

Протокол динамической настройки хоста (DHCP)

Dynamic Host Configuration Protocol

Статус документа

Этот документ задаёт проект стандартного протокола Internet для сообщества Internet и служит приглашением к дискуссии в целях развития и совершенствования протокола. Текущий статус стандартизации протокола можно узнать из документа Internet Official Protocol Standards (STD 1). Распространение документа не ограничивается.

Аннотация

Протокол динамической настройки конфигурации хоста (Dynamic Host Configuration Protocol или DHCP) обеспечивает основу для передачи хостам конфигурационных параметров через сеть TCP/IP. DHCP основан на протоколе начальной загрузки (Bootstrap Protocol или BOOTP) [7] и добавляет автоматическое выделение сетевых адресов, а также дополнительные конфигурационные опции [19]. DHCP может работать с ретрансляторами BOOTP [7, 21], а участники DHCP могут взаимодействовать с участниками BOOTP [9].

Оглавление

1. Введение.....	2
1.1 Отличия от RFC 1541.....	2
1.2 Смежные работы.....	2
1.3 Постановка задачи.....	3
1.4 Уровни требований.....	3
1.5 Терминология.....	3
1.6 Цели.....	3
2. Краткое описание протокола.....	4
2.1 Репозиторий конфигурационных параметров.....	5
2.2 Динамическое выделение сетевых адресов.....	6
3. Протокол клиент-сервер.....	6
3.1 Выделение сетевого адреса.....	6
3.2 Повторное использование адресов.....	8
3.3 Представление и интерпретация значений времени.....	9
3.4 Получение параметров с заданным извне сетевым адресом.....	9
3.5 Параметры клиента в DHCP.....	9
3.6 Использование DHCP на клиентах с несколькими интерфейсами.....	9
3.7 Когда клиенту следует применять DHCP.....	9
4. Спецификация протокола DHCP.....	10
4.1 Создание и передача сообщений DHCP.....	10
4.2 Элементы администрирования сервера DHCP.....	11
4.3 Поведение сервера DHCP.....	11
4.3.1 Сообщение DHCPDISCOVER.....	11
4.3.2 Сообщение DHCPREQUEST.....	13
4.3.3 Сообщение DHCPDECLINE.....	14
4.3.4 Сообщение DHCPRELEASE.....	14
4.3.5 Сообщение DHCPINFORM.....	14
4.3.6 Сообщения клиента.....	14
4.4 Поведение клиента DHCP.....	14
4.4.1 Инициализация и выделение сетевого адреса.....	15
4.4.2 Инициализация с известным сетевым адресом.....	16
4.4.3 Инициализация с назначенным извне сетевым адресом.....	17
4.4.4 Использование широковещания и индивидуальной адресации.....	17
4.4.5 Завершение и повторная аренда.....	17
4.4.6 DHCPRELEASE.....	17
5. Благодарности.....	18
6. Литература.....	18
7. Вопросы безопасности.....	18
8. Адрес автора.....	18
A. Конфигурационные параметры хоста.....	19

Список рисунков

Рисунок 1. Формат сообщения DHCP.....	4
Рисунок 2. Формат поля flags.....	5
Рисунок 3. Обмен сообщениями между клиентом и сервером при выделении сетевого адреса.....	7
Рисунок 4. Обмен сообщениями между клиентом и сервером при запросе прежнего сетевого адреса.....	8
Рисунок 5. Диаграмма смены состояний клиента DHCP.....	15

Список таблиц

Таблица 1. Описание полей сообщения DHCP.....	5
Таблица 2. Сообщения DHCP.....	6
Таблица 3. Поля и опции, используемые сервером DHCP.....	12
Таблица 4. Клиентские сообщения для разных состояний.....	14
Таблица 5. Поля и опции, используемые клиентом DHCP.....	16

1. Введение

Протокол DHCP обеспечивает настройку конфигурационных параметров хостов Internet. DHCP включает два компонента - протокол доставки конфигурационных параметров конкретного хоста с сервера DHCP и механизм выделения сетевых адресов для хостов.

DHCP работает на основе модели «клиент-сервер», где хосты, выполняющие роль серверов DHCP, выделяют сетевые адреса и доставляют параметры конфигурации динамически настраиваемым хостам. В оставшейся части документа термин «сервер» будет служить для обозначения хоста, обеспечивающего инициализацию параметров по протоколу DHCP, а термином «клиент» будут обозначаться хосты, запрашивающие параметры инициализации у сервера DHCP.

Хосту не следует выступать в качестве сервера DHCP, пока это явно не задано в его конфигурации администратором системы. Разнообразие оборудования и реализаций протоколов в Internet будет препятствовать нормальной работе, если произвольным хостам будет разрешено отвечать на запросы DHCP. Например, IP требует установки множества параметров в программах, реализующих протокол. Поскольку протокол IP может применяться на разнотипном сетевом оборудовании, для этих параметров невозможно предсказать используемые по умолчанию значения. Кроме того, распределенные схемы выделения адресов зависят от механизмов опроса и защиты, используемых для обнаружения уже выделенных адресов. Хосты IP не всегда могут защитить свои адреса, поэтому нельзя гарантировать отсутствие дубликатов при выделении сетевых адресов.

DHCP поддерживает три механизма выделения адресов IP. В автоматическом режиме DHCP назначает клиенту постоянный адрес IP, в динамическом адрес выделяется на ограниченное время (или до явного освобождения адреса клиентом). В ручном режиме адрес для клиента задаёт сетевой администратор и DHCP просто передаёт этот адрес клиенту. В конкретной сети может использоваться один или несколько механизмов в зависимости от политики.

Динамическое распределение является единственным из трёх механизмов, который позволяет автоматически использовать освободившиеся адреса. Поэтому динамическое распределение особенно полезно при выделении адресов клиентам, временно подключающимся к сети, или клиентам, совместно использующим ограниченный набор адресов IP для группы клиентов, которым постоянный адрес не требуется. Динамическое выделение может быть также хорошим выбором для назначения адресов IP новым клиентам, постоянно подключённым к сети, где пространство адресов достаточно мало и важно возвращать адреса при удалении старых клиентов. Выделение вручную позволяет использовать DHCP для предотвращения ошибок при ручной настройке хостов в среде, где (по той или иной причине) желательно управлять назначением адресами вне механизмов DHCP.

Формат сообщений DHCP основан на формате сообщений BOOTP для поддержки функций ретранслятора BOOTP, описанных в спецификации BOOTP [7, 21], и обеспечения взаимодействия имеющихся клиентов BOOTP с серверами DHCP. Использование агентов ретрансляции BOOTP избавляет от необходимости организации сервера DHCP в каждом физическом сегменте сети.

1.1 Отличия от RFC 1541

Этот документ обновляет спецификацию протокола DHCP, заданную в RFC1541. Добавлен новый тип сообщений DHCPINFORM (см. параграфы 3.4, 4.3 и 4.4). Механизм классов для идентификации клиентов DHCP на сервере DHCP был расширен путём добавления классов vendor, заданных в параграфах 4.2 и 4.3. Было снято ограничение для минимального срока аренды. Кроме того, внесены многочисленные редакторские правки, разъясняющие текст с учётом опыта тестирования функциональной совместимости DHCP.

1.2 Смежные работы

Имеется несколько протоколов Internet и связанных с ними механизмов, которые решают часть задачи динамической настройки конфигурации хостов. Протокол обратного преобразования адресов (Reverse Address Resolution Protocol или RARP [10] (за счёт расширения DRARP¹ [5]) явно решает задачу автоматического обнаружения сетевых адресов и включает механизм автоматического назначения адресов IP. Протокол TFTP² [20] обеспечивает транспортировку загрузочного образа с сервера загрузки. Протокол ICMP³ [16] обеспечивает информирование хостов о дополнительных маршрутах с помощью сообщений ICMP redirect. ICMP также обеспечивает информацию о текущей маске подсети с помощью сообщений ICMP mask request и другую информацию, доступную с помощью (отменённых) сообщений ICMP information request. Хосты могут находить маршрутизаторы с помощью механизма ICMP router discovery [8].

BOOTP является транспортным механизмом для набора конфигурационных сведений. Протокол BOOTP является расширяемым и официальные расширения [17] могут быть определены для некоторых конфигурационных параметров. Morgan предложил расширение BOOTP для динамического назначения адресов IP [15]. Протокол NIP⁴, используемый в проекте Athena института MIT, является распределённым механизмом динамического назначения адресов IP [19]. Протокол RLP⁵ [1] обеспечивает определение места расположения служб верхних уровней. Бездисковые станции Sun Microsystems используют процедуру загрузки на основе RARP, TFTP и механизма RPC, названного bootparams, для доставки конфигурационной информации и кода операционной системы на бездисковые рабочие станции (Sun Microsystems, Sun Workstation и SunOS - торговые знаки Sun Microsystems, Inc.). Некоторые сети Sun используют также

¹Dynamic RARP - динамический RARP.

