Internet Engineering Task Force (IETF)
Request for Comments: 8947
Category: Standards Track
ISSN: 2070-1721

B. Volz
Cisco
T. Mrugalski
ISC
CJ. Bernardos
UC3M

December 2020

Link-Layer Address Assignment Mechanism for DHCPv6

Механизм назначения адресов канального уровня для DHCPv6

Аннотация

В некоторых средах, например, в больших системах с виртуализацией, новые устройства создаются автоматически и адреса канального уровня могут устанавливаться для них автоматизированным способом. В больших системах при случайном распределении адресов могут возникать совершенно неприемлемые конфликты адресов, поэтому требуется механизм контролируемого назначения. В этом документе предложено расширение DHCPv6, которое позволяет создать расширяемую системы назначения адресов канального уровня с исключением недопустимых (например, выделенных производителям оборудования) или нежелательных адресов.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc8947.

Оглавление

[1] Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2] Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

1. Введение

Имеется несколько типов развертывания, где нужно инициализировать большое число устройств. Одним из них являются системы с большим числом создаваемых виртуальных машин (VM). Обычно новым экземплярам VM назначаются адреса канального уровня, но случайное назначение не обеспечивает нужной расширяемости в силу риска совпадения адресов (см. Приложение A.1 к [RFC4429]). Другой вариант связан с устройствами «Интернета вещей» (Internet of Things или IoT) [RFC7228]. Огромное число таких устройств может исчерпать глобальное пространство адресов IEEE OUI[1]. Хотя глобальная уникальность таких адресов обычно не требуется, нужно предотвращать конфликты адресов в рамках административного домена. Поэтому желательно иметь тот или иной механизм, который обеспечит в локальном масштабе уникальность адресов MAC[2].

В этом документе предложен новый механизм расширяющий DHCPv6 для распределения адресов канального уровня.

Поскольку протокол DHCPv6 [RFC8415] может распределять различные типы ресурсов (временные и постоянные адреса, префиксы и пр.) и имеет требуемую инфраструктуру для поддержки такого назначения (множество реализаций клиентов и серверов, инфраструктура развернутых ретрансляторов и вспомогательные решения, такие как как запрос аренды и аварийное переключение), он является подходящим кандидатом для решения задачи.

Хотя в документе описано решение, применимое к любому типу адресов канального уровня, некоторые детали связаны с 48-битовыми MAC-адресами IEEE 802 [IEEEStd802]. Документы для иных адресов могут быть созданы в будущем.

Комитет IEEE 802 изначально выделил половину пространства 48-битовых адресов MAC для локального применения (бит U/L[3] имеет значение 1). В 2017 г. IEEE была опубликована поправка [IEEEStd802c], разделяющая пространство адресов на квадранты с разными правилами, которые описаны в Приложении A.

В IEEE также разрабатываются протоколы и процедуры для назначения уникальных в локальном масштабе адресов (IEEE 802.1CQ). Эта работа может обеспечить дополнительный вариант назначения адресов. Дополнительную информацию можно найти в [IEEE-P802.1CQ-Project].

2. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

3. Терминология

В документе используются относящиеся к задаче термины DHCP из [RFC8415]. Ниже приведены определения терминов, которые отличаются от указанного документа или введены заново.

address - адрес
: Если явно не указано иное, это адрес канального уровня (MAC-адрес) [IEEEStd802]. Обычно адрес имеет размер 6 октетов, но иногда применяются другие размеры.

address block - блок адресов
: Множество последовательных адресов канального уровня. Блок указывается первым адресом и числом дополнительно выделяемых адресов. Один адрес можно представить блоком из этого адреса и 0 дополнительных.

client - клиент
: Узел, заинтересованный в получении адреса канального уровня. Он реализует базовые механизмы DHCP, описанные в [RFC8415], и поддерживает новые опции, заданные этим документом (IA_LL и LLADDR). Клиент может поддерживать назначение адресов IPv6 и делегирование префиксов в соответствии с [RFC8415].

IA_LL
: Identity Association для Link-Layer Address - ассоциация отождествления (IA - identity association), используемая для запроса или назначения адресов канального уровня (параграф 11.1).

LLADDR
: Опция адреса канального уровня, используемая для запроса или назначения блока адресов (параграф 11.2).

server - сервер
: Узел, который поддерживает назначение адресов канального уровня и способен отвечать на запросы клиентов. Узел реализует базовую функциональность сервера DHCP [RFC8415] и поддерживает новые опции, заданные этим документом (IA_LL и LLADDR). Сервер может поддерживать назначение адресов IPv6 и делегирование префиксов в соответствии с [RFC8415].

