, e.g. to disrupt service or intercept data.

These concerns can be mitigated by restricting access to DNS zones containing EUI48 or EUI64 RRs to specific, authorised clients and by provisioning them in DNS zones that exist in private namespaces only.

This document recommends that EUI-48 or EUI-64 addresses SHOULD NOT be published in the public DNS.

[9.](#) Acknowledgements

The author acknowledges the contributions of Olafur Gudmundsson, Mark Smith, Andrew Sullivan, Roy Arends, Michael StJohns, Donald Eastlake III, Randy Bush and John Klensin.

[10.](#) References

[10.1.](#) Normative References

- [EUI48] IEEE, "Guidelines for use of a 48-bit Extended Unique Identifier (EUI-48)".
- [EUI64] IEEE, "Guidelines for use of a 64-bit Extended Unique Identifier (EUI-64)".
- [RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, [RFC 1034](#), November 1987.
- [RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, [RFC 1035](#), November 1987.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC5342] Eastlake, D., "IANA Considerations and IETF Protocol Usage for IEEE 802 Parameters", [BCP 141](#), [RFC 5342](#), September 2008.

[10.2.](#) Informative References

[NTRE038D]

CRTC Interconnection Steering Committee Network Working Group, "Implementation of IP Address Tracking in DOCSIS Networks (TIF18)", October 2006.

[10.3.](#) Informative References

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", [RFC 4291](#), February 2006.

Abley

Expires February 16, 2014

[Page 12]

Internet-Draft

Resource Records for EUI-48, EUI-64

August 2013

[Appendix A.](#) Editorial Notes

This section (and sub-sections) to be removed prior to publication.

[A.1.](#) RRTYPE Parameter Allocation Template

DNS RRTYPE PARAMETER ALLOCATION TEMPLATE

A. Submission Date: 2013-03-18

B.1 Submission Type: ☒ New RRTYPE ☐ Modification to RRTYPE

B.2 Kind of RR: ☒ Data RR ☐ Meta-RR

C. Contact Information for submitter (will be publicly posted):

Name: Joe Abley

Email Address: jabley@teksavvy.ca

International telephone number: +1 519 670 9327

Other contact handles:

D. Motivation for the new RRTYPE application.

The purpose of this RRTYPE application is to allow EUI-48 and EUI-64 addresses to be stored in the DNS. EUI-48 addresses are those used, for example, in ethernet.

E. Description of the proposed RR type.

See [draft-jabley-dnsext-eui48-eui64-rrtypes](#) for a full description.

F. What existing RRTYPE or RRTYPEs come closest to filling that need and why are they unsatisfactory?

The TXT record can be used to store arbitrary, unstructured data in the DNS and hence could be used to store EUI-48 and EUI-64 addresses. This approach is unsatisfactory for the usual reasons, i.e. there is no opportunity for validating data before it is stored, and typographical errors must consequently be detected after data retrieval.

G. What mnemonic is requested for the new RRTYPE (optional)?

EUI48 for EUI-48 addresses; EUI64 for EUI-64 addresses.

H. Does the requested RRTYPE make use of any existing IANA registry or require the creation of a new IANA sub-registry in DNS Parameters? If so, please indicate which registry is to be used or created. If a new sub-registry is needed, specify

the allocation policy for it and its initial contents. Also include what the modification procedures will be.

No.

I. Does the proposal require/expect any changes in DNS servers/resolvers that prevent the new type from being processed as an unknown RRTYPE (see [[RFC3597](#)])?

No.

J. Comments:

See [draft-jabley-dnsexst-eui48-eui64-rrtypes](#) for a complete specification.

[A.2.](#) Change History

- 00 Initial idea, circulated for the purposes of entertainment.
- 01 Presentation format changed from colon-separated to hyphen-separated, to better match conventional usage for big-endian representations of EUI-48 and EUI-64 addresses. IEEE trademarks acknowledged. Code-points assigned by expert review. Other minor tweaks and fixes based on early review.
- 02 Example EUI64 presentation format in text corrected (colons -> hyphens). Examples changed to use to-be-assigned addresses under the IANA OUI.
- 03 Example EUI48 and EUI64 addresses changed to match the guidance in [draft-eastlake-5342bis-00](#). "EUI48" corrected to "EUI64" in the text of [Section 4.1](#). Incorporated suggestions on DNS resolution and privacy considerations from Michael StJohns and Donald Eastlake III. Added example use case relating to Canadian DOCSIS networks.
- 04 Incorporated suggestions from John Klensin. Intended status changed to informational from standards track. Moved examples to a more sensible place.
- 05 Add emphasis that the publication of link-layer addresses in the DNS has potentially severe privacy implications, and is not recommended by this document. Recommend that publication of link-layer addresses in the public DNS should not happen at all. Various wordsmithing for the purposes of clarity.

- 06 Add text regarding MAC cloning in the Security Considerations section. Make text that mentions the "Global bit" more consistent with [\[RFC5342\]](#) and [\[RFC4291\]](#).

07 Make the "SHOULD NOT publish in the public DNS" recommendation stronger.

Author's Address

Joe Abley
TekSavvy Solutions, Inc.
470 Moore Street
London, ON N6C 2C2
Canada

Phone: +1 519 670 9327
Email: jabley@teksavvy.ca

Abley

Expires February 16, 2014

[Page 16]