Network Working Group
Request for Comments: 4361
Updates: 2131, 2132, 3315
Category: Standards Track

T. Lemon
Nominum
B. Sommerfield
Sun Microsystems

February 2006

Связанные с узлом идентификаторы клиентов для DHCPv4

Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)

Статус документа

Это документ содержит проект стандарта протокола Internet для сообщества Internet и служит приглашением к дискуссии в целях развития и совершенствования протокола. Текущее состояние стандартизации и статус протокола можно узнать из текущей версии документа Internet Official Protocol Standards (STD 1). Распространение документа не ограничивается.

Авторские права

Тезисы

В этом документе задан формат, который может использоваться для представления идентификаторов клиентов DHCPv4[1], которые будут взаимозаменяемыми с идентификаторами, используемыми в протоколе DHCPv6. Документ также рещает некоторые проблемы RFC 2131 и RFC 2132 в части обработки идентификаторов клиентов DHCP.

Оглавление

1. Введение

Этот документ задает способ, с помощью которого клиентам DHCPv4 [RFC2131] следует идентифицировать себя. Соответствующие данной спецификации клиенты DHCPv4 используют уникальный идентификатор DUID[2], как указано в спецификации DHCPv6 [RFC3315]. Значение DUID инкапсулируется в опцию идентификатора клиента DHCPv4 в соответствии с DHCP Options and BOOTP Vendor Extensions [RFC2132]. Описанное здесь поведение заменяет поведение, заданное в RFC2131 и RFC2132.

Причина внесения изменений заключается в том, что в процессе перехода от IPv4 к IPv6 некоторые сетевые устройства должны будут поддерживать сразу DHCPv4 и DHCPv6. Для пользователей таких устройств переход окажется более плавным, нежели в случае, когда устройства идентифицируют себя независимо используемой в данный момент версии DHCP. Наиболее очевидно, что обновления DNS, выполняемые сервером DHCP от имени клиента, будет обрабатываться более корректно. Изменение также решает некоторые проблемы ограничения при использовании идентификаторов клиентов DHCP в стиле RFC 2131/2132.

Документ является первым описанием решаемой проблемы и предлагает новый метод ее решения. Кроме того, описаны изменения, вносимые в RFC 2131 и RFC 2132 для снятия противоречий с данным документом.

2. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с RFC 2119 [RFC2119].

[1]Dynamic Host Configuration Protocol Version Four — протокол динамической настройки конфигурации хоста, версия 4.
[2]DHCP Unique Identifier.

3. Применимость

Этот документ обновляет RFC 2131 и RFC 2132, а также задает поведение, требуемое от клиентов DHCPv4 и DHCPv6, предназначенных для работы в конфигурации с двумя протоколами (dual-stack). Кроме того, документ рекомендует поведение для конфигураций хоста, где для полной настройки требуется последовательная работа нескольких клиентов DHCP (например, использование сетевого загрузчика, а затем загрузка операционной системы).

Клиенты и серверы DHCPv4, реализованные в соответствии с этим документом, должны вести себя так, будто изменения, заданные в параграфах 6.4 и 6.5[1], внесены в документы RFC 2131 и RFC 2132. Клиентам DHCPv4 дополнительно следует обеспечивать поведение, заданное в параграфе 6.1, а клиентам DHCPv6 — заданное в параграфе 6.2. Серверам DHCPv4 следует обеспечивать поведение, заданное в параграфе 6.3.

4. Постановка задачи

4.1. Непостоянные идентификаторы клиентов

RFC 2132 рекомендует создавать идентификаторы клиентов с использованием постоянного адреса канального уровня на сетевом интерфейсе, который клиент пытается настроить. Результатом этого является смена идентификатора клиента при замене в клиентском компьютере сетевого интерфейса. Клиент потеряет свой адрес IP и другие ресурсы, связанные с прежним идентификатором (например, доменное имя, получаемое от сервера DHCPv4).

4.2. Множество идентификаторов у клиента

Рассмотрим клиента DHCPv4 с двумя сетевыми интерфейсами, одним из которых связан с проводной сетью, второй — с беспроводной. Клиент DHCPv4 может потерпеть полную неудачу, а также настроить один или оба интерфейса. В соответствии с данной спецификацией каждый сетевой интерфейс будет получать свой адрес IP. Сервер DHCPv4 будет считать каждый сетевой интерфейс независимым клиентом DHCPv4 на полностью независимых хостах.

