Network Working Group
Request for Comments: 3315
Category: Standards Track

R. Droms, Ed.
Cisco
J. Bound
Hewlett Packard
B. Volz
Ericsson
T. Lemon
Nominum
C. Perkins
Nokia Research Center
M. Carney
Sun Microsystems

July 2003

Протокол динамической настройки хостов DHCPv6

Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

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

Аннотация

Протокол DHCP[1] для IPv6 позволяет серверам DHCP передавать параметры конфигурации типа сетевых адресов IPv6 узлам IPv6. Протокол обеспечивает возможность динамического выделения сетевых адресов многократного применения и дополнительную гибкость конфигурации. Этот протокол является учитывающим состояние двойником IPv6 Stateless Address Autoconfiguration (RFC 2462) и может использоваться вместе с ним или самостоятельно для получения конфигурационных параметров.

Оглавление

1. Введение и обзор....4
1.1. Протоколы и адресация....4
1.2. Обмен между клиентом и сервером в форме двух сообщений....4
1.3. Обмен между клиентом и сервером в форме четырех сообщений....4
2. Требования....4
3. Предпосылки....5
4. Терминология....5
4.1. Терминология IPv6....5
4.2. Терминология DHCP....6
5. Константы DHCP....6
5.1. Групповые адреса....6
5.2. Порты UDP....7
5.3. Типы сообщений DHCP....7
5.4. Коды состояний....7
5.5. Параметры передачи и повтора передачи....7
5.6 Представление значений времени и Infinity в качестве значения....8
6. Формат сообщений....8
7. Формат сообщений между серверами и ретрансляторами....8
7.1. Сообщение Relay-forward....9
7.2. Сообщение Relay-reply....9
8. Представление и использование доменных имен....9
9. Уникальный идентификатор DHCP (DUID)....9
9.1. Содержимое DUID....10
9.2. DUID на основе адреса канального уровня и времени [DUID-LLT]....10
9.3. DUID, заданный производителем на базе Enterprise Number [DUID-EN]....10
9.4. DUID на базе адреса канального уровня [DUID-LL]....11
10. Идентификационная ассоциация....11
11. Выбор адресов для назначения IA....11
12. Управление временными адресами....12
13. Передача сообщений клиентом....12

[1]Dynamic Host Configuration Protocol - протокол динамической настройки конфигурации хоста.

14. Надежность инициированного клиентом обмена сообщениями....12
15. Проверка пригодности сообщений....13
15.1. Использование идентификаторов транзакций....13
15.2. Сообщение Solicit....13
15.3. Сообщение Advertise....13
15.4. Сообщение Request....13
15.5. Сообщение Confirm....13
15.6. Сообщение Renew....13
15.7. Сообщение Rebind....13
15.8. Сообщение Decline....13
15.9. Сообщение Release....14
15.10. Сообщение Reply....14
15.11. Сообщение Reconfigure....14
15.12. Сообщение Information-request....14
15.13. Сообщение Relay-forward....14
15.14. Сообщение Relay-reply....14
16. Выбор клиентом адреса отправителя и интерфейса....14
17. Запрос сервера DHCP....15
17.1. Поведение клиента....15
17.1.1. Создание сообщений Solicit....15
17.1.2. Передача сообщений Solicit....15
17.1.3. Прием сообщений Advertise....16
17.1.4. Прием сообщений Reply....16
17.2. Поведение сервера....16
17.2.1. Прием сообщений Solicit....16
17.2.2. Создание и передача сообщений Advertise....16
17.2.3. Создание и передача сообщений Reply....17
18. Инициированный клиентом конфигурационный обмен DHCP....17
18.1. Поведение клиента....17
18.1.1. Создание и передача сообщений Request....17
18.1.2. Создание и передача сообщений Confirm....18
18.1.3. Создание и передача сообщений Renew....18
18.1.4. Создание и передача сообщений Rebind....19
18.1.5. Создание и передача сообщений Information-request....19
18.1.6. Создание и передача сообщений Release....19
18.1.7. Создание и передача сообщений Decline....20
18.1.8. Прием сообщений Reply....20
18.2. Поведение сервера....21
18.2.1. Прием сообщений Request....21
18.2.2. Прием сообщений Confirm....22
18.2.3. Прием сообщений Renew....22
18.2.4. Прием сообщений Rebind....22
18.2.5. Прием сообщений Information-request....22
18.2.6. Прием сообщений Release....23
18.2.7. Прием сообщений Decline....23
18.2.8. Передача сообщений Reply....23
19. Обмен сообщениями по инициативе сервера DHCP....23
19.1. Поведение сервера....23
19.1.1. Создание и передача сообщений Reconfigure....23
19.1.2. Тайм-аут и повтор сообщений Reconfigure....24
19.2. Прием сообщений Renew....24
19.3. Прием сообщений Information-request....24
19.4. Поведение клиента....24
19.4.1. Прием сообщений Reconfigure....24
19.4.2. Создание и передача сообщений Renew....24
19.4.3. Создание и передача сообщений Information-request....25
19.4.4. Тайм-аут и повтор для сообщения Renew и Information-request....25
19.4.5. Прием сообщений Reply....25
20. Поведение ретранслятора....25
20.1. Трансляция сообщений Client и Relay-forward....25
20.1.1. Трансляция сообщений от клиента....25
20.1.2. Трансляция сообщений от ретранслятора....25
20.2. Трансляция сообщений Relay-reply....25
20.3. Создание сообщений Relay-reply....25
21. Проверка подлинности сообщений DHCP....26
21.1. Защита сообщений между серверами и ретрансляторами....26
21.2. Проверка подлинности DHCP....27
21.3. Обнаружение повторного использования....27
21.4. Протокол отложенной аутентификации....27
21.4.1. Использование опции Authentication при отложенной аутентификации....27
21.4.2. Проверка пригодности сообщения....28
21.4.3. Использование ключей....28
21.4.4. Поведение клиента при отложенной аутентификации....28
21.4.4.1. Передача сообщений Solicit....28
21.4.4.2. Прием сообщений Advertise....28
21.4.4.3. Передача сообщений Request, Confirm, Renew, Rebind, Decline, Release....28
21.4.4.4. Передача сообщений Information-request....28

21.4.4.5. Прием сообщений Reply....28
21.4.4.6. Прием сообщений Reconfigure....28
21.4.5. Поведение сервера при отложенной аутентификации....28
21.4.5.1. Прием сообщений Solicit и отправка Advertise....29
21.4.5.2. Прием сообщений Request, Confirm, Renew, Rebind, Release и отправка Reply....29
21.5. Протокол проверки подлинности ключа реконфигурации....29
21.5.1. Опция Authentication в протоколе Reconfigure Key Authentication....29
21.5.2. Поведение сервера для протокола Reconfigure Key....29
21.5.3. Поведение клиента для протокола Reconfigure Key....29
22. Опции DHCP....30
22.1. Формат опций DHCP....30
22.2. Опция Client Identifier....30
22.3. Опция Server Identifier....30
22.4. Опция IA_NA....31
22.5. Опция IA_TA....31
22.6. Опция IA Address....32
22.7. Опция Option Request....33
22.8. Опция Preference....33
22.9. Опция Elapsed Time....33
22.10. Опция Relay Message....34
22.11. Опция Authentication....34
22.12. Опция Server Unicast....34
22.13. Опция Status Code....35
22.14. Опция Rapid Commit....35
22.15. Опция User Class....35
22.16. Опция Vendor Class....36
22.17. Опция Vendor-specific Information....36
22.18. Опция Interface-Id....37
22.19. Опция Reconfigure Message....38
22.20. Опция Reconfigure Accept....38
23. Вопросы безопасности....38
24. Взаимодействие с IANA....39
24.1. Групповые адреса....39
24.2. Типы сообщения DHCP....39
24.3. Опции DHCP....39
24.4. Коды состояний....40
24.5. DUID....40
25. Благодарности....40
26. Литература....40
26.1. Нормативные документы....40
26.2. Дополнительная литература....41
A. Опции в разных типах сообщений....41
B. Опции в поле Options опций DHCP....42
Адрес председателя....42
Адреса авторов....42
Полное заявление авторских прав....43

1. Введение и обзор

Этот документ описывает протокол DHCP для IPv6 (DHCP) - клиент-серверный протокол, обеспечивающий управляемую настройку конфигурации устройств.

DHCP может обеспечивать устройства адресами, выделенными сервером DHCP, и другими конфигурационными данными, которые передаются в опциях. Протокол DHCP поддерживает расширения путем определения новых опций для передачи информации, не заданной в этом документе.

DHCP является «протоколом автоматической настройки адресов с учетом состояния» и «протоколом автоматической настройки конфигурации с учетом состояния», как указано в документе IPv6 Stateless Address Autoconfiguration [17].

Операционные режимы и соответствующие конфигурационные данные для DHCPv4 [18][19] и DHCPv6 существенно различаются, поэтому объединение двух этих служб не рассматривается в данном документе. Если такая интеграция окажется достаточно интересной и востребованной, она может быть описана в отдельном документе, который расширит действие DHCPv6 для поддержки адресов и конфигурационных параметров IPv4.

В оставшейся части введения кратко описана работа DHCP, разъяснены механизмы обмена сообщениями и приведены примеры последовательностей сообщений. Последовательности сообщений в параграфах 1.2 и 1.3 предназначены для иллюстрации работы DHCP и не включают полный набор возможных взаимодействий между клиентами и серверами. Более подробное описание операций клиентов и серверов приведено в разделах 17 - 19.

1.1. Протоколы и адресация

Клиенты и серверы обмениваются сообщениями DHCP по протоколу UDP [15]. Клиент использует для передачи и приема сообщений DHCP локальный адрес (link-local) или адрес, определенный с помощью других механизмов.

Серверы DHCP получают сообщения от клиентов с использованием зарезервированного группового адреса, областью действия которого служит локальное соединение (link-scoped multicast). Клиент DHCP передает большинство сообщений по этому зарезервированному групповому адресу, поэтому на строне клиента адреса серверов DHCP не настраиваются.

Для того, чтобы клиент DHCP мог передавать сообщения серверу DHCP, подключенному к другому каналу, агент ретрансляции DHCP (relay agent) на канале клиента будет обеспечивать пересылку сообщений между клиентом и сервером. Работа ретранслятора не видна клиенту и рассмотрение обмена сообщениями между клиентами и серверами в оставшейся части этого раздела не включает описание трансляции сообщений.

После того, как клиент узнал адрес сервера, он может при выполнении некоторых условий отправлять сообщения серверу по его индивидуальному адресу.

1.2. Обмен между клиентом и сервером в форме двух сообщений

Когда клиенту DHCP не нужно получать от сервера DHCP свой адрес IP, клиент может получить конфигурационные данные типа списка доступных серверов DNS [20] или NTP [21] с помощью одного сообщения и отклика на него от сервера DHCP. Для получения конфигурационных параметров клиент сначала передает сообщение Information-Request по групповому адресу All_DHCP_Relay_Agents_and_Servers. Серверы отвечают сообщением Reply с конфигурационной информацией для клиента.

Такой обмен сообщениями предполагает, что клиенту нужна лишь конфигурационная информация и не требуется назначение адреса IPv6.

Когда у сервера имеются адреса IPv6 и другие конфигурационные данные для клиента, обмен между клиентом и сервером может ограничиться двумя сообщениями вместо 4, описанных в следующем параграфе. В этом случае клиент передает сообщение Solicit по адресу All_DHCP_Relay_Agents_and_Servers, запрашивая адрес и другие конфигурационные данные. Это сообщение включает индикацию готовности клиента сразу же принять сообщение Reply от сервера. Сервер, который готов сразу назначить клиенту адрес, отвечает сообщением Reply. Конфигурационные параметры и адреса из сообщения Reply готовы для их использования клиентом.

Каждый адрес, назначенный клиенту, имеет уровень предпочтения и срок допустимого использования, указанные сервером. Для запроса продолжения срока использования адреса клиент передает серверу сообщение Renew. Сервер в ответ передает сообщение Reply с новым сроком, позволяющее клиенту продолжить использование адреса без прерывания работы.

1.3. Обмен между клиентом и сервером в форме четырех сообщений

Для запроса назначения одного или более адресов IPv6 клиент сначала находит сервер DHCP а затем запрашивает выделение адресов и другую конфигурационную информацию у сервера. Клиент передает сообщение Solicit по адресу All_DHCP_Relay_Agents_and_Servers для поиска доступных серверов DHCP. Любой сервер, соответствующий требованиям клиента, отвечает сообщением Advertise. После этого клиент выбирает один из серверов и передает ему сообщение Request, прося подтвержденное назначение адресов и дугие данные конфигурации. Сервер отвечает сообщением Reply с подтвержденными адресами и конфигурацией.

Как указано в предыдущем параграфе, клиент передает серверу сообщение Renew для продления срока использования адресов, позволяющее клиенту продолжать работать с этими адресами без перерыва.

2. Требования

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 [1].

В этом документе также используются внутренние концептуальные переменные для описания поведения протокола и внешние переменные, которые реализация должна позволять изменять администратору. Конкретные имена

переменных, диапазоны значений и влияние на работу протокола приводятся для демонстрации поведения протокола. Реализации не обязаны точно соблюдать приведенные здесь формы, но внешнее поведение реализации должно совпадать с описанным в этом документе.

3. Предпосылки

Спецификация IPv6 описывает базовую архитектуру и устройство IPv6. Связанные с этим документы, которые помогут разработчикам, включают спецификацию IPv6 [3], архитектуру адресации IPv6 [5], автоматическую настройку IPv6 без учета состояния [17], обнаружение соседей IPv6 [13] и динамические обновления DNS [22]. Эти спецификации позволяют создать DHCP для работы в IPv6 с обеспечением отказоустойчивой настройки конфигурации с учетом состояния и автоматической регистрацией имен хостов в DNS.

Спецификация архитектуры адресации IPv6 [5] определяет область действия адресов, которые могут применяться в реализациях IPv6, и содержит архитектурные рекомендации для сетевых дизайнеров в части адресного пространства IPv6. Двумя преимуществами IPv6 являются необходимость поддержки групповой адресации и возможность выбора узлами локальных (link-local) адресов в процессе инициализации. Доступность этих возможностей означает, что клиент может использовать свой адрес link-local и общеизвестный групповой адрес для обнаружения серверов DHCP и ретрансляторов на локальном канале и взаимодействия с ними.

Автоматическая настройка адреса IPv6 без учета состояния [17] задает процедуры, с помощью которых узел может автоматически настроить адрес на основе анонсов маршрутизаторов [13] и использовать его в течение допустимого времени для поддержки смены адресов в Internet. В дополнение к этому заданы протокольные взаимодействия, с помощью которых узел начинает автоматическую настройку адреса с учетом или без учета состояния. DHCP является одним из способов автоматической настройки с учетом состояния. Совместимость с автоматической настройкой адресов без учета состояния заложена в DHCP.

Механизм IPv6 Neighbor Discovery [13] обеспечивает протокол обнаружения узлов IPv6 и используется взамен ARP [14]. Для понимания IPv6 и автоматической настройки адреса без учета состояния разработчикам настоятельно рекомендуется разобраться с обнаружением соседей IPv6.

Динамические обновления в DNS [22] обеспечивают поддержку динамического обновления записей DNS для IPv4 и IPv6. DHCP может использовать динамическое обновление DNS для объединения пространств имен и адресов не только с целью автоматической настройки, но и для автоматической регистрации в IPv6.

4. Терминология

В этом разделе даны определения используемых в документе терминов, относящихся к IPv6 и DHCP.

4.1. Терминология IPv6

Ниже приведены относящиеся к этой спецификации термины IPv6 из спецификации протокола IPv6 [3], архитектуры адресации IPv6 [5] и автоматической настройки адресов IPv6 без учета состояния [17].

address - адрес
: Идентификатор уровня IP для интерфейса или набора интерфейсов.

host - хост
: Любой узел, не являющийся маршрутизатором.

IP
: Протокол Internet версии 6 (IPv6). Термины IPv4 и IPv6 используются лишь в тех случаях когда требуется указать конкретную версию протокола.

interface - интерфейс
: Подключение узла к каналу.

link – канал, соединение
: Линия связи или среда, через которую узлы могут взаимодействовать на канальном уровне (уровень, непосредственно ниже IP). Примерами являются Ethernet (простая сеть или с мостами), Token Ring, каналы PPP, сети X.25, Frame Relay или ATM, туннели уровня Internet (или выше) типа туннелей IPv4 или IPv6.

link-layer identifier – идентификатор канального уровня
: Идентификатор интерфейса на канальном уровне. Примеры включают адреса IEEE 802 для сетевых интерфейсов Ethernet и Token Ring, а также адреса E.164 для каналов ISDN.

link-local address – локальный адрес
: Адрес IPv6, имеющий локальную значимость, указываемую префиксом FE80::/10. Может применяться для взаимодействия с соседями, подключенными к тому же каналу. Адрес link-local имеет каждый интерфейс.

multicast address – групповой адрес
: Идентификатор набора интерфейсов (обычно относящихся к разным узлам). Переданный по групповому адресу пакет доставляется всем интерфейсам, идентифицируемым таким адресом.

neighbor - сосед
: Узел, подключенный к тому же каналу.

node - узел
: Устройство, реализующее IP.

packet - пакет
: Заголовок IP и данные (payload).

prefix - префикс
: Начальные биты адреса или набор адресов IP, начальные биты которых совпадают.

prefix length – размер префикса
: Число битов в префиксе.

router - маршрутизатор
: Узел, которые пересылает пакеты, не адресованные явно ему.

unicast address – индивидуальный адрес
: Идентификатор одного интерфейса. Пакет, переданный по индивидуальному адресу, доставляется только одному интерфейсу.

4.2. Терминология DHCP

Ниже приведены определения терминов, связанных с DHCP.

appropriate to the link – подходящий для канала адрес
Адрес считается подходящим для канала, если он согласуется с представлением сервера DHCP о сетевой топологии, а также правилах назначения префикса и адресов.

binding - привязка
Привязка (привязка клиента) является группой записей сервера, содержащей информацию, которую сервер имеет об адресах в IA или конфигурационных параметров, явно выделенных клиенту. Конфигурационная информация, возвращаемая клиенту в соответствии с правилами (например, информация, возвращаемая всем клиентам, подключенным к одному каналу), не требует привязки. Привязка с информацией об IA индексируется триплетом <DUID, IA-type, IAID> (IA-type - тип адреса в IA, например, временный). Привязка с конфигурационной информацией для клиента индексируется значением <DUID>.

configuration parameter – конфигурационный параметр
Элемент конфигурационной информации, заданный на сервере и возвращаемый клиенту с использованием DHCP. Такие параметры могут служить, например, для переноса информации, используемой узлом для настройки своей сетевой подсистемы и активизации сетевых коммуникаций.

DHCP
Протокол динамической настройки конфигурации хоста для IPv6. В тех случаях, когда нужно различать версии, используются термины DHCPv4 и DHCPv6.

DHCP client (client) – клиент DHCP (клиент)
Узел, инициирующий запрос через канал для получения конфигурационных параметров от одного или нескольких серверов DHCP.

DHCP domain - домен DHCP
Набор каналов, управляемых DHCP и обслуживаемых одним административным органом.

DHCP realm – область (сфера действия) DHCP
Имя, используемое для идентификации административного домена DHCP, из которого был выбран ключ аутентификации DHCP.

DHCP relay agent (relay agent) – ретранслятор DHCP (ретранслятор)
Узел, выступающий посредником при обмене сообщениями DHCP между клиентами и серверами, который находится на одном канале с клиентом.

DHCP server (server) – сервер DHCP (сервер)
Узел, отвечающий на запросы клиентов. Может находится на одном или разных каналах с клиентами.

DUID
Уникальный идентификатор DHCP для участника DHCP. Каждый клиент и сервер DHCP имеет единственное значение DUID. Способы генерации значений DUID рассмотрены в разделе 9.

Identity association (IA) – идентификационная ассоциация
Набор адресов, назначенных клиенту. Каждая ассоциация IA имеет свой идентификатор IAID. Клиент может иметь несколько IA (например, для каждого интерфейса).
Каждая ассоциация IA содержит один тип адресов, например, ассоциация для временных адресов (IA_TA) содержит выделенные на ограниченное время адреса (см. identity association for temporary addresses). В этом документе термин IA служит для обозначения идентификационных ассоциаций без указания типа адресов в них.

Identity association identifier (IAID) – идентификатор IA
Идентификатор для ассоциации IA, выбранный клиентом. Каждая ассоциация IA имеет идентификатор IAID, который выбирается так, чтобы обеспечивалась уникальность всех IAID для относящихся к клиенту ассоциаций IA.

Identity association for non-temporary addresses (IA_NA) – IA для адресов, не являющихся временными
Ассоциация IA, содержащая адреса, которые не являются временными (см. identity association for temporary addresses).

Identity association for temporary addresses (IA_TA) – IA для временных адресов
Ассоциация IA, содержащая временные адреса (см. RFC 3041 [12]).

message - сообщение
Модуль данных, передаваемый в качестве данных (payload) дейтаграммы UDP, для обмена информацией между серверами DHCP, ретрансляторами и клиентами.

Reconfigure key – ключ Reconfigure
Ключ, представляемый клиенту сервером для защиты сообщений Reconfigure.

relaying - ретрансляция
Ретранслятор DHCP (relay agent) транслирует сообщения DHCP между участниками процесса DHCP.

transaction ID – идентификатор транзакции
Неинтерпретируемое (opaque) значение, служащее запросов с откликами.

5. Константы DHCP

В этом разделе описаны различные программные и сетевые константы, используемые DHCP.

5.1. Групповые адреса

DHCP использует перечисленные ниже групповые адреса.

All_DHCP_Relay_Agents_and_Servers (FF02::1:2) – все серверы и ретрансляторы DHCP
Групповой адрес, действующий в рамках канала (link-scope) и используемый клиентами для коммуникаций с соседними (подключенными к тому же каналу) ретрансляторами и серверами. Все серверы и трансляторы являются членами этой multicast-группы.

All_DHCP_Servers (FF05::1:3) – все серверы DHCP
Групповой адрес, действующий в рамках канала (link-scope) и используемый ретрансляторами для коммуникаций с серверами по причине того, что ретранслятор хочет передавать сообщения всем серверам или просто не знает индивидуальных адресов серверов. Отметим, что для использования этого адреса ретранслятором последний должен иметь адрес с зоной действия, доступной всем серверам. Все серверы сайта являются членами этой multicast-группы.

5.2. Порты UDP

Клиент прослушивают сообщения DHCP на порту UDP 546, серверы и ретрансляторы - на порту UDP 547.

5.3. Типы сообщений DHCP

DHCP определяет перечисленные ниже типы сообщений. Более подробные описания этих сообщений приведены в разделах 6 и 7. Не указанные здесь типы сообщений зарезервированы для использования в будущем. Номера сообщений приведены в скобках.