4. Варианты развертывания

Механизм предназначен на роль базового и приемлемого в разных системах, но имеется два основных варианта, где механизм пытается решить задачу назначения адресов - (i) режим прокси-клиента (proxy client) и (ii) режим прямого клиента (direct client).

4.1. Режим прокси-клиента

Этот режим применяется в тех случаях, когда выступающий клиентом DHCP элемент запрашивает у доступных серверов DHCP один или множество (блок) адресов для последующего распределения конечным устройствам. Большие системы с виртуализацией являются примером использования прокси-клиентов. В таких средах запрашивающий адреса элемент часто называется гипервизором и он зачастую нужен для создания новых VM, которым гипервизор должен назначать новые адреса. Гипервизор сам не использует полученные адреса, а распределяет их создаваемым VM. Следует отметить кумулятивных характер этого режима - гипервизор скорей всего будет позднее запрашивать дополнительные адреса. Адреса удаленных VM могут применяться для новых.

[1]Organizationally Unique Identifier - уникальный идентификатор организации.
[2]Media Access Control - управление доступом к среде.
[3]Universal/Local - универсальный или локальный адрес.

4.2. Режим прямого клиента

Этот режим применяется в тех случаях, когда выступающий клиентом DHCP элемент запрашивает у доступных серверов DHCP один или множество (блок) адресов для своих нужд. Этот вариант связан с IoT (раздел 1). При первой загрузке устройство использует для каждого интерфейса временный адрес, как описано в [IEEEStd802.11] и IEEE 802.1CQ [IEEE-P802.1CQ-Project], для отправки начальных пакетов DHCP доступным серверам DHCP, у которых клиент запрашивает 1 адрес для данного интерфейса. После получения такого адреса устройство отбрасывает (забывает) временный адрес и пользуется полученным (арендованным).

Отметим, что работающий в соответствии с приведенным описанием клиент не имеет глобально уникального адреса ни на одном из своих интерфейсов и ему **недопустимо** применять основанный на канальном уровне идентификатор DUID (DHCP Unique Identifier), описанный в разделе 11 [RFC8415]).

Кроме того, такой клиент может столкнуться с проблемами, если коммутатор, к которому он подключен, запрещает или ограничивает смену адресов канального уровня. Это может ограничивать применимость данного режима или потребовать от администратора изменить конфигурацию коммутатора, чтобы можно было менять адреса.

5. Обзор механизма

В описанных в разделе 4 вариантах протокол работает в основном одинаково. Устройство, запрашивающее адрес, действуя в качестве клиента DHCP, передает сообщение Solicit с опцией IA_LL всем доступным серверам DHCP. Эта опция IA_LL **должна** включать опцию LLADDR, указывающую link-layer-type и link-layer-len, а также может задавать желаемый адрес или блок в качестве совета серверу. Каждый из доступных серверов отвечает сообщением Reply с подтвержденными адресами (если было запрошено и выполнено Rapid Commit) или сообщением Advertise с предложенными адресами. Клиент выбирает отклик в соответствии с [RFC8415]. При необходимости клиент передает сообщение Request, по которому сервер назначит адреса и передаст их в сообщении Reply. После приема сообщения Reply клиент может начать использование полученных адресов.

Используются обычные механизмы DHCP. Предполагается, что клиент периодически обновляет адреса в соответствии с таймерами T1 и T2 и прекращает использовать адрес по истечении срока его действия. Обновление может быть запрещено сервером административно путем установки бесконечного значения (infinity) для таймеров T1 и T2 (см. параграф 7.7 в [RFC8415]). Администратор может сделать выделенные адреса постоянными, указав бесконечный (infinity) срок действия, как указано в параграфе 7.7 [RFC8415].

Клиент может освободить адреса, когда они не нужны, передав сообщение Release (см. параграф 18.2.7 в [RFC8415]).

На рисунке 9 в [RFC8415] показана временная диаграмма обмена сообщениями между клиентом и двумя серверами для типичного срока действия одной или нескольких аренд.

Сообщения Confirm и Information-request не применяются при назначении адресов канального уровня. Сообщение Decline технически требоваться не должно, но в разделе 12 описан случай, где такое сообщение требуется.

Использующим этот механизм клиентам **следует** задавать опцию Rapid Commit, как указано в параграфах 5.1 и 18.2.1 [RFC8415], для получения адресов в результате обмена лишь двумя сообщениями, когда это возможно.