Таким образом, если клиент представляет некую информацию для обновления сетевой службы каталогов (например, имя DNS), для обоих интерфейсов будет представлена одна информация, но разные отождествления (идентификаторы). В результате один интерфейс получит имя, которое будет действовать в течение всего срока аренды (даже при потере соединения с сетью), а второй интерфейс имени не получит. В некоторых случаях это будет давать желаемый результат — при подключении единственного интерфейса будет публиковаться его адрес, в других случаях IP-адрес подключенного интерфейса не будет совпадать с опубликованным. При наличии двух интерфейсов иногда будет публиковаться корректный адрес, иногда - некорректный.

Вероятно будет возникать особая проблема с современными ноутбуками, имеющими проводной и беспроводный интерфейс Ethernet. Пользователь, находящийся вблизи розетки, может подключиться к проводной сети, поскольку она обеспечит защиту и более высокую скорость, но этот же пользователь может уйти от розетки и подключиться к беспроводной сети. Если при реализации такой схемы адрес проводного интерфейса будет одним из опубликованных, клиент будет виден другим хостам и они могут попытаться связаться с ним через проводную сеть, хотя в реальности этот клиент уже подключен через беспроводный интерфейс.

Другая распространенная ситуация дублирования идентификаторов возникает в тех случаях, когда монитор загрузки типа загрузчика PXE[2] задает один идентификатор клиента DHCP, а загруженная операционная система указывает иной идентификатор.

4.3. Несовместимость идентификаторов RFC 2131/2132 и RFC 3315

Опция client identifier используется клиентами и серверами DHCPv4 для обозначения клиентов. В некоторых случаях значение опции client identifier служит для управления доступом к ресурсам (например, для публикации доменного имени клиента через сервер DHCPv4). В RFC 2132 и RFC 3315 заданы разные методы создания идентификатора клиента. Эти методы гарантируют различие идентификаторов DHCPv4 и DHCPv6, что ведет к некорректной работе контроля доступа к ресурсам по идентификатору, если узел может настраиваться иной раз с использованием DHCPv4, другой — с DHCPv6.

4.4. RFC 2131 не требует использовать идентификатора клиента

RFC 2131 позволяет серверам DHCPv4 идентифицировать клиентов с помощью переданной клиентом опции client identifier или адреса канального уровня, если клиент не передал идентификатора. Как и формат идентификатора, рекомендуемый в RFC 2131, это связано с проблемами, описанными в параграфах 4.2 и 4.3.

5. Требования

Для решения проблем, описанных в разделе 4, идентификаторы клиентов DHCPv4 должны обладать перечисленными ниже характеристиками.

- Постоянство — идентификатор клиента должен сохраняться при удалении или добавлении компонент сетевого оборудования.
- Клиент должен иметь возможность указать наличие более одного сетевого идентификатора. Например, клиент с двумя сетевыми интерфейсами может указать серверу DHCPv4, что эти два интерфейса должны получить разные адреса IP в случае их подключения к одному каналу.
- В случае предоставления клиентом DHCPv4 более одного сетевого идентификатора сервер DHCPv4 должен иметь возможность определить их принадлежность одному хосту.
- В некоторых случаях для клиента DHCP желательно представлять один идентификатор для двух интерфесов, чтобы при подключении к одной сети оба интерфейса получали один адрес IP. В таких случаях клиенту должна обеспечиваться возможность представлять один и тот же идентификатор для каждого интерфейса.
- Серверы DHCPv4, которые не соответствуют данному документу, но соответствуют старой спецификации для идентификаторов клиента, должны корректно обрабатывать идентификаторы, отправленные клиентами, которые соответствуют данной спецификации.

[1] В оригинале ошибочно указаны параграфы 6.3 и 6.4. См. https://www.rfc-editor.org/errata/eid5424. *Прим. перев.*
[2] Pre-Boot Execution Environment — среда исполнения до загрузки.