SOLICIT (1)
Клиент передает сообщение Solicit для поиска серверов.

ADVERTISE (2)
Сервер передает сообщение Advertise для индикации доступности сервиса DHCP в ответ на сообщение Solicit от клиента.

REQUEST (3)
Клиент передает сообщение Request для запроса конфигурационных параметров (включая адрес IP) от конкретного сервера.

CONFIRM (4)
Клиент передает сообщение Confirm любому доступному серверу для определения пригодности назначенного ему адреса на канале, к которому этот клиент подключен.

RENEW (5)
Клиент передает сообщение Renew серверу, который ранее предоставил ему адрес и конфигурационные параметры, для продления срока использования адреса и обновления параметров конфигурации.

REBIND (6)
Клиент передает сообщение Rebind любому доступному серверу для продления срока действия выделенного ему адреса и обновления своих конфигурационных параметров. Это сообщение передается после того, как не будет получено отклика на сообщение Renew.

REPLY (7)
Сервер передает сообщение Reply с назначенным клиенту адресом и конфигурационными параметрами в ответ на сообщение Solicit, Request, Renew или Rebind от клиента. Сервер передает сообщение Reply с конфигурационными параметрами в ответ на сообщение Information-request. Сервер передает сообщение Reply в ответ на сообщение Confirm, подтверждая или отвергая пригодность назначенного клиенту адреса для канала, к которому подключен клиент. Сервер передает сообщение Reply для подтверждения приема сообщения Release или Decline.

RELEASE (8)
Клиент передает сообщение Release серверу, назначившему для него адрес, для информирования о том, что он прекратит использование одного или нескольких назначенных ему адресов.

DECLINE (9)
Клиент передает сообщение Decline серверу для индикации того, что один или несколько назначенных клиенту этим сервером адресов уже используются на канале, к которому подключен клиент.

RECONFIGURE (10)
Сервер передает сообщение Reconfigure клиенту для информирования того о наличии у сервера новых или обновленных параметров конфигурации и необходимости инициировать транзакцию Renew/Reply или Information-request/Reply с сервером для получения обновленной информации.

INFORMATION-REQUEST (11)
Клиент передает сообщение Information-request серверу для запроса параметров конфигурации без назначения адреса IP.

RELAY-FORW (12)
Ретранслятор передает сообщение Relay-forward для трансляции сообщений серверам напрямую или через другой ретранслятор. Полученное от клиента сообщение или сообщение Relay-forward от другого ретранслятора инкапсулируется в опцию сообщения Relay-forward.

RELAY-REPL (13)
Сервер передает сообщение Relay-reply ретранслятору для доставки клиенту. Сообщение Relay-reply может доставляться клиенту напрямую или через другой ретранслятор.
Сервер инкапсулирует сообщение для клиента в опцию сообщения Relay-reply, которую ретранслятор извлекает и транслирует клиенту.

5.4. Коды состояний

DHCPv6 использует коды состояний для индикации успеха или отказа операций, запрошенных в сообщениях от клиента или сервера, а также передачи дополнительных данных о конкретной причине отказа. Конкретные коды состояний описаны в параграфе 24.4.

5.5. Параметры передачи и повтора передачи

В этом параграфе представлена таблица значений, используемых для описания поведения клиентов и серверов при передаче сообщений.

Параметр	*Значение по умолчанию*	*Описание*
`SOL_MAX_DELAY`	1 сек.	Максимальная задержка первого сообщения Solicit.
`SOL_TIMEOUT`	1 сек.	Первоначальный тайм-аут для сообщения Solicit.
`SOL_MAX_RT`	120 сек.	Максимальное значение тайм-аута для сообщения Solicit.
`REQ_TIMEOUT`	1 сек.	Первоначальный тайм-аут для сообщения Request.
`REQ_MAX_RT`	30 сек.	Максимальное значение тайм-аута для сообщения Request.
`REQ_MAX_RC`	10	Максимальное число повторов сообщения Request.

CNF_MAX_DELAY	1 сек.	Максимальная задержка первого сообщения Confirm.
CNF_TIMEOUT	1 сек.	Первоначальный тайм-аут для сообщения Confirm.
CNF_MAX_RT	4 сек.	Максимальное значение тайм-аута для сообщения Confirm.
CNF_MAX_RD	10 сек.	Максимальная продолжительность для сообщения Confirm.
REN_TIMEOUT	10 сек.	Первоначальный тайм-аут для сообщения Renew.
REN_MAX_RT	600 сек.	Максимальное значение тайм-аута для сообщения Renew.
REB_TIMEOUT	10 сек.	Первоначальный тайм-аут для сообщения Rebind.
REB_MAX_RT	600 сек.	Максимальное значение тайм-аута для сообщения Rebind.
INF_MAX_DELAY	1 сек.	Максимальная задержка первого сообщения Information-request.
INF_TIMEOUT	1 сек.	Первоначальный тайм-аут для сообщения Information-request.
INF_MAX_RT	120 сек.	Максимальное значение тайм-аута для сообщения Information-request.
REL_TIMEOUT	1 сек.	Первоначальный тайм-аут для сообщения Release.
REL_MAX_RC	5	Максимальное число повторов сообщения Release.
DEC_TIMEOUT	1 сек.	Первоначальный тайм-аут для сообщения Decline.
DEC_MAX_RC	5	Максимальное число повторов сообщения Decline.
REC_TIMEOUT	2 сек.	Первоначальный тайм-аут для сообщения Reconfigure.
REC_MAX_RC	8	Максимальное число повторов сообщения Reconfigure.
HOP_COUNT_LIMIT	32	Максимальное число интервалов в сообщении Relay-forward.

5.6 Представление значений времени и Infinity в качестве значения

Все значения времени для срока действия, T1 и T2 являются целыми числами без знака. Значение 0xffffffff означает неограниченное время (infinity - бесконечность) для срока действия (как в RFC2461 [17]), T1 или T2.

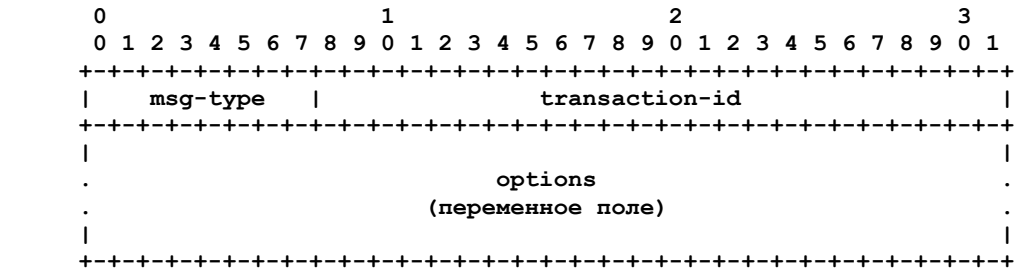
6. Формат сообщений

Во всех сообщениях DHCP между клиентами и серверами используется общий фиксированный формат заголовка и область опций с переменным форматом.

Во всех значениях полей заголовка и опций используется сетевой порядок байтов.

Опции размещаются последовательно в поле options без использования заполнений между ними. Опции выравниваются по границе байта, но не выравниваются по 2-х или 4-байтовым границам.

Ниже показан формат сообщений DHCP передаваемых между клиентами и серверами.



msg-type

Указывает тип сообщения DHCP (см. параграф 5.3).

transaction-id

Идентификатор транзакции, к которой относится сообщение.

options

Опции, передаваемые в сообщении (см. раздел 22).

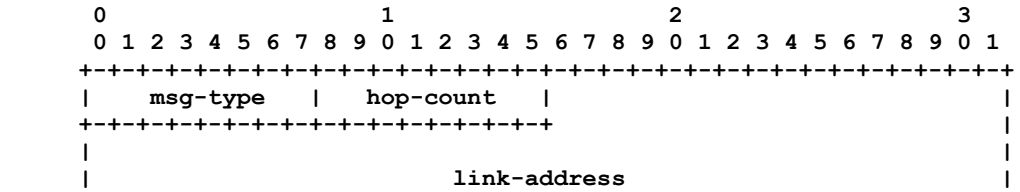
7. Формат сообщений между серверами и ретрансляторами

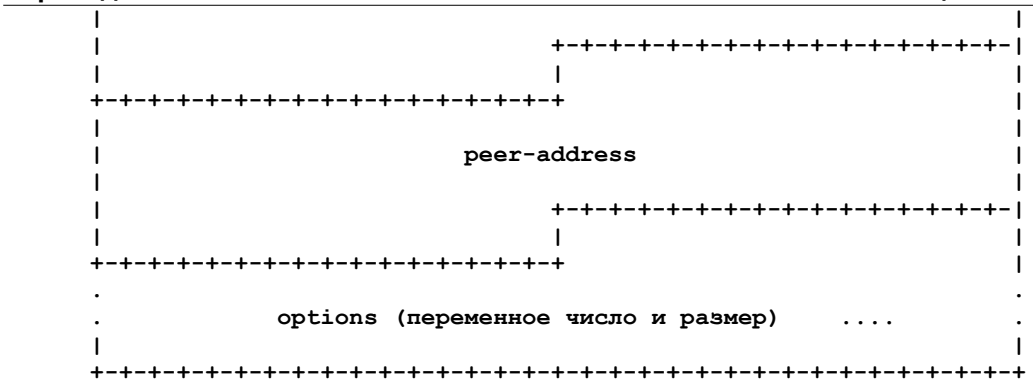
Ретрансляторы обмениваются сообщениями с сервером для трансляции сообщения между клиентами и серверами, подключенными к разным каналам.

Все значения в заголовке сообщений используют сетевой порядок байтов.

Опции размещаются последовательно в поле options без использования заполнений между ними. Опции выравниваются по границе байта, но не выравниваются по 2-х или 4-байтовым границам.

Имеется два типа сообщений ретрансляторов, имеющих одинаковый формат.





Использование заголовков сообщений Relay Agent.

7.1. Сообщение Relay-forward

Ниже описаны поля сообщений Relay-forward.

msg-type
RELAY-FORW

hop-count
Число ретрансляторов, транслировавших это сообщение.

link-address
Глобальный или локальный для сайта адрес, который будет использоваться сервером для идентификации канала, на котором находится клиент.

peer-address
Адрес клиента или ретранслятора, с которого было получено транслируемое сообщение.

options
Это поле **должно** включать опцию Relay Message (параграф 22.10) и **может** включать опции, добавленные ретранслятором.

7.2. Сообщение Relay-reply

Ниже описаны поля сообщений Relay-reply.

msg-type
RELAY-REPL

hop-count
Копируется из сообщения Relay-forward.

link-address
Копируется из сообщения Relay-forward.

peer-address
Копируется из сообщения Relay-forward.

options
Это поле **должно** включать опцию Relay Message (параграф 22.10) и **может** включать другие опции.

8. Представление и использование доменных имен

Для обеспечения однотипного представления доменных имен или их списков используется метод кодирования, описанный в параграфе 3.1 RFC 1035 [10]. Доменные имена и их списки в DHCP **недопустимо** сохранять в сжатой форме, как описано в параграфе 4.1.4 RFC 1035.

9. Уникальный идентификатор DHCP (DUID)

Каждый клиент и сервер DHCP имеет идентификатор DUID. Серверы DHCP используют DUID для идентификации клиентов с целью выбора параметров конфигурации и связанных с клиентами IA. Клиенты DHCP используют DUID для указания сервера в сообщениях, где это требуется. Представление DUID в сообщениях DHCP описано в параграфах 22.2 и 22.3.

Клиенты и серверы **должны** считать DUID не интерпретируемыми значениями и **должны** лишь проверять совпадение DUID. Клиентам и серверам **недопустимо** придавать значениям DUID какой-либо смысл. Клиентам и серверам **недопустимо** ограничивать DUID типами, определенными в этом документе, поскольку в будущем могут быть определены новые типы DUID.

Идентификаторы DUID передаются в опциях, поскольку их размер может меняться и они не требуются в некоторых сообщениях DHCP. Значения DUID должны быть уникальными для всех клиентов и серверов DHCP и стабильными для любого клиента и сервера, т. е. идентификатор DUID, используемый клиентом или сервером, не следует менять с течением времени, если это возможно (например, не следует менять DUID устройства в результате замены его сетевого оборудования).

Мотивация использования множества типов DUID связана с необходимостью обеспечить уникальность DUID в глобальном масштабе и простоту генерации идентификаторов. Типы уникальных в глобальном масштабе идентификаторов, которые легко создать для любого данного устройства, могут достаточно сильно различаться. Некоторые устройства могут не иметь постоянного хранилища. Хранить сгенерированный идентификатор DUID в таком устройстве невозможно поэтому схема DUID должна быть приспособлена для таких устройств.

9.1. Содержимое DUID

DUID состоит из двухоктетного кода типа, представленного в сетевом порядке байтов, за которым следует переменное число октетов действительного идентификатора. DUID может иметь размер не более 128 октетов (без учета кода типа). Ниже перечислены определенные в этом документе типы.

1 адрес канального уровня и время;

2 заданный производителем уникальный идентификатор на основе Enterprise Number;

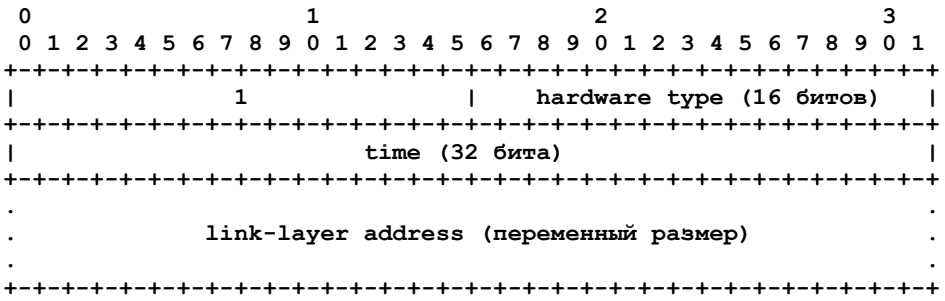
3 адрес канального уровня.

Форматы переменный полей каждого из этих типов DUID описаны ниже.

9.2. DUID на основе адреса канального уровня и времени [DUID-LLT]

Этот тип DUID включает 2-октетное поле типа со значением 1, два октета типа оборудования, четыре октета времени и адрес канального уровня одного (любого) из сетевых интерфейсов, подключенных к устройству DHCP в момент генерации DUID. Значение времени указывает момент генерации DUID в секундах после полуночи 1 января 200 года в часовом поясе UTC по модулю 2^{32}. Поле типа оборудования должно содержать корректное значение, выделенное IANA, как описано в RFC 826 [14]. Время и тип оборудования представляются в сетевом порядке байтов, адрес канального уровня указывается в канонической форме, как описано в RFC 2464 [2].

Формат DUID-LLT представлен на рисунке.



Выбор сетевого интерфейса может быть совершенно произвольным, если интерфейс имеет уникальный в глобальном масштабе адрес канального уровня для этого типа канала. **Следует** использовать одно значение DUID-LLT для настройки всех сетевых интерфейсов устройства, независимо от того, чей адрес был использован при генерации DUID-LLT.

Клиенты и серверы, использующие этот тип DUID, **должны** записать DUID-LLT в стабильное хранилище и **должны** продолжать использование этого DUID-LLT даже при удалении интерфейса, адрес которого применялся для генерации DUID-LLT. Клиентам и серверам без стабильного хранилища **недопустимо** применять этот тип DUID.

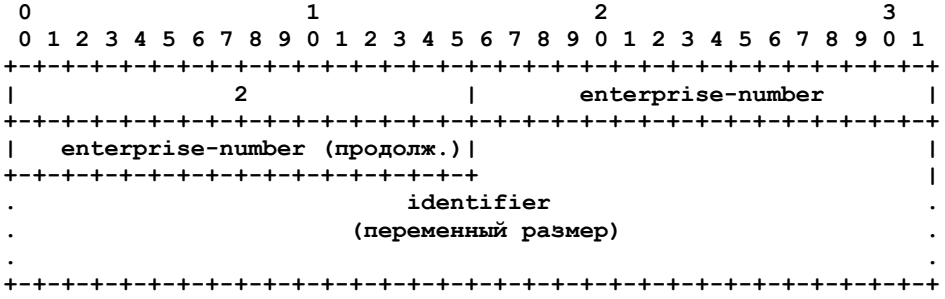
Клиентам и серверами с таким DUID **следует** пытаться настроить время до генерации DUID, если это возможно, и они **должны** использовать некий тип источника времени (например, встроенные часы устройства) при генерации DUID, даже если этот источник не был настроен до создания DUID. Использование источника времени делает маловероятным создание двух идентичных DUID-LLT, если сетевой интерфейс будет удален из клиентского устройства и использован другим клиентом для генерации DUID-LLT. Вероятность совпадения DUID-LLT будет очень мала даже в том случае, когда часы не были настроены до генерации DUID.

Этот метод создания DUID рекомендуется для всех компьютерных устройств общего назначения типа настольных и переносных компьютеров, а также принтеров, маршрутизаторов и т. п., которые имеют тот или иной тип энергонезависимой памяти с возможностью записи в нее.

Несмотря на усилия разработчиков, этот алгоритм генерации DUID может приводить к совпадению идентификаторов. Клиент DHCP, создающий DUID-LLT с помощью этого механизма, **должен** обеспечивать административный интерфейс для замены имеющегося идентификатора DUID созданным заново DUID-LLT.

9.3. DUID, заданный производителем на базе Enterprise Number [DUID-EN]

Этот вариант DUID назначается производителем устройства и состоит из зарегистрированного производителем значения Private Enterprise Number из реестра IANA [6], за которым следует заданное производителем уникальное значение. Ниже приведен формат идентификатора DUID-EN.



Выбор источника значений поля identifier остается за производителем, но значения identifier в каждом DUID-EN **должны** быть уникальными и **должны** задаваться при создании устройства и записываться в его энергонезависимую память. Созданный идентификатор DUID **следует** записывать в хранилище, не позволяющее его удалить. Поле enterprise-number содержит зарегистрированное производителем значение Private Enterprise Number из реестра IANA [6]. Значение enterprise-number представляет собой 32-битовое целое число без знака.

Пример DUID этого типа показан ниже.

```
+---+---+---+---+---+---+---+---+
| 0 | 2 | 0 | 0 | 0 |  9| 12|192|
+---+---+---+---+---+---+---+---+
|132|211| 3 | 0 | 9 | 18|
+---+---+---+---+---+---+
```

Этот пример включает 2-октетное поле типа со значением 2, поле Enterprise Number (9) и 8 октетов данных идентификатора (0x0CC084D303000912).

9.4. DUID на базе адреса канального уровня [DUID-LL]

Этот тип DUID содержит двухоктетный идентификатор типа со значением 3, два октета кода типа оборудования и адрес канального уровня любого сетевого интерфейса, постоянно присутствующего на клиентском или серверном устройстве. Например, хосту с сетевым интерфейсом, реализованным в микросхеме, вероятность удаления которой весьма мала, следует использовать DUID-LL. Поле hardware type **должно** содержать корректный идентификатор типа, выделенный IANA, как описано в RFC 826 [14]. Тип оборудования указывается с сетевым порядком байтов. Адрес канального уровня задается в канонической форме, как описано в RFC 2464 [2]. Ниже приведен формат DUID-LL.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               3               |    hardware type (16 битов)   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
.                                                               .
.             link-layer address (переменный размер)           .
.                                                               .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Выбор сетевого интерфейса может быть совершенно произвольным, если интерфейс имеет уникальный адрес канального уровня и интерфейс постоянно присутствует на устройстве, где создается DUID-LL. **Следует** использовать одно значение DUID-LL для настройки всех сетевых интерфейсов устройства, независимо от того, чей адрес был использован при генерации DUID.

DUID-LL рекомендуется для устройств, имеющих постоянно присутствующий сетевой интерфейс с адресом канального уровня и не имеющих энергонезависимой памяти для записи идентификатора. DUID-LL **недопустимо** применять на клиентах и серверах DHCP, которые не могут сказать постоянно ли присутствует у них сетевой интерфейс.

10. Идентификационная ассоциация

Идентификационная ассоциация (IA) представляет собой конструкцию, с помощью которой сервер и клиент могут указывать, группировать и управлять набором связанных адресов IPv6. Каждая ассоциация IA содержит идентификатор IAID и соответствующие конфигурационные данные.

Клиент должен связать хотя бы одну отличающуюся от других IA с каждым сетевым интерфейсом, для которого он запрашивает назначение адреса IPv6 у сервера DHCP. Клиент использует IA связанные с интерфейсами для получения от сервера конфигурационных данных для этого интерфейса. Каждая ассоциация IA должна быть связана только с одним интерфейсом.

Идентификатор IAID однозначно указывает IA и должен отличаться от всех других IAID того же клиента. Значения IAID выбираются клиентом. Для каждой используемой клиентом ассоциации IA идентификатор IAID этой IA **должен** сохраняться согласованным при перезапуске клиента DHCP. Клиент может обеспечивать согласованность путем записи IAID в энергонезависимое хранилище или использования алгоритма, создающего постоянное же значение IAID, пока сохраняется конфигурация клиента. У клиента может не оказаться возможности обеспечить согласованность IAID, если у него нет энергонезависимой памяти и аппаратная конфигурация клиента изменилась.

Конфигурационная информация в IA содержит один или множество адресов IPv6 с временами T1 и T2 для IA. Представление IA в сообщениях DHCP описано в параграфе 22.4.

Каждый адрес в IA имеет предпочтительный и действительный срок действия, как определено в RFC 2462 [17]. Сроки действия передаются от сервера DHCP клиенту в опции IA. Эти сроки применимы к использованию адресов IPv6, как описано в параграфе 5.5.4 RFC 2462.

11. Выбор адресов для назначения IA

Сервер выбирает адреса для назначения IA в соответствии с правилами распределения адресов, заданными сетевым администратором, и конкретной информацией, которую сервер получает о клиенте из перечисленных ниже источников.

- Канал, к которому подключен клиент. Сервер определяет канал, как описано ниже.
  - Если сервер получил сообщение от клиента напрямую и адрес отправителя в содержащей сообщение дейтаграмме IP является локальным (link-local), клиент подключен к тому же каналу, что и принявший сообщение интерфейс сервера.
  - Если сервер получил сообщение через ретранслятор, клиент подключен к тому же каналу, что и интерфейс, указанный адресом канального уровня в сообщении от ретранслятора.
  - Если сервер получил сообщение от клиента напрямую и адрес отправителя в содержащей сообщение дейтаграмме IP не является локальным (link-local), клиент подключен к каналу, указанному адресом отправителя дейтаграммы IP (отметим, что это возможно лишь в случаях, когда сервер разрешает использовать индивидуальную адресацию сообщений и клиент передал сообщение по разрешенному индивидуальному адресу).
- Идентификатор DUID, представленный клиентом.