Устройства, поддерживающие это предложение, **могут** поддерживать также механизм реконфигурации, описанный в параграфе 18.2.11 [RFC8415]. Если механизм реконфигурации поддерживается клиентом и сервером, он позволяет администратору своевременно уведомлять клиентов об изменении конфигурации и инициировать незамедлительное получение соответствующих изменений, не ожидая таймера T1. Поскольку для этого механизма нужна реализация протокола Reconfiguration Key Authentication (раздел 20.4 в [RFC8415]), мелкие устройства могут не поддерживать его.

6. Допущения

Одним из важных свойств механизма является его кумулятивная природа, особенно при работе с гипервизором. Отношения «клиент-сервер» не похожи на другие транзакции DHCP в сценарии с гипервизором. В типичной среде будет использоваться один сервер и небольшое (возможно 1) число гипервизоров. Однако с течением времени число запрашиваемых гипервизором адресов будет расти по мере создания VM.

Другим аспектом, важным для эффективного проектирования, является то, что один клиент-гипервизор вероятно будет использовать тысячи адресов. Подход, аналогичный применяемому при назначении адресов или префиксов IPv6 (контейнер IA со списком назначенных адресов, по одной записи на адрес), здесь работать не будет. Поэтому механизм должен работать не с отдельными адресами, а с их блоками. При этом отдельный адрес считается просто блоком с одним адресом.

Механизмы DHCP часто применяются многократно, в частности, используются одинаковые форматы сообщений и опций, механизмы передачи, инфраструктура ретрансляторов и пр. Однако устройствам, желающим лишь распределять адреса канального уровня, не обязательно полностью поддерживать DHCP. Иными словами, устройство может выделять лишь адреса канального уровня, не поддерживая назначение адресов или префиксов IPv6.

7. Представление информации

Клиент **должен** передавать опцию LLADDR, инкапсулированную в опцию IA_LL, для задания значений link-layer-type и link-layer-len. Для link-layer-type 1 (Ethernet) и 6 (IEEE 802 Networks) клиент устанавливает поле link-layer-address как показано ниже.

1. Все 0, если клиент не указывает начального адреса блока индивидуальных адресов. В таких адресах бит IEEE 802 individual/group имеет значение 0 (индивидуальный).
2. Любое другое значение указывате начальный адрес запрашиваемого блока.

Представление других link-layer-type может быть добавлено в новых RFC.

Клиент указывает в поле extra-addresses значение 0 (один адрес) или размер запрашиваемого блока минус 1.

Клиент **должен** установить valid-lifetime = 0 (сервер **должен** игнорировать это поле).

8. Запрос адреса

Адреса выделяются блоками с минимальным размером 1. Для запроса адресов клиент передает сообщение Solicit с опцией IA_LL, которая **должна** включать опцию LLADDR, как указано в разделе 7.

Сервер при получении опции IA_LL проверяет ее содержимое и может предложить адрес или адреса для каждой опции LLADDR в соответствии со своими правилами. Сервер **может** учитывать блок адресов, запрошенный клиентом в опции LLADDR. Однако сервер **может** игнорировать все или часть параметров, запрошенного блока адресов. В частности, сервер может выделить другой начальный адрес или меньшее число адресов в блоке. Сервер передает в ответ сообщение Advertise с опцией IA_LL, содержащей опцию LLADDR, которая указывает предложенные адреса. Если сервер не способен выделить адреса, он **должен** передать опцию IA_LL с опцией Status Code (см. параграф 21.13 в [RFC8415]), указывающей NoAddrsAvail.

Отметим, что сервер, не поддерживающий опцию IA_LL, будет игнорировать ее и не будет возвращать сообщение Advertise (и Reply). Передающий опции IA_LL клиент **должен** рассматривать это как возврат сервером статуса NoAddrsAvail для этих опций IA_LL.

Клиент ждет от доступных серверов отклики Advertise и выбирает один сервер, как указано в параграфе 18.2.9 [RFC8415]. Затем клиент передает сообщение Request с контейнером IA_LL, содержащим опцию LLADDR, скопированную из сообщения Advertise от выбранного сервера.

Клиент **должен** обрабатывать блок адресов из сообщения Advertise, а не тот, который он передавал в сообщении Solicit, и может учитывать предложенные адреса при выборе сообщения Advertise. Сервер может предложить меньшее число адресов или блок, отличающихся от запрошенного. Клиенту **недопустимо** использовать ресурсы, указанные в сообщении Advertise, для каких-либо целей, кроме выбора сервера и включения данных в сообщение Request для этого сервера. Доступные клиенту ресурсы будут возвращены в сообщении Reply.