- Серверы DHCPv4, соответствующие данной спецификации, должны корректно взаимодействовать с не соответствующими этом спецификации клиентами DHCPv4, за исключением того, что могут возникать проблемы, описанные в параграфе 4.2[1].
- Использование клиентами DHCPv4 поля chaddr в пакетах DHCPv4 в качестве идентификатора должно быть прекращено.
- Идентификаторы клиентов DHCPv4 на хостах с двойным стеком, которые используют также DHCPv6, должны указывать одну строку идентификации для DHCPv4 и DHCPv6. Например, сервер DHCPv4, использующий идентификатор клиента для обновления DNS от имени клиента DHCPv4, должен указывать этот же идентификатор клиента в DNS при регистрации через сервер DHCPv6 клиента DHCPv6 на том же хосте и наоборот.

Для выполнения всех этих требований (кроме последнего) нужно создать идентификатор клиента DHCPv4 из двух частей. Одна часть должна быть уникальной для хоста, а другая должна представлять собой уникальный сетевой идентификатор. Этим условиям удовлетворяют уникальный идентификатор DHCP (DUID) и идентификатор отождествления ассоциации (IAID[2]), заданные в RFC 3315.

Для выполнения последнего требования нужно использовать DUID для идентификации клиента DHCPv4. Поэтому с учетом всех требований идентификаторы DUID и IAID, описанные в RFC 3315 обеспечивают единственное возможное решение.

При выполнении этих правил соответствующий спецификации клиент DHCPv4 будет корректно взаимодействовать с серверами DHCPv4 независимо от их соответствия этой спецификации. Несоответствующие спецификации клиенты DHCPv4 также смогут взаимодействовать с поддерживающим спецификацию сервером DHCPv4. Если клиенты и сервер не соответствуют спецификации, цели этого документа не достигаются, но функциональность сохраняется.

6. Реализация

Здесь описаны изменения в поведении клиентов и серверов DHCPv4, а также указаны изменения по сравнению с RFC 2131 и RFC 2132. Клиенты, серверы и ретрансляторы DHCPv4, соответствующие данной спецификации, должны выполнять RFC 2131 и RFC 2132 с учетом изменений, указанных в параграфах 6.4 и 6.5[3].

6.1. Поведение клиента DHCPv4

Соответствующие спецификации клиенты DHCPv4 **должны** использовать стабильные идентификаторы узла DHCPv4 в опции dhcp-client-identifier. Клиентам DHCPv4 **недопустимо** использовать идентификаторы, основанные лишь на адресах канального уровня, жестко заданных в оборудовании (например, Ethernet MAC), как предложено в RFC 2131 за исключением случаев, разрешенных параграфом 9.2 в RFC 3315. Клиенты DHCPv4 **должны** передавать опцию client identifier с уникальным идентификатором IAID, как указано в разделе 10 RFC 3315 и DUID, определенным в разделе 9 RFC 3315. Вместе они образуют идентификатор привязки в стиле RFC 3315.

Базовый формат опции DHCPv4 client identifier определен в параграфе 9.14 RFC 2132.

Для передачи идентификатора привязки стиля RFC 3315 в опции DHCPv4 client identifier в поле типа опции client identifier указывается 255. За полем типа сразу следует 32-битовое (не анализируемое) значение IAID, а за ним — значение DUID, занимающее оставшуюся часть опции client identifier.

```
Code  Len  Type  IAID                DUID
+----+----+-----+----+----+----+----+----+----+---
| 61 | n  | 255 | i1 | i2 | i3 | i4 | d1 | d2 |...
+----+----+-----+----+----+----+----+----+----+---
```

Всем клиентам DHCPv4, которые соответствуют этой спецификации, **следует** обеспечивать способ, с помощью которого оператор может узнать выбранное клиентом значение DUID. Таким клиентам **следует** предоставлять оператору возможность настроить DUID. Устройствам, на которых обычно настроена оба клиента DHCPv4 и DHCPv6, **следует** автоматически использовать одно значение DUID для DHCPv4 и DHCPv6 без участия оператора.

Клиентам DHCPv4 с несколькими сетевыми интерфейсами **следует** использовать одно значение DUID для всех интерфейсов, при этом значения IAID **следует** делать разными.

Клиент DHCPv4, создающий значением DUID и имеющий стабильное хранилище, **должен** сохранять это значение для использования в последующих сообщениях DHCPv4 даже после перезагрузки.