- Другая информация и опции, представленные клиентом.
- Другая информация и опции, представленные ретранслятором.

Любой назначенный сервером адрес, который основан на идентификаторе EUI-64, **должен** включать идентификатор интерфейса с битами u (universal/local) и g (individual/group), установленными в соответствии с параграфом 2.5.1 RFC 2373 [5].

Серверу **недопустимо** назначать для клиента адрес, зарезервированный для другой цели. Например, недопустимо назначать зарезервированный адрес anycast (RFC 2526) из любой подсети.

12. Управление временными адресами

Клиент может запросить назначение временных адресов (см. определение в RFC 3041 [12]). Обслуживание DHCPv6 для временных адресов не имеет каких-либо отличий. DHCPv6 ничего не говорит о деталях временных адресов типа срока их действия, способа использования клиентом, правил генерации последующих временных адресов и пр.

Клиенты запрашивают временные адреса и серверы назначают их. Временные адреса передаются в опции Identity Association for Temporary Addresses (IA_TA), описанной в параграфе 22.5. Каждая опция IA_TA содержит не более одного временного адреса для каждого из префиксов канала, к которому подключен клиент.

Пространство значений IAID для опции IA_TA отделено от пространства IAID для опции IA_NA.

Сервер **может** обновлять DNS для временных адресов, как описано в разделе 4 RFC 3041.

13. Передача сообщений клиентом

Если в этом документе или в документе описывающем передачу IPv6 для конкретного типа канала (для каналов безгрупповой адресации), клиент передает сообщения DHCP по адресу All_DHCP_Relay_Agents_and_Servers.

Глиент использует групповую адресацию для доступа ко всем серверам или отдельному серверу. Отдельный сервер указывается значением DUID в опции Server Identifier (раздел 22.3) клиентского сообщения (это сообщений получат все серверы, но ответит лишь указанный). Для обращения ко всем серверам эта опция не указывается.

Клиент может передавать некоторые сообщения напрямую серверу по его индивидуальному адресу, как описано в параграфе 22.12.

14. Надежность инициированного клиентом обмена сообщениями

Клиенты DHCP отвечают за надежную доставку сообщений в инициированных ими обменах, описанных в разделах 17 и 18. Если клиент DHCP не получает ожидаемого ответа от сервера, он должен повторить передачу сообщения. В этом параграфе описана стратегия повторов, используемая клиентами в инициированных ими обменах сообщениями.

Отметим, что описанная в этом параграфе процедура слегка отличается для сообщений Solicit (см. параграф 17.1.2).

Клиент начинает обмен сообщениями с передачи сообщения серверу. Обмен завершается, когда клиент получает от сервера все нужные отклики или констатируется отказ в соответствии с описанным ниже механизмом повтора.

Поведение клиента при повторе передачи описывается и управляется перечисленными ниже переменными.

RT	тайм-аут повтора.
IRT	первоначальное время повтора.
MRC	максимальное число повторов.
MRT	максимальное время повторения.
MRD	максимальная продолжительность повторов.
RAND	фактор случайности.

При каждом повторе передачи клиент устанавливает RT в соответствии с приведенными ниже правилами. Если RT истекает до завершения обмена сообщениями, клиент заново рассчитывает RT и повторяет сообщение.

Каждый из расчетов нового значения RT включает фактор случайности (RAND), который представляет собой случайное значение из интервала от -0,1 до +0,1. Случайное отклонение добавляется для предотвращения синхронной передачи сообщений клиентами DHCP.

Алгоритм выбора случайного значения не требуется делать криптографическим. Алгоритму **следует** выдавать разные последовательности случайных значений при каждом вызове клиента DHCP.

RT для первого повтора рассчитывается на основе IRT

```
RT = IRT + RAND*IRT
```

RT для каждого последующего повтора вычисляется на основе предыдущего значения RT

```
RT = 2*RTprev + RAND*RTprev
```

MRT задает верхнюю границу значений RT (без учета случайного отклонения RAND). Если MRT = 0, верхнего предела для RT не задается. В противном случае

```
if (RT > MRT)
   RT = MRT + RAND*MRT
```

MRC задает верхний предел числа повторов передачи сообщения клиентом. Если MRC не равно 0, обмен сообщениями прерывается после MRC повторов.

MRD задает верхний предел продолжительности времени повтора сообщений клиентом. Если MRD не равно 0, обмен прерывается по прошествии MRD с момента передачи первого сообщения.

Если MRC и MRD отличаются от 0, обмен сообщениями достигается при достижении первого из заданных пределов.

Если MRC и MRD равны 0, клиент продолжает повтор передачи сообщений до получения отклика.

15. Проверка пригодности сообщений

Клиентам и серверам **следует** отбрасывать любые сообщения, которые содержат опции, не разрешенные для принятого сообщения. Например, присутствие опции IA не разрешено для сообщений Information-request. Клиенты и серверы **могут** извлекать информацию из таких сообщений, если эта информация используется получателем.

Сервер **должен** отбрасывать любые сообщения Solicit, Confirm, Rebind или Information-request, полученные по индивидуальному адресу.

Проверка пригодности сообщений на основе аутентификации DHCP рассматривается в параграфе 21.4.2.

Если сервер получает сообщение, содержащее опции, которых в нем не должно быть (например, Information-request с опцией IA), не содержащее требуемой опции или непригодное по иной причине, он **может** передать сообщение Reply (или Advertise, если это пригодно) с опцией Server Identifier, опцией Client Identifier, если она была включена в принятое сообщение и опцией Status Code со значением UnSpecFail.

15.1. Использование идентификаторов транзакций

Поле transaction-id содержит значение, используемое клиентами и серверами для привязки откликов сервера к сообщениям клиента. Клиенту **следует** генерировать случайное значение, которое сложно угадать или предсказать, в качестве идентификатора транзакции для каждого передаваемого нового сообщения. Отметим, что при генерации клиентом предсказуемых идентификаторов транзакций он может стать более уязвимым для некоторых атак. Клиент **должен** сохранять неизменным идентификатор транзакции при повторной передаче сообщения.

15.2. Сообщение Solicit

Клиенты **должны** отбрасывать все полученные сообщения Solicit.

Серверы **должны** отбрасывать все сообщения Solicit без опции Client Identifier или с опцией Server Identifier.

15.3. Сообщение Advertise

Клиенты **должны** отбрасывать все принятые сообщения Advertise при выполнении любого из приведенных условий:

- сообщение не включает опции Server Identifier;
- сообщение не включает опции Client Identifier;
- содержимое опции Client Identifier не соответствует DUID клиента;
- значение поля transaction-id не соответствует значению, использованному клиентом в сообщении Solicit.

Серверы и ретрансляторы **должны** отбрасывать все принятые сообщения Advertise.

15.4. Сообщение Request

Клиенты **должны** отбрасывать любые принятые сообщения Request.

Серверы **должны** отбрасывать все принятые сообщения Request при выполнении любого из приведенных условий:

- сообщение не включает опции Server Identifier;
- содержимое опции Server Identifier не соответствует DUID сервера.
- сообщение не включает опции Client Identifier.

15.5. Сообщение Confirm

Клиенты **должны** отбрасывать любые принятые сообщения Confirm.

Серверы **должны** отбрасывать все принятые сообщения Confirm, которые не включают опции Client Identifier или Server Identifier.

15.6. Сообщение Renew

Клиенты **должны** отбрасывать любые принятые сообщения Renew.

Серверы **должны** отбрасывать все принятые сообщения Renew при выполнении любого из приведенных условий:

- сообщение не включает опции Server Identifier;
- содержимое опции Server Identifier не соответствует идентификатору сервера;
- сообщение не включает опции Client Identifier.

15.7. Сообщение Rebind

Клиенты **должны** отбрасывать любые принятые сообщения Rebind.

Серверы **должны** отбрасывать все принятые сообщения Rebind, которые не включают опции Client Identifier или Server Identifier.

15.8. Сообщение Decline

Клиенты **должны** отбрасывать любые принятые сообщения Decline.

Серверы **должны** отбрасывать все принятые сообщения Decline при выполнении любого из приведенных условий:

- сообщение не включает опции Server Identifier;
- содержимое опции Server Identifier не соответствует идентификатору сервера;
- сообщение не включает опции Client Identifier.

15.9. Сообщение Release

Клиенты **должны** отбрасывать любые принятые сообщения Release.

Серверы **должны** отбрасывать все принятые сообщения Release при выполнении любого из приведенных условий:

- сообщение не включает опции Server Identifier;
- содержимое опции Server Identifier не соответствует идентификатору сервера;
- сообщение не включает опции Client Identifier.

15.10. Сообщение Reply

Клиенты **должны** отбрасывать все принятые сообщения Reply при выполнении любого из приведенных условий:

- сообщение не включает опции Server Identifier;
- поле transaction-id в сообщении не совпадает с идентификатором транзакции в исходном сообщении.

Если клиент включил в исходное сообщение опцию Client Identifier, сообщение Reply **должно** также включать эту опцию, а ее содержимое **должно** совпадать с DUID клиента. Если клиент не включил в исходное сообщение опцию Client Identifier, в сообщение Reply **недопустимо** включать опцию Client Identifier.

Серверы и ретрансляторы **должны** отбрасывать все принятые сообщения Reply.

15.11. Сообщение Reconfigure

Серверы и ретрансляторы **должны** отбрасывать все принятые сообщения Reconfigure.

Клиенты **должны** отбрасывать все принятые сообщения Reconfigure при выполнении любого из приведенных условий:

- сообщение не было передано по индивидуальному адресу клиента;
- сообщение не включает опции Server Identifier;
- содержимое опции Client Identifier не соответствует DUID клиента;
- сообщение не включает опции Reconfigure Message с корректным значением msg-type;
- сообщение включает какие-либо опции IA и msg-type в опции Reconfigure Message имеет значение INFORMATION-REQUEST;
- сообщение не включает аутентификации DHCP:
  - нет опции аутентификации;
  - сообщение не прошло проверку подлинности у клиента.

15.12. Сообщение Information-request

Клиенты **должны** отбрасывать любые принятые сообщения Information-request.

Серверы **должны** отбрасывать все принятые сообщения Information-request при выполнении любого из условий:

- сообщение включает опцию Server Identifier, значение DUID в которой не совпадает с DUID сервера;
- сообщение включает опцию IA.

15.13. Сообщение Relay-forward

Клиенты **должны** отбрасывать любые принятые сообщения Relay-forward.

15.14. Сообщение Relay-reply

Серверы и клиенты **должны** отбрасывать все принятые сообщения Relay-reply.

16. Выбор клиентом адреса отправителя и интерфейса

Когда клиент передает сообщение DHCP по адресу All_DHCP_Relay_Agents_and_Servers, ему **следует** отправлять это сообщение через интерфейс, для которого запрашивается конфигурация. Однако клиент **может** передать такое сообщение через другой интерфейс, подключенный к тому же каналу, если таковой интерфейс имеется. Клиент **должен** использовать в качестве адреса отправителя дейтаграммы IP локальный (link-local) адрес, назначенный интерфейсу, для которого запрашивается конфигурация.

Когда клиент передает сообщение DHCP напрямую серверу по индивидуальному адресу (после получения от этого сервера опции Server Unicast), в качестве адреса отправителя в заголовке дейтаграммы IP **должен** использоваться адрес, назначенный интерфейсу, для которого клиент заинтересован в конфигурационной информации, и пригодный для отправки сервером отклика клиенту.

17. Запрос сервера DHCP

В этом разделе описано как клиент находит серверы, которые будут назначать адреса для IA, относящихся к клиенту.

Клиент отвечает за создание IA и запрос у серверов назначения адресов IPv6 для этих IA. Клиент сначала создает IA и назначает ей идентификатор IAID. Затем клиент передает сообщение Solicit с опцией IA, описывающей ассоциацию IA. Сервер, который может назначить адреса для IA, отвечает сообщением Advertise. После этого клиент инициирует конфигурационный обмен, как описано в разделе 18.

Если клиент будет воспринимать сообщение Reply с назначенными адресами и другими ресурсами в ответ на сообщение Solicit, он включает опцию Rapid Commit (параграф 22.14) в сообщение Solicit.

17.1. Поведение клиента

Клиент использует сообщение Solicit для обнаружения серверов DHCP, настроенных на выделение адресов и возврат других конфигурационных параметров на канале, к которому подключен клиент.

17.1.1. Создание сообщений Solicit

Клиент указывает в поле msg-type значение SOLICIT, генерирует идентификатор транзакции и помещает его в поле transaction-id.

Клиент **должен** включить в сообщение опцию Client Identifier для представления себя серверу. Клиент включает опции IA для всех ассоциаций IA, которым нужно получить адреса от сервера. Клиент **может** включить в опции IA предпочитаемые адреса, которые будут служить серверу советами. Клиенту **недопустимо** включать в сообщение Solicit опции, в определении которых не указано включение в этот тип сообщений.

Клиент использует опции IA_NA для запроса назначения адресов, не являющихся временными, и IA_TA для запроса временных адресов. В сообщение может быть включена любая из опций IA_NA и IA_TA или их комбинация.

Клиенту **следует** включить в сообщение опцию Option Request (параграф 22.7) для указания опций, в получении которых он заинтересован. Клиент **может** дополнительно включить экземпляры опций, указанных в Option Request, со значениями, которые будут служить серверу советами в части значений параметров, которые клиент хочет получить.

Клиент включает опцию Reconfigure Accept (параграф 22.20), если он хочет принимать от сервера сообщения Reconfigure.

17.1.2. Передача сообщений Solicit

Первое сообщение Solicit от клиента на интерфейсе **должно** быть задержано на случайное время в диапазоне от 0 до SOL_MAX_DELAY. В случае передачи сообщения Solicit при инициировании DHCP механизмом IPv6 Neighbor Discovery задержка после IPv6 Neighbor Discovery заставляет клиента вызвать протокол автоматической настройки адреса с учетом состояния (параграф 5.5.3 RFC 2462). Эта случайная задержка предотвращает ненужную синхронизацию клиентов (например, после сбоя по питанию).

Клиент передает сообщение в соответствии с разделом 14, используя параметры:

IRT SOL_TIMEOUT;

MRT SOL_MAX_RT;

MRC 0;

MRD 0.

Если клиент включил опцию Rapid Commit в свое сообщение Solicit, он прекращает процесс ожидания, как только будет получено сообщение Reply с опцией Rapid Commit.

Если клиент ждет сообщения Advertise, описанный в разделе 14 механизм изменяется для сообщений Solicit, как описано ниже. Обмен сообщениями не прерывается при получении сообщения Advertise до завершения первого интервала RT. Вместо этого клиент собирает сообщения Advertise, пока не завершится первый интервал RT. Кроме того, первое значение RT **должно** быть задано строго больше IRT путем выбора значения RAND, строго превышающего 0.

Клиент **должен** собирать сообщения Advertise в течение первых RT секунд, пока он не получит сообщение Advertise с уровнем предпочтения 255 в опции Preference (параграф 22.8). Все сообщения Advertise без опции Preference считаются имеющими нулевой уровень предпочтения. Если клиент получает сообщение Advertise с опцией Preference, задающей уровень 255, он незамедлительно инициирует обмен сообщениями (как описано в разделе 18), передавая сообщение Request серверу, от которого получено сообщение Advertise. Если клиент получает сообщение Advertise, не включающее опции Preference с уровнем предпочтения 255, он продолжает сбор сообщений до истечения первого интервала RT. Если первый интервал RT завершился и клиент получил сообщение Advertise, ему **следует** инициировать обмен сообщениями путем передачи сообщения Request.

Если клиент не получил ни одного сообщения Advertise в течение первого интервала RT, он запускает механизм повтора, описанный в разделе 14. Клиент прерывает процесс повтора передачи при получении любого сообщения Advertise и действует далее без ожидания приема дополнительных сообщения Advertise.

Клиенту DHCP **следует** выбирать для MRC и MRD значение 0. Если клиент DHCP настроен на использование отличного от 0 значения MRC или MRD, он **должен** прекратить попытки настроить интерфейс в случае отказа при обмене сообщениями. После прекращения клиентом DHCP попытки настроить интерфейс, ему **следует** заново запустить процесс настройки конфигурации после того или иного внешнего события типа ввода от пользователя, перезагрузки системы или подключения клиента к другому каналу.

17.1.3. Прием сообщений Advertise

Клиент **должен** игнорировать все IA в сообщениях Advertise с опцией Status Code, содержащей NoAddrsAvail, за исключением того, что клиент **может** выводить связанный с сообщением статус пользователю[1].

При получении одного или более пригодных сообщений Advertise, клиент выбирает среди них одно или несколько в соответствии с приведенными ниже критериями.

- Сообщения Advertise с более высоким уровнем предпочтения по сравнению с другими сообщениями Advertise.
- В группе сообщений Advertise с одинаковым уровнем предпочтения клиент **может** выбрать сообщения, анонсирующие интересную для клиента информацию. Например, клиент может выбрать сервер, который возвращает интересные для клиента конфигурационные опции.
- Клиент **может** выбрать менее предпочтительный сервер, если он анонсирует более интересный набор параметров (например, доступные адреса в IA).

После того, как клиент выбрал одно или несколько сообщений Advertise, он обычно будет сохранять информацию о каждом сервере типа уровня предпочтения, анонсируемых адресов, времени получения анонсов и т. п.

Если выбранный сервер не отвечает, клиент выбирает следующий сервер в соответствии с приведенными критериями.

17.1.4. Прием сообщений Reply

Если клиент включает опцию Rapid Commit в сообщение Solicit, он будет ожидать в ответ сообщения Reply с опцией Rapid Commit. Клиент отбрасывает все сообщения Reply без опции Rapid Commit. Если клиент получает пригодное сообщение Reply с опцией Rapid Commit, он обрабатывает его в соответствии с параграфом 18.1.8. Если клиент не получил такого сообщения Reply, а получил пригодное сообщение Advertise, он обрабатывает Advertise в соответствии с параграфом 17.1.3.

Если потом клиент получает пригодное сообщение Reply с опцией Rapid Commit, он выбирает один из двух вариантов:

- обработка сообщения Reply в соответствии с параграфом 18.1.8 и отбрасывание любых сообщений Reply, полученных в ответ на сообщение Request;
- обработка любый сообщений Reply, полученных в ответ на Request, и отбрасывание всех сообщений Reply с опцией Rapid Commit.

17.2. Поведение сервера

Сервер передает сообщение Advertise в ответ на полученные сообщения Solicit для анонсирования клиенту своих возможностей.

17.2.1. Прием сообщений Solicit

Сервер определяет информацию о клиенте и его местоположении, как описано в разделе 11 и проверяет свои административные правила применительно к отклику клиенту. Если серверу не разрешено отвечать клиенту, он отбрасывает сообщение Solicit. Например, если административные правила сервера разрешают отвечать только клиентам, которые указали восприятие сообщений Reconfigure, а клиент не указал опцию Reconfigure Accept (параграф 22.20) в сообщении Solicit, сервер отбрасывает сообщение Solicit[2].

Если клиент включил опцию Rapid Commit в сообщение Solicit и сервер настроен отвечать с предлагаемым назначением адресов и других ресурсов, сервер отвечает на Solicit сообщением Reply, как описано в параграфе 17.2.3. В противном случае сервер игнорирует опцию Rapid Commit и обрабатывает оставшуюся часть сообщения как будто опции Rapid Commit в нем нет.

17.2.2. Создание и передача сообщений Advertise

Сервер устанавливает в поле msg-type значение ADVERTISE и копирует поле transaction-id из сообщения Solicit от клиента в свое сообщение Advertise. Сервер включает свой идентификатор в опцию Server Identifier и копирует Client Identifier из сообщения Solicit в сообщение Advertise.

Сервер **может** добавить опцию Preference для передачи уровня предпочтения в сообщении Advertise. Реализации сервера **следует** обеспечивать администратору возможность задавать уровень предпочтения. По умолчанию уровень предпочтения **должен** быть равен 0, если администратор не задал иное значение.

Сервер включает опцию Reconfigure Accept если он хочет потребовать чтобы клиент воспринимал сообщения Reconfigure.

Сервер включает опции, которые он будет возвращать клиенту в последующем сообщении Reply. Информация из этих опций может применяться клиентом при выборе сервера, если клиент получит более одного сообщения Advertise. Если клиент включил опцию Option Request в сообщение Solicit, сервер включает в сообщение Advertise опции, содержащие параметры конфигурации для всех опций, указанных в Option Request, которые сервер настроен возвращать клиенту. Сервер **может** возвращать клиенту дополнительные опции, если он настроен на это. Сервер должен быть осведомлен о рекомендуемых размерах пакетов и использовать фрагментацию в соответствии с разделом 5 RFC 2460.

Если сообщение Solicit от клиента включает одну или несколько опций IA, сервер **должен** включить в сообщение Advertise опции IA, содержащие все адреса, которые будут назначены для IA, указанных в сообщении Solicit от клиента. Если клиент включил адреса в IA в сообщении Solicit, сервер использует эти адреса как рекомендации по части адресов, которые клиент хочет получить.

Если сервер не будет назначать каких-либо адресов для IA из последующих сообщений Request от клиента, он **должен** передать клиенту сообщение Advertise с IA, содержащей опцию Status Code со значением NoAddrsAvail и сообщением

[1] В оригинале была допущена ошибка. См. https://www.rfc-editor.org/errata/eid2471. *Прим. перев.*
[2] В оригинале была допущена ошибка. См. https://www.rfc-editor.org/errata/eid2928. *Прим. перев.*

о состоянии для пользователя, опцией Server Identifier с DUID сервера и опцией Client Identifier с DUID клиента. Серверу **следует** включать в сообщение Advertise другие опции IA (типа IA_PD), учитывающие состояние, а также иные конфигурационные опции[1].

Если сообщение Solicit было принято сервером напрямую, он передает сообщение Advertise напрямую клиенту по индивидуальному адресу из поля адреса отправителя в дейтаграмме IP, содержавшей сообщение Solicit. Сообщение Advertise **должно** передаваться по индивидуальному адресу на канале, из которого было принято сообщение Solicit.

Если сообщение Solicit было получено в сообщении Relay-forward, сервер создает сообщение Relay-reply с сообщением Advertise в данных опции relay-message. Если сообщение Relay-forward включало опцию Interface-id, сервер копирует ее в сообщениме Relay-reply. Сервер передает сообщение Relay-reply напрямую ретранслятору по индивидуальному адресу из поля отправителя в дейтаграмме IP, содержавшей сообщение Relay-forward.

17.2.3. Создание и передача сообщений Reply
Сервер **должен** зафиксировать назначение каких-либо адресов и другой конфигурационной информации до отправки клиенту сообщения Reply в ответ на сообщение Solicit.