При получении сообщения Request с контейнером опции IA_LL сервер выделяет запрошенные адреса в соответствии с настроенными на нем правилами. Сервер **может** выделить другой (или меньший) блок, нежели указано в сообщении Request. Затем сервер создает и отправляет клиенту сообщение Reply.

При получении сообщения Reply клиент анализирует контейнер опции IA_LL и может начать использование предоставленных адресов. Клиент **должен** заново запустить таймеры T1 и T2, используя значения из опции IA_LL.

Клиент **должен** использовать блоки адресов из сообщения Reply, которые могут быть меньше запрошенных или просто другими.

Клиент, включивший опцию Rapid Commit в сообщение Solicit, может получить ответное сообщение Reply и пропустить описанные выше этапы с сообщениями Advertise и Request (см. параграф 18.2.1 в [RFC8415]).

Клиенту, меняющему адрес канального уровня на своем интерфейсе, **следует** выполнять рекомендации параграфа 7.2.6 [RFC4861] для быстрого информирования своих соседей о новом адресе канального уровня.

9. Обновление адреса

Обновление адресов выполняется по обычной процедуре DHCP, описанной в параграфе 18.2.4 [RFC8415]. По завершении времени T1 клиент начинает отправку сообщений Renew с опцией IA_LL, содержащей опцию LLADDR для обновляемого блока адресов. Сервер отвечает сообщением Reply с обновленным блоком адресов. Серверу **недопустимо** сокращать или расширять блок адресов. Когда блок адресов назначен и имеет ненулевой срок действия, его размер, начальный и конечный адрес менять **недопустимо**.

Если запрашивающему клиенту нужны дополнительные адреса (например, гипервизору нужны адреса для новых VM), он **должен** отправить опцию IA_LL с другим идентификатором отождествления (IAID - Identity Association IDentifier) для создания другого «контейнера» с дополнительными адресами.

Если клиент не способен обновить адреса к моменту T2, он начинает передачу сообщений Rebind, как описано в параграфе 18.2.5 [RFC8415].

10. Освобождение адреса

Клиент может принять решение об освобождении выделенных ему адресов. Клиент **должен** освобождать выделенный блок целиком. Для освобождения блока клиент передает сообщение Release с опцией IA_LL, содержащей опцию LLADDR для освобождаемого блока адресов. Механизм передачи Release описан в параграфе 18.2.7 [RFC8415].

Отметим, что клиент, освобождающий свой адрес канального уровня, **должен** прекратить его использование до отправки сообщения Release (как указано в [RFC8415]) и для отправки сообщения Release клиент **должен** использовать иной адрес (например, тот, который применялся при инициировании DHCPv6 для получения выделенного адреса канального уровня).

11. Определения опций

В этом механизме используется подход, похожий на имеющиеся механизмы DHCP. Имеется контейнерная опция IA_LL с фактическими адресами в опциях LLADDR. Каждая опция LLADDR представляет блок адресов, который указывается начальным адресом и числом адресов.

11.1. Опция IA_LL

Опция IA_LL (Identity Association for Link-Layer Addresses[1]) служит для передачи параметров и адресных блоков, связанных с IA_LL. Формат опции показан на рисунке 1.

option-code

OPTION_IA_LL (138).

[1]Идентификационная ассоциация для адресов канального уровня.

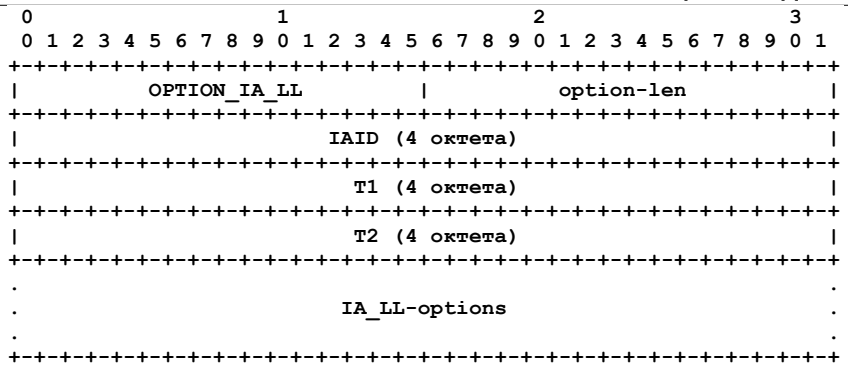

Рисунок 1. Формат опции IA_LL.

option-len
12 + размер поля IA_LL-options.