²Trivial File Transfer Protocol - ограниченный (тривиальный) протокол переноса файлов.

³Internet Control Message Protocol - протокол управляющих сообщений Internet.

⁴Network Information Protocol - протокол сетевой информации.

⁵Resource Location Protocol - протокол определения местоположения ресурсов.

DRARP и механизм автоматической инсталляции для автоматизации настройки конфигурации хостов в существующей сети.

В других смежных работах алгоритм определения MTU¹ позволяет найти значение MTU для произвольного пути через сеть [14]. Протокол распознавания адресов (Address Resolution Protocol или ARP) был предложен в качестве транспорта для определения местоположения и выбора ресурсов [6]. В документах Host Requirements [3, 4] указаны конкретные требования для реконфигурации хостов и предложен сценарий начальной настройки бездисковых хостов.

1.3 Постановка задачи

Протокол DHCP разработан для предоставления клиентам DHCP конфигурационных параметров, определённых в документах Host Requirements RFC. После получения параметров по протоколу DHCP клиент должен иметь возможность обмена пакетами с любым хостом в сети Internet. Параметры стека TCP/IP, предоставляемые протоколом DHCP, перечислены в Приложении А. Не все эти параметры требуются для инициализируемого клиента. Клиент и сервер могут согласовать между собой передачу лишь тех параметров, которые нужны клиенту или требуются для конкретной подсети.

DHCP позволяет, но не требует настройку параметров конфигурации клиентов, не связанных напрямую с протоколом IP. Протокол DHCP также не решает вопросов регистрации адресов недавно настроенных клиентов в системе доменных имён (Domain Name System или DNS) [12, 13].

Протокол DHCP не предназначен для настройки конфигурации маршрутизаторов.

1.4 Уровни требований

В этом документе слова, используемые для определения значимости конкретных требований выделены шрифтом. Эти уровни перечислены ниже.

MUST - необходимо

Это слово, а также термин **требуется** (REQUIRED) используется для требований, которые являются абсолютно необходимыми в данной спецификации.

MUST NOT - недопустимо

Эта фраза означает абсолютный запрет в рамках спецификации.

SHOULD - следует

Это слово, а также глагол **рекомендуется** (RECOMMENDED) используется для обозначения требований, от выполнения которых можно отказаться при наличии разумных причин. Однако при таком отказе следует помнить о возможных проблемах в результате отказа и принимать взвешенное решение.

SHOULD NOT - не следует

Эта фраза используется применительно к особенностям или функциям, которые допустимы и могут быть полезными, но могут и вызывать проблемы. При реализации таких опций следует учитывать возможность возникновения проблем и принимать взвешенное решение.

MAY - возможно

Это слово, а также прилагательное **необязательный** (OPTIONAL) обозначают элементы, реализация которых является необязательной. Одни разработчики могут включать такие опции в свою продукцию для расширения возможностей, а другие - опускать в целях упрощения.

1.5 Терминология

Ниже приведены определения используемых в документе терминов.

DHCP client – клиент DHCP

Клиентом DHCP является хост Internet, использующий протокол DHCP для получения параметров конфигурации, например сетевого адреса.

DHCP server – сервер DHCP

Сервером DHCP является хост Internet, который возвращает параметры конфигурации клиентам DHCP.

BOOTP relay agent – агент-ретранслятор BOOTP

Агент ретрансляции BOOTP или просто агент ретрансляции является хостом Internet или маршрутизатором, который передаёт сообщения DHCP между клиентами и серверами DHCP. Протокол DHCP устроен так, чтобы обеспечивать такое же поведение агента ретрансляции, как задано в спецификации протокола BOOTP.

Binding - привязка

Привязкой называется набор параметров конфигурации, включающий как минимум адрес IP, который привязан к клиенту DHCP. Привязками управляет сервер DHCP.

1.6 Цели

Ниже перечислены основные цели, заданные при разработке протокола DHCP.

- Протоколу следует быть механизмом, а не политикой. DHCP должен предоставлять администраторам локальной системы контроль над желаемыми конфигурационными параметрами (например, локальному администратору следует иметь возможность применить локальные правила, относящиеся к выделению ресурсов и доступу к ним).
- От клиентов следует требовать минимальной ручной настройки. Каждому клиенту следует обеспечивать возможность обнаружения локальных конфигурационных параметров без участия пользователя и включать эти параметры в свою конфигурацию.
- Сетям не следует требовать ручной настройки отдельных клиентов. В нормальных условиях от сетевого администратора не должно требоваться задание параметров конфигурации на уровне отдельных хостов.
- Протоколу DHCP не следует требовать сервера в каждой подсети. В целях расширяемости и экономии сервер DHCP должен работать через маршрутизаторы или с привлечением агентов ретрансляции BOOTP.

¹Maximum transmission unit - максимальный передаваемый блок. В оригинале ошибочно сказано «минимальный», см. <https://www.rfc-editor.org/errata/eid488>. Прим. перев.

- Клиент DHCP должен быть готов к получению множества откликов на запрос конфигурационных параметров. В некоторых сетях может использоваться множество перекрывающихся серверов DHCP для обеспечения надёжности и производительности.
- DHCP должен сосуществовать со статически настроенными, не участвующими в работе протокола хостами и существующими реализациями сетевых протоколов.
- DHCP должен быть функционально совместим с агентами ретрансляции BOOTP, поведение которых соответствует RFC 951 и RFC 1542 [21].
- DHCP должен обеспечивать обслуживание имеющихся клиентов BOOTP.

Ниже перечислены цели разработки, связанные с передачей параметров сетевого уровня. Протокол DHCP должен:

- гарантировать, что в каждый момент любой конкретный сетевой адрес будет использоваться лишь одним клиентом DHCP;
- сохранять конфигурационные параметры клиента DHCP при его перезагрузке; одному и тому же клиенту следует по возможности предоставлять один набор конфигурационных параметров (например, сетевой адрес) при каждом запросе;
- сохранять конфигурационные параметры клиента DHCP при перезагрузке сервера; клиенту DHCP следует назначать тот же сетевой адрес, который был выдан ему до перезапуска механизма DHCP;
- разрешать автоматизированное назначение конфигурационных параметров новых клиентов во избежание их настройки вручную;
- поддерживать фиксированное или постоянное выделение параметров конфигурации для конкретных клиентов.

2. Краткое описание протокола

С точки зрения клиентов, DHCP является расширением механизма BOOTP. Такое поведение позволяет имеющимся клиентам BOOTP взаимодействовать с серверами DHCP без каких-либо изменений в программах инициализации клиентов. В RFC 1542 [2] подробно описано взаимодействие клиентов BOOTP и DHCP с серверами [9]. Имеется несколько новых необязательных транзакций, которые оптимизируют взаимодействие между клиентами DHCP и серверами, эти транзакции описаны в разделах 3 и 4.

На рисунке 1 показан формат сообщений DHCP, а в таблице 1 описано каждое из полей сообщения DHCP. Числа в скобках указывают размер каждого поля в октетах. Представленные на рисунке имена полей используются в этом документе для указания полей в сообщениях DHCP.

Имеется два основных различия между DHCP и BOOTP. Первое состоит в том, что DHCP задаёт механизмы, с помощью которых клиентам может назначаться сетевой адрес на ограниченный срок, что позволяет позднее использовать этот же адрес для других клиентов. Вторым различием является то, что DHCP обеспечивает механизм, с помощью которого клиент получает все конфигурационные параметры IP, которые нужны ему для работы.

DHCP несколько меняет терминологию в части прояснения смысла одного из полей. Поле vendor extensions из BOOTP переименовано в options для протокола DHCP. Помеченные элементы данных, использовавшиеся в поле BOOTP vendor extensions, которые назывались «фирменными расширениями», стали просто «опциями».

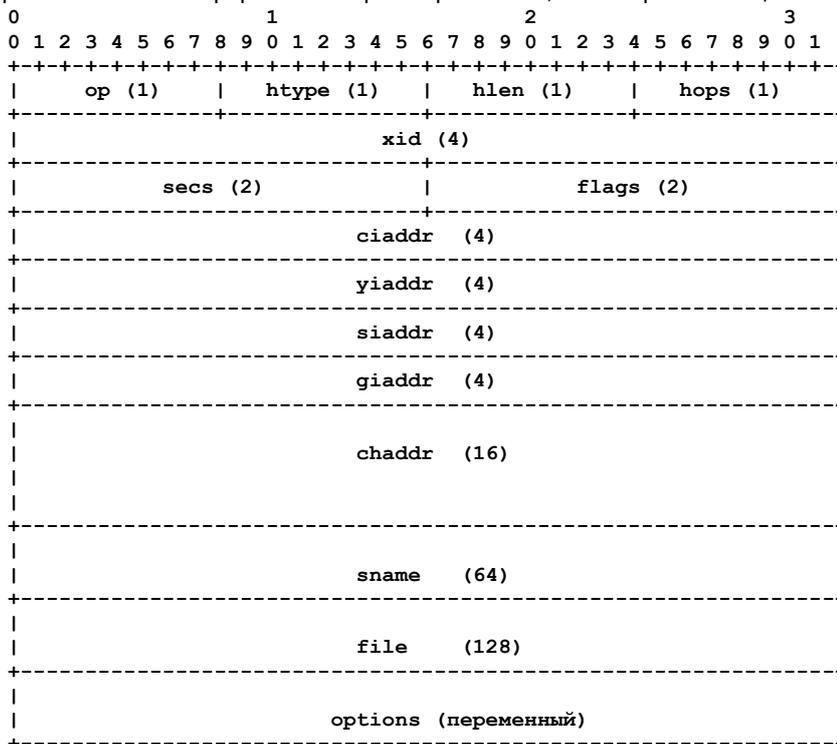


Рисунок 1. Формат сообщения DHCP.

DHCP определяет новую опцию client identifier, которая служит для передачи явного идентификатора клиента серверу DHCP. Это избавляет от перегрузки поле chaddr в сообщениях BOOTP, где это поле служило в качестве аппаратного адреса для передачи откликов BOOTP и идентификатора клиента. Поле client identifier является ключом, который не интерпретируется сервером, - это поле может содержать, например, аппаратный адрес, идентичный содержимому поля

chaddr, или быть идентификатором другого типа (скажем, именем DNS)¹. Значение client identifier, выбранное клиентом DHCP, **должно** быть уникальным для каждого клиента в подсети, где этот клиент размещается. Если клиент использует client identifier в одном сообщении, он **должен** использовать такой же идентификатор во всех последующих сообщениях, чтобы все серверы могли корректно распознать этого клиента.

DHCP уточняет интерпретацию поля siaddr как адреса сервера, для использования на следующем этапе протокола загрузки клиента. Сервер DHCP может возвращать свой адрес в поле siaddr, если он готов обеспечить следующий этап процесса загрузки (например, доставку исполняемого образа операционной системы). Сервер DHCP всегда возвращает свой адрес в опции server identifier.

Таблица 1. Описание полей сообщения DHCP.

Поле	Размер	Описание
op	1	Операция (тип сообщения). 1 = BOOTREQUEST, 2 = BOOTREPLY
htype	1	Тип аппаратного адреса (см. раздел ARP в Assigned Numbers RFC ²), например, 1 для Ethernet 10 Мбит/с.
hlen	1	Размер аппаратного адреса (например, 6 для Ethernet 10 Мбит/с).
hops	1	Клиент устанавливает 0, поле может использоваться ретрансляторами при загрузке через них.
xid	4	Идентификатор транзакции - случайное число, выбираемое клиентом. Используется клиентом и сервером для сопоставления сообщений и откликов на них.
secs	2	Число секунд с начала процесса получения или обновления адреса, указываемое клиентом.
flags	2	Флаги (см. рисунок 2).
ciaddr	4	IP-адрес клиента; указывается только в том случае, когда клиент находится в состоянии BOUND, RENEW или REBINDING и может отвечать на запросы ARP.
yiaddr	4	«Ваш» (клиента) адрес IP.
siaddr	4	IP-адрес следующего сервера для использования при загрузке. Возвращается сервером в сообщениях DHCPOFFER, DHCPACK.
giaddr	4	IP-адрес агента ретрансляции, используемый при загрузке через агент.
chaddr	16	Аппаратный адрес клиента.
sname	64	Необязательное имя сервера - строка, завершающаяся null-символом.
file	128	Имя загрузочного файла (строка, завершающаяся null-символом); базовое (generic) имя или null в DHCPDISCOVER, полный путь к файлу в DHCPOFFER.
options	переменный	Поле необязательных параметров. Список опций можно найти в дополнительных документах.

Поле options имеет переменный размер. Клиент DHCP должен быть готов к получению сообщений DHCP с размером поля options по меньшей мере 312 октетов. Это требование предполагает, что клиент DHCP должен быть готов принимать сообщения размером до 576 октетов (минимальный размер дейтаграммы IP, который хост IP должен быть готов принимать [3]). Клиенты DHCP могут согласовать использование более крупных сообщений DHCP с помощью опции maximum DHCP message size. Поле опций может быть дополнительно расширено за счёт полей file и sname.

Если клиент использует DHCP для начальной настройки (до полной настройки клиентских программ TCP/IP), DHCP требует творческого использования клиентских программ TCP/IP и мягкой интерпретации RFC 1122. Программам TCP/IP **следует** воспринимать и передавать на уровень IP все пакеты IP, доставленные на аппаратный адрес клиента, до того, как будет настроен протокол IP, поскольку серверы DHCP и агенты ретрансляции BOOTP могут быть не способны доставлять сообщения DHCP клиентам, которые не могут воспринимать дейтаграммы с индивидуальным аппаратным адресом до завершения настройки программ TCP/IP.

Для работы с клиентами, которые не способны воспринимать индивидуальные дейтаграммы IP до настройки программ TCP/IP, как отмечено выше, DHCP использует поле flags [21]. Левый бит этого поля служит флагом широковещания (BROADCAST) - В. Семантика этого флага рассматривается в параграфе 4.1. Остальные биты поля зарезервированы на будущее. Они **должны** устанавливаться в 0 клиентами и игнорироваться серверами и агентами ретрансляции. Формат поля flags показан на рисунке 2.

```

          1 1 1 1 1 1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-----+-----+-----+-----+
|В|                MBZ                |
+-----+-----+-----+-----+
В - флаг широковещания;
MBZ - должны иметь нулевое значение (резерв)

```

Рисунок 2. Формат поля flags.

2.1 Репозиторий конфигурационных параметров

Первой услугой, обеспечиваемой DHCP, является предоставление постоянного хранилища сетевых параметров клиентов. Модель постоянного хранилища DHCP основана на хранении для каждого клиента пар «ключ-значение», где ключом служит некий уникальный идентификатор клиента (например, номер подсети IP и уникальный идентификатор в этой подсети), а значение содержит конфигурационные параметры для этого клиента. Ключом может быть пара (номер подсети IP, аппаратный адрес³), позволяющая последовательно или одновременно использовать один аппаратный адрес в разных подсетях, а также не заботиться о глобальной уникальности аппаратных адресов. Кроме того, ключом может служить пара (номер подсети IP, имя хоста), позволяющая серверу DHCP интеллектуально задавать параметры клиенту при его перемещении в другую подсеть или смене аппаратного адреса (возможно, в результате замены сетевого интерфейса). Протокол определяет использование в качестве ключа пары (номер подсети IP, аппаратный адрес), если клиент не предоставил свой идентификатор явно с помощью опции client identifier. Клиент может запросить у службы DHCP получение своих конфигурационных параметров. Интерфейс клиента в репозиторий конфигурационных параметров состоит из протокольных сообщений для запроса параметров и откликов сервера, содержащих эти параметры.

¹В соответствии с RFC 4361 текст «- это поле может содержать, например, аппаратный адрес, идентичный содержимому поля chaddr, или быть идентификатором другого типа (скажем, именем DNS)» удалён из спецификации. Прим. перев.

²В настоящее время эта информация доступна по [ссылке](#). Прим. перев.

³Отметим, что аппаратный адрес должен определяться типом оборудования для предотвращения дублирования адресов, связанного с разным порядком битов в смешанных сетях с мостами.

2.2 Динамическое выделение сетевых адресов

Второй услугой DHCP является выделение временных или постоянных сетевых (IP) адресов клиентам. Базовый механизм динамического выделения сетевых адресов прост - клиент запрашивает использование адреса на некоторый интервал времени. Механизм выделения (набор серверов DHCP) может (но не обязан) предоставить аренду на запрошенный срок и гарантирует, что в течение предложенного времени этот адрес не будет предоставляться другим клиентам, а по истечении времени будет предпринята попытка выделить тот же адрес при последующем запросе этого клиента¹. В этом документе период, на который сетевой адрес предоставляется клиенту, называется арендой (lease) [11]. Клиент может расширить свою аренду с помощью последующего запроса. Клиент может передать сообщение для возврата арендованного адреса серверу, когда потребность в этом адресе отпадёт. Клиент может запросить постоянное предоставление адреса, указав бесконечный срок аренды. Даже при назначении «постоянного» адреса сервер может выбрать очень продолжительный, но конечный срок аренды, чтобы можно было видеть уход клиента.

В некоторых средах требуется переназначать сетевые адреса по причине нехватки доступного адресного пространства. В таких случаях механизм выделения адресов будет снова выделять клиентам освобождённые адреса. Серверам следует использовать доступную в конфигурационном репозитории информацию при выборе адресов для повторного использования. Например, сервер может выбрать адрес, который дольше всего оставался свободным. В качестве проверки согласованности выделяющему адрес серверу **следует** протестировать адрес до его назначения (например, с помощью запроса ICMP echo), а клиенту **следует** проверить недавно полученный адрес (например, с помощью ARP).

3. Протокол клиент-сервер

DHCP использует формат сообщений BOOTP, заданный в RFC 951 и представленный на рисунке 1 и в таблице 1. Поле оп каждого сообщения DHCP от клиента к серверу содержит значение BOOTREQUEST, а BOOTREPLY используется в поле оп каждого отклика DHCP от сервера.

Первые 4 октета поля options в сообщении DHCP содержат десятичные значения 99, 130, 83 и 99 (это значение magic cookie, заданное в RFC 1497 [17]). Остальная часть поля options содержит список параметров с метками, которые называются опциями. Все фирменные расширения (vendor extensions), перечисленные в RFC 1497, являются также опциями DHCP. В RFC 1533 приведён полный набор опций, определённых для использования в DHCP.

До настоящего момента было определено несколько опций. Одна из таких опций - DHCP message type (тип сообщения) - должна включаться в каждое сообщение DHCP и определяет тип сообщения. Другие опции могут разрешаться, требоваться или запрещаться в зависимости от типа сообщения DHCP.

В этом документе сообщения DHCP с опцией DHCP message type будут указываться типом сообщения. Например, сообщение с DHCP message type 1 будет называться DHCPDISCOVER.

3.1 Выделение сетевого адреса

Приведённая ниже сводка протокольного обмена между клиентами и серверами относится к сообщениям DHCP, описанным в таблице 2. Временная диаграмма на рисунке 3 показывает последовательность типичного взаимодействия между клиентом и сервером. Если клиент уже знает свой адрес, некоторые этапы могут быть опущены, - это сокращённое взаимодействие описано в параграфе 3.2.

1. Клиент передаёт в широковещательном режиме сообщение DHCPDISCOVER в свою локальную физическую подсеть. Сообщение DHCPDISCOVER **может** включать опции, которые предлагают значения для сетевого адреса и срока аренды. Агенты ретрансляции BOOTP могут передавать это сообщение серверам DHCP в других физических подсетях.
2. Каждый сервер может ответить сообщением DHCPOFFER, которое включает доступный сетевой адрес в поле yiaddr (и другие конфигурационные параметры в опциях DHCP). Сервер не обязан резервировать предложенный сетевой адрес, хотя протокол будет работать более эффективно, если сервер не будет предлагать тот же адрес другим клиентам. При выделении нового адреса серверам **следует** проверить предлагаемый адрес на предмет его занятости (например, сервер может отправить по этому адресу сообщение ICMP Echo Request). Серверы **следует** реализовать так, чтобы сетевые администраторы **могли** отключать проверку занятости недавно выделённых адресов. Сервер передаёт сообщение DHCPOFFER клиенту, используя при необходимости агент трансляции BOOTP.

Таблица 2. Сообщения DHCP.

Сообщение	Применение
DHCPDISCOVER	Широковещательное сообщение клиента для поиска доступных серверов.
DHCPOFFER	Отклик сервера на сообщение DHCPDISCOVER от клиента, предлагающий параметры конфигурации.
DHCPREQUEST	Сообщение от клиента для (а) запроса предложенных параметров и неявного отказа от всех прочих предложений, (б) подтверждения корректности ранее выделённого адреса (например, после перезагрузки) или (с) расширения срока аренды сетевого адреса.
DHCPACK	Сервер передаёт клиенту параметры конфигурации, включая назначенный сетевой адрес.
DHCPNAK	Сервер сообщает клиенту о непригодности указанного тем сетевого адреса (например, при переносе клиента в другую подсеть) или окончании аренды для этого клиента.
DHCPDECLINE	Клиент сообщает серверу о том, что сетевой адрес уже занят.
DHCPRELEASE	Клиент сообщает серверу об освобождении сетевого адреса и отказе от аренды.
DHCPINFORM	Клиент запрашивает у сервера только конфигурационные параметры, поскольку уже имеет сетевой адрес, заданный другим способом.

3. Клиент получает одно или несколько сообщений DHCPOFFER от серверов и может принять решение об ожидании дополнительных откликов. Далее клиент выбирает один из серверов на основе параметров конфигурации, предложенных в сообщениях DHCPOFFER. Клиент передаёт в широковещательном режиме сообщение DHCPREQUEST, которое **должно** включать опцию server identifier для указания выбранного сервера и **может** включать другие опции, задающие желаемые параметры конфигурации. Опция requested IP address **должна** указывать значение yiaddr из сообщения DHCPOFFER от сервера. Сообщение

¹В оригинале это предложение отличалось, см. <https://www.rfc-editor.org/errata/eid6447>. Прим. перев.

DHCPREQUEST передается в широковещательном режиме и пересылается агентами ретрансляции DHCP/BOOTP. Чтобы ретрансляторы BOOTP пересылали сообщение DHCPREQUEST тем же серверам DHCP, которые получили исходное сообщение DHCPDISCOVER, в заголовке DHCPREQUEST должно использоваться то же значение поля `secs` и тот же широковещательный адрес IP, которые были заданы в исходном сообщении DHCPDISCOVER. Если клиент не получает сообщений DHCPPOFFER, он повторяет передачу DHCPDISCOVER по тайм-ауту.



Рисунок 3. Обмен сообщениями между клиентом и сервером при выделении сетевого адреса.

- Серверы получают широковещательное сообщение DHCPREQUEST от клиента. Те серверы, которые не указаны в сообщении DHCPREQUEST, используют его в качестве уведомления об отказе от сделанного ими предложения. Указанный в DHCPREQUEST сервер фиксирует привязку для клиента в своём постоянном хранилище и отвечает сообщением DHCPACK, содержащим конфигурационные параметры для запрашивающего клиента. Комбинация `client identifier` или `chaddr`¹ с назначенным сетевым адресом создаёт уникальный идентификатор клиентской аренды, который используется клиентом и сервером для указания аренды во всех последующих сообщениях DHCP. Конфигурационным параметрам в сообщении DHCPACK **не следует** противоречить параметрам из сообщения DHCPPOFFER, на которое клиент ответил. Серверу **не следует** проверять предложенный сетевой адрес на этом этапе. В поле `yiaddr` сообщения DHCPACK указывается выбранный сетевой адрес.

Если выбранный сервер не может выполнить запрос DHCPREQUEST (например, в результате того, что сетевой адрес уже был назначен), ему **следует** передать сообщение DHCPNAK.

Сервер **может** помечать адреса, предложенные клиентам в сообщениях DHCPPOFFER, как недоступные. Серверу **следует** снова помечать предложенный клиенту в сообщении DHCPPOFFER адрес как доступный при отсутствии от этого клиента сообщения DHCPREQUEST.

- Клиент получает сообщение DHCPACK с конфигурационными параметрами. Ему **следует** окончательно проверить параметры (например, передать запрос ARP для выделенного сетевого адреса) и зафиксировать продолжительность аренды, указанную в сообщении DHCPACK. С этого момента клиент настроен. Если будет обнаружено, что адрес уже занят (например, с помощью ARP), клиент **должен** передать серверу сообщение DHCPDECLINE и повторить процесс настройки. Клиенту следует выждать не менее 10 секунд перед началом нового процесса настройки для предотвращения избыточного трафика в случае петли.

При получении сообщения DHCPNAK клиент начинает процедуру настройки заново.

Клиент повторяет передачу DHCPREQUEST по тайм-ауту, если не было получено DHCPACK или DHCPNAK. Повтор выполняется в соответствии с алгоритмом, описанным в параграфе 4.1. Клиенту следует повторить передачу DHCPREQUEST неоднократно для обеспечения достаточной вероятности контакта с сервером, не заставляя себя (и пользователя) ждать слишком долго. Например, клиент выполняющий процедуру повтора в соответствии с параграфом 4.1, может передать сообщение DHCPREQUEST четыре раза с общей задержкой

¹В соответствии с RFC 4361 текст «или `chaddr`» удалён из спецификации. Прим. перев.

60 секунд, прежде чем начать процедуру инициализации заново. Если клиент не получил DHCPACK или DHCPNAK в процессе повтора передачи, он возвращается в состояние INIT и начинает процесс инициализации заново. Клиенту **следует** уведомить пользователя об отказе и перезапуске процесса.

- Клиент может отказаться от аренды сетевого адреса, передав серверу сообщение DHCPRELEASE. Клиент указывает освобождаемую аренду с помощью client identifier или chaddr¹ и сетевого адреса в сообщении DHCPRELEASE. Если клиент использовал client identifier при получении аренды, этот же идентификатор **должен** указываться в сообщении DHCPRELEASE.

3.2 Повторное использование адресов

Если клиент помнит и хочет снова использовать выделенный ранее сетевой адрес, он может опустить некоторые этапы, описанные в предыдущем параграфе. На рисунке 4 показаны этапы типичного взаимодействия между клиентом и сервером для клиента, желающего снова получить прежний сетевой адрес.

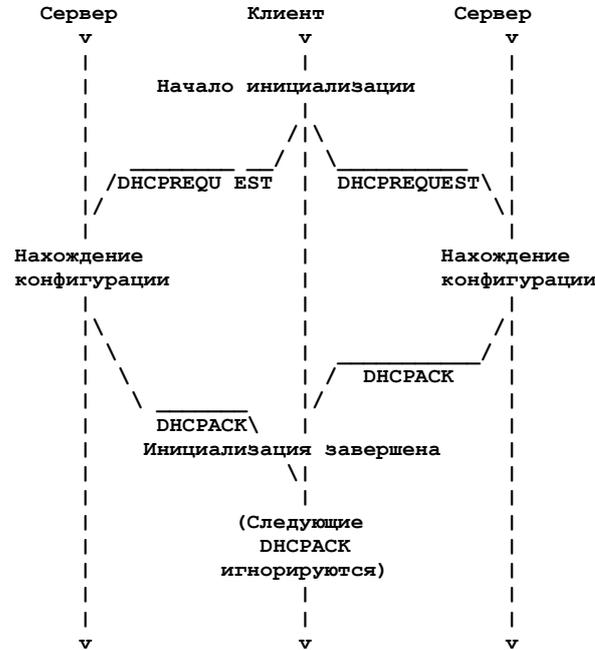


Рисунок 4. Обмен сообщениями между клиентом и сервером при запросе прежнего сетевого адреса.

- Клиент передаёт широковещательное сообщение DHCPREQUEST в свою локальную подсеть. Сообщение включает сетевой адрес клиента в опции requested IP address. Поскольку клиент не получил адрес, ему **недопустимо** заполнять поле ciaddr. Агенты ретрансляции BOOTP передают сообщение серверам DHCP из других подсетей. Если клиент использовал для получения адреса client identifier, он **должен** указать это же значение в сообщении DHCPREQUEST.

- Сервер, знающий конфигурационные параметры клиента, отвечает сообщением DHCPACK. Серверам **не следует** проверять занятость сетевого адреса, поскольку клиент может ответить на запрос ICMP Echo.

Если запрос клиента не пригоден (например, клиент перемещён в другую подсеть), серверу **следует** отвечать сообщением DHCPNAK. Серверу **не следует** отвечать, если он не гарантирует точность своей информации. Например, серверу определившему запрос как истекшую привязку, которой владел другой сервер, **не следует** отвечать сообщением DHCPNAK, если между серверами не организован явный механизм согласованности.

Если в сообщении DHCPREQUEST задано giaddr = 0x0, клиент относится к одной подсети с сервером. Сервер **должен** передать широковещательное сообщение DHCPNAK по адресу 0xffffffff, поскольку у клиента может не быть корректного сетевого адреса или маски сети и он не может ответить на запросы ARP. В ином случае сервер **должен** передать сообщение DHCPNAK по IP-адресу ретранслятора BOOTP, указанному в giaddr. Агент ретрансляции, в свою очередь, перешлёт сообщение напрямую по аппаратному адресу клиента и сообщение DHCPNAK может быть доставлено даже при переносе клиента в другую подсеть.

- Клиент получает сообщение DHCPACK с конфигурационными параметрами. Он выполняет окончательную проверку параметров (параграф 3.1) и отмечает продолжительность аренды, указанную в DHCPACK. Конкретная аренда неявно указывается client identifier или chaddr¹ и сетевым адресом. С этого момента конфигурация клиента настроена.

Если клиент обнаружит, что IP-адрес из сообщения DHCPACK уже занят, он **должен** передать серверу сообщение DHCPDECLINE и начать конфигурационный процесс заново, запросив новый сетевой адрес. Это действие соответствует переходу клиента в состояние INIT на диаграмме состояний DHCP, описанной в параграфе 4.4.

Если клиент получил сообщение DHCPNAK, он больше не может пользоваться сохранённым сетевым адресом и должен запросить новый адрес, начав (полную) процедуру настройки конфигурации, описанную в параграфе 3.1. Это действие также соответствует переходу клиента в состояние INIT на диаграмме состояний DHCP.

Клиент повторяет передачу DHCPREQUEST по тайм-ауту, если не было получено DHCPACK или DHCPNAK. Повтор выполняется в соответствии с алгоритмом, описанным в параграфе 4.1. Клиенту следует повторить передачу DHCPREQUEST неоднократно для обеспечения достаточной вероятности контакта с сервером, не заставляя себя (и пользователя) ждать слишком долго. Например, клиент выполняющий процедуру повтора в

¹В соответствии с RFC 4361 текст «или chaddr» удален из спецификации. Прим. перев.

соответствии с параграфом 4.1, может передать сообщение DHCPREQUEST четыре раза с общей задержкой 60 секунд, прежде чем начать процедуру инициализации заново. Если клиент не получил DHCPACK или DHCPNAK в процессе повтора передачи, он **может** продолжить использование полученного ранее сетевого адреса и параметров конфигурации до завершения срока аренды. Это соответствует переходу в состояние BOUND на диаграмме, показанной на рисунке 5.

4. Клиент может отказаться от аренды сетевого адреса, передав серверу сообщение DHCPRELEASE. Клиент указывает освобождаемую аренду с помощью client identifier или chaddr¹ и сетевого адреса в сообщении DHCPRELEASE.

Отметим, что в случае, когда клиент сохраняет свой сетевой адрес локально, он обычно не освобождает аренду при аккуратном выключении. Лишь при явной потребности клиента отказаться от своей аренды (например, при перемещении в другую подсеть) этот клиент будет передавать сообщение DHCPRELEASE.

3.3 Представление и интерпретация значений времени

Клиент арендует сетевой адрес на фиксированный интервал времени (который может быть бесконечным). В этом протоколе время указывается в секундах. Значение 0xffffffff зарезервировано для представления «бесконечности».

Поскольку часы клиентов и серверов могут быть не синхронизированы, в сообщениях DHCP указывается относительное время для интерпретации по локальным часам клиента. Время в секундах указывается 32-битовым значением без знака, позволяющим задать интервал от 0 приблизительно до 100 лет, что достаточно для работы DHCP.

Алгоритм интерпретации продолжительности аренды, описанной в предыдущем параграфе, предполагает, что часы клиента и сервера работают согласованно. Если скорости часов различаются, сервер может счесть аренду завершившейся раньше, чем это сделает клиент. Для компенсации этого сервер может возвращать клиенту более короткий срок аренды, нежели он передаёт в свою базу данных с информацией о клиентах.

3.4 Получение параметров с заданным извне сетевым адресом

Если клиент получает сетевой адрес каким-то иным способом (например, путём настройки вручную), он может воспользоваться запросом DHCPINFORM для получения остальных конфигурационных параметров. Серверы, получившие сообщение DHCPINFORM, создают сообщение DHCPACK со всеми подходящими для клиента параметрами конфигурации, но без выделения нового адреса, проверки существующей привязки, заполнения yiaddr и включения срока аренды. Серверу **следует** передавать отклик DHCPACK по индивидуальному адресу, указанному в поле ciaddr сообщения DHCPINFORM.

Серверу **следует** проверить согласованность адреса в сообщении DHCPINFORM, но **недопустимо** проверять наличие аренды. Сервер формирует сообщение DHCPACK, содержащее параметры конфигурации для запрашивающего клиента, и передаёт ему сообщение DHCPACK напрямую.

3.5 Параметры клиента в DHCP

Не каждому клиенту нужна инициализация всех параметров, перечисленных в Приложении А. Применяется два метода снижения числа параметров, передаваемых от сервера к клиенту. В первом методе для большинства параметров используются принятые по умолчанию значения из Host Requirements RFC - если клиент не получает тот или иной параметр, он использует заданное по умолчанию значение. Во втором варианте клиент может указать серверу список нужных параметров в начальном сообщении DHCPDISCOVER или DHCPREQUEST. Если клиент включил список параметров в DHCPDISCOVER, он **должен** включать тот же список в последующие сообщения DHCPREQUEST.

Клиенту **следует** включать опцию maximum DHCP message size, чтобы сообщить серверу максимальный размер сообщений DHCP. Но и в этом случае возвращаемые клиенту параметры могут превысить размер доступного для опций пространства в сообщении DHCP. В таких случаях два дополнительных флага (они должны присутствовать в поле options) указывают, что поля file и sname также используются для опций.

Клиент может указать серверу нужные конфигурационные параметры с помощью опции parameter request list, данные которой явно перечисляют номера тегов запрашиваемых опций.

Кроме того, клиент может предложить значения для сетевого адреса и срока аренды в сообщении DHCPDISCOVER. Клиент может включить опцию requested IP address, чтобы предложить определённый адрес IP для назначения и опцию IP address lease time для указания предлагаемого срока аренды. В сообщениях DHCPDISCOVER и DHCPREQUEST разрешены и другие опции с советами в части значений параметров. Однако эти опции могут игнорироваться сервером и разные серверы могут давать различные отклики. Опция requested IP address указывается только в сообщении DHCPREQUEST, когда клиент проверил полученные ранее параметры. Поле ciaddr клиент заполняет лишь в том случае, когда он имеет корректно настроенный адрес IP в состоянии BOUND, RENEWING или REBINDING.

Если сервер получает сообщение DHCPREQUEST с неприемлемым requested IP address, ему **следует** передать в ответ сообщение DHCPNAK. Информация об этом может быть также передана системному администратору. Сервер может включить сообщение об ошибке в опцию message.

3.6 Использование DHCP на клиентах с несколькими интерфейсами

Клиент, имеющий несколько сетевых интерфейсов, должен независимо использовать DHCP для каждого интерфейса при получении конфигурационных параметров для этих интерфейсов.

3.7 Когда клиенту следует применять DHCP

Клиенту **следует** использовать DHCP для повторного получения или проверки адреса IP и сетевых параметров, если эти параметры могли быть изменены локально (например, при перезагрузке или отключении от локальной сети), поскольку конфигурация сети могла измениться без ведома клиента или пользователя.

¹В соответствии с RFC 4361 текст «или chaddr» удален из спецификации. Прим. перев.

Если клиент знает прежний сетевой адрес и не может связаться с локальным сервером DHCP, он может продолжать использование прежнего адреса до завершения срока аренды. Если аренда закончится до того, как клиент сможет связаться с сервером DHCP, клиент должен незамедлительно прекратить использование сетевого адреса и может сообщить локальным пользователям о проблеме.

4. Спецификация протокола DHCP

В этом разделе предполагается, что сервер DHCP имеет блок сетевых адресов, из которого он может выделять значения по запросам клиентов. Каждый сервер также поддерживает базу данных о выделенных адресах и сроках аренды в локальном постоянном хранилище.

4.1 Создание и передача сообщений DHCP

Клиенты и серверы DHCP создают сообщения DHCP, заполняя поля в разделах с фиксированным форматом и добавляют помеченные элементы данных в область опций переменного размера. Область опций содержит в первых 4 октетах magic cookie (см. раздел 3), за которыми следуют опции. Последней всегда должна указываться опция end.

DHCP использует транспортный протокол UDP. Сообщения DHCP от клиента к серверу передаются в порт DHCP server (67), а сообщения DHCP от сервера к клиенту - в порт DHCP client (68). Сервер с множеством сетевых адресов (например, многодомный хост) **может** использовать любой из своих адресов для исходящих сообщений DHCP.

Поле server identifier используется для идентификации сервера DHCP в сообщении, а также в качестве адреса получателя сообщений от клиента. Сервер с множеством сетевых адресов **должен** быть готов воспринимать любой из своих адресов в качестве идентификатора сервера в сообщении DHCP. С учётом возможности неполной связности сети сервер **должен** выбирать в качестве server identifier тот адрес, который с его точки зрения будет доступен для клиента. Например, если сервер и клиент DHCP подключены к одной подсети (т. е. в поле giaddr сообщения от клиента установлен 0), серверу **следует** выбрать IP-адрес, используемый для связи с этой подсетью, в качестве server identifier. Если сервер использует множество адресов IP в этой подсети, он может указать любой из них. Если сервер получил сообщение через ретранслятор DHCP, ему **следует** выбрать адрес интерфейса, через который он получил такое сообщение, в качестве server identifier (если у сервера нет лучшей информации для этого выбора). Клиент DHCP **должен** использовать IP-адрес из опции server identifier для любых запросов к серверу DHCP, направляемых по индивидуальному адресу.

Сообщения DHCP, передаваемые клиентом в широковещательном режиме до получения им адреса IP, должны указывать в поле IP-адреса отправителя значение 0.

Если поле giaddr в сообщении DHCP от клиента отлично от 0, сервер передаёт все отклики на сообщения в порт DHCP server транслятора BOOTP, адрес которого указан в поле giaddr. Если giaddr = 0, а поле ciaddr отлично от нуля, сервер передаёт сообщения DHCP OFFER и DHCP ACK по индивидуальному адресу ciaddr. Если giaddr = 0, ciaddr = 0 и установлен флаг broadcast, сервер передаёт сообщения DHCP OFFER и DHCP ACK по широковещательному адресу 0xffffffff. Если флаг broadcast не установлен, а giaddr и ciaddr имеют значение 0, сервер передаёт сообщения DHCP OFFER и DHCP ACK по индивидуальному аппаратному адресу клиента и yiaddr. Во всех случаях, когда giaddr = 0, сервер отправляет сообщения DHCP NAK по широковещательному адресу 0xffffffff.

Если опции в сообщении DHCP используют поля sname и file, в поле options **должна** присутствовать опция option overload со значением 1, 2 или 3, как указано в RFC 1533. Если опция option overload присутствует в поле options, опции этого поля **должны** завершаться опцией end и **могут** включать одну или несколько опций pad для заполнения. Опции в полях sname и file (если их использование указано опцией option overload) **должны** начинаться с первого октета этих полей и **должны** завершаться опцией end, за которой **должны** следовать опции pad для заполнения оставшейся части поля. Любая отдельная опция в поле options, sname или file **должна** полностью помещаться в это поле. Опции в поле options **должны** обрабатываться первыми, чтобы могли быть интерпретированы любые опции option overload. Следующим **должно** обрабатываться поле file (если опция option overload указывает, что это поле содержит опции DHCP), а затем - поле sname.

Данные для передачи в опции могут оказаться слишком велики для включения в 255 октетов, доступных для одной опции (например, список маршрутизаторов в опции router [21]). Опции могут включаться лишь однократно, если иного не указано в спецификации конкретной опции. Клиент объединяет значения множества экземпляров одной опции в один список параметров.

Клиенты DHCP отвечают за повторную передачу сообщений. Клиент **должен** применять стратегию повторов, использующую алгоритм случайного увеличения интервалов между сообщениями. Задержку между повторами **следует** выбирать так, чтобы времени хватило на доставку откликов от сервера с учётом характеристик соединения между клиентом и сервером. Например, в сети Ethernet 10 Мбит/с, задержку перед первым повтором **следует** устанавливать 4 секунды с добавлением случайного значения из интервала от -1 до +1 с однородным распределением. Клиенты, часы которых обеспечивают точность лучше 1 секунды, могут выбирать дробные значения задержки. Перед следующим повтором **следует** выбирать задержку 8 секунд с добавлением случайного значения из интервала от -1 до +1 с однородным распределением. Задержку повтора **следует** удваивать при каждом повторе до достижения максимального интервала в 64 секунды. Клиент **может** показывать попытки повтора пользователю для индикации процесса настройки конфигурации.

Поле xid используется клиентом для сопоставления входящих сообщений DHCP с ожидающими запросами. Клиент DHCP **должен** вбирать значения xid так, чтобы минимизировать вероятность совпадения с xid другого клиента. Например, клиент может выбирать новое случайное начальное значение xid при каждой загрузке, а затем увеличивать значение идентификатора при каждом запросе до следующей перезагрузки. Выбор нового значения xid для каждого повтора определяется реализацией. Клиент может при каждом повторе выбирать новое значение xid или использовать прежнее.

Обычно серверы DHCP и трансляторы BOOTP пытаются напрямую доставить сообщения DHCP OFFER и DHCP ACK¹ клиенту с использованием индивидуальной адресации. IP-адрес получается (в заголовке IP) устанавливается в соответствии с полем yiaddr, а адрес получателя канального уровня - в соответствии с полем chaddr из сообщения

¹ В оригинале здесь было ошибочно указано ещё сообщение DHCP NAK. См. <https://www.rfc-editor.org/errata/eid5100>. Прим. перев.

DHCP. К сожалению некоторые реализации клиентов не способны принимать такие индивидуальные дейтаграммы, пока не будет настроен действующий адрес IP (возникает тупик, когда IP-адрес не может быть доставлен клиенту, пока у того не настроен адрес IP).

Клиенту, который не способен принимать индивидуальные дейтаграммы IP, пока в его программах не настроен адрес IP, **следует** устанавливать бит BROADCAST в поле flags всех передаваемых сообщений DHCPDISCOVER и DHCPREQUEST. Флаг BROADCAST подсказывает серверам DHCP и ретрансляторам BOOTP, что сообщения нужно передавать в подсеть клиента с использованием широковещания. Клиенту, способному принимать индивидуальные дейтаграммы IP до настройки протокола, **следует** сбрасывать флаг BROADCAST. Последствия использования флага BROADCAST обсуждаются в документе, разъясняющем протокол BOOTP [21].

Серверам и ретрансляторам, передающим или пересылающим сообщения DHCP напрямую клиентам (т. е. без указания транслятора в поле giaddr), **следует** проверять бит BROADCAST в поле flags. При установленном (1) флаге сообщение DHCP **следует** передавать в широковещательном режиме, указывая широковещательный адрес IP (предпочтительно 0xffffffff) в поле получателя IP и широковещательный адрес канального уровня в поле адресата канального уровня. Если флаг BROADCAST сброшен (0), **следует** передавать сообщение по индивидуальному адресу IP из поля yiaddr и индивидуальному адресу канального уровня из поля chaddr. Если индивидуальная адресация невозможна, сообщение **можно** передать с использованием широковещательного адреса IP (предпочтительно 0xffffffff) и широковещательного адреса канального уровня.

4.2 Элементы администрирования сервера DHCP

Серверы DHCP не обязаны отвечать на каждое полученное сообщение DHCPDISCOVER и DHCPREQUEST. Например, администратор для сохранения контроля над подключёнными к сети клиентами может настроить серверы DHCP так, что они отвечали только клиентам, зарегистрированным с помощью того или иного внешнего механизма. Спецификация DHCP описывает лишь взаимодействие между клиентами и серверами, которые выбрали такое взаимодействие - описание административных мер контроля, применяемых администраторами, выходит за рамки спецификации. Конкретные реализации серверов DHCP могут включать любые средства контроля и правила, нужные администратору.

В некоторых средах сервер DHCP будет принимать во внимание значения фирменных опций в сообщениях DHCPDISCOVER и DHCPREQUEST при определении подходящих параметров для конкретного клиента.

Серверу DHCP нужно использовать некий уникальный идентификатор для привязки клиента к его аренде. Клиент **может** явно предоставлять идентификатор в опции client identifier. В таких случаях клиент **должен** указывать этот же идентификатор во всех последующих сообщениях, а сервер **должен** использовать это значение для идентификации клиента. Если клиент не использует опцию client identifier, сервер **должен** использовать для идентификации клиента содержимое поля chaddr¹. Для клиента крайне важно обеспечивать уникальность значения опции client identifier в рамках подсети. Использование chaddr в качестве идентификатора клиента может приводить к неожиданным результатам, поскольку этот идентификатор может быть связан с аппаратным интерфейсом, который может перейти к другому клиенту. Некоторые сайты могут использовать в качестве client identifier серийный номер оборудования для предотвращения неожиданного изменения сетевого адреса клиента при переносе интерфейса в другой компьютер. В качестве client identifier может использоваться имя DNS для привязки аренды к имени, а не к оборудованию².

Клиенты DHCP свободны в выборе сервера DHCP из числа ответивших сообщениями DHCP OFFER. Реализациям клиентов DHCP **следует** давать пользователю механизм непосредственного выбора значений vendor class identifier.

4.3 Поведение сервера DHCP

Сервер DHCP обрабатывает входящие сообщения DHCP от клиентов на основе текущего состояния привязки для данного клиента. Сервер DHCP может получать от клиента сообщения:

- DHCPDISCOVER;
- DHCPREQUEST;
- DHCPDECLINE;
- DHCPRELEASE;
- DHCPINFORM.

В таблице 3 описано использование полей и опций сообщений сервером DHCP. В оставшейся части этого параграфа описываются действия сервера DHCP для всех входящих сообщений.

4.3.1 Сообщение DHCPDISCOVER

При получении от клиента сообщения DHCPDISCOVER сервер выбирает для этого клиента сетевой адрес. Если доступных адресов нет, сервер может сообщить об этом системному администратору. Если доступные адреса имеются, при выборе **следует** руководствоваться приведённым ниже порядком:

- адрес клиента, записанный в текущей привязке для этого клиента;
- предыдущий адрес клиента, сохранённый в (истекшей или освобождённой) привязке, если этот адрес доступен и свободен;
- адрес, указанный в опции Requested IP Address, если он пригоден и не занят;

¹В соответствии с RFC 4361 текст «Клиент **может** явно предоставлять идентификатор в опции client identifier. В таких случаях клиент **должен** указывать этот же идентификатор во всех последующих сообщениях, а сервер **должен** использовать это значение для идентификации клиента. Если клиент не использует опцию client identifier, сервер **должен** использовать для идентификации клиента содержимое поля chaddr» заменён словами «Клиент **должен** явно предоставить свой идентификатор с помощью опции client identifier. Клиент **должен** использовать одинаковую опцию client identifier во всех сообщениях». Прим. перев.

²В соответствии с RFC 4361 текст «Использование chaddr в качестве идентификатора клиента может приводить к неожиданным результатам, поскольку этот идентификатор может быть связан с аппаратным интерфейсом, который может перейти к другому клиенту. Некоторые сайты могут использовать в качестве client identifier серийный номер оборудования для предотвращения неожиданного изменения сетевого адреса клиента при переносе интерфейса в другой компьютер. В качестве client identifier может использоваться имя DNS для привязки аренды к имени, а не к оборудованию» заменён текстом «Клиенту DHCP **недопустимо** опираться на поле chaddr для идентификации». Прим. перев.

- новый адрес из пула доступных с учётом подсети, из которой получено сообщение (если giaddr = 0), или адреса транслятора, переславшего сообщение (giaddr отличается от 0).

Как сказано в параграфе 4.2, сервер **может** по административным причинам выделить адрес, отличающийся от запрошенного, или отвергнуть запрос конкретного клиента даже при наличии доступных адресов.

Отметим, что в некоторых вариантах архитектуры сетей (например, при наличии в одном физическом сегменте более одной подсети IP), клиенту DHCP следует выделять адрес из подсети, отличающейся от указанной в giaddr. Поэтому DHCP не обязан выделять клиенту адрес из подсети, указанной giaddr. Сервер может выбрать другую подсеть и способы такого выбора выходят за рамки спецификации DHCP.

Хотя для корректной работы DHCP это не требуется, серверам **не следует** повторно использовать выбранный сетевой адрес до того, как клиент ответит на сообщение DHCP OFFER. Сервер может записывать адрес, предложенный клиенту.

Сервер также должен выбрать срок аренды адреса в соответствии с приведёнными ниже правилами и порядком.

- Если клиент не указал конкретный срок аренды в сообщении DHCPDISCOVER и уже имеет выделенный сетевой адрес, сервер возвращает срок завершения аренды для этого адреса (отметим, что клиент должен явно запросить конкретный срок для расширения времени аренды уже назначенного ему адреса).
- Если клиент не указал конкретный срок аренды в сообщении DHCPDISCOVER и не ещё имеет сетевого адреса, сервер задаёт принятое по умолчанию время аренды.
- Если клиент указал конкретный срок аренды в сообщении DHCPDISCOVER (независимо от наличия у него сетевого адреса), сервер может установить запрошенный срок (если локальная политика позволяет это) или выбрать другую продолжительность аренды.

Таблица 3. Поля и опции, используемые сервером DHCP.