Обсуждение

> При использовании обмена сообщениями Solicit-Reply сервер фиксирует назначение каких-либо адресов до отправки сообщения Reply. Клиент может предположить, что ему были назначены адреса из сообщения Reply и не нужно передавать для них сообщение Request.
>
> Обычно серверы, настроенные на использование обмена сообщениями Solicit-Reply, развертываются так, что на сообщения Solicit будет отвечать лишь один сервер. Если отвечает несколько серверов, клиент будет использовать адреса лишь одного из них, тогда как адреса, назначенные другими серверами, будут зафиксированы для клиента, но не будут им использованы.

Сервер включает в сообщение Reply опцию Rapid Commit для индикации того, что Reply является откликом на Solicit.

Сервер включает опцию Reconfigure Accept, если он хочет потребовать от клиента восприятия сообщений Reconfigure.

Сервер создает сообщение Reply, как будто он получил сообщение Request, как описано в параграфе 18.2.1. Сервер передает сообщение Reply в соответствии с параграфом 18.2.8.

18. Инициированный клиентом конфигурационный обмен DHCP
Клиент инициирует обмен сообщениями с одним или несколькими серверами для получения или обновления интересующей его конфигурационной информации. Клиент может инициировать обмен в процессе настройки конфигурации операционной системы по запросу приложения или системы автоматической настройки адресов без учета состояния (Stateless Address Autoconfiguration), а также для продления срока действия адресов (сообщения Renew и Rebind).

18.1. Поведение клиента
Клиент использует сообщения Request, Renew, Rebind, Release и Decline в течение обычного жизненного цикла адресов. Сообщение Confirm служит для проверки пригодности адресов при перемещении клиента на новый канал. Сообщение Information-Request используется в тех случаях, когда нужна конфигурационная информация, но не адреса.

Если клиент имеет адрес отправителя с достаточной областью действия, который сервер может использовать в качестве адреса возврата, и клиент получил от сервера опцию Server Unicast (параграф 22.12), ему **следует** передавать все сообщения Request, Renew, Release и Decline по индивидуальному адресу сервера.

Обсуждение

> Использование индивидуального адреса может предотвратить задержки, связанные с трансляцией сообщений ретрансляторами, а также избежать издержек и дублирования откликов серверами в результате доставки сообщений клиента множеству серверов. Требование к клиенту передавать все сообщения DHCP через ретранслятор позволяет включить опции ретранслятора во все сообщения, передаваемые клиентом. Серверу следует разрешать использование индивидуальной адресации только в тех случаях, когда опции ретранслятора не будут использоваться.

18.1.1. Создание и передача сообщений Request
Клиент использует сообщение Request для заполнения ассоциаций IA адресами и получения другой конфигурационной информации. Клиент включает в сообщение Request по меньшей мере одну опцию IA. Сервер возвращает адреса и другую конфигурационную информацию для IA в опциях IA сообщения Reply.

Клиент генерирует идентификатор транзакции и помещает его в поле transaction-id.

Клиент помещает идентификатор целевого сервера в опцию Server Identifier.

Клиент **должен** включить опцию Client Identifier для представления себя серверу. Клиент также добавляет другие подходящие опции, включая одну или несколько опций IA (если ему нужно получить от сервера адреса).

Клиент **должен** включить опцию Option Request (параграф 22.7) для указания опций, которые он хочет получить. Клиент **может** указать для опций значения данных, которые будут служить советами серверу при выборе значений параметров для возврата клиенту.

Клиент включает опцию Reconfigure Accept (параграф 22.20), показывающую желает ли он получать от сервера сообщения Reconfigure.

Клиент передает сообщение в соответствии с разделом 14, используя приведенные ниже параметры:

[1]В оригинале была допущена ошибка. См. https://www.rfc-editor.org/errata/eid2472. *Прим. перев.*

IRT REQ_TIMEOUT;

MRT REQ_MAX_RT;

MRC REQ_MAX_RC;

MRD 0.

Если при обмене сообщениями возникает отказ, клиент предпринимает действия, заданные локальной политикой. Примерами таких действий могут служить:

- выбор другого сервера из списка известных клиенту (например, серверы, ответившие сообщением Advertise);
- запуск процесса обнаружения серверов, описанного в разделе 17;
- прерывание процесса настройки и уведомление пользователя об отказе.

18.1.2. Создание и передача сообщений Confirm

При переключении клиента на другой канал префиксы назначенных интерфейсу адресов могут оказаться не пригодными для нового канала. Примеры переключения клиента на другой канал включают:

- перезагрузку клиента;
- физическое подключение клиента к кабелю;
- возврат клиента из состояния «сна»;
- смена точки доступа при использовании беспроводной связи.

В любой ситуации, когда клиент мог переключиться на другой канал, он **должен** инициировать обмен сообщениями Confirm-Reply. Клиент включает все ассоциации IA, связанный с интерфейсом, переключенным на другой канал, вместе с назначенными этим IA адресами в свое сообщение Confirm. Все отвечающие серверы будут указывать пригодны ли эти адреса для канала, к которому подключен клиент, значением статуса в возвращаемом клиенту сообщении Reply.

Клиент устанавливает в поле msg-type значение CONFIRM, генерирует идентификатор транзакции и помещает его в поле transaction-id.

Клиент **должен** включить в сообщение опцию Client Identifier для представления себя серверу. Клиент включает опции IA для всех ассоциаций интерфейса, с которым связано передаваемое сообщение Confirm. Опции IA включают все адреса, которые назначены у клиента для соответствующей IA. Клиенту **следует** установить поля T1 и T2 во всех опциях IA_NA, а для полей preferred-lifetime и valid-lifetime в в опциях IA Address установить значение 0, поскольку сервер будет игнорировать эти поля.

Первое сообщение Confirm от клиента на данном интерфейсе **должно** быть задержано на случайное время от 0 до CNF_MAX_DELAY. Клиент передает сообщения в соответствии с разделом 14, используя параметры:

IRT CNF_TIMEOUT;

MRT CNF_MAX_RT;

MRC 0;

MRD CNF_MAX_RD.

Если клиент не получает отклика до прерывания процесса повтора, как описано в разделе 14, ему **следует** продолжать использование адресов IP и последнего известного срока действия этих адресов, а также **следует** продолжать использование полученных ранее конфигурационных параметров.

18.1.3. Создание и передача сообщений Renew

Для продления действительного и предпочтительного срока действия адресов, связанных с IA, клиент передает сообщение Renew серверу, от которого были получены адреса, с указанием этих адресов в опции IA для ассоциации IA. Клиент включает опцию IA Address в опцию IA для адресов, связанных с данной IA. Сервер определяет новые сроки действия адресов в IA на основании административной конфигурации сервера. Сервер может также добавить новые адреса для IA или удалить адреса из IA, установив для них нулевые значения действительного и предпочтительного срока действия.

Сервер контролирует время, когда клиент контактировал с ним для расширения срока действия назначенных адресов, с помощью параметров T1 и T2, назначенных для IA.

В момент T1 для ассоциации IA клиент инициирует обмен сообщениями Renew-Reply для расширения срока действия всех адресов в IA. Клиент включает опцию IA со всеми адресами, назначенными в данный момент IA, в свое сообщение Renew.

Если сервер установил значение 0 для T1 или T2 (для IA_NA) или значение T1 или T2 не задано (для IA_TA), клиент может передать сообщение Renew или Rebind, соответственно, по своему усмотрению.

Клиент устанавливает в поле msg-type значение RENEW, генерирует идентификатор транзакции и помещает его в поле transaction-id.

Клиент помещает идентификатор целевого сервера в поле Server Identifier.

Клиент **должен** включить в сообщение опцию Client Identifier для представления себя серверу. Клиент добавляет любые подходящие опции, включая одну или несколько опций IA. Клиент **должен** включить список своих адресов, связанных в данный момент с ассоциациями IA, в сообщение Renew.

Клиент **должен** включить опцию Option Request (параграф 22.7) для указания опций, которые он хочет получить. Клиент **может** указать для опций значения данных, которые будут служить советами серверу при выборе значений параметров для возврата клиенту.

Клиент передает сообщения в соответствии с разделом 14, используя параметры:

IRT REN_TIMEOUT;

MRT REN_MAX_RT;

MRC 0;

MRD оставшееся до T2 время.

Обмен прерывается по достижении времени T2 (параграф 18.1.4) и клиент начинает обмен сообщениями Rebind.

18.1.4. Создание и передача сообщений Rebind

В момент T2 для ассоциации IA (этот момент может быть достигнут лишь в том случае, когда сервер, которому было передано сообщение Renew в момент T1, не ответил) клиент инициирует обмен сообщениями Rebind-Reply с любым доступным сервером. Клиент включает опцию IA со всеми назначенными данной ассоциации IA адресами в свое сообщение Rebind.

Клиент помещает в поле msg-type значение REBIND, генерирует идентификатор транзакции и помещает его в поле transaction-id.

Клиент **должен** включить в сообщение опцию Client Identifier для представления себя серверу. Клиент добавляет любые подходящие опции, включая одну или несколько опций IA. Клиент **должен** включить список своих адресов, связанных в данный момент с ассоциациями IA, в сообщение Rebind.

Клиент **должен** включить опцию Option Request (параграф 22.7) для указания опций, которые он хочет получить. Клиент **может** указать для опций значения данных, которые будут служить советами серверу при выборе значений параметров для возврата клиенту.

Клиент передает сообщения в соответствии с разделом 14, используя параметры:

IRT REB_TIMEOUT;

MRT REB_MAX_RT;

MRC 0;

MRD время, оставшееся до истечения действительного срока действия всех адресов.

Обмен сообщениями прерывается по истечении действительного срока действия всех адресов, назначенных IA (раздел 10) и клиент может выбрать один из возможных вариантов дальнейшего поведения. Например,

- использовать сообщение Solicit для поиска нового сервера DHCP и передать найденному серверу сообщение Request для IA с истекшим сроком действия;
- при наличии других адресов в других IA отбросить просроченную IA и использовать адреса из других IA.

18.1.5. Создание и передача сообщений Information-request

Клиент использует сообщение Information-request для получения конфигурационной информации без назначения ему адресов.

Клиент помещает в поле msg-type значение INFORMATION-REQUEST, генерирует идентификатор транзакции и помещает его в поле transaction-id.

Клиенту **следует** включить в сообщение опцию Client Identifier для представления себя серверу. Если клиент не включит в сообщение опцию Client Identifier, сервер не сможет возвратить относящуюся именно к этому клиенту информацию или может не ответить на сообщение совсем. Клиент **должен** включить опцию Client Identifier, если подлинность сообщения Information-Request будет проверяться (аутентификация).

Клиент **должен** включить опцию Option Request (параграф 22.7) для указания опций, которые он хочет получить. Клиент **может** указать для опций значения данных, которые будут служить советами серверу при выборе значений параметров для возврата клиенту.

Первое сообщение Information-request от клиента на данном интерфейсе **должно** быть задержано на случайное время от 0 до INF_MAX_DELAY. Клиент передает сообщения в соответствии с разделом 14, используя параметры:

IRT INF_TIMEOUT;

MRT INF_MAX_RT;

MRC 0;

MRD 0.

18.1.6. Создание и передача сообщений Release

Клиент передает серверу сообщение Release для освобождения одного или множества назначенных ему адресов.

Клиент помещает в поле msg-type значение RELEASE, генерирует идентификатор транзакции и помещает его в поле transaction-id.

Клиент указывает идентификатор выделившего адреса сервера в опцию Server Identifier.

Клиент **должен** включить в сообщение опцию Client Identifier для представления себя серверу. Клиент включает опции, содержащие ассоциации IA для освобождаемых адресов в поле options. Освобождаемые адреса **должны** быть включены в IA. Любые адреса IA, которые клиент хочет продолжать использовать, **недопустимо** указывать в IA.

Клиенту **недопустимо** указывать какой-либо из освобождаемых адресов в качестве адреса отправителя сообщения Release и любых последующих сообщений.

Поскольку сообщения Release могут теряться, клиенту следует повторять передачу Release, если он не получил ответного сообщения Reply. Однако возможны ситуации, когда клиент не захочет ждать обычного тайм-аута повтора (например, при выключении питания). Реализациям **следует** повторять передачу один или более раз, но процедура повтора **может** быть прервана раньше обычного.

Клиент передает сообщения в соответствии с разделом 14, используя параметры:

IRT REL_TIMEOUT;

MRT 0;

MRC REL_MAX_RC;

MRD 0.

Клиент **должен** прекратить использование всех освобождаемых адресов, как только он начнет процедуру обмена Release. Если адреса были освобождены, но сообщение Reply от сервера DHCP потеряно, клиент будет повторять передачу сообщения Release и сервер может ответить сообщением Reply со статусом NoBinding. Поэтому клиентам не следует воспринимать сообщение Reply со статусом NoBinding в обмене Release как индикацию ошибки.

Отметим, что в случае отказа при попытке клиента освободить адреса, каждый выделенный для IA будет освобожден (reclaimed) сервером по окончании действительного срока действия адреса.

18.1.7. Создание и передача сообщений Decline

Если клиент обнаруживает, что один или несколько назначенных ему адресов уже используются другим узлом, он передает серверу сообщение Decline для информирования о «сомнительности» адресов.

Клиент помещает в поле msg-type значение DECLINE, генерирует идентификатор транзакции и помещает его в поле transaction-id.

Клиент помещает идентификатор выделившего адрес(а) сервера в опцию Server Identifier.

Клиент **должен** включить в сообщение опцию Client Identifier для представления себя серверу. Клиент включает опции, содержащие ассоциации IA для отвергаемых адресов в поле options. Отвергаемые адреса **должны** быть включены в ассоциации IA. Любые адреса IA, которые клиент хочет продолжать использовать, не следует указывать в IA.

Клиенту **недопустимо** использовать любой из отвергаемых адресов в качестве адреса отправителя сообщения Decline и любых последующих сообщений.

Клиент передает сообщения в соответствии с разделом 14, используя параметры:

IRT DEC_TIMEOUT;

MRT 0;

MRC DEC_MAX_RC;

MRD 0.

Если адреса были отвергнуты, но сообщение Reply от сервера DHCP потеряно, клиент будет повторять передачу сообщения Decline и сервер может ответить сообщением Reply со статусом NoBinding. Поэтому клиентам не следует воспринимать сообщение Reply со статусом NoBinding в обмене Decline как индикацию ошибки.

18.1.8. Прием сообщений Reply

При получении корректного сообщения Reply в ответ на сообщение Solicit (с опцией Rapid Commit), Request, Confirm, Renew, Rebind или Information-request клиент извлекает конфигурационную информацию из сообщения Reply. Клиент **может** передать пользователю статус или сообщение из опции с кодом состояния в сообщении Reply.

Клиенту **следует** выполнить проверку дублирования адресов [17] для каждого из адресов во всех IA, полученных в сообщении Reply до начала использования этих адресов. Если для какого-либо адреса обнаружено дублирование, клиент передает серверу сообщение Decline, как описано в параграфе 18.1.7.

Если сообщение Reply было получено в ответ на сообщение Solicit (без опции Rapid Commit option), Request, Renew или Rebind, клиент обновляет сохраненную информацию для IA из опций IA в сообщении Reply:

- записываются значения T1 и T2;
- добавляются все новые адреса из опции IA к ассоциации IA, сохраненной клиентом;
- обновляются сроки действия для всех адресов из опции IA, которые клиент уже хранит для IA;
- отбрасываются из IA все записанные ранее клиентом адрес, для которых значение действительного срока действия в опции IA Address имеет значение 0;
- сохраняется без изменений вся информация об адресах, которую клиент сохранил ранее в IA, если она не включена в IA от сервера.

Обработка конкретной конфигурационной информации рассмотрена в определении каждой опции в разделе 22.

Если клиент получает сообщение Reply со Status Code = UnspecFail, это говорит о том, что сервер не способен обработать сообщение без указания конкретной причины. Если клиент повторяет передачу сообщения тому же серверу для продолжения попыток, он **должен** ограничить частоту и продолжительность повторов.

Когда клиент получает сообщение Reply с опцией Status Code = UseMulticast, он фиксирует прием сообщения и передает последующие сообщения серверу через интерфейс, на который было получено сообщение, с использованием групповой адресации. Клиент передает повторно исходное сообщение по групповому адресу.

Когда клиент получает статус NotOnLink в ответе сервера на сообщение Confirm, он выполняет поиск сервера DHCP (solicitation), как описано в разделе 17 и настройку конфигурации по своей инициативе, как описано в разделе 18. Если клиент получает какое-либо сообщение Reply, не содержащее статуса NotOnLink, он может использовать адреса ассоциации IA и игнорировать любые сообщения со статусом NotOnLink.

Когда клиент получает статус NotOnLink от сервера в ответ на сообщение Request, он может заново передать сообщение Request без указания адреса или возобновить процесс поиска сервера DHCP (раздел 17).

Клиент проверяет код статуса отдельно в каждой ассоциации IA. Код NoAddrsAvail указывает, что клиент не получил пригодных к использованию адресов в IA и клиент может попытаться получить адреса для IA от другого сервера. Клиент использует адреса и другую информацию из любой ассоциации IA, которая не содержит кода статуса NoAddrsAvail. Если клиент не получает адреса ни для одной ассоциации IA, он может попытаться использовать другой сервер (например, возобновив процесс поиска серверов DHCP) или передать сообщение Information-request для получения конфигурационной информации без адресов.

Когда клиент получает сообщение Reply в ответ на Renew или Rebind, он проверяет независимо каждую ассоциацию IA. Для каждой IA в исходном сообщении Renew или Rebind клиент:

- передает сообщение Request, если IA содержит опцию Status Code со значением NoBinding (и не передает дополнительных сообщений Renew/Rebind);
- передает сообщение Renew/Rebind, если в сообщении Reply нет IA;
- в остальных случаях воспринимает информацию IA

Когда клиент получает корректное сообщение Reply в ответ на Release, он считает освобождение адресов завершенным, независимо от возвращенного сервером Status Code.

Когда клиент получает корректное сообщение Reply в ответ на Decline, он считает отказ от адресов завершенным, независимо от возвращенного сервером Status Code.

18.2. Поведение сервера

В этом обсуждении предполагается, что сервер настроен в соответствии с особенностями реализации для предоставления конфигураций, представляющих интерес для клиентов.

Большинство экземпляров серверов будут передавать Reply в ответ на сообщение от клиента. Сообщение Reply всегда **должно** включать опцию Server Identifier с идентификатором DUID этого сервера и опцию Client Identifier из сообщения клиента, если она была включена.

В большинство сообщений Reply сервер будет включать опции с конфигурационными данными для клиента. Сервер должен быть осведомлен о рекомендуемых размерах пакетов и использовании фрагментации, как описано в разделе 5 RFC 2460. Если клиент включил в свое сообщение опцию Option Request, сервер включает в сообщение Reply опции с конфигурационными параметрами для всех опций, указанных в Option Request, для которых на сервере настроен возврат информации клиентам. Сервер **может** возвращать клиенту дополнительные опции, если он настроен на это.

18.2.1. Прием сообщений Request

Когда сервер получает по индивидуальному адресу сообщение Request от клиента, которому он не передавал опцию unicast, сервер отбрасывает сообщение Request и отвечает сообщением Reply с опцией Status Code = UseMulticast, опцией Server Identifier с DUID сервера, опцией Client Identifier из сообщения клиента, не добавляя других опций.

При получении сервером пригодного сообщения Request он создает для клиента привязку в соответствии со своими правилами и конфигурационной информацией, записывая все IA и другую информацию, запрошенную клиентом.

Сервер создает сообщение Reply, устанавливая msg-type = REPLY и копируя идентификатор транзакции из сообщения Request в поле transaction-id.

Сервер **должен** включить в сообщение Reply опцию Server Identifier со своим DUID и опцию Client Identifier из сообщения Request.

Если сервер обнаружил, что один или несколько адресов IP в любой из ассоциаций IA из клиентского сообщения не пригодны для канала, к которому подключен клиент, сервер **должен** возвратить клиенту IA со Status Code = NotOnLink.

Если сервер не может назначить адресов для IA из сообщения клиента, он **должен** включить в сообщение Reply эту ассоциацию IA без адресов и со Status Code = NoAddrsAvail.

Для всех ассоциаций IA, которым сервер может назначить адреса, он включает в сообщение IA с адресами и другими конфигурационными параметрами, записывая IA как новую привязку клиента.

Сервер включает опцию Reconfigure Accept, если он хочет, чтобы клиент воспринимал от него сообщения Reconfigure.

Сервер включает другие опции с конфигурационными данными для клиента, как описано в параграфе 18.2.

Если сервер определил что клиент включил в сообщение Request ассоциацию IA, для которой у сервера уже есть привязка к данному клиенту, это означает, что клиент повторно передал сообщение Request, для которого не получил Reply. Сервер в таком случае повторно передает кэшированное сообщение Reply или создает и отправляет новое сообщение Reply.

18.2.2. Прием сообщений Confirm

При получении сообщения Confirm сервер проверяет пригодность включенных в него адресов для канала, к которому подключен клиент. Если все адреса из сообщения Confirm пригодны, сервер возвращает статус Success, в противном случае возвращается статус NotOnLink. Если сервер не может выполнить проверку (например, не имеет данных о префиксах на канале, к которому подключен клиент) или в сообщении клиента нет адресов в какой-либо из ассоциаций IA, серверу **недопустимо** передавать отклик.

Сервер игнорирует поля T1 и T2 в опциях IA, а также поля preferred-lifetime и valid-lifetime в опциях IA Address.

Сервер создает сообщение Reply, устанавливая msg-type = REPLY и копируя идентификатор транзакции из сообщения Request в поле transaction-id.

Сервер **должен** включить в сообщение Reply опцию Server Identifier со своим DUID и опцию Client Identifier из сообщения Confirm. The server includes a Status Code option indicating the status of the Confirm message.

18.2.3. Прием сообщений Renew

Когда сервер получает по индивидуальному адресу сообщение Renew от клиента, которому он не передавал опцию unicast, сервер отбрасывает сообщение Renew и отвечает сообщением Reply с опцией Status Code = UseMulticast, опцией Server Identifier с DUID сервера, опцией Client Identifier из сообщения клиента, не добавляя других опций.

Когда сервер получает от клиента сообщение Renew с опцией IA, он находит привязку этого клиента и проверяет соответствие информации из IA с сохраненной для клиента информацией.

Если сервер не может найти привязку клиента для полученной IA, сервер в сообщении Reply возвращает IA без адресов и со Status Code = NoBinding.

Если сервер определяет непригодность адресов для канала, к которому подключен клиент, он возвращает клиенту адреса со сроком действия 0.

Если сервер находит привязку адресов из IA для клиента, он возвращает клиенту IA с новыми сроками действия и значениями T1/T2. Сервер может изменить список и сроки действия адресов в IA, возвращаемых клиенту.