IAID
Уникальный идентификатор для данной опции IA_LL. Значение IAID должно быть уникальным среди всех IA_LL этого клиента. Пространство номеров для IA_LL IAID отделено от пространства номеров других типов опций IA (IA_NA, IA_TA и IA_PD). Выражается 4-октетным целым числом без знака.

T1
Временной интервал, по истечении которого клиенту следует контактировать с сервером, предоставившим адреса в IA_LL, для расширения срока их действия. T1 указывается в секундах относительно текущего времени 4-октетным целым числом без знака.

T2
Временной интервал, по истечении которого клиенту следует контактировать с любым доступным сервером для расширения срока действия адресов, назначенных в IA_LL. T2 указывается в секундах относительно текущего времени 4-октетным целым числом без знака.

IA_LL-options
Опции, связанные с данной опцией IA_LL. Поле имеет переменный размер (на 12 меньше значения option-len).

Опция IA_LL может указыватьмя лишь в области опций сообщения DHCP. Можно включать в сообщение DHCP несколько опций IA_LL, каждая из которых должна иметь уникальное значение IAID.

Статус операций, связанных с этой опцией IA_LL, указывается в опции Status Code (раздел 21.13 в [RFC8415]) поля IA_LL-options.

Отметим, что IA_LL не имеет явного срока действия (lifetime или lease length). Когда истекает срок действия всех адресов в IA_LL, можно считать IA_LL просроченной. Параметры T1 и T2 дают серверам явный контроль над повторными контактами клиента с сервером для конкретной опции IA_LL. В сообщении от клиента поля T1 и T2 **должны** иметь значение 0. Сервер **должен** игнорировать значения этих полей в сообщениях от клиентов. Клиент **должен** использовать значения полей T1 и T2 из сообщения от сервера для таймеров T1 и T2, если эти значения отличны от 0. Поля T1 и T2 указывают значения одноименных таймеров в секундах. В соответствии с разделом 7.7 [RFC8415], значение 0xffffffff указывает «бесконечный» (infinity) срок действия и должно применяться с осторожностью.

Сервер выбирает значения T1 и T2, чтобы позволить клиенту расширить срок действия блоков адресов в IA_LL, даже если сервер недоступен в течение короткого промежутка времени. Для T1 и T2 рекомендуются значения 0,5 и 0,8 от кратчайшего срока действия блока адресов в IA, который сервер желает продлить. Если «кратчайший» срок действия задан значением 0xffffffff (неограничен), для T1 и T2 также рекомендуется значение 0xffffffff. Если выбор времени обновления адресов в IA_LL следует оставить за клиентом, сервер устанавливает в T1 и T2 значение 0. Клиент **должен** следовать правилам, указанным в параграфе 14.2 [RFC8415].

Если клиент получает IA_LL с T1 > T2 > 0, он отбрасывает опцию IA_LL и обрабатывает остальное сообщение как будто в нем нет опции IA_LL.

Поле IA_LL-options обычно включает одну или множество опций LLADDR (см. раздел 11.2). Если клиент не включил опцию LLADDR в сообщение Solicit или Request, сервер **должен** считать это запросом одного адреса без рекомендованного клиентом значения.

11.2. Опция LLADDR

Опция адресов канального уровня (LLADDR - Link-Layer Addresses) служит для указания блока адресов, связанного с IA_LL. Опция должна инкапсулироваться в поле IA_LL-options опции IA_LL, включающее опции, относящиеся к данному блоку адресов. Формат опции показан на рисунке 2.

option-code
OPTION_LLADDR (139).

option-len
12 + значение поля link-layer-len + размер поля LLaddr-options. В предположении 6-битовых значений link-layer-address и отсутствия дополнительных опций поле option-len будет иметь значение 18.

link-layer-type
Поле link-layer-type **должно** указывать действительный тип оборудования, выделенный IANA, как описано в [RFC5494], и включенный в реестр Hardware Types, доступный по ссылке https://www.iana.org/assignments/arp-parameters. Значение является 2-октетным целым числом без знака.

link-layer-len
Задает размер поля link-layer-address в октетах (обычно 6 для link-layer-type = 1 (Ethernet) и 6 (IEEE 802 Networks)). Это поле включено с учетом канальных уровней, которые могут использовать адреса переменного размера. Значение является 2-октетным целым числом без знака.

