

## Записи RR в DNS для адресов EUI-48 и EUI-64

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

#### Аннотация

48-битовые идентификаторы EUI<sup>1</sup>-48 и 64-битовые EUI-64 представляют собой форматы адресов, заданных IEEE для использования в различных сетях L2, например, Ethernet.

В этом документе описаны два новых типа записей о ресурсах DNS - EUI48 и EUI64, служащие для представления адресов Ethernet в DNS.

В этом документе описаны потенциально важные последствия для конфиденциальности (приватности), которые могут возникнуть в результате неразборчивой публикации адресов канального уровня в DNS. Адреса EUI-48 и EUI-64 **не следует** публиковать в общедоступных DNS. Этот документ задаёт функционально совместимое представление этих типов адресов для использования в пространствах имён частных DNS, где проблемы конфиденциальности могут быть ограничены и смягчены.

#### Статус документа

Этот документ не является спецификацией Internet Standards Track и публикуется с информационными целями.

Документ является результатом работы IETF<sup>2</sup> и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG<sup>3</sup>. Дополнительную информацию о BCP можно найти в разделе 2 в RFC 5741.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке <http://www.rfc-editor.org/info/rfc7043>.

#### Авторские права

Авторские права (Copyright (c) 2013) принадлежат IETF Trust и лицам, указанным в качестве авторов документа. Все права защищены.

К документу применимы права и ограничения, указанные в BCP 78 и IETF Trust Legal Provisions и относящиеся к документам IETF (<http://trustee.ietf.org/license-info>), на момент публикации данного документа. Прочтите упомянутые документы внимательно. Фрагменты программного кода, включённые в этот документ, распространяются в соответствии с упрощённой лицензией BSD, как указано в параграфе 4.e документа IETF Trust Legal Provisions, без каких-либо гарантий (как указано в Simplified BSD License).

## Оглавление

1. Введение.....	1
2. Терминология.....	2
3. EUI48 RR.....	2
3.1. Формат передачи EUI48 RDATA.....	2
3.2. Формат представления EUI48 RR.....	2
3.3. Пример.....	2
4. EUI64 RR.....	2
4.1. Формат передачи EUI64 RDATA.....	2
4.2. Формат представления EUI64 RR.....	2
4.3. Пример.....	2
5. Пример использования - отслеживание адреса IP в сети DOCSIS.....	2
6. Протокол DNS.....	3
7. Взаимодействие с IANA.....	3
8. Вопросы безопасности.....	3
9. Благодарности.....	3
10. Литература.....	3
10.1. Нормативные документы.....	3
10.2. Дополнительная литература.....	4

## 1. Введение

Система доменных имён (DNS<sup>4</sup>) описана в [RFC1034] и [RFC1035]. Эти базовые спецификации определяют множество типов записей о ресурсах (RR<sup>5</sup>), а в последующих документах определены дополнительные типы. Каждый определённый тип RR обеспечивает способ представления в DNS неких конкретных данных.

<sup>1</sup>Extended Unique Identifier - расширенный уникальный идентификатор.

<sup>2</sup>Internet Engineering Task Force - комиссия по решению инженерных задач Internet.

<sup>3</sup>Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

<sup>4</sup>Domain Name System.

<sup>5</sup>Resource record.

Расширенные уникальные идентификаторы EUI-48 [EUI48] и EUI-64 [EUI64] представляют собой форматы адресов, заданные IEEE для использования в разных сетях L2, например Ethernet.

В этом документе определены два новых типа RR - EUI48 и EUI64, используемые для представления адресов EUI-48 и EUI-64 в DNS.

Возможны потенциально важные последствия для конфиденциальности (приватности) в результате неразборчивой публикации адресов канального уровня в DNS (раздел 8). В соответствии с этим документом адреса EUI-48 и EUI-64 **не следует** публиковать в DNS общего пользования. Документ задаёт функционально совместимое кодирование этих типов адресов для использования в пространствах имён частных DNS, где проблемы конфиденциальности могут быть ограничены и смягчены.

## 2. Терминология

В этом документе слова типа **должен** и **может** для описания требований к использованию зарегистрированных типов RR выделены шрифтом. Значение этих слов в данном документе совпадает с описанным в [RFC2119]. Хотя такое выделение обычно используется при задании нормативных требований в стандартах IETF, их использование в данном документе не предполагает, что документ задаёт какой-либо стандарт.

## 3. EUI48 RR

Запись о ресурсах EUI48 используется для хранения одного адреса EUI-48 в DNS.

Поле Type для EUI48 RR имеет значение 108 (десятичное).

Запись EUI48 RR не зависит от класса.

EUI48 RR не имеет специальных требований к сроку действия (TTL<sup>1</sup>).

### 3.1. Формат передачи EUI48 RDATA

RDATA для EUI48 RR состоит из одного 6-октетного поля Address, кодируемого с сетевым (big-endian) порядком.

```

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. Формат представления EUI48 RR

Поле Address **должно** представляться в форме 6 двухзначных шестнадцатеричных чисел, разделённых символами дефиса (hyphen). Шестнадцатеричные цифры от А до F **можно** указывать в любом регистре.

### 3.3. Пример

Приведённая ниже EUI48 RR содержит индивидуальный адрес EUI-48 со значением 00-00-5e-00-53-2a.

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

## 4. EUI64 RR

Запись о ресурсах EUI64 используется для хранения одного адреса EUI-64 в DNS.

Поле Type для EUI64 RR имеет значение 109 (десятичное).

Запись EUI64 RR не зависит от класса.

EUI64 RR не имеет специальных требований TTL.

### 4.1. Формат передачи EUI64 RDATA

RDATA для EUI64 RR состоит из одного 8-октетного поля Address, кодируемого с сетевым (big-endian) порядком.

```

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. Формат представления EUI64 RR

Поле Address **должно** представляться в форме 8 двухзначных шестнадцатеричных чисел, разделённых символами дефиса (hyphen). Шестнадцатеричные цифры от А до F **можно** указывать в любом регистре.

### 4.3. Пример

Приведённая ниже EUI64 RR содержит индивидуальный адрес EUI-64 со значением 00-00-5e-ef-10-00-00-2a.

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

## 5. Пример использования - отслеживание адреса IP в сети DOCSIS

Пользователи канадских кабельных сетей Internet получают адреса IP от сервера DHCP, обеспечиваемого кабельной компанией. В случаях когда кабельная компания обеспечивает соединения «последней мили» от имени другой

<sup>1</sup>Time-to-Live - время жизни.

компании (реселлера), сервер DHCP выдаёт адреса из пула, предоставленного реселлером. Реселлер имеет информацию об адресах EUI-48 модемов DOCSIS, предоставленных пользователям, но не имеет информации о выделенных им адресах IP. Для того, чтобы реселлер мог отображать выделенные пользователям адреса IP на адреса EUI-48 (и следовательно, отождествление абонентов), кабельная компания может предоставлять информацию от сервера DHCP, которая указывает отображение (EUI-48, IP).

Канадские кабельные компании должны [NTRE038D] делать это отображение адресов доступным через DNS. Зоны, содержащие соответствующую информацию, публикуются на серверах DNS, доступ к которым разрешён лишь реселлерам, соответствующим конкретным множествам абонентов. Информация об адресах абонентов не публикуется а общедоступных DNS.

Имеющиеся схемы DNS для представления отображений (EUI-48, IP), используемых канадскими кабельными компаниями, разнообразны и неэффективны. В отсутствие типа RR для прямого кодирования адресов EUI-48 адреса разными способами кодируются в имена владельцев и публикуются в записях TXT.

Представленная в этом документе спецификация облегчает более эффективное, согласованное и надёжное представление отображений (EUI-48, IP) по сравнению со всеми, доступными ранее.

## 6. Протокол DNS

Спецификация новых типов RR в этом документе не оказывает влияния на преобразование адресов в каких-либо имеющихся сетевых процессах или протоколах. Предложения или спецификации для изменения или дополнения процессов или протоколов преобразования адресов с помощью этих типов RR должны включать обнаружение и обслуживание всех адресных конфликтов или обработку использования множества EUI48/EUI64 RR.

## 7. Взаимодействие с IANA

Агентство IANA выделило тип RR со значением 108 (десятичное) для EUI48 и со значением 109 (десятичное) для EUI64. Соответствующие записи в субреестре Resource Record (RR) TYPEs (<http://www.iana.org/assignments/dns-parameters/>) содержат приведённые ниже данные.

Тип	Значение	Смысл	Документ
EUI48	108	адрес EUI-48	данный документ
EUI64	109	адрес EUI-64	данный документ

## 8. Вопросы безопасности

Существуют проблемы приватности при публикации адресов канального уровня в DNS. Адреса EUI-48 и EUI-64 со сброшенным (0) битом Local/Global [RFC7042] (в [RFC4291] этот бит называется universal/local) предназначены для представления уникальных идентификаторов подключённого к сети оборудования, несмотря на неоднократно отмеченные случаи дублирования в результате ошибок производителей, неправомерного использования идентификаторов OUI<sup>1</sup> и подмены адресов при настройке сетевых интерфейсов. Публикация адресов EUI-48 или EUI-64 в DNS может вызывать проблемы приватности за счёт появления уникальных отслеживаемых идентификаторов, которые в некоторых случаях могут быть постоянными.

Хотя адреса IP и имена DNS для сетевых устройств обычно меняются с течением времени, адреса EUI-48 и EUI-64 на тех же устройствах обычно более стабильны (во многих случаях просто неизменны). Публикация адресов EUI-48, связанных с пользовательскими устройствами, с возможностью сопоставить эти адреса с назначенными адресами IP позволит отслеживать поведение этих пользователей посторонними лицами независимо от места и способа подключения пользователя к Internet. Это может приводить к потере конфиденциальности (приватности) пользователя.

Публикация адресов EUI-48 или EUI-64, связанных с развёрнутым оборудованием, с помощью описанного здесь или иного механизма может способствовать клонированию MAC<sup>2</sup> и последующему упрощению организации на канальном уровне атак на подключённые устройства (например, для нарушения обслуживания или перехвата данных).

Эти проблемы можно смягчить за счёт ограничения доступа к зонам DNS, содержащим EUI48 или EUI64 RR, предоставляя его лишь уполномоченным клиентам и лишь в зонах DNS, существующих лишь в приватном пространстве имён.

В соответствии с рекомендациями этого документа адреса EUI-48 и EUI-64 **не следует** публиковать в DNS общего пользования.

## 9. Благодарности

Автор благодарит участников работы - Olafur Gudmundsson, Mark Smith, Andrew Sullivan, Roy Arends, Michael StJohns, Donald Eastlake III, Randy Bush, John Klensin.

## 10. Литература

### 10.1. Нормативные документы

[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.

<sup>1</sup>Organizationally Unique Identifier - уникальный идентификатор организации.

<sup>2</sup>Media Access Control - управление доступом к среде.

[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. Дополнительная литература

[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.

### Адрес автора

**Joe Abley**

Dyn, Inc.

470 Moore Street

London, ON N6C 2C2

Canada

Phone: +1 519 670 9327

EMail: [jabley@dyn.com](mailto:jabley@dyn.com)

### Перевод на русский язык

Николай Малых

[nmalykh@protokols.ru](mailto:nmalykh@protokols.ru)