Сервер создает сообщение Reply, устанавливая msg-type = REPLY и копируя идентификатор транзакции из сообщения Renew в поле transaction-id.

Сервер **должен** включить в сообщение Reply опцию Server Identifier со своим DUID и опцию Client Identifier из сообщения Renew.

Сервер включает другие опции с конфигурационной информацией для клиента, как указано в параграфе 18.2.

18.2.4. Прием сообщений Rebind

Когда сервер получает от клиента сообщение Rebind с опцией IA, он находит привязку этого клиента и проверяет соответствие информации из IA с сохраненной для клиента информацией.

Если сервер не может найти клиентскую запись для IA и определяет, что адрес в IA не подходит для канала, к которому подключен клиентский интерфейс в соответствии с явной конфигурационной информации на сервере, сервер **может** передать клиенту сообщение Reply с IA клиента, где установлены нулевые сроки действия адресов. Такое сообщение Reply служит явным уведомлением клиенту о том, что адреса в IA больше не действуют. Если в такой ситуации сервер не передает сообщения Reply, он просто отбрасывает Rebind без уведомления.

Если сервер определяет непригодность адресов для канала, к которому подключен клиент, он возвращает клиенту адреса со сроком действия 0.

Если сервер находит привязку адресов из IA для клиента, ему **следует** возвратить клиенту IA с новыми сроками действия и значениями T1/T2.

Сервер создает сообщение Reply, устанавливая msg-type = REPLY и копируя идентификатор транзакции из сообщения Rebind в поле transaction-id.

Сервер **должен** включить в сообщение Reply опцию Server Identifier со своим DUID и опцию Client Identifier из сообщения Rebind.

Сервер включает другие опции с конфигурационной информацией для клиента, как указано в параграфе 18.2.

18.2.5. Прием сообщений Information-request

Получение сервером сообщения Information-request означает запрос клиентом конфигурационной информации без назначения ему адресов. Сервер определяет все подходящие для клиента конфигурационные параметры на основе известных ему правил настройки конфигурации.

Сервер создает сообщение Reply, устанавливая msg-type = REPLY и копируя идентификатор транзакции из сообщения Information-request в поле transaction-id.

Сервер **должен** включить в сообщение Reply опцию Server Identifier со своим DUID. Если клиент включил в сообщение Information-request опцию Client Identifier, сервер копирует эту опцию в сообщение Reply.

Сервер включает другие опции с конфигурационной информацией для клиента, как указано в параграфе 18.2.

Если сообщение Information-request получено от клиента без опции Client Identifier, серверу **следует** ответить сообщением Reply содержащим все конфигурационные параметры, которые не зависят от конкретного клиента. Если сервер решит не отвечать на такое сообщение клиент может начать бесконечный повтор сообщения Information-request.

18.2.6. Прием сообщений Release

Когда сервер получает по индивидуальному адресу сообщение Release от клиента, которому он не передавал опцию unicast, сервер отбрасывает сообщение Release и отвечает сообщением Reply с опцией Status Code = UseMulticast, опцией Server Identifier с DUID сервера, опцией Client Identifier из сообщения клиента, не добавляя других опций.

При получении пригодного сообщения Release сервер проверяет пригодность IA и включенных в них адресов. Если все ассоциации IA в сообщении привязаны к клиенту и адреса в IA были назначены сервером для этих IA, сервер удаляет адреса из IA и делает их доступными для назначения другим клиентам. Сервер игнорирует адреса, не назначенные IA и может записать информацию об этом в журнал ошибок.

После обработки всех адресов сервер генерирует сообщение Reply, включая в него опцию Status Code со значением Success, опцию Server Identifier со своим DUID и опцию Client Identifier с DUID клиента. Для каждой ассоциации IA из сообщения Release, не имеющей информации о привязке, сервер добавляет опцию IA, используя идентификатор IAID из сообщения Release и включает опцию Status Code со значением NoBinding в опцию IA. Другие опции в опцию IA не включаются.

Сервер может сохранять записи с назначенными адресами и IA после завершения их срока действия, чтобы можно было позднее предоставить клиенту те же адреса.

18.2.7. Прием сообщений Decline

Когда сервер получает по индивидуальному адресу сообщение Decline от клиента, которому он не передавал опцию unicast, сервер отбрасывает сообщение Decline и отвечает сообщением Reply с опцией Status Code = UseMulticast, опцией Server Identifier с DUID сервера, опцией Client Identifier из сообщения клиента, не добавляя других опций.

При получении пригодного сообщения Decline сервер проверяет пригодность IA и включенных в них адресов. Если все ассоциации IA в сообщении привязаны к клиенту и адреса в IA были назначены сервером для этих IA, сервер удаляет адреса из IA. Сервер игнорирует адреса, не назначенные IA и может записать информацию об этом в журнал ошибок.

Для указанных в сообщении Decline клиент обнаружил, что они уже используются на его канале. Поэтому серверу **следует** пометить отвергнутые клиентом адреса так, чтобы они не были назначены другим клиентам. Сервер также **может** передать уведомление об отвергнутых адресах. Возможность последующего назначения указанных в сообщении Decline адресов определяется локальной политикой сервера.

После обработки всех адресов сервер генерирует сообщение Reply, включая в него опцию Status Code со значением Success, опцию Server Identifier со своим DUID и опцию Client Identifier с DUID клиента. Для каждой ассоциации IA из сообщения Decline, не имеющей информации о привязке, сервер добавляет опцию IA, используя идентификатор IAID из сообщения Decline и включает опцию Status Code со значением NoBinding в опцию IA. Другие опции в опцию IA не включаются[1].

18.2.8. Передача сообщений Reply

Если исходное сообщение было получено сервером напрямую, он передает сообщение Reply напрямую клиенту по индивидуальному адресу из поля отправителя в заголовке дейтаграммы IP с исходным сообщением. Сообщение Reply **должно** передаваться по индивидуальному адресу через интерфейс, принявших исходное сообщение.

Если исходное сообщение было получено в сообщении Relay-forward, сервер создает сообщение Relay-reply с сообщением Reply в данных опции Relay Message (параграф 22.10). Если сообщение Relay-forward включает опцию Interface-id, сервер копирует ее в сообщение Relay-reply. Сервер передает сообщение Relay-reply напрямую ретранслятору по индивидуальному адресу из поля отправителя в заголовке IP дейтаграммы с сообщением Relay-forward.

19. Обмен сообщениями по инициативе сервера DHCP

Сервер инициирует обмен конфигурационными сообщениями, чтобы заставить клиентов DHCP получить новые адреса и другую конфигурационную информацию. Например, администратор может использовать инициированный сервером обмен сообщениями при смене адресов на каналах в домене DHCP. Другими примерами могут служить смена местоположения серверов каталогов, добавление новых служб (например, сетевой печати) или доступность новых программ.

19.1. Поведение сервера

Сервер передает сообщение Reconfigure, чтобы заставить клиентов незамедлительно инициировать обмен сообщениями Renew/Reply или Information-request/Reply с сервером.

19.1.1. Создание и передача сообщений Reconfigure

Сервер устанавливает в поле msg-type значение RECONFIGURE, а в поле transaction-id - 0. Сервер включает в сообщение Reconfigure опцию Server Identifier со своим DUID и опцию Client Identifier с DUID клиента.

Сервер **может** включить в сообщение опцию Option Request для информирования клиента об изменении информации или добавлении новой информации. В частности, сервер задает опцию IA в опции Option Request, если он хочет, чтобы клиент получил новую адресную информацию. Если сервер указывает опцию IA в опции Option Request, он **должен** включить опцию IA, которая не содержит других субопций для идентификации каждой ассоциации IA, которая будет заново настроена клиентом.

По причине наличия риска атак на отказ служб против клиентов DHCP, для сообщений Reconfigure требуется использовать защиту. Сервер **должен** применять в сообщениях Reconfigure проверку подлинности DHCP.

Сервер **должен** включить в сообщение опцию Reconfigure Message (параграф 22.19), чтобы задать ответ клиента с использованием сообщения Renew или Information-Request.

[1] В оригинале была допущена ошибка. См. https://www.rfc-editor.org/errata/eid295. *Прим. перев.*

Серверу **недопустимо** включать в сообщение какие-либо другие опции, за исключением тех, в определении которых это указано явно.

Сервер передает каждое сообщение Reconfigure одному клиенту DHCP, используя индивидуальный адрес IPv6 с достаточной областью действия, включающей этого клиента. Если у сервера нет адреса, по которому можно передать сообщение Reconfigure напрямую клиенту, он использует сообщение Relay-reply (как описано в прагарафе 20.3) для отправки сообщения Reconfigure ретранслятору, который перешлет его клиенту. Сервер может получить адрес клиента (и подходящего агента при необходимости) из информации о клиентах, которые с ним взаимодействуют, или от того или иного внешнего агента.

Для перенастройки множества клиентов сервер передает отдельное сообщение каждому такому клиенту. Сервер может инициировать перенастройку множества клиентов одновременно, например, передавая сообщение Reconfigure дополнительным клиентам, когда предшествующие обмены сообщениями реконфигурации еще не завершены.

Сообщение Reconfigure заставляет клиента инициировать обмен сообщениями Renew/Reply или Information-request/Reply с сервером. Сервер воспринимает получение сообщений Renew или Information-request (вызванных исходным сообщением Reconfigure) от клиента как выполнение запроса Reconfigure.

19.1.2. Тайм-аут и повтор сообщений Reconfigure

Если сервер не получает от клиента сообщения Renew или Information-request в течение REC_TIMEOUT мсек, он повторяет сообщение Reconfigure, удваивает REC_TIMEOUT и снова ждет. Попытки продолжаются, пока не будет достигнуто число неудачных попыток REC_MAX_RC, после чего серверу **следует** прервать процесс перенастройки для данного клиента.

Принятые по умолчанию и начальные значения параметров REC_TIMEOUT и REC_MAX_RC даны в параграфе 5.5.

19.2. Прием сообщений Renew

Сервер генерирует и передает клиенту сообщение Reply, как описано в параграфах 18.2.3 и 18.2.8, включая опции для параметров конфигурации.

Сервер может включить в сообщение Reply опции, содержащие IA и новые значения для других параметров, даже в том случае, когда эти IA и параметры не были запрошены в сообщении Renew от клиента.

19.3. Прием сообщений Information-request

Сервер генерирует и передает клиенту сообщение Reply, как описано в параграфах 18.2.3 и 18.2.8, включая опции для параметров конфигурации.

Сервер может включить в сообщение Reply опции, содержащие IA и новые значения для других параметров, даже в том случае, когда эти IA и параметры не были запрошены в сообщении Information-request от клиента.

19.4. Поведение клиента

Клиент получает сообщения Reconfigure, направленные в порт UDP 546, на интерфейсах, для которых он получал конфигурационные параметры от DHCP. Эти сообщения могут передаваться в любой момент. Поскольку результат изменения конфигурации может влиять на программы прикладного уровня, клиенту **следует** записывать такие события в системный журнал и он **может** уведомлять об изменениях программы через определяемый реализацией интерфейс.

19.4.1. Прием сообщений Reconfigure

При получении действительного сообщения Reconfigure клиент отвечает на него сообщением Renew или Information-request, как указано в опции Reconfigure Message (параграф 22.19). Клиент игнорирует поле transaction-id в полученном сообщении Reconfigure. Пока транзакция продолжается, клиент отбрасывает без уведомления другие сообщения Reconfigure.

Обсуждение.

> Сообщение Reconfigure служит триггером, указывающим клиенту на завершение успешного обмена сообщениями. После получения клиентом сообщения Reconfigure он продолжает обмен сообщениями (передавая при необходимости сообщение Renew или Information-request), игнорируя все дополнительные сообщения Reconfigure до завершения обмена. Последующие сообщения Reconfigure заставляют клиента начать новый обмен.
>
> Как этот механизм работает с учетом дублирования и повторной передачи сообщений Reconfigure? Дубликаты сообщений будут игнорироваться, поскольку клиент будет начинать обмен после первого сообщения Reconfigure. Повторные сообщения будут инициировать обмен (если первое сообщение Reconfigure не получено клиентом) или игнорироваться. Сервер может прервать повтор сообщений Reconfigure после приема от клиента сообщения Renew или Information-request.
>
> Дубликаты и повторные сообщения Reconfigure могут достаточно сильно задерживаться (и доставляться с нарушением порядка) и приходить к клиенту после завершения обмена, инициированного первым сообщением Reconfigure. В таких случаях клиент будут инициировать избыточный обмен. Вероятность столь длительной задержки достаточно мала и ее можно игнорировать. Результатом избыточной реконфигурации является лишь снижение эффективности без возникновения ошибок.

19.4.2. Создание и передача сообщений Renew

При ответе на сообщение Reconfigure клиент создает и отправляет сообщение Renew, как описано в параграфе 18.1.3, за исключениям копирования опции Option Request и всех опций IA из сообщения Reconfigure в сообщение Renew.

19.4.3. Создание и передача сообщений Information-request

При ответе на сообщение Reconfigure клиент создает и отправляет сообщение Information-request, как описано в параграфе 18.1.5, за исключением того, что клиент указывает опцию Server Identifier с индикатором из сообщения Reconfigure, на которое клиент отвечает.

19.4.4. Тайм-аут и повтор для сообщения Renew и Information-request

Клиент использует такие же переменные и алгоритм повтора, как для сообщений Renew и Information-request при обмене по инициативе клиента (параграфы 18.1.3 и 18.1.5). Если клиент не получает от сервера отклика до завершения процесса повторной передачи, он игнорирует и отбрасывает сообщение Reconfigure.

19.4.5. Прием сообщений Reply

При получении действительного сообщения Reply клиент обрабатывает опции и устанавливает (или сбрасывает) соответствующие параметры конфигурации. Клиент обновляет и записывает сроки действия всех адресов, указанных в IA из сообщения Reply.

20. Поведение ретранслятора

Ретранслятор **может** быть настроен на использование списка адресов получателей, который **может** включать индивидуальные адреса, групповой адрес All_DHCP_Servers и другие адреса, заданные администратором сети. При отсутствии явной настройки транслятор **должен** использовать по умолчанию групповой адрес All_DHCP_Servers.

При трансляции сообщений по адресу All_DHCP_Servers и другим групповым адресам ретранслятор устанавливает Hop Limit = 32.

20.1. Трансляция сообщений Client и Relay-forward

Ретранслятор транслирует сообщения от клиентов и сообщения Relay-forward от других ретрансляторов. При получении пригодного для трансляции сообщения ретранслятор создает новое сообщение Relay-forward. Ретранслятор копирует адрес отправителя из заголовка дейтаграммы IP с исходным сообщением в поле peer-address сообщения Relay-forward. Полученное сообщение DHCP (без заголовков IP и UDP) копируется в опцию Relay Message нового сообщения. Ретранслятор добавляет в сообщение Relay-forward другие опции в соответствии со скоей конфигурацией.

20.1.1. Трансляция сообщений от клиента

Если ретранслятор получает сообщение для трансляции от клиента, он помещает в поле link-address глобальный или действующий в рамках сайта адрес с префиксом, назначенным для канала, на котором клиенту следует назначить адрес. Этот адрес будет использоваться сервером при определении канала, для которого клиенту следует назначить адрес и другие параметры конфигурации. В поле hop-count сообщения Relay-forward устанавливается значение 0.

Если ретранслятор не может использовать адрес в поле link-address для указания интерфейса, через который будет транслироваться отклик клиенту, он **должен** включить в сообщение Relay-forward опцию Interface-id (параграф 22.18). Сервер будет включать опцию Interface-id в свое сообщение Relay-reply. Ретранслятор устанавливает поле link-address, как описано в предыдущем параграфе, независимо от включения опции Interface-id в сообщение Relay-forward.

20.1.2. Трансляция сообщений от ретранслятора

Ретранслятор отбрасывает принятые сообщения Relay-forward со значением hop-count не меньше HOP_COUNT_LIMIT.

Ретранслятор копирует адрес отправителя из заголовка дейтаграммы IP с принятым сообщением от другого ретранслятора в поле peer-address сообщения Relay-forward и устанавливает в поле hop-count значение одноименного поля из принятого сообщения, увеличенное на 1[1].

Если адрес отправителя из заголовка принятой дейтаграммы IP является глобальным или локальным для сайта (и устройство, на котором работает ретранслятор, относится лишь к одному сайту), ретранслятор устанавливает в поле link-address значение 0;. В остальных случаях в поле link-address ретранслятор указывает глобальный или локальный для сайта адрес, связанный с интерфейсом, на котором получено сообщение, или включает опцию Interface-ID для указания принявшего сообщение интерфейса.

20.2. Трансляция сообщений Relay-reply

Ретранслятор обрабатывает все опции, включенные в сообщение Relay-reply в дополнение к опции Relay Message, затем отбрасывает эти опции.

Ретранслятор извлекает сообщение из опции Relay Message и транслирует его по адресу, указанному в поле peer-address сообщения Relay-reply.

Если сообщение Relay-reply включает опцию Interface-id, ретранслятор транслирует сообщение от сервера клиенту в канал, указанный опцией Interface-id. В противном случае, если поле link-address не равно 0, ретранслятор передает сообщение в канал, указанный полем link-address.

20.3. Создание сообщений Relay-reply

Сервер использует сообщения Relay-reply для возврата клиенту отклика, если исходное сообщение от клиента было передано серверу в опции Relay-forward или для отправки сообщения Reconfigure клиенту, для которого у сервера нет адреса, подходящего для отправки сообщения напрямую клиенту.

Отклик клиенту **должен** транслироваться через те же ретрансляторы, что и исходное сообщение от клиента. Сервер реализует это путем создания сообщения Relay-reply с опцией Relay Message, содержащей сообщение для следующего ретранслятора на пути к клиенту. Это сообщение Relay-reply содержит свою опцию Relay Message для

[1]В оригинале была допущена ошибка. См. https://www.rfc-editor.org/errata/eid294. *Прим. перев.*

передачи следующему ретранслятору и т. д. Сервер должен сохранять содержимое полей peer-address из принятых сообщений, чтобы можно было создать подходящее сообщение Relay-reply с откликом.

Например, если сообщение клиента C было транслировано ретранслятором A ретранслятору B, а затем серверу, последний будет передавать агенту B сообщение Relay-Reply

msg-type	RELAY-REPLY
hop-count	1
link-address	0
peer-address	A

С опцией Relay Message

msg-type	RELAY-REPLY
hop-count	0
link-address	адрес на канале, к которому подключен клиент C
peer-address	C
Relay Message	<отклик от сервера>

При получении от клиента сообщения Reconfigure через ретранслятор сервер создает сообщение Relay-reply с опцией Relay Message, включающей сообщение Reconfigure для следующего ретранслятора на пути к клиенту. Сервер указывает в поле peer-address заголовка сообщения Relay-reply адрес клиента и устанавливает значение поля link-address в соответствии с требованиями ретранслятора для трансляции сообщения Reconfigure клиенту. Сервер получает адрес клиента и ретранслятора из предшествующего взаимодействия с клиентом или от внешнего механизма.

21. Проверка подлинности сообщений DHCP

Некоторым сетевым администраторам может потребоваться проверка подлинности (аутентификация) источников и содержимого сообщений DHCP. Например, клиенты могут подвергаться DoS-атакам[1] путем использования подставных серверов DHCP или просто могут быть некорректно настроены в результате неумышленного создания ненужных серверов DHCP. Сетевые администраторы могут захотеть ограничить назначение адресов хостам для предотвращения DoS-атак во «враждебных» средах, где среда передачи не защищена физически, типа беспроводных сетей или сетей студенческих общежитий.

Механизм проверки подлинности DHCP основан на механизме аутентификации для DHCPv4 [4].

21.1. Защита сообщений между серверами и ретрансляторами

Для защиты обмена сообщениями между серверами и ретрансляторами используются механизмы IPsec для IPv6 [7]. Если клиентское сообщение проходит через множество ретрансляторов, для каждого из них должны быть организованы независимые парные отношения доверия. Т. е. если сообщение от клиента C будет транслироваться ретранслятором A ретранслятору B, а затем серверу, ретрансляторы A и B должны быть настроены на использование IPSec при обмене сообщениями между собой, а ретранслятор B и сервер должны использовать IPSec для защиты своих сообщений.

Ретрансляторы и серверы, обеспечивающие защищенную трансляцию, используют IPsec в соответствии с приведенным ниже описанием.

Селекторы

На ретрансляторах вручную задаются адреса других ретрансляторов и серверов, которым пересылаются сообщения DHCP. Каждый ретранслятор и сервер, использующий IPsec для защиты сообщений DHCP, должен также иметь список ретрансляторов, которым сообщения будут возвращаться. Селекторами для ретрансляторов и серверов будут пары адресов, определяющие стороны обмена сообщениями DHCP через порты DHCPv6 UDP 546 и 547.

Режим

Ретрансляторы и серверы используют транспортный режим и ESP. Информация в сообщениях DHCP обычно не является конфиденциальной, поэтому шифрование не применяется (т. е. можно задать NULL-шифрование).

Управление ключами

Ретрансляторы и серверы применяются внутри организации, поэтому схема с открытыми ключами не требуется. Поскольку ретрансляторы и серверы настраиваются вручную, ручная настройка ключей может оказаться достаточной, но она не обеспечит защиты от повторного использования сообщений. Поэтому **следует** поддерживать IKE с заранее распространенными секретами и **можно** применять IKE с открытыми ключами.

Политика безопасности

Сообщения DHCP между трансляторами и серверами следует принимать лишь от партнеров DHCP указанных в локальной конфигурации.

Проверка подлинности

Общие ключи, индексированные по IP-адресам отправителей в принятых сообщениях DHCP обеспечивают достаточную защиту для данного случая.

Доступность

Подходящие реализации IPsec очевидно будут доступны для серверов и ретрансляторов в многофункциональных устройствах, применяемых в корпоративных сетях и сетях ISP. Доступность IPsec для домашних устройств и оборудования, используемого в небольших сетях, менее очевидна.

[1] Denial of service attack - атака, нацеленная на отказ в обслуживании.

21.2. Проверка подлинности DHCP

Аутентификации сообщений DHCP обеспечивается с помощью опции Authentication (параграф 22.11). Аутентификационные данные из опции Authentication могут служить для надежного определения источника сообщения DHCP и подтвержения неизменности содержимого этого сообщения.

Опция Authentication обеспечивает основу для множества протоколов проверки подлинности. Два таких протокола определены здесь. Другие протоколы могут быть описаны в отдельных документах.

В сообщения DHCP **недопустимо** включать более одной опции Authentication.

Поле protocol в опции Authentication указывает конкретный протокол, используемый для генерации аутентификационных данных, включаемых в опцию. Поле algorithm указывает конкретный алгоритм для протокола аутентификации (например, поле algorithm может задавать алгоритм хэширования, служащий для создания кода MAC[1] в опции). Поле RDM[2] указывает метод обнаружения повторного использования.