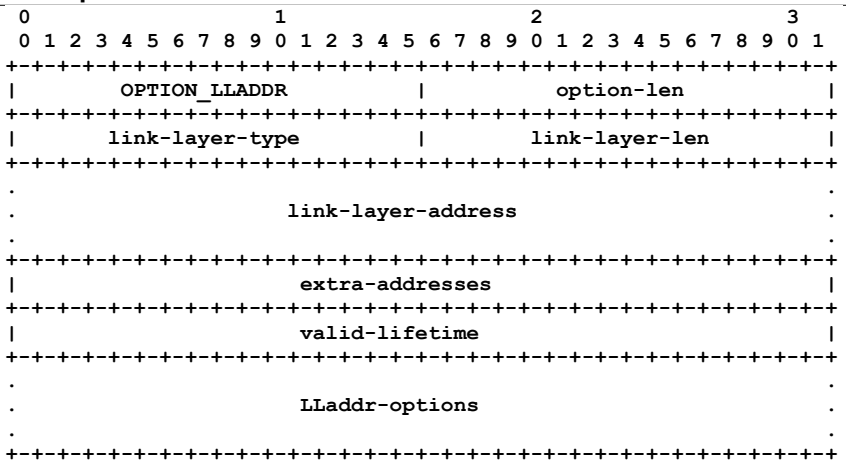

Рисунок 2. Формат опции LLADDR.

link-layer-address

Задает первый адрес канального уровня, который запрашивается или выделяется (в зависимости от сообщения). Клиент **может** передать специальное значение для запроса любого адреса. Для link-layer-type 1 и 6 подробности приведены в разделе 7. Поле имеет размер link-layer-len.

extra-addresses

Задает число дополнительных адресов, следующих за указанным полем link-layer-address. Для выделения одного адреса используется значение 0. Например, при указании link-layer-address 02:04:06:08:0a и extra-addresses 3 будет назначаться 4 адреса, начиная с 02:04:06:08:0a и заканчивая 02:04:06:08:0d (включительно). Значение является 4-октетным целым числом без знака.

valid-lifetime

Действительный срок действия для адресов в опции, указанный в секундах. Значение является 4-октетным целым числом без знака.

LLaddr-options

Любые инкапсулированные опции, связанные с этим конкретным блоком адресов. В настоящее время таких опций нет, но они могут быть определены в будущем.

В сообщении от клиента поле valid-lifetime **должно** иметь значение 0, сервер **должен** игнорировать значение поля.

Клиент **должен** использовать значение valid-lifetime из сообщения от сервера для установки срока действия блока адресов. Поле задает число секунд, в течение которого адреса блока будут действительны.

В соответствии с разделом 7.7 [RFC8415] valid-lifetime со значением 0xffffffff задает неограниченный срок действия адресов (infinity) и следует использовать это значение с осторожностью.

В опцию IA_LL можно включать более одной опции LLADDR.

12. Выбор адресов канального уровня для назначения IA_LL

Сервер выбирает адреса канального уровня для IA_LL в соответствии с правилами, заданными администратором и требованиями к пространству адресов.

Адреса канального уровня обычно зависят от типа соединения и серверу **следует** выполнять процедуры раздела 13.1 в [RFC8415] для определения типа клиентского канала.

Для адресов IEEE 802 MAC ([IEEEStd802] с дополнением [IEEEStd802c]) процедура выбора описана ниже.

1. Администратору сервера **следует** соблюдать спецификации IEEE 802 в части пулов индивидуальных адресов, доступных для назначения (см. Приложение A и [IEEEStd802c]). Распределять можно лишь адресное пространство, выделенное для локального использования, или при наличии полномочий назначать иные адреса.

2. Для серверов **недопустимо** позволять администратору настраивать пул адресов, который будет пересекать границу 2^{42} битов (для 48-битовых адресов MAC), чтобы предотвратить проблемы при изменении первого октета адреса и специальных битов в нем (Приложение A). Клиенты **должны** отвергать назначения, в которых блок пересекает эту границу (клиент **должен** отвергать назначение, см. параграф 18.2.8 в [RFC8415]).

3. Сервер **может** использовать опции, представленные ретранслятором или клиентом, для выбора квадранта (Приложение A), из которого будут назначаться адреса. Это **могут** быть опции из [RFC8948].

13. Взаимодействие с IANA

Агентство IANA выделило код опции OPTION_IA_LL (138) из субреестра Option Codes в реестре Dynamic Host Configuration Protocol for IPv6 (DHCPv6), доступном по ссылке http://www.iana.org/assignments/dhcpv6-parameters.

```
Value:        138
Description:  OPTION_IA_LL
Client ORO:   No
Singleton Option:  No
Reference:    RFC 8947
```

Агентство IANA выделило код опции OPTION_LLADDR (139) из субреестра Option Codes в реестре Dynamic Host Configuration Protocol for IPv6 (DHCPv6), доступном по ссылке http://www.iana.org/assignments/dhcpv6-parameters.

```
Value:        139
Description:  OPTION_LLADDR
Client ORO:   No
```

```
Singleton Option:  No
Reference:    RFC 8947
```

14. Вопросы безопасности

Вопросы безопасности DHCP рассмотрены в разделе 22 [RFC8415] и разделе 23 [RFC7227], для IPv6 -в [RFC8200].