6.2. Поведение клиента DHCPv6

Любому клиенту DHCPv6, соответствующему этой спецификации, **следует** обеспечивать способ, с помощью которого оператор может узнать выбранное клиентом значение DUID. Таким клиентам **следует** предоставлять оператору возможность настроить DUID. Устройствам, на которых обычно настроена оба клиента DHCPv4 и DHCPv6, **следует** автоматически использовать одно значение DUID для DHCPv4 и DHCPv6 без участия оператора.

6.3. Поведение сервера DHCPv4

Этот документ не требует менять поведение серверов DHCPv4 или DHCPv6, соответствующих RFC 2131 и RFC 2132. Однако некоторые серверы DHCPv4 могут быть настроены с отклонением от RFC 2131 и RFC 2132 в том смысле, что они будут игнорировать опцию client identifier и использовать вместо нее аппаратный адрес клиента.

Соответствующие этой спецификации серверы DHCPv4 **должны** использовать для идентификации клиента опцию client identifier, если клиент передает ее.

Серверы DHCPv4 **могут** использовать предоставленные администратором значения chaddr и htype для идентификации клиента, если администратор выделил клиенту фиксированный адрес IP, даже при указании клиентом опции client identifier. Это разрешено **лишь** в том случае, когда администратор сервера DHCPv4 предоставил значения для chaddr и htype, поскольку в такой ситуации при возникновении проблем администратор может исправить дело, удалив неверную информацию.

[1]В оригинале ошибочно указан раздел 2. См. https://www.rfc-editor.org/errata/eid5425. *Прим. перев.*
[2]Identity Association Identifier.
[3]В оригинале ошибочно указаны параграфы 6.3 и 6.4. См. https://www.rfc-editor.org/errata/eid5426. *Прим. перев.*

6.4. Изменения в RFC 2131

В разделе 2 RFC 2131 на странице 9[1] удаляется текст «это поле может содержать, например, аппаратный адрес, идентичный содержимому поля chaddr, или быть идентификатором другого типа (скажем, именем DNS)».

В параграфе 4.2 RFC 2131 текст «Клиент **может** явно предоставлять идентификатор в опции client identifier. В таких случаях клиент **должен** указывать этот же идентификатор во всех последующих сообщениях, а сервер **должен** использовать это значение для идентификации клиента. Если клиент не использует опцию client identifier, сервер **должен** использовать для идентификации клиента содержимое поля chaddr» заменяется словами «Клиент **должен** явно предоставить свой идентификатор с помощью опции client identifier. Клиент **должен** использовать одинаковую опцию client identifier во всех сообщениях».

В том же параграфе текст «Использование chaddr в качестве идентификатора клиента может приводить к неожиданным результатам, поскольку этот идентификатор может быть связан с аппаратным интерфейсом, который может перейти к другому клиенту. Некоторые сайты могут использовать в качестве client identifier серийный номер оборудования для предотвращения неожиданного изменения сетевого адреса клиента при переносе интерфейса в другой компьютер. В качестве client identifier может использоваться имя DNS для привязки аренды к имени, а не к оборудованию» заменяется текстом «Клиенту DHCP **недопустимо** опираться на поле chaddr для идентификации».

В параграфе 4.4.1 RFC 2131 текст «Клиент **может** включить в поле client identifier другой уникальный идентификатор» заменяется тестом «Клиент **должен** включить уникальный идентификатор».

В параграфе 3.1, пп. 4 и 6, параграфе 3.2 пп. 3 и 4, параграфе 4.3.1, где в RFC 2131 сказано, что chaddr можно использовать вместо опции client identifier, текст «или chaddr» и «chaddr или» удален.

Отметим, что внесенные изменения не отменяют обязанность сервера DHCPv4 использовать chaddr в качестве идентификатора, если клиент не передал опцию client identifier. Скорее они обязывают клиента, соответствующего данному документу, передавать опцию client identifier, не опираясь на chaddrдля идентификации. Серверы DHCPv4 **должны** использовать chaddr в качестве идентификатора в тех случаях, когда опция client identifier не была передана, для поддержки старых клиентов, которые не соответствуют этому документу.