21.3. Обнаружение повторного использования

Поле RDM определяет тип детектирования повторного использования, применяемый в поле Replay Detection.

Если поле RDM содержит значение 0x00, в поле детектирования повторного использования **должно** помещаться значение монотонно возрастающего счетчика. Использование счетчика типа текущего времени (например, временной мети NTP [9]) может снизить опасность атак с повторным использованием пакетов. Этот метод должны поддерживать все протоколы.

21.4. Протокол отложенной аутентификации

Если поле protocol имеет значение 2, для сообщения используется механизм «отложенной аутентификации» (delayed authentication). В этом случае клиент запрашивает проверку подлинности в соем сообщении Solicit и сервер отвечает сообщением Advertise, включающим аутентификационные данные. Эти данные включают значение nonce, создаваемое отправителем сообщения в качестве кода MAC для проверки подлинности сообщения и отправителя.

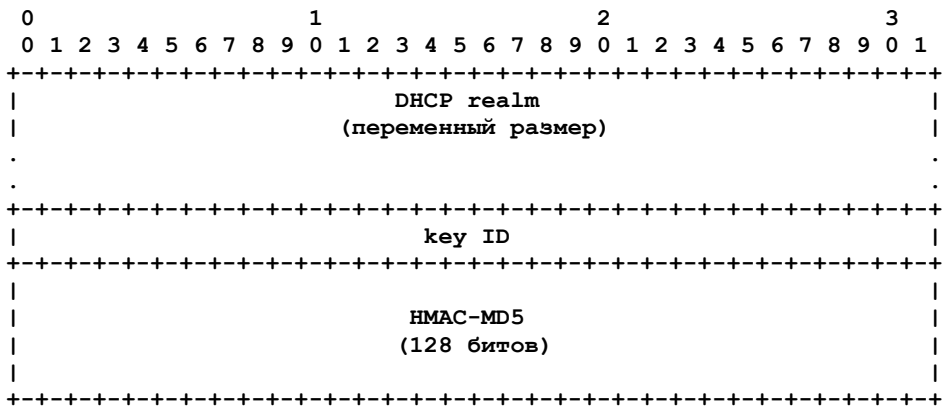
Здесь определено использование конкретного метода на основе протокола HMAC [8] с применением кода MD5 [16].

21.4.1. Использование опции Authentication при отложенной аутентификации

В сообщении Solicit клиент заполняет поля protocol, algorithm и RDM опции Authentication в соответствии со своими предпочтениями. Клиент устанавливает в поле replay detection значение 0 и опускает поле данных аутентификации. В поле option-len клиент устанавливает значение 11.

Во всех остальных сообщениях поля protocol и algorithm указывают метод, используемый для создания поля аутентификационных данных. Поле RDM указывает метод, применяемый для создания поля replay detection.

Формат аутентификационных данных (Authentication information) показан ниже.



DHCP realm

Область DHCP (realm), указывающая ключ, используемый для генерации значения HMAC-MD5.

key ID

Идентификатор, указывающий ключ, ичпользуемый для генерации значения HMAC-MD5.

HMAC-MD5

Код аутентификации сообщения, создаваемый путем применения алгоритма MD5 к сообщению DHCP с использованием ключа, заданного DHCP realm, client DUID и key ID.

Отправитель рассчитывает MAC с использованием алгоритма генерации HMAC [8] и хэш-функции MD5 [16]. В качестве входных данных функции HMAC-MD5 используется все сообщение DHCP (в поле MAC опции Authentication устанавливается значение 0), включая заголовок сообщения DHCP и поле опций.

Обсуждение.

Алгоритм 1 задает использование HMAC-MD5. Применение других механизмов (типа HMAC-SHA) будет описано как отдельный протокол.

Область DHCP используется для идентификации ключей проверки подлинности выбираемых так, чтобы обеспечивалась уникальность для каждого административного домена. Использование DHCP realm позволяет администраторам DHCP предотвратить конфликты идентификаторов ключей и обеспечить использующему DHCP хосту возможность аутентификации DHCP при переходе из одного административного домена в другой.

[1]Message authentication code - код аутентификации сообщения.
[2]Replay detection method - метод обнаружения повторного использования.

21.4.2. Проверка пригодности сообщения

Любые сообщения DHCP, содержащие более одной опции Authentication, **должны** отбрасываться.

Для проверки пригодности входящего сообщения получатель сначала проверяет значение поля обнаружения повторов в соответствии с методом, заданным в поле RDM. Затем рассчитывается значение MAC в соответствии с [8]. В качестве входных данных функции HMAC-MD5 используется все сообщение DHCP (поле MAC считается равным 0). Если рассчитанное получателем значение MAC отличается от содержащегося в опции Authentication, получатель **должен** отбросить сообщение DHCP.

21.4.3. Использование ключей

Каждый клиент DHCP имеет набор ключей, каждый из которых идентифицируется значениями <DHCP realm, client DUID, key id>. Для каждого ключа задан срок действия и ключ не может применяться раньше или позже этого срока. Ключи распространяются клиентам с использованием того или иного механизма (out-of-band) вместе со сроками их действия. Механизмы распространения ключей и задания их срока действия выходят за рамки этого документа.

Клиент и сервер используют один ключ клиента для аутентификации сообщений DHCP во время сессии (пока клиент не передаст следующее сообщение Solicit).

21.4.4. Поведение клиента при отложенной аутентификации

Клиент объявляет о своем намерении использовать аутентификацию DHCP путем включения опции Authentication в сообщение Solicit. Сервер выбирает ключ для клиента на основе клиентского DUID. Далее этот ключ используется клиентом и сервером для аутентификации всех сообщений DHCP в течение сессии.

21.4.4.1. Передача сообщений Solicit

Когда клиент передает сообщение Solicit с намерением использовать аутентификацию, он включает опцию Authentication с желаемым протоколом, алгоритмом и RDM, как описано в параграфе 21.4. Клиент не включает данных обнаружения повторного использования и проверки подлинности в опцию Authentication.

21.4.4.2. Прием сообщений Advertise

Клиент проверяет пригодность всех сообщений Advertise с опцией Authentication, задающей протокол отложенной аутентификации, как описано в параграфе 21.4.2.

Поведение клиента в случаях, когда Advertise не содержит аутентификационных данных или проверка пригодности не проходит, определяется локальной политикой клиента. В соответствии со своей политикой клиент **может** ответить на сообщение Advertise, которое не было аутентифицировано.

Решение об установке локальной политики, позволяющей принимать неаутентифицированные сообщения, следует принимать с осторожностью. Восприятие таких сообщений Advertise может сделать клиента уязвимым для подмен и других атак. Если локальные пользователи не уведомляются явно о восприятии клиентом неаутентифицированного сообщения, пользователи согут сделать некорректный вывод о получении аутентифицированного адреса и не заметить атаки с использованием неаутентифицированных сообщений DHCP.

Клиенты **должны** быть настроены на отбрасывание неуатентифицированных сообщений и **следует** задавать по умолчанию отбрасывание неаутентифицированных сообщений, если у клиента настроен ключ аутентификации или другие аутентификационные данные. Клиент **может** различать сообщения Advertise без данных аутентификации и сообщения, не прошедшие проверку на пригодность. Например, клиент может воспринимать первый тип сообщений и отбрасывать второй. Если клиент воспринимает неаутентифицированные сообщения, ему **следует** уведомлять об этом пользователей и делать запись в системном журнале.

21.4.4.3. Передача сообщений Request, Confirm, Renew, Rebind, Decline, Release

Если клиент подтвердил подлинность сообщения Advertise, с помощью которого клиент выбрал сервер, клиент **должен** генерировать аутентификационные данные для последующих сообщений Request, Confirm, Renew, Rebind и Release, передаваемых серверу, как описано в параграфе 21.4. При отправке последующих сообщений клиент **должен** использовать тот же ключ, который сервер применил для генерации аутентификационных данных.

21.4.4.4. Передача сообщений Information-request

Если сервер выбрал ключ для клиента в предшествующем обмене сообщениями (параграф 21.4.5.1), клиент **должен** использовать этот ключ для генерации аутентификационных данных в течение всей сессии.

21.4.4.5. Прием сообщений Reply

Если клиент подтвердил подлинность воспринятого им сообщения Advertise, он **должен** проверять пригодность сообщений Reply от сервера. Клиент **должен** отбрасывать сообщение Reply, если оно не прошло проверку на пригодность и **может** записывать такие факты в системный журнал. Если сообщение Reply не прошло проверку на пригодность, клиент **должен** перезапустить процесс DHCP, передав новое сообщение Solicit.

Если клиент воспринял сообщение Advertise без аутентификационных данных или не прошедшее проверки на пригодность, он **может** воспринимать от сервера неаутентифицированные сообщения Reply.

21.4.4.6. Прием сообщений Reconfigure

Клиент **должен** отбрасывать сообщения Reconfigure, если оно не прошло проверку на пригодность и **может** записывать такие события в системный журнал.

21.4.5. Поведение сервера при отложенной аутентификации

После приема сообщения Solicit с опцией Authentication сервер выбирает ключ для клиента на базе DUID клиента и заданных для сервера правил выбора ключей. Сервер указывает выбранный ключ в сообщении Advertise и использует его для проверки пригодности последующих сообщений от этого клиента.

21.4.5.1. Прием сообщений Solicit и отправка Advertise

Сервер выбирает ключ для клиента и включает аутентификационные данные в сообщение Advertise, возвращаемое клиенту, как описано в параграфе 21.4. Сервер **должен** записать идентификатор выбранного для клиента ключа и использовать этот ключ для проверки последующих сообщений от клиента.

21.4.5.2. Прием сообщений Request, Confirm, Renew, Rebind, Release и отправка Reply

Сервер использует указанный в сообщении ключ и проверяет сообщение в соответствии с параграфом 21.4.2. Если сообщение не проходит проверку на пригодность или сервер на знает ключа, указанного в поле key ID, он **должен** отбросить сообщение и может записать этот факт в системный журнал.

Если сообщение прошло проверку на пригодность, сервер отвечает на него соответствующим сообщением, как описано в параграфе 18.2. Сервер **должен** включить в ответ аутентификационную информацию, созданную с использованием ключа, который указан в принятом сообщении, как описано в параграфе 21.4.

21.5. Протокол проверки подлинности ключа реконфигурации

Протокол проверки подлинности ключа реконфигурации обеспечивает защиту от некорректной настройки клиента, вызванную сообщением Reconfigure от вредоносного сервера DHCP. В этом протоколе сервер DHCP передает клиенту ключ реконфигурации (Reconfigure Key) в начальном обмене сообщениями DHCP. Клиент записывает ключ для проверки подлинности последующих сообщений Reconfigure от этого сервера. Сервер включает в последующие сообщения Reconfigure значение HMAC, рассчитанное с использованием Reconfigure Key.

Ключ Reconfigure Key от сервера и значения HMAC в последующих сообщениях Reconfigure передаются в виде аутентификационных данных в опции Authentication. Формат аутентификационных данных описан ниже.

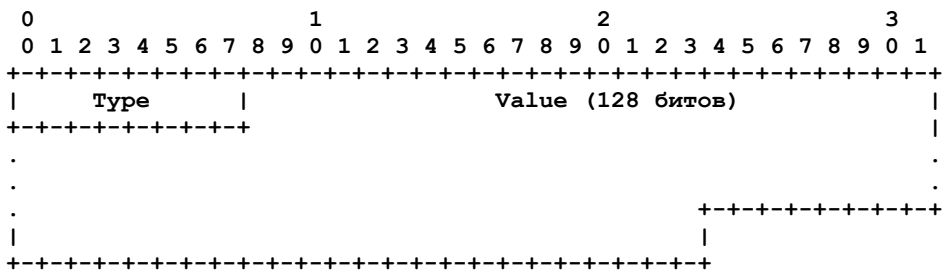
Протокол Reconfigure Key используется (по инициативе сервера) лишь в тех случаях, когда клиент и сервер не применяют какого-либо иного протокола аутентификации, согласованного ими для сообщений Reconfigure.

21.5.1. Опция Authentication в протоколе Reconfigure Key Authentication

Ниже приведены поля, используемые для протокола аутентификации ключа перенастройки.

protocol	3
algorithm	1
RDM	0

Формат опции Authentication для протокола Reconfigure Key Authentication показан ниже.



Type

Тип данных в поле Value:

1 значение ключа реконфигурации (используется в сообщении Reply);
2 значение HMAC-MD5 для сообщения (используется в сообщении Reconfigure).

Value

Данные, определяемые типом поля.

21.5.2. Поведение сервера для протокола Reconfigure Key

Сервер выбирает ключ реконфигурации (Reconfigure Key) для клиента в процессе обмена сообщениями Request/Reply, Solicit/Reply или Information-request/Reply. Сервер записывает Reconfigure и передает его клиенту в опции Authentication сообщения Reply.

Ключ реконфигурации имеет размер 128 битов и **должен** быть криптостойким случайным или псевдослучайным значением, которое сложно предсказать.

Для обеспечения аутентификации сообщения Reconfigure сервер выбирает значение детектирования повторного использования в соответствии с выбранным сервером методом RDM и рассчитывает значение HMAC-MD5 сообщения Reconfigure, используя ключ реконфигурации для клиента. При расчете HMAC-MD5 сервер учитывает все сообщение DHCP Reconfigure, включая опцию Authentication (при расчете значение поля HMAC-MD5 в опции Authentication принимается равным 0). Сервер включает HMAC-MD5 в аутентификационные данные опции Authentication в передаваемом клиенту сообщении Reconfigure.

21.5.3. Поведение клиента для протокола Reconfigure Key

Клиент будет получать Reconfigure Key от сервера в начальном отклике Reply. Клиент записывает Reconfigure Key для последующей аутентификации сообщений Reconfigure.

Для аутентификации сообщения Reconfigure клиент рассчитывает значение HMAC-MD5 для всего сообщения DHCP, используя полученный от сервера ключ реконфигурации. Если полученное значение HMAC-MD5 совпадает с принятым в опции Authentication, клиент воспринимает сообщение Reconfigure.

22. Опции DHCP

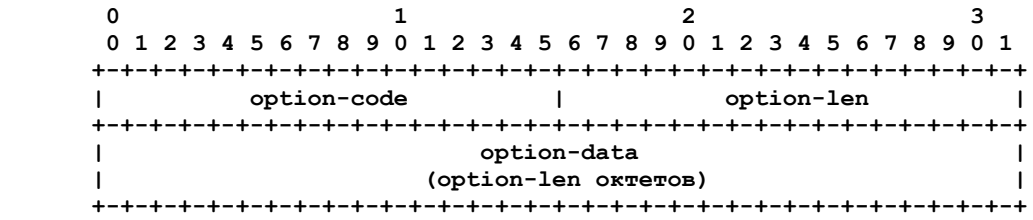
Опции служат для передачи дополнительной информации и параметров в сообщениях DHCP. Во всех опциях используется общий базовый формат, описанный в параграфе 22.1. Значения представляются в сетевом порядке байтов.

Этот документ представляет опции, определенные как часть спецификации DHCP. Другие опции могут быть описаны в отдельных документах.

Если явно не указано иное, каждая опция может появляться только в области опций сообщения DHCP и только один раз. Если опция может присутствовать в нескольких экземплярах, каждый из них рассматривается отдельно и области данных таких опций **недопустимо** объединять или комбинировать иным способом.

22.1. Формат опций DHCP

Формат опций DHCP показан ниже.



option-code
Целое число без знака, указывающее конкретный тип данной опции.

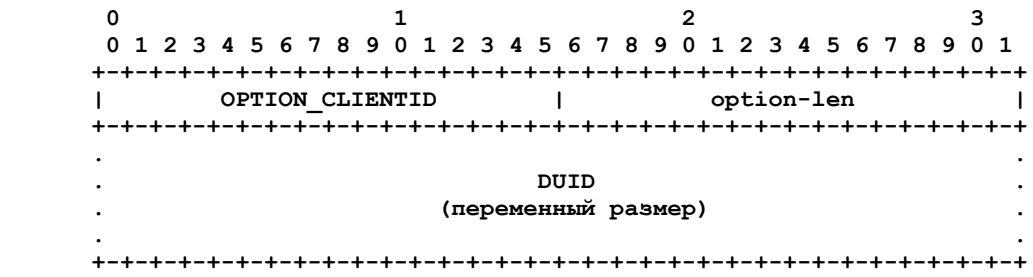
option-len
Целое число без знака, указывающее размер поля option-data в октетах.

option-data
Данные опции, формат которых зависит от определения конкретной опции.

Область действия опции DHCPv6 определяется инкапсуляцией. Некоторые опции применимы к клиенту в целом, некоторые относятся к IA, а некоторые - к конкретным адресам в ассоциации IA. Два последних случая рассматриваются в параграфах 22.4 и 22.6.

22.2. Опция Client Identifier

Опция Client Identifier служит для передачи значения DUID (раздел 9), указывающего клиента в сообщениях между клиентом и сервером. Формат опции Client Identifier показан ниже.



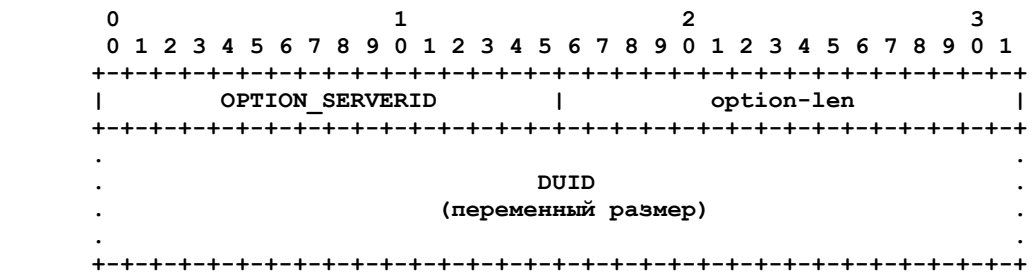
option-code
OPTION_CLIENTID (1).

option-len
Размер DUID в октетах.

DUID
Идентификатор DUID для клиента.

22.3. Опция Server Identifier

Опция Server Identifier служит для передачи значения DUID (раздел 9), указывающего сервер в сообщениях между клиентом и сервером. Формат опции Server Identifier показан ниже.



option-code
OPTION_SERVERID (2).

option-len
Размер DUID в октетах.

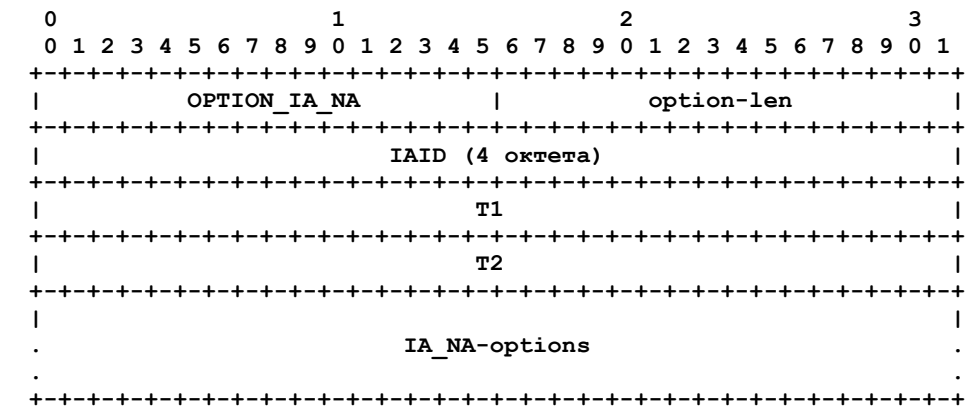
DUID
Идентификатор DUID для сервера.

22.4. Опция IA_NA

Опция Identity Association for Non-temporary Addresses (IA_NA) служит для передачи параметров и адресов, связанных с IA_NA.

Адреса в опции IA_NA не являются временными (параграф 22.5).

Формат опции показан ниже



option-code
OPTION_IA_NA (3).

option-len
12 + размер поля IA_NA-options.

IAID
Уникальный идентификатор для этой ассоциации IA_NA. Значение IAID должно быть уникальным среди всех IA_NA данного клиента. Пространство значений IA_NA IAID отделено от пространства IA_TA IAID.

T1
Время контакта клиента с сервером, от которого были получены адреса в IA_NA, для продления срока действия этих адресов. T1 указывает продолжительность в секундах относительно текущего времени.

T2
Время контакта клиента с любым доступным сервером для продления срока действия адресов, назначенных IA_NA. T2 указывает продолжительность в секундах относительно текущего времени.

IA_NA-options
Опции, связанные с данной ассоциацией IA_NA.

Поле опций IA_NA-options инкапсулирует опции, относящиеся к данной ассоциации IA_NA. Например, все опции IA Address с адресами, относящимися к данной IA_NA, помещаются в поле IA_NA-options.

Опция IA_NA может присутствовать только в области опций сообщения DHCP. Сообщение DHCP может содержать множество опций IA_NA.

Статус любой операции, включающей данную ассоциацию IA_NA, указывается опцией Status Code в поле IA_NA-options.

Следует отметить, что IA_NA не имеет явного срока действия или продолжительности аренды. Когда действительные сроки действия всех адресов в IA_NA завершаются, IA_NA может рассматриваться как просроченная. Значения T1 и T2 включены для того, чтобы предоставить серверам явный контроль над повторным обращением клиента к серверу по поводу конкретной ассоциации IA_NA.

В сообщении, отправленном клиентом серверу, поля T1 и T2 указывают предпочитаемые клиентом значения этих параметров. Клиент указывает в полях T1 и T2 значение 0, если у него нет предпочтений. Клиент **должен** использовать значения полей T1 и T2 для своих параметров T1 и T2, если в этих полях не указаны нулевые значения. В полях T1 и T2 указывается число секунд.

Сервер выбирает значения T1 и T2 так, чтобы позволить клиенту продлить срок действия любых адресов в IA_NA до его завершения даже в случае кратковременной недоступности сервера. Рекомендуемые значения T1 и T2 составляют 0,5 и 0,8 (соответственно) от кратчайшего предпочтительного срока действия адресов в IA, которые сервер готов продлить. Если «кратчайшее» предпочтительное время задано бесконечным (0xffffffff), для T1 и T2 также рекомендуется установить 0xffffffff. Если время обновления адресов в IA_NA отдается на откуп клиенту, сервер устанавливает для T1 и T2 значения 0.