В разделе 22 [RFC8415] отмечено:

> В DHCP отсутствует сквозное шифрование между клиентами и серверами, что открывает возможность для атак с захватом, подменой и прослушиванием трафика.

В некоторых средах можно обеспечить защиту на основе рекомендаций раздела 22 в [RFC8415].

Если не все узлы на канале используют этот механизм для получения адресов из пространства, выделенного серверу DHCP, возможно назначение одного адреса канального уровня нескольким устройствам. Отметим, что эта проблема будет присутствовать в таких сетях даже без использования DHCP для получения адресов.

Реализациям серверов **следует** рассмотреть использование опции конфигурации для ограничения числа выделяемых клиенту адресов (в одном запросе и в целом). Однако следует отметить, что это не помешает злоумышленнику притвориться разными клиентами для запроса всех доступных адресов.

15. Вопросы конфиденциальности

Вопросы конфиденциальности DHCP рассмотрены в разделе 23 [RFC8415].

Для клиента, запрашивающего адрес канального уровня напрямую у сервера, выделенный адрес скорей всего будет использован клиентом на этом канале и раскроется тем, кто может прослушивать канал. Партнеры по каналу, способные прослушивать обмен DHCP, могут также сопоставить выделенный адрес с отождествлением клиента (на основе DUID). Для повышения уровня анонимности могут применяться механизмы, подобные описанным в [RFC7844], которые минимизируют раскрытие информации.

Как отмечено в разделе 23 [RFC8415], серверам DHCP и гипервизорам может потребоваться учитывать влияние последовательного выделения адресов. Хотя в общем случае относится лишь к локальным соединениям в отличие от назначения адресов и префиксов IPv6, которые могут использоваться для коммуникаций через Internet.

16. Литература

16.1. Нормативные документы

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/info/rfc8415>.

16.2. Дополнительная литература

[IEEE-P802.1CQ-Project] IEEE, "P802.1CQ - Standard for Local and Metropolitan Area Networks: Multicast and Local Address Assignment", <https://standards.ieee.org/project/802_1CQ.html>.

[IEEEStd802] IEEE, "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture, IEEE Std 802", IEEE STD 802-2014, DOI 10.1109/IEEESTD.2014.6847097, <https://doi.org/10.1109/IEEESTD.2014.6847097>.

[IEEEStd802.11] IEEE, "IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11, DOI 10.1109/IEEESTD.2016.7786995, <https://doi.org/10.1109/IEEESTD.2016.7786995>.

[IEEEStd802c] IEEE, "IEEE Standard for Local and Metropolitan Area Networks:Overview and Architecture--Amendment 2: Local Medium Access Control (MAC) Address Usage", IEEE Std 802c-2017, DOI 10.1109/IEEESTD.2017.8016709, <https://doi.org/10.1109/IEEESTD.2017.8016709>.

[RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, DOI 10.17487/RFC2464, December 1998, <https://www.rfc-editor.org/info/rfc2464>.

[RFC4429] Moore, N., "Optimistic Duplicate Address Detection (DAD) for IPv6", RFC 4429, DOI 10.17487/RFC4429, April 2006, <https://www.rfc-editor.org/info/rfc4429>.

[RFC5494] Arkko, J. and C. Pignataro, "IANA Allocation Guidelines for the Address Resolution Protocol (ARP)", RFC 5494, DOI 10.17487/RFC5494, April 2009, <https://www.rfc-editor.org/info/rfc5494>.

[RFC7227] Hankins, D., Mrugalski, T., Siodelski, M., Jiang, S., and S. Krishnan, "Guidelines for Creating New DHCPv6 Options", BCP 187, RFC 7227, DOI 10.17487/RFC7227, May 2014, <https://www.rfc-editor.org/info/rfc7227>.

[RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, DOI 10.17487/RFC7228, May 2014, <https://www.rfc-editor.org/info/rfc7228>.

[RFC7844] Huitema, C., Mrugalski, T., and S. Krishnan, "Anonymity Profiles for DHCP Clients", RFC 7844, DOI 10.17487/RFC7844, May 2016, <https://www.rfc-editor.org/info/rfc7844>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[RFC8948] Bernardos, CJ. and A. Mourad, "Structured Local Address Plan (SLAP) Quadrant Selection Option for DHCPv6", RFC 8948, DOI 10.17487/RFC8948, December 2020, <https://www.rfc-editor.org/info/rfc8948>.