6.5. Изменения в RFC 2132

В параграфе 9.14 абзац, начинающийся с «Идентификатор клиента **может** содержать» и следующий за ним абзац заменяются текстом «Идентификатор клиента состоит из поля типа, которое обычно имеет значение 255, за которым следует 4-байтовое поле IA_ID, а затем значение DUID для клиента в соответствии с определением раздела 9 в RFC 3315». Текст «, а минимальный размер составляет 2 октета» из следующего абзаца удаляется.

7. Клиенты DHCP при многоэтапной загрузке из сети

В некоторых случаях одно устройство может реально запускать последовательно более одного клиента DHCP в процессе загрузки операционной системы через сеть. В таких случаях на первом этапе загрузки может применяться иной идентификатор или у клиента совсем не будет идентификатора.

Результатом этого для протокола DHCPv4 будет представление разных идентификаторов на двух (иногда и больше) этапах загрузки. Сервер DHCPv4 при этом будет выделять для разных этапов загрузки разные адреса IP.

Некоторые серверы DHCP решают эту проблему для общего случая, когда в памяти PROM[2] не присутствует идентификатора клиента а клиент DHCP в операционной системе представляет идентификатор на основе аппаратного (MAC[3]) адреса сетевого интерфейса, трактуя оба случая как один идентификатор. Это предотвращает выделение двух адресов IP.

Соответствующий этому документу клиент DHCPv4 не использует идентификатор на базе MAC-адреса сетевого интерфейса, поскольку интерфейсы могут меняться. В результате соответствующие спецификации клиенты DHCPv4 не будут поддерживаться описанным выше решением и этом может быть важно для некоторых сайтов.

Мы не может представить решение этой проблемы в виде набора требований, поскольку обстоятельства, при которых проблема возникает, могут сильно меняться. Однако ниже приведены некоторые предложения.

Во-первых, клиентам DHCP в сетевых загрузчиках предлагается запрашивать краткосрочную аренду, чтобы адрес IP быстро освобождался. Таким клиентам следует передавать сообщение DHCPRELEASE серверу DHCP перед переходом на следующий этап процесса загрузки. Таким клиента следует обеспечивать для клиентов DHCP из операционной системы способ настройки DUID, используемого при последующих загрузках. Клиентам DHCP на финальной стадии загрузки следует по возможности задавать значение DUID, используемое в PROM.

Во-вторых, разработчикам клиентов DHCPv4, которые предполагается использовать только в конфигурации с многоэтапной загрузкой, где не предполагается сетевая загрузка с использованием DHCPv6 и MAC-адрес не может быть легко изменен, может не потребоваться реализация изменений, внесенных данной спецификацией. Такое допущение таит в себе некоторые опасности и первое предложение значительно лучше. Компромиссным решением может быть детектирование клиентом DHCP финальной стадии работы на устаревшем (унаследованном) оборудовании и использование в этом случае второго предложения, а в остальных - первого.

8. Вопросы безопасности

Этот документ не создает новых проблем безопасности. Возможность атак на протокол DHCPv4 рассмотрена в разделе 7 спецификации протокола DHCP [RFC2131] и документе «Authentication for DHCP Messages» [RFC3118]. Возможность атак на DHCPv6 рассмотрена в разделе 23 RFC 3315.

9. Литература

9.1. Нормативные документы

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[1]В переводе на сайте www.protocols.ru этот текст расположен на стр. 6. *Прим. перев.*
[2]Programmable Read Only Memory — программируемое постоянное запоминающее устройство.
[3]В оригинале ошибочно указан код аутентификации сообщения (https://www.rfc-editor.org/errata/eid3954). *Прим. перев.*

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

9.2. Дополнительная литература

[RFC3118] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 2001.

Адреса авторов

Ted Lemon
Nominum
2385 Bay Road
Redwood City, CA 94063 USA
Phone: +1 650 381 6000
EMail: mellon@nominum.com

Bill Sommerfeld
Sun Microsystems
1 Network Drive
Burlington, MA 01824
Phone: +1 781 442 3458
EMail: sommerfeld@sun.com

Перевод на русский язык

Николай Малых
nmalykh@gmail.com

Полное заявление авторских прав

Интеллектуальная собственность

Подтверждение

Финансирование функций RFC Editor обеспечено IASA[1].

[1]IETF Administrative Support Activity.