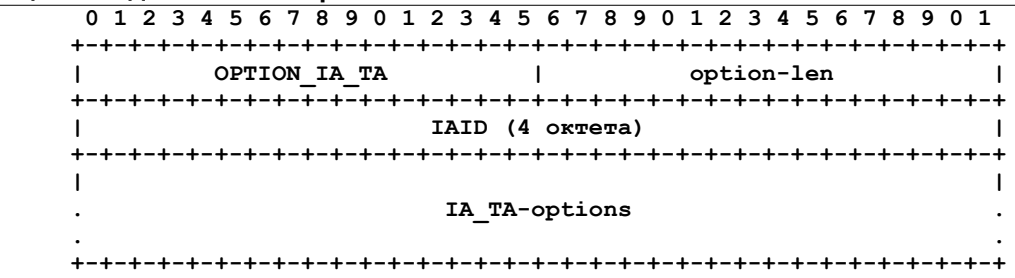
Если сервер получает IA_NA с T1 > T2, а T1 и T2 > 0, он игнорирует непригодные значения T1 и T2, обрабатывая IA_NA как будто клиент установил для T1 и T2 значение 0.

Если клиент получает IA_NA с T1 > T2, а T1 и T2 > 0, он отбрасывает опцию IA_NA и обрабатывает оставшуюся часть сообщения как будто в нем нет непригодной опции IA_NA.

Следует с осторожностью использовать значение 0xffffffff (бесконечность) для T1 или T2. Клиент не будет пытаться продлить срок действия каких-либо адресов в IA с T1 = 0xffffffff и никогда не будет пытаться использовать сообщение Rebind для поиска другого сервера с целью продления срока действия адресов в IA при T2 = 0xffffffff.

22.5. Опция IA_TA

Опция Identity Association for the Temporary Addresses (IA_TA) служит для передачи параметров и адресов, связанных с IA_TA. Все адреса из этой опции используются клиентом в качестве временных, как определено в RFC 3041 [12]. Формат опции IA_TA показан ниже.



option-code
OPTION_IA_TA (4).

option-len
4 + размер поля IA_TA-options.

IAID
Уникальный идентификатор для этой ассоциации IA_TA. Значение IAID должно быть уникальным среди всех IA_TA данного клиента. Пространство значений IA_TA IAID отделено от пространства IA_NA IAID.

IA_TA-options
Опции, связанные с данной ассоциацией IA_TA.

Поле опций IA_TA-options инкапсулирует опции, относящиеся к данной ассоциации IA_TA. Например, все опции IA Address с адресами, относящимися к данной IA_TA, помещаются в поле IA_TA-options.

Каждая опция IA_TA содержит «набор» временных адресов, т. е. не более одного адреса для каждого префикса, назначенного каналу, к которому подключен клиент.

Опция IA_TA может присутствовать только в области опций сообщения DHCP. Сообщение DHCP может содержать множество опций IA_TA.

Статус любой операции, включающей эту ассоциацию IA_NA, указывается опцией Status Code в поле IA_NA-options.

Следует отметить, что IA не имеет явного срока действия или продолжительности аренды. Когда действительные сроки действия всех адресов в IA_TA завершаются, IA может рассматриваться как просроченная.

Опция IA_TA не включает значений T1 и T2. Клиент **может** запросить продление срока действия временных адресов путем включения адресов в опцию IA_TA переданного серверу сообщения Renew или Rebind. Например, клиент будет запрашивать продление срока действия временных адресов, чтобы позволить приложению сохранить соединение TCP.

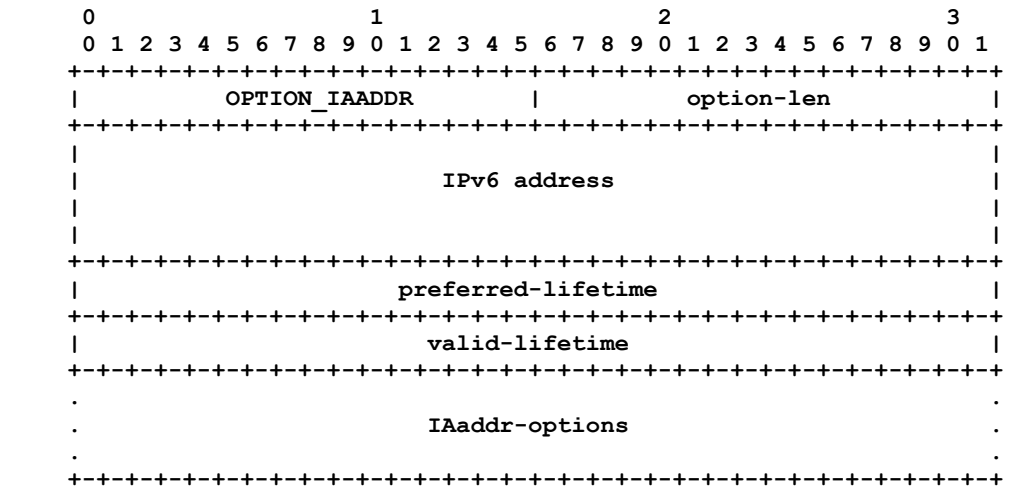
Клиент получает новые временные адреса путем передачи серверу опции IA_TA с новым идентификатором IAID. Запрос новых временных адресов у сервера эквивалентен генерации новых временных адресов, описанной в RFC 3041. Сервер создаст новые адреса и возвратит их клиенту. Клиенту следует запрашивать новые временные адреса до завершения срока действия полученных ранее временных адресов.

Сервер **должен** возвращать прежний набор временных адресов для ассоциации IA_TA (указанной IAID), если эти адреса остаются пригодными. По истечении срока действия адресов в IA_TA идентификатор IAID может использоваться для другой ассоциации IA_TA с новыми временными адресами.

Эта опция **может** присутствовать в сообщениях Confirm, если сроки действия временных адресов в соответствующей IA еще не истекли.

22.6. Опция IA Address

Опция IA Address служит для задания адресов IPv6, связанных с IA_NA или IA_TA и должна инкапсулироваться в поле Options опции IA_NA или IA_TA. Поле Options инкапсулирует опции, относящиеся к данному адресу.



option-code
OPTION_IAADDR (5).

option-len
24 + размер поля IAaddr-options.

IPv6 address
Адрес IPv6.

preferred-lifetime
Предпочтительный срок действия адреса IPv6, указанный в секундах.

valid-lifetime

Действительный срок годности адреса IPv6, указанный в секундах.

IAaddr-options

Опции, связанные с этим адресом.

В сообщении от клиента значения предпочтительного и действительного срока годности указывают предпочтения клиента. Клиент может указать значения 0, если у него нет предпочтений. Клиент **должен** использовать значения предпочтительного и действительного срока годности адресов из сообщения от сервера. Значения в этих полях указывают число секунд оставшегося срока действия.

Клиент отбрасывает любые адреса, для которых предпочтительный срок действия превышает действительный. Сервер игнорирует указанные клиентом сроки действия, если предпочтительное время превышает действительное, а также игнорирует установленные клиентом значения T1 и T2, если они больше предпочтительного срока действия.

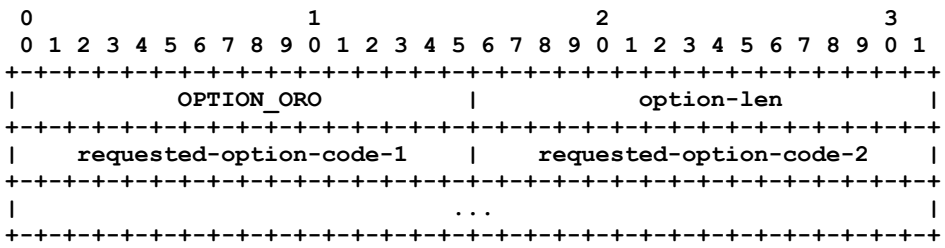
Следует соблюдать осторожность при задании действительного срока годности 0xffffffff (бесконечно), поскольку это ведет к постоянному назначению адреса для клиента.

Опция IA Address может присутствовать лишь в опции IA_NA или IA_TA. Допускается наличие множества опций IA Address в опции IA_NA или IA_TA.

Статус любой операции, включающей IA Address, указывается опцией Status Code в поле IAaddr-options.

22.7. Опция Option Request

Опция Option Request служит для указания списка опций в сообщении между клиентом и сервером.



option-code

OPTION_ORO (6).

option-len

2 * число запрашиваемых опций.

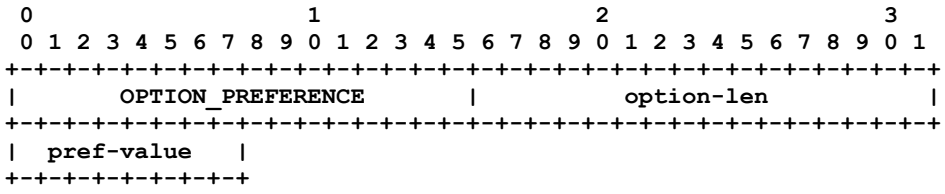
requested-option-code-n

Код запрашиваемой клиентом опции.

Клиент **может** включать опцию Option Request в сообщения Solicit, Request, Renew, Rebind, Confirm, Information-request для информирования сервера об опциях, которые он хочет получить от сервера. Сервер **может** включить опцию Option Request в сообщение Reconfigure[1] для индикации опций, которые клиенту следует запросить у сервера.

22.8. Опция Preference

Опция Preference передается сервером клиенту для указания предпочтительности данного сервера.



option-code

OPTION_PREFERENCE (7).

option-len

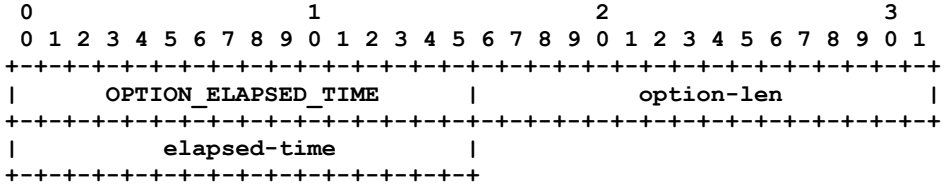
1.

pref-value

Значение уровня предпочтения для данного сервера.

Сервер **может** включать опцию Preference в сообщение Advertise для воздействия на выбор сервера клиентом. Использование опции и интерпретация ее значений рассмотрены в параграфе 17.1.3.

22.9. Опция Elapsed Time



option-code

OPTION_ELAPSED_TIME (8).

option-len

2.

elapsed-time

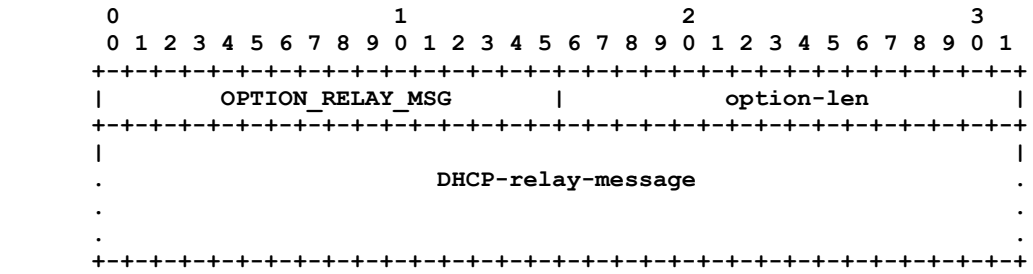
Время, прошедшее с момента инициирования клиентом текущей транзакции DHCP, в сотых долях секунды (10^{-2}).

[1] В оригинале ошибочно сказано «в опцию Reconfigure». См. https://www.rfc-editor.org/errata/eid2509. *Прим. перев.*

Клиент **должен** включать опцию Elapsed Time в сообщения для индикации продолжительности попыток завершить обмен сообщениями DHCP. Время отсчитывается с момента передачи клиентом первого сообщения (в нем поле elapsed-time имеет значение 0). Серверы и ретрансляторы используют данные этой опции в качестве входной информации правил управления откликами сервера на сообщения клиентов. Например, эта опция позволяет вторичному серверу DHCP ответить на запрос, когда основной сервер не смог ответить в течение приемлемого времени. Время указывается 16-битовым целым числом без знака. Клиент использует значение 0xffff для индикации того, что прошло времени больше, чем можно указать в опции Elapsed Time.

22.10. Опция Relay Message

Опция Relay Message служит для передачи сообщений DHCP в сообщении Relay-forward или Relay-reply.



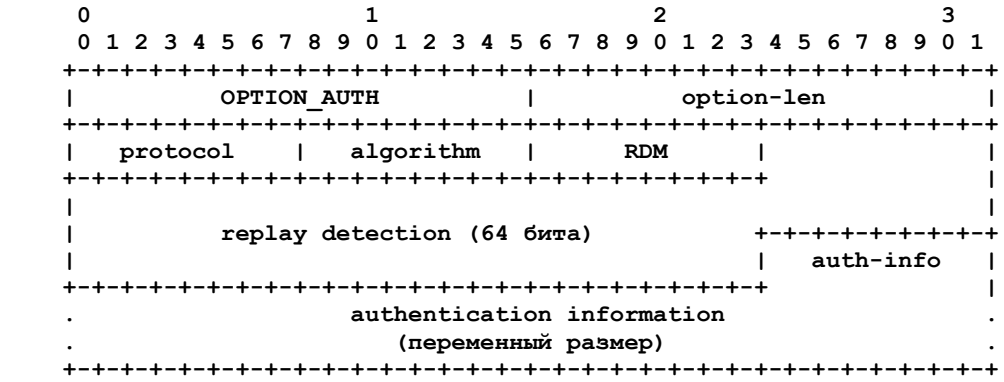
option-code
OPTION_RELAY_MSG (9)

option-len
Размер DHCP-relay-message.

DHCP-relay-message
В сообщении Relay-forward принятое сообщение передается «дословно» следующему ретранслятору или серверу, в сообщении Relay-reply исходное сообщение копируется и транслируется коиенту или следующему ретранслятору, чей адрес указан в поле peer-address сообщения Relay-reply.

22.11. Опция Authentication

Опция Authentication передает аутентификационные данные для проверки подлинности отправителя и содержимого сообщений DHCP. Использование опции Authentication описано в разделе 21, формат показан ниже.



option-code
OPTION_AUTH (11)

option-len
11 + размер поля authentication information.

protocol
Протокол проверки подлинности, используемый в данной опции.

algorithm
Алгоритм, используемый протоколом аутентификации.

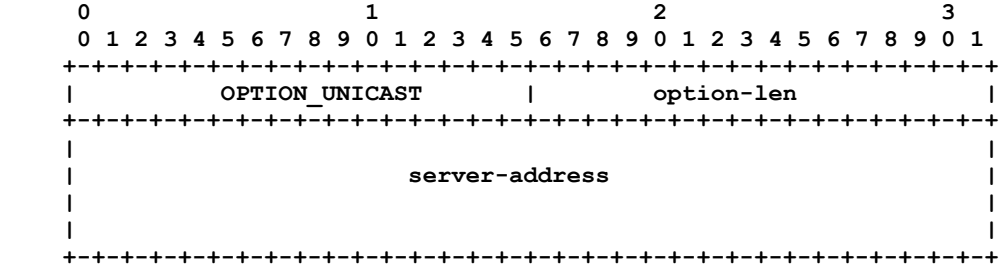
RDM
Метод обнаружения повторного использования, применяемый в этой опции.

Replay detection
Информация детектирования повторного использования для RDM.

authentication information
Аутентификационные данные, определяемые протоколом и алгоритмом проверки подлинности в этой опции.

22.12. Опция Server Unicast

Сервер передает эту опцию клиенту для индикации возможности взаимодействия с сервером по индивидуальному адресу. Формат опции показан ниже.



option-code
OPTION_UNICAST (12).
option-len
16.
server-address
IP-адрес, по которому клиенту следует отправлять сообщения для сервера.

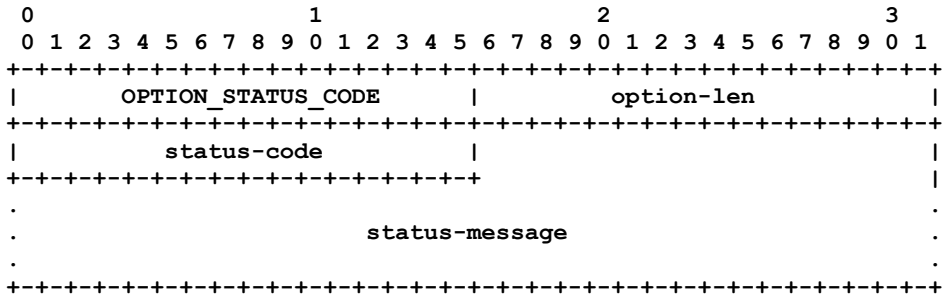
Сервер указывает адрес IPv6 по которому клиент передает свои сообщения, в поле server-address. Получивший эту опцию клиент при наличии возможности и целесообразности передает сообщения напрямую серверу, используя адрес IPv6, указанный в поле server-address этой опции.

Когда сервер передал клиенту опцию Unicast, некоторые сообщения от клиента не будут транслироваться ретрансляторами и не будут включать опцию Relay Agent от ретрансляторов. Поэтому серверам следует использовать для клиента опцию Unicast лишь в тех случаях, когда ретрансляторы не передают опции Relay Agent. Сервер DHCP отвергает все сообщения, неправомерно переданные по индивидуальному адресу, чтобы обеспечить трансляцию сообщений ретрансляторами при использовании опции Relay Agent.

Подробное описание ситуаций, когда клиент может отправлять сообщения по индивидуальному адресу сервера, приведено в разделе 18.

22.13. Опция Status Code

Эта опция возвращает информацию о состоянии, относящуюся к сообщению DHCP или опции, в которой она указана.

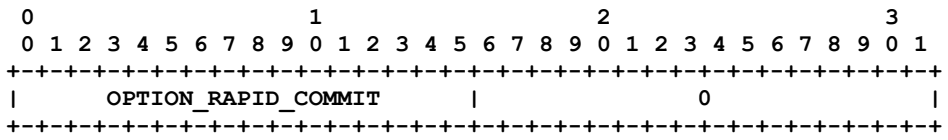


option-code
OPTION_STATUS_CODE (13).
option-len
2 + размер status-message.
status-code
Числовой код состояния для этой опции (параграф 24.4).
status-message
Текстовая строка в кодировке UTF-8, пригодная для вывода конечному пользователю. Использование null-символа в конце **недопустимо**.

Опция Status Code может присутствовать в поле опций сообщения DHCP и/или другой опции. Если опции Status Code нет в сообщении, где такая опция может присутствовать, предполагается статус Success.

22.14. Опция Rapid Commit

Опция Rapid Commit служит сигналом использования обмена из двух сообщений для назначения адресов.



option-code
OPTION_RAPID_COMMIT (14).
option-len
0.

Клиент **может** включать эту опцию в сообщение Solicit, если он готов к обмену Solicit-Reply, описанному в параграфе 17.1.1.

Сервер **должен** включать эту опцию в сообщение Reply, передаваемое в ответ на Solicit, при завершении обмена сообщениями Solicit-Reply.

Обсуждение.

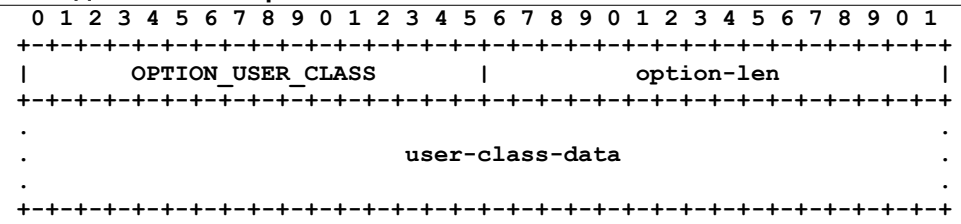
Каждый сервер, передающий сообщение Reply в ответ на Solicit с опцией Rapid Commit, будет представлять назначенные адреса в сообщении Reply и не будет получать от клиента подтверждения приема данного сообщения Reply. Поэтому при наличии нескольких серверов, отвечающих на сообщение Solicit с опцией Rapid Commit некоторые серверы будут назначать адреса, которые клиент не будет использовать.

Проблема неиспользованных адресов может быть смягчена, например, организацией службы DHCP так, чтобы на запросы Solicit отвечал лишь один сервер или адреса назначались на короткое время.

22.15. Опция User Class

Опция User Class используется клиентом для указания типа или категории представляемого им пользователя или приложения.

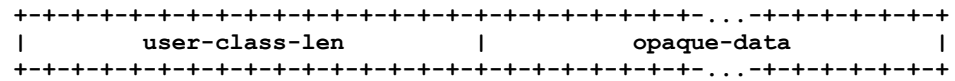
Формат опции User Class показан ниже.



option-code
OPTION_USER_CLASS (15).
option-len
Размер поля данных опции (user-class-data).
user-class-data
Классы пользователей, поддерживаемые клиентом.

Информация в области данных этой опции содержит одно или несколько неанализируемых (opaque) полей, представляющих класс или классы пользователей, к которым относится клиент. Сервер выбирает конфигурационные данные для клиента на основе классов, указанных в этой опции. Например, опция User Class может быть использована для настройки для сотрудников бухгалтерии принтера, отличающегося от используемого отделом маркетинга. Информация о классе, передаваемая в этой опции, **должна** быть настраиваемой со стороны клиента.

Область данных этой опции **должна** содержать один или несколько экземпляров данных класса пользователей. Формат этих экземпляров показан ниже.

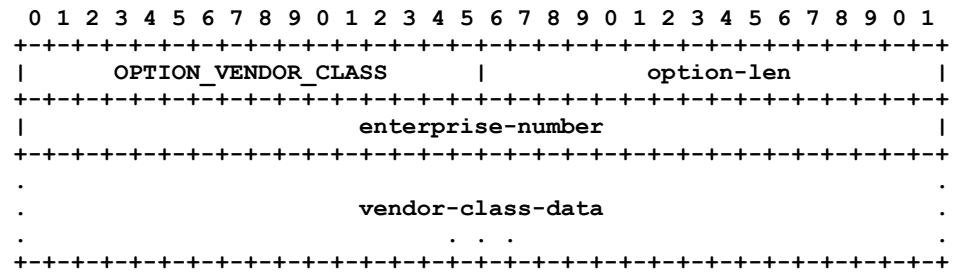


Поле user-class-len имеет размер 2 октета и задает размер данных класса пользователя (сетевой порядок байтов).

Сервер интерпретирует указанные этой опцией классы в соответствии со своими настройками для выбора подходящей клиенту конфигурационной информации. Сервер может использовать лишь те классы пользователей, которые настроены на нем для выбора конфигурационных данных клиента, и будет игнорировать все прочие классы. В отклики на сообщения с опцией User Class сервер включает опцию User Class, содержащую те классы, которые сервер успешно интерпретировал, так что клиент может быть проинформирован об интерпретируемых сервером классах.