Приложение A. IEEE 802c

В этом приложении дана краткая сводка IEEE 802c [IEEEStd802c].

Исходная спецификация IEEE 802 выделяет половину 48-битового пространства MAC-адресов для локального использования. Эти адреса имеют установленный бит U/L (1) и администрируются локально без задания структуры.

В 2017 г. была выпущена спецификация IEEE Std 802c с определением необязательного плана структурированной локальной адресации (Structured Local Address Plan или SLAP), который задает разные подходы к четырем указанным областям пространства локальных адресов MAC. В соответствии с этим планом для 4 квадрантов SLAP заданы разные правила назначения адресов.

В первом (младшем) октете MAC-адреса биты Z и Y определяют квадрант для назначаемых локально адресов (бит X имеет значение 1). Представление IEEE для этих битов показано на рисунке 3

```
LSB                 MSB
M  X  Y  Z  -  -  -  -
|  |  |  |
|  |  |  +------------ SLAP бит Z
|  |  +--------------- SLAP бит Y
|  +------------------ бит X (U/L) = 1 для локальных адресов
+--------------------- бит M (I/G) (unicast/group)
```

Рисунок 3. Биты SLAP.

Квадранты SLAP описаны в таблице 1.

Таблица 1. Квадранты SLAP.

Квадрант	*Бит Y*	*Бит Z*	*Тип локального идентификатора*	*Локальный идентификатор*
01	0	1	Расширенный локальный идентификатор	ELI
11	1	1	Стандартное назначение	SAI
00	0	0	Административное назначение	AAI
10	1	0	Резерв	Резерв

MAC-адреса из квадранта расширенных локальных идентификаторов (Extended Local Identifier - ELI) основаны на идентификаторе компании (CID) размером 24 бита (включая M, X, Y, Z) для 48-битовых MAC-адресов. Это оставляет 24 бита для локального назначения с каждым идентификатором CID для индивидуальных (M = 0) и групповых (M = 1) адресов. Значения CID распределяются IEEE Registration Authority (RA).

MAC-адреса из квадранта стандартных идентификаторов (Standard Assigned Identifier - SAI) назначаются протоколом, заданным в стандарте IEEE 802. Для 48-битовых адресов MAC доступны 44 бита. Для назначения SAI в стандартах IEEE может быть задано множество протоколов. Сосуществование разных протоколов может поддерживаться за счет ограничения субпространства, доступного каждому протоколу.

MAC-адреса из квадранта административно выделяемых идентификаторов (Administratively Assigned Identifier - AAI) назначаются локально. Администраторы поддерживают пространство адресов по своему разумению. Отметим, что групповые пакеты IPv6 [RFC2464] используют адрес получателя, начинающийся с 33-33, поэтому адреса AAI не следует выделять из этого диапазона. Для 48-битовых MAC-адресов доступны 44 бита.

Последний квадрант зарезервирован на будущее. Хотя этот квадрант можно использовать аналогично пространству AAI, администраторам следует учитывать, что будущие спецификации могут задать иное использование адресов, что может привести к несовместимости.

Благодарности

Спасибо члена рабочей группы DHC за рецензирование документа, комментарии и поддержку. Отдельная благодарность Ian Farrer за внимательное рецензирование и помощь при прохождении процесса IETF. Спасибо также рецензентам от директората Samita Chakrabarti, Roni Even, Tianran Zhou и членам IESG Martin Duke, Benjamin Kaduk, Murray Kucherawy, Warren Kumari, Barry Leiba, Alvaro Retana, Éric Vyncke, Robert Wilton за их предложения. Спасибо Roger Marks, Robert Grow, Antonio de la Oliva за комментарии, относящиеся к работе IEEE, и ссылки.

Адреса авторов

Bernie Volz

Cisco Systems, Inc.

300 Beaver Brook Rd

Boxborough, MA 01719

United States of America

Email: volz@cisco.com

Tomek Mrugalski

Internet Systems Consortium, Inc.

PO Box 360

Newmarket, NH 03857

United States of America

Email: tomasz.mrugalski@gmail.com

Carlos J. Bernardos

Universidad Carlos III de Madrid

Av. Universidad, 30

28911 Leganes, Madrid

Spain

Phone: +34 91624 6236

Email: cjbc@it.uc3m.es

URI: http://www.it.uc3m.es/cjbc/

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru