          Resource Records for EUI-48 and EUI-64 Addresses in the DNS

Abstract

   48-bit Extended Unique Identifier (EUI-48) and 64-bit Extended Unique
   Identifier (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 EUI-48 or EUI-64 addresses SHOULD NOT be published in the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 document is not an Internet Standards Track specification; it is
   published for informational purposes.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Not all documents
   approved by the IESG are a candidate for any level of Internet
   Standard; see Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc7043.

Copyright Notice

Table of Contents

1. Introduction

   The Domain Name System (DNS) is described in [RFC1034] and [RFC1035].
   This base specification defines many resource record (RR) types, and
   subsequent specifications have defined others. Each defined RR type
   provides a means of encoding particular data in the DNS.

   48-bit Extended Unique Identifier (EUI-48) [EUI48] and 64-bit
   Extended Unique Identifier (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 RR types, 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   SHOULD NOT be published in the public DNS.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 capitalized keywords such as MUST and MAY to
   describe the requirements for using the registered RR types. 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
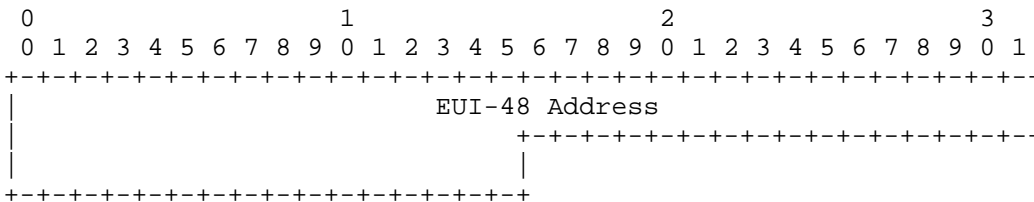   address in the DNS.

   The Type value for the EUI48 RR 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 Address
   field, encoded in network (big-endian) order.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                        EUI-48 Address                         |
   |                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                        EUI-64 Address                         |
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
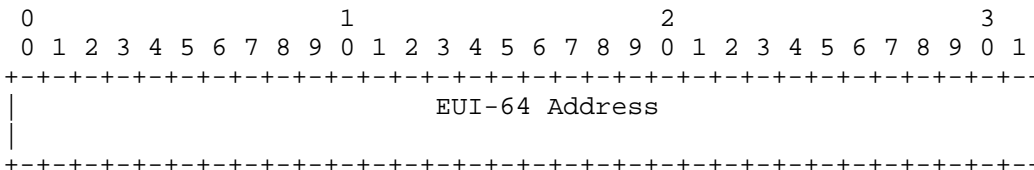
4.2. EUI64 RR Presentation Format

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

4.3. Example

   The following EUI64 RR stores the EUI-64 unicast address
   00-00-5e-ef-10-00-00-2a.

     host.example. 86400 IN EUI64 00-00-5e-ef-10-00-00-2a

5. Example Use Case: IP Address Tracking in DOCSIS Networks

   Canadian cable Internet subscribers are assigned IP addresses using
   DHCP, using a DHCP server operated by a cable company. In the case
   where a cable company provides last-mile connectivity to a subscriber
   on behalf of a third-party company (reseller), the DHCP server
   assigns addresses from a pool supplied by the reseller. The reseller
   retains knowledge of the EUI-48 address of the DOCSIS modem supplied
   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 that provides (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 an RR type 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.

6. DNS Protocol Considerations

   The specification of the new RR types in this document has no effect
   on the address resolution behavior 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 RR types should specify how any address conflicts or use of
   multiple EUI48/EUI64 RRs are handled.

7. IANA Considerations

   IANA has assigned the RR type value 108 (decimal) for EUI48 and 109
   (decimal) for EUI64. The corresponding entries in the "Resource
   Record (RR) TYPEs" subregistry (http://www.iana.org/assignments/
   dns-parameters/) 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 [RFC7042] (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, unauthorized use of
   Organizationally Unique Identifiers (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 behavior 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 Media Access
Control (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, authorized 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)",
               <http://standards.ieee.org/develop/regauth/tut/eui48.pdf>.

   [EUI64]   IEEE, "Guidelines for 64-bit Global Identifier (EUI-64)",
               November 2012,
               <http://standards.ieee.org/develop/regauth/tut/eui64.pdf>.

   [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.

   [RFC7042]   Eastlake 3rd, D. and J. Abley, "IANA Considerations and
               IETF Protocol and Documentation Usage for IEEE 802
               Parameters", BCP 141, RFC 7042, October 2013.

10.2. Informative References

   [NTRE038D]
             CRTC Interconnection Steering Committee (CISC) Network
             Working Group, "Implementation of IP Address Tracking in
             DOCSIS Networks (TIF18)", NTRE038D Consensus Report,
             October 2006,
             <http://www.crtc.gc.ca/public/cisc/nt/NTRE038D.doc>.

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

Author's Address

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

   Phone: +1 519 670 9327
   EMail: jabley@dyn.com