22.16. Опция Vendor Class

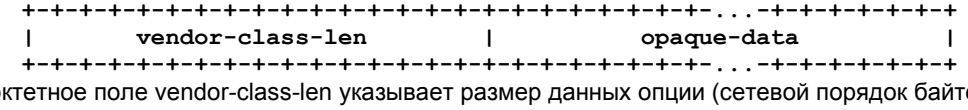
Эта опция используется клиентом для указания производителя оборудования, на котором работает клиент. Информация в области данных этой опции содержит одно или несколько неанализируемых (opaque) полей, которые указывают детали аппаратной конфигурации. Формат опции Vendor Class показан ниже.



option-code
OPTION_VENDOR_CLASS (16).
option-len
4 + размер поля данных опции.
enterprise-number
Зарегистрированный производителем в IANA [6] идентификатор Enterprise Number.
vendor-class-data
Аппаратная конфигурация хоста, на котором работает клиент.

Поле vendor-class-data содержит последовательность отдельных элементов, каждый из которых описывает ту или иную характеристику аппаратной конфигурации клиента. Примерами экземпляров vendor-class-data могут служить версия операционной системы, в которой работает клиент, или объем оперативной памяти у клиента.

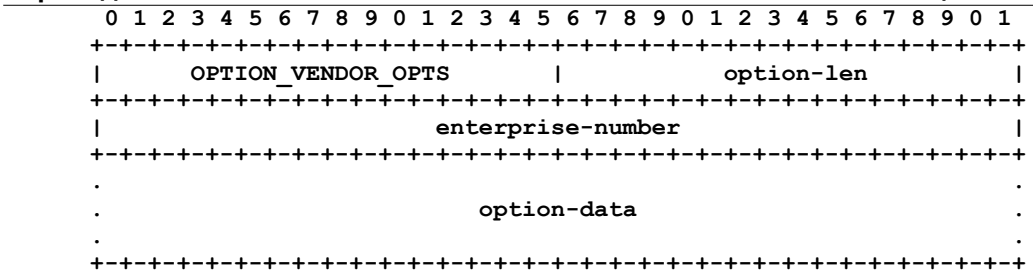
Каждый экземпляр vendor-class-data использует показанный ниже формат.



Двухоктетное поле vendor-class-len указывает размер данных опции (сетевой порядок байтов).

22.17. Опция Vendor-specific Information

Эта опция используется клиентами и серверами для обмена фирменной информацией производителей.



option-code
OPTION_VENDOR_OPTS (17)

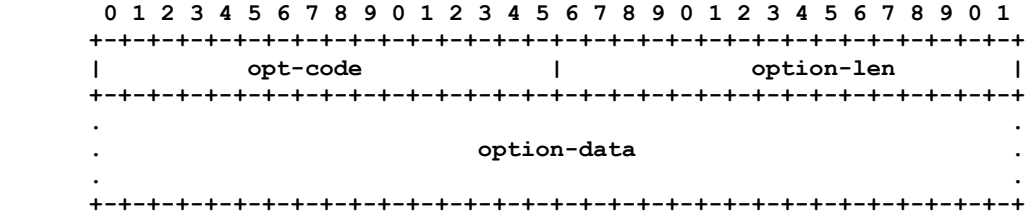
option-len
4 + размер поля option-data.

enterprise-number
Зарегистрированное производителем значение Enterprise Number из реестра IANA [6].

option-data
Неанализируемый объект, интерпретируемый клиентом и сервером по фирменному коду производителя[1].

Определение информации, передаваемой в этой опции, зависит от производителя, который указывается в поле enterprise-number. Использование фирменной информации позволяет улучшить работу за счет дополнительных возможностей фирменной реализации DHCP. Клиент DHCP, не получивший запрошенной фирменной информации, будет настроен так, чтобы стек протоколов IPv6 на устройстве функционировал нормально.

Поле инкапсулированных фирменных опций **должно** кодироваться в виде последовательности полей код-размер-значение, идентичных формату поля опций DHCP. Коды опций определяются производителем, указанным в поле enterprise-number, и не регистрируются в IANA. Каждая инкапсулированная опция использует показанный ниже формат.



opt-code
Код инкапсулированной опции.

option-len
Целое число без знака, определяющее размер поля option-data инкапсулированной опции в октетах.

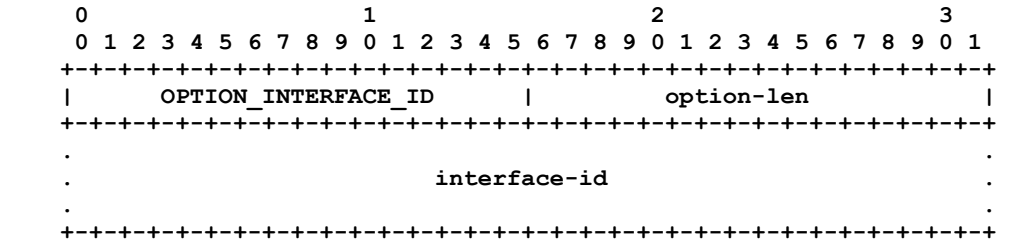
option-data
Область данных инкапсулированной опции.

В сообщении DHCP может присутствовать множество экземпляров опции Vendor-specific Information, каждый из которых интерпретируется в соответствии с кодом, определенным производителем, который указан значением Enterprise Number в данной опции.

22.18. Опция Interface-Id

Ретранслятор **может** передавать опцию Interface-id для указания интерфейса, на котором было получено сообщение от клиента. Если ретранслятор получает сообщение Relay-reply с опцией Interface-id, он транслирует сообщение клиенту через указанный опцией интерфейс.

Формат опции Interface ID показан ниже.



option-code
OPTION_INTERFACE_ID (18).

option-len
Размер поля interface-id.

interface-id
Неанализируемое (opaque) значение произвольного размера, генерируемое ретранслятором для идентификации одного из своих интерфейсов.

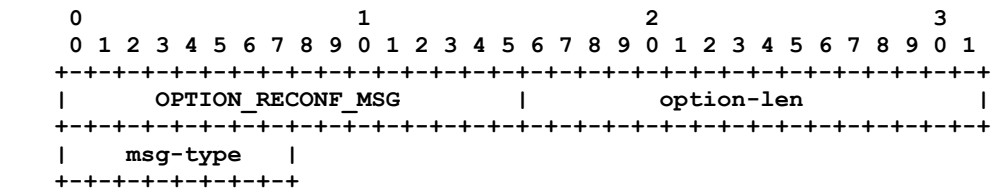
Сервер **должен** копировать опцию Interface-Id из сообщения Relay-Forward в сообщение Relay-Reply, передаваемое сервером ретранслятору в ответ на сообщение Relay-Forward. Эту опцию **недопустимо** использовать в каких-либо сообщениях, за исключением Relay-Forward и Relay-Reply.

Серверы **могут** использовать Interface-ID в правилах назначения параметров. Значение Interface-ID **следует** считать неинтерпретируемым и применять в правилах лишь точное совпадение, т. е. значения Interface-ID серверу **не следует** анализировать. Значение Interface-ID для интерфейса **следует** сохранять стабильным, например, оно не должно меняться при перезагрузке ретранслятора. Если значение Interface-ID будет меняться, сервер не сможет корректно применять его в правилах назначения параметров.

[1]В оригинале допущена ошибка. См. https://www.rfc-editor.org/errata/eid1373. *Прим. перев.*

22.19. Опция Reconfigure Message

Сервер включает опцию Reconfigure Message в сообщение Reconfigure для указания ответа клиента на него сообщением Renew или Information-request. Формат опции показан ниже.



option-code
OPTION_RECONF_MSG (19).

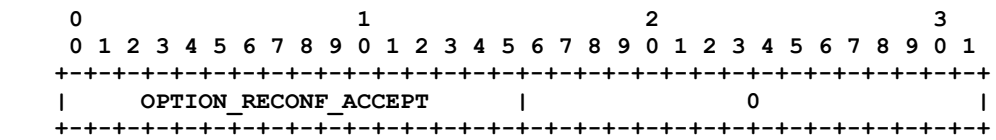
option-len
1.

msg-type
5 для сообщений Renew, 11 для Information-request.

Опция Reconfigure Message разрешена только в сообщениях Reconfigure.

22.20. Опция Reconfigure Accept

Клиент использует опцию Reconfigure Accept для анонсирования серверу своего намерения воспринимать сообщения Reconfigure, а сервер использует опцию для информирования клиента следует ли тому воспринимать сообщения Reconfigure. По умолчанию отсутствие этой опции означает нежелание воспринимать сообщения Reconfigure или инструкцию не воспринимать такие сообщения со стороны клиента и сервера, соответственно. Формат опции показан ниже.



option-code
OPTION_RECONF_ACCEPT (20).

option-len
0.

23. Вопросы безопасности

Угрозы DHCP исходят прежде всего изнутри (в предположении корректно настроенной сети, где порты DHCPv6 блокируются на граничных шлюзах сети). Однако независимо от конфигурации шлюза возможные атаки внутренних и внешних злоумышленников одинаковы.

Использование заданных вручную предварительно распределяемых (preshared) ключей для IPsec на ретрансляторах и серверах не защищает от атак с повторным использованием сообщений DHCP. Используемые повторно сообщения можно считать DoSатакой, направленной на истощение ресурсов обработки, но не на ошибочную настройку или истощение других ресурсов типа адресов для распределения.

Одной из атак на клиентов DHCP является организация подставных серверов, которые будут предоставлять клиентам неприемлемую информацию. Мотивом такой атаки может служить организация MITM-атак[1], в результате которых клиент будет взаимодействовать с подставными серверами (например, DNS или NTP) вместо легитимных. Враждебный сервер позволяет также организовать DoS-атаку за счет некорректной настройки клиента, которая приведет для него к отказам сетевых коммуникаций.

Другой угрозой для клиентов DHCP являются ошибочно или случайно организованные серверы DHCP, которые будут отвечать на запросы клиентов DHCP, предоставляя тем непригодные параметры конфигурации.

Клиент DHCP может быть также атакован с помощью сообщений Reconfigure от вредоносного сервера, которые вынуждают клиента принять некорректные параметры конфигурации от такого сервера. Следует отметить, что даже при передаче клиентами своих откликов (сообщение Renew или Information-request) через ретранслятор, когда они могут быть получены только серверами, для которых транслируются сообщения DHCP, вредоносный сервер может направить клиенту свое сообщение Reconfigure, за которым следует (с некоторой задержкой) сообщение Reply, которое будет воспринято клиентом. Таким образом вредоносный сервер, который не находится на пути между клиентом и сервером может организовать атаку на клиента с помощью сообщений Reconfigure. Использование криптостойких идентификаторов транзакций, которые сложно предсказать, существенно снижает вероятность успеха таких атак.

Угрозой для серверов DHCP является маскировка недопустимых клиентов под легитимных. Мотивом таких атак может служить неправомерное использование услуг или обход системы аудита для сокрытия неблаговидных целей.

Угрозой для клиентов и серверов являются DoS-атаки на ресурсы. Такие атаки обычно ведут к истощению доступных адресов, ресурсов CPU или пропускной способности сети и могут возникать везде, где есть общие ресурсы.

В тех случаях, где ретрансляторы добавляют опции в сообщения Relay Forward, сообщения между сервером и ретранслятором могут использоваться для организации MITM- или DoS-атак.

В этой модели угроз не рассматривается вопрос конфиденциальности сообщений DHCP, поскольку протокол DHCP не используется для обмена аутентификационными или конфигурационными данными, которые должны храниться в секрете от других узлов.

[1]Man in the middle - перехват и изменение данных с участием человека.

Аутентификация DHCP обеспечивает проверку подлинности клиентов и серверов DHCP, а также целостности сообщений, передаваемых между ними. Аутентификация DHCP не обеспечивает защиты конфиденциальности сообщений DHCP.

Протокол отложенной аутентификации (Delayed Authentication), описанный в параграфе 21.4, использует секретный ключ, известный клиенту и серверу. Использование DHCP realm в общем ключе позволяет идентифицировать административные домены, чтобы клиент мог выбрать подходящий ключ или ключи при перемещении из одного домена в другой. Однако отложенная аутентификация не определяет механизма распространения ключей, поэтому клиенту будут нужны ключи для всех доменов, в которых он может находиться. Использование общих ключей не обеспечивает достаточного масштабирования и не предусматривает отзыва скомпрометированных ключей. Этот протокол предназначен для решения задач внутри одного домена, где можно организовать доставку ключей в режиме out-of-band (по отдельному каналу).

По причине возможности организации атак через сообщения Reconfigure клиент DHCP **должен** отбрасывать любые сообщения Reconfigure, которые не включают аутентификации или не могут пройти проверку подлинности.

Протокол Reconfigure Key, описанный в параграфе 21.5, обеспечивает защиту от использования враждебными серверами сообщений Reconfigure для организации DoS- или MITM-атак на клиентов. Этот протокол может быть взломан атакующими, которые могут перехватить начальное сообщение, где сервер DHCP указывает ключ для клиента.

Коммуникации между серверами и ретрансляторами, а также между парами ретрансляторов можно защитить с помощью IPSec, как описано в параграфе 21.1. Использование настройки вручную и установка статических ключей возможны в таких случаях, поскольку ретрансляторы и серверы относятся к одному административному домену и на ретрансляторах требуется специфическая настройка (например, задание списка адресов серверов DHCP) в дополнение к обычным настройкам IPSec.

24. Взаимодействие с IANA

Этот документ определяет несколько новых пространств имен, связанных с DHCPv6 и опциями DHCPv6:

- типы сообщений;
- коды состояний;
- идентификаторы DUID;
- коды опций.

Агентство IANA организовало реестры для хранения значений этих пространств имен, описанные в последующих параграфах. Эти пространства управляются агентством IANA и поддерживаются отдельно от пространств DHCPv4.

Новые групповые адреса, типы сообщений, коды состояний и типы DUID назначаются по процедуре Standards Action [11].

Новые коды опций DHCP назначаются предварительно после выпуска соответствующей спецификации в виде Internet Draft с рецензией назначенных экспертов [11]. Окончательное назначение кодов опций DHCP происходит по процедуре Standards Action в соответствии с RFC 2434 [11].

В этом документе указаны также три пространства имен (раздел 21), связанных с опцией Authentication (параграф 22.11). Эти пространства определены механизмами аутентификации для DHCPv4 в RFC 3118 [4].

Пространство имен для аутентификации, зарегистрированное IANA, является общим для DHCPv6 и DHCPv4. В будущем спецификации, определяющие новые протоколы, алгоритмы и механизмы RDM, будут явно указывать их применимость для DHCPv4, DHCPv6 или обоих протоколов.

24.1. Групповые адреса

В параграфе 5.1 определены приведенные ниже групповые адреса, которые выделены агентством IANA для DHCPv6.

All_DHCP_Relay_Agents_and_Servers	**FF02::1:2**
All_DHCP_Servers	**FF05::1:3**

24.2. Типы сообщения DHCP

Агентство IANA зафиксировало приведенные ниже типы сообщений (определены в параграфе 5.3) и будет поддерживать реестр типов сообщений DHCP.

SOLICIT	**1**
ADVERTISE	**2**
REQUEST	**3**
CONFIRM	**4**
RENEW	**5**
REBIND	**6**
REPLY	**7**
RELEASE	**8**
DECLINE	**9**
RECONFIGURE	**10**
INFORMATION-REQUEST	**11**
RELAY-FORW	**12**
RELAY-REPL	**13**

24.3. Опции DHCP

Агентство IANA зафиксировало приведенные ниже коды опций (определены в разделе 22) и будет поддерживать реестр кодов опций DHCP.

```
OPTION_CLIENTID       1
OPTION_SERVERID       2
OPTION_IA_NA          3
OPTION_IA_TA          4
OPTION_IAADDR         5
OPTION_ORO            6
OPTION_PREFERENCE     7
OPTION_ELAPSED_TIME   8
OPTION_RELAY_MSG      9
OPTION_AUTH           11
OPTION_UNICAST        12
OPTION_STATUS_CODE    13
OPTION_RAPID_COMMIT   14
OPTION_USER_CLASS     15
OPTION_VENDOR_CLASS   16
OPTION_VENDOR_OPTS    17
OPTION_INTERFACE_ID   18
OPTION_RECONF_MSG     19
OPTION_RECONF_ACCEPT  20
```

24.4. Коды состояний

Агентство IANA зафиксировало приведенные в таблице коды и будет поддерживать определение новых кодов.

Имя	*Код*	*Описание*
Success	0	Успех
UnspecFail	1	Отказ по не указанной причине. Этот код передается клиентом или сервером для индикации отказа, не описанного явно в этом документе
NoAddrsAvail	2	У сервера нет адреса, доступного для назначения . IA.
NoBinding	3	Запись о привязке клиент недоступна.
NotOnLink	4	Префикс адреса не подходит для канала, к которому подключен клиент.
UseMulticast	5	Передается сервером клиенту, чтобы заставить того передавать сообщения серверу по адресу All_DHCP_Relay_Agents_and_Servers.

24.5. DUID

Агентство IANA зафиксировало приведенные ниже типы DUID (определены в параграфе 9.1) и будет поддерживать определения дополнительных типов DUID.

```
DUID-LLT                1
DUID-EN                 2
DUID-LL                 3
```

25. Благодарности

Спасибо рабочей группе DHC и членам IETF за потраченное время и вклад в спецификацию. В частности, благодарим за согласованные предложения, идеи и рецензирование (в алфавитном порядке) Bernard Aboba, Bill Arbaugh, Thirumalesh Bhat, Steve Bellovin, A. K. Vijayabhaskar, Brian Carpenter, Matt Crawford, Francis Dupont, Richard Hussong, Kim Kinnear, Fredrik Lindholm, Tony Lindstrom, Josh Littlefield, Gerald Maguire, Jack McCann, Shin Miyakawa, Thomas Narten, Erik Nordmark, Jarno Rajahalme, Yakov Rekhter, Mark Stapp, Matt Thomas, Sue Thomson, Tatuya Jinmei и Phil Wells.

Спасибо Steve Deering и Bob Hinden, которые постоянно отдавали свое время на обсуждение наиболее сложных частей спецификаций IPv6.

Спасибо также Steve Deering за то, что он указал на конференции IETF 51 в Лондоне самое большое число ревизий спецификации DHCPv6 среди документов Internet Draft.

26. Литература

26.1. Нормативные документы

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

[2] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, December 1998.

[3] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460[1], December 1998.

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

[5] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 2373[2], July 1998.

[6] IANA. Private Enterprise Numbers. http://www.iana.org/assignments/enterprise-numbers.html.

[7] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401[3], November 1998.

[8] Krawczyk, H., Bellare, M. and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[1]Заменён RFC 8200. *Прим. перев.*
[2]Документ заменен RFC 3513, а тот - RFC 4291. *Прим. перев.*
[3]Документ заменен RFC 4301. *Прим. перев.*

[9] Mills, O., «Network Time Protocol (Version 3) Specification, Implementation», RFC 1305, March 1992.

[10] Mockapetris, P., "Domain names - implementation and specification", RFC 1035, November 1987.

[11] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[12] Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001.

[13] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461[1], December 1998.

[14] Plummer, D.C., "Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware", STD 37, RFC 826, November 1982.

[15] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[16] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[17] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462[2], December 1998.

26.2. Дополнительная литература

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

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

[20] R. Droms, Ed. DNS Configuration options for DHCPv6. April 2002. Work in Progress[3].

[21] A. K. Vijayabhaskar. Time Configuration Options for DHCPv6. May 2002. Work in Progress.

[22] Vixie, P., Ed., Thomson, S., Rekhter, Y. and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

A. Опции в разных типах сообщений

С таблице знак + указывает опции, разрешенные для каждого типа сообщений DHCP.

	Client ID	*Server IP*	*IA_NA, IA_TA*	*Option Request*	*Pref*	*Time*	*Relay Msg.*	*Auth.*	*Server Unicast*
Solicit	+		+	+		+		+	
Advert	+	+	+		+			+	
Request	+	+	+	+		+		+	
Confirm	+		+	+		+		+	
Renew	+	+	+	+		+		+	
Rebind	+		+	+		+		+	
Decline	+	+	+	+		+		+	
Release	+	+	+	+		+		+	
Reply	+	+	+		+			+	+
Reconf	+	+		+				+	
Inform	+	+[4]		+		+		+	
R-forw							+	+	
R-repl							+	+	

	Status Code	*Rap. Comm.*	*User Class*	*Vendor Class*	*Vendor Spec.*	*Inter. ID*	*Recon. Msg.*	*Recon. Accept*
Solicit		+	+	+	+			+
Advert	+		+	+	+			+
Request			+	+	+			+
Confirm			+	+	+			
Renew			+	+	+			+
Rebind			+	+	+			+
Decline			+	+	+			
Release			+	+	+			
Reply	+	+	+	+	+			+
Reconf							+	

[1]Документ заменен RFC 4861. *Прим. перев.*
[2]Документ заменен RFC 4862. *Прим. перев.*
[3]Работа опубликована в RFC 3646. *Прим. перев.*
[4]Только в сообщениях, передаваемый в ответ на сообщение Reconfigure (параграф19.4.3).

Inform			+	+	+			+
R-forw			+	+	+	+		
R-repl			+	+	+	+		

B. Опции в поле Options опций DHCP

В таблице знак + указывает, где опции могут появляться в поле опций другой опции.

	Option Field	*IA_NA, IA_TA*	*IAADDR*	*Relay Forward*	*Relay Reply*
Client ID	+				
Server ID	+				
IA_NA/IA_TA	+				
IAADDR		+			
ORO	+				
Preference	+				
Elapsed Time	+				
Relay Message				+	+
Authentication	+				
Server Unicast	+				
Status Code	+	+	+		
Rapid Commit	+				
User Class	+				
Vendor Class	+				
Vendor Info.	+				
Interface ID				+	+
Reconfigure Message	+				
Reconfigire Accept	+				

Примечание. Опции Relay Forward/Relay Reply появляются в поле опций, но только в этих сообщениях.

Адрес председателя

С рабочей группой можно связаться через ее текущего председателя.

Ralph Droms

Cisco Systems

1414 Massachusetts Avenue

Boxborough, MA 01719

Phone: (978) 936-1674

EMail: rdroms@cisco.com

Адреса авторов

Jim Bound

Hewlett Packard Corporation

ZK3-3/W20

110 Spit Brook Road

Nashua, NH 03062-2698

USA

Phone: +1 603 884 0062

EMail: Jim.Bound@hp.com

Bernie Volz

116 Hawkins Pond Road

Center Harbor, NH 03226-3103

USA

Phone: +1-508-259-3734

EMail: volz@metrocast.net

Ted Lemon

Nominum, Inc.

950 Charter Street

Redwood City, CA 94043

USA

EMail: Ted.Lemon@nominum.com

Charles E. Perkins

Communications Systems Lab

Nokia Research Center

313 Fairchild Drive

Mountain View, California 94043

USA

Phone: +1-650 625-2986

EMail: charles.perkins@nokia.com

Mike Carney

Sun Microsystems, Inc

17 Network Circle

Menlo Park, CA 94025

USA

Phone: +1-650-786-4171

EMail: michael.carney@sun.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.