Поле	DHCPOFFER	DHCPACK	DHCPNAK
op	BOOTREPLY	BOOTREPLY	BOOTREPLY
htype	Из RFC Assigned Numbers		
hlen	Размер аппаратного адреса в октетах.		
hops	0	0	0
xid	xid из DHCPDISCOVER	xid из DHCPREQUEST	xid из DHCPREQUEST
secs	0	0	0
ciaddr	0	ciaddr из DHCPREQUEST или 0	0
yiaddr	Предложенный клиенту адрес IP		
siaddr	IP-адрес следующего сервера загрузки	IP-адрес следующего сервера загрузки	0
flags	Flags из DHCPDISCOVER	flags из DHCPREQUEST	flags из DHCPREQUEST
giaddr	giaddr из DHCPDISCOVER	giaddr из DHCPREQUEST	giaddr из DHCPREQUEST
chaddr	chaddr из DHCPDISCOVER	chaddr из DHCPREQUEST	chaddr из DHCPREQUEST
sname	Имя сервера или опции		
file	Имя файла для загрузки клиента или опции		
options	Опции		
Опция	DHCPOFFER	DHCPACK	DHCPNAK
Запрошенный адрес IP	Недопустимо	Недопустимо	Недопустимо
Время аренды адреса IP	Требуется	Требуется (DHCPREQUEST) Недопустимо (DHCPINFORM)	Недопустимо
Использование полей file/sname	Возможно	Возможно	Недопустимо
Тип сообщения DHCP	DHCPOFFER	DHCPACK	DHCPNAK
Список параметров запроса	Недопустимо	Недопустимо	Недопустимо
Сообщение	Следует	Следует	Следует
Идентификатор клиента	Недопустимо	Недопустимо	Возможно
Идентификатор класса производителя	Возможно	Возможно	Возможно
Идентификатор сервера	Требуется	Требуется	Требуется
Максимальный размер сообщения	Недопустимо	Недопустимо	Недопустимо
Все прочие	Возможно	Возможно	Недопустимо

После определения сетевого адреса и срока аренды сервер создаёт сообщение DHCP OFFER с предлагаемыми параметрами конфигурации. Важно, чтобы все серверы DHCP возвращали одинаковые параметры (возможно за исключением недавно выделенного сетевого адреса) для обеспечения предсказуемого поведения клиента независимо от выбора им того или иного сервера. Конфигурационные параметры **должны** выбираться в соответствии с приведёнными ниже правилами и сетевой администратор отвечает за согласованность откликов от разных серверов DHCP. Сервер **должен** возвращать клиенту перечисленные ниже параметры.

- Сетевой адрес клиента в соответствии с правилами, приведёнными выше.
- Срок завершения аренды, заданный в соответствии с приведёнными выше правилами.
- Параметры, запрошенные клиентом, в соответствии с приведёнными ниже правилами в указанном порядке:
 - если на сервере явно задано принятое по умолчанию значение параметра, сервер **должен** включать это значение в соответствующую опцию поля option;
 - если сервер распознает параметр, как заданный в документе Host Requirements, он **должен** включить принятое по умолчанию значение из Host Requirements в соответствующую опцию поля option;

- в остальных случаях серверу **недопустимо** возвращать значение параметра.

Сервер **должен** представить как можно большее число запрошенных параметров и **должен** опускать все параметры, которые он не может предоставить. Сервер **должен** включать каждый запрошенный параметр только один раз, если иное явно не разрешено документом описывающим опции DHCP и фирменные расширения BOOTP.

- Все параметры из существующих привязок, которые отличаются от принятых по умолчанию в Host Requirements.
- Все специфические параметры клиента (как указывает содержимое полей `chaddr`¹ и `client identifier` в сообщении DHCPDISCOVER или DHCPREQUEST), например, заданные администратором сети.
- Все специфические для данного класса клиентов параметры (в соответствии с содержимым опции `vendor class identifier` в DHCPDISCOVER или DHCPREQUEST), например, заданные администратором сети. Параметры **должны** указываться с точным совпадением идентификаторов `vendor class` для клиента и идентификаторов классов клиентов на сервере.
- Параметры, с отличающимися от принятых по умолчанию значениями для подсети клиента.

Сервер **может** возвращать `vendor class identifier`, используемый для определения параметров, в сообщении DHCPDISCOVER, чтобы помочь клиенту при выборе приемлемого DHCPDISCOVER. Сервер помещает поле `xid` из DHCPDISCOVER в поле `xid` сообщения DHCPDISCOVER и передаёт последнее запрашивающему клиенту.

4.3.2 Сообщение DHCPREQUEST

Сообщения DHCPREQUEST могут приходиться от клиентов, отвечающих на серверные сообщения DHCPDISCOVER, от клиентов, проверяющих выделенный ранее адрес IP, или от клиентов, желающих продлить аренду адреса. Если сообщение DHCPREQUEST включает опцию `server identifier`, оно является откликом на DHCPDISCOVER. В остальных случаях сообщение служит для проверки или продления имеющейся аренды. Если клиент использует `client identifier` в сообщении DHCPREQUEST, он **должен** указывать тот же идентификатор во всех последующих сообщениях. Если клиент указал список запрашиваемых параметров в сообщении DHCPDISCOVER, он **должен** включать этот же список параметров в последующие сообщения.

Конфигурационным параметрам в DHCPACK **не следует** противоречить параметрам из предыдущего сообщения DHCPDISCOVER, на которое клиент ответил. Клиенту **следует** применять параметры из DHCPACK для своей настройки.

Клиент передаёт сообщения DHCPREQUEST в соответствии с приведёнными ниже описаниями.

- DHCPREQUEST в состоянии SELECTING.

Клиент помещает адрес выбранного сервера в `server identifier`, поле `ciaddr` **должно** быть равно 0, поле `requested IP address` **должно** содержать значение `yiaddr` из выбранного сообщения DHCPDISCOVER.

Отметим, что клиент может собрать несколько сообщений DHCPDISCOVER и выбрать среди них «лучшее». Свой выбор клиент указывает включением предложившего его сервера в сообщение DHCPREQUEST. Если клиент не получил приемлемых предложений, он может повторить передачу сообщения DHCPDISCOVER. Поэтому серверы могут не получить конкретного сообщения DHCPREQUEST, из которого можно понять, было ли предложение принято клиентом. Поскольку серверы не фиксируют назначения сетевых адресов на основе своих предложений DHCPDISCOVER, они могут снова указать предлагавшийся ранее адрес в откликах на последующие запросы. В соответствии с деталями реализации некоторым серверам **не следует** снова использовать предложенные адреса и они могут использовать определяемые реализацией механизмы таймаутов для определения возможности снова использовать адрес.

- DHCPREQUEST в состоянии INIT-REBOOT.

Поле `server identifier` **недопустимо** заполнять, опция `requested IP address` **должна** указывать ранее назначенный адрес клиента, а поле `ciaddr` **должно** иметь значение 0. Клиент проверяет ранее выделенную, кэшированную им конфигурацию. Серверу **следует** передать в ответ сообщение DHCPNAK, если `requested IP address` указывает некорректный адрес или относится к неподходящей сети.

Для определения корректности сети клиента в состоянии INIT-REBOOT проверяется содержимое `giaddr`, опция `requested IP address` и выполняется просмотр базы данных. Если сервер DHCP обнаруживает, что клиент находится в неподходящей сети (т. е. результат применения локальной или удалённой (если `giaddr` отличается от 0) маски подсети к значению опции `requested IP address` даёт несоответствие), серверу **следует** вернуть клиенту сообщение DHCPNAK.

Если сеть корректна, серверу DHCP следует проверить корректность указанного клиентом адреса IP. Если адрес не подходит, серверу **следует** передать сообщение DHCPNAK. Если у сервера DHCP нет записи для этого клиента, он **должен** оставить сообщение без ответа и **может** передать предупреждение администратору сети. Такое поведение требуется для «мирного сосуществования» не взаимодействующих серверов DHCP в одном физическом сегменте.

Если в сообщении DHCPREQUEST `giaddr = 0x0`, клиент расположен в одной подсети с сервером. Сервер **должен** передать сообщение DHCPNAK по широковещательному адресу `0xffffffff`, поскольку у клиента может не быть корректного сетевого адреса и маски подсети и он может не отвечать на запросы ARP.

Если в сообщении DHCPREQUEST установлено отличное от нуля значение `giaddr`, клиент находится в другой подсети. Сервер **должен** установить флаг `B` в сообщении DHCPNAK, чтобы транслятор передал сообщение DHCPNAK клиенту по широковещательному адресу, поскольку у клиента может не быть корректного сетевого адреса и маски подсети и он может не отвечать на запросы ARP.

- DHCPREQUEST в состоянии RENEWING.

¹В соответствии с RFC 4361 текст «`chaddr`» удален из спецификации. Прим. перев.

Поле server identifier и опцию requested IP address **недопустимо** заполнять, а в поле ciaddr **должен** быть указан IP-адрес клиента. В этой ситуации клиент полностью настроен и пытается продлить срок аренды. Это сообщение будет передаваться по индивидуальному адресу без привлечения агентов ретрансляции. Поскольку giaddr в этом случае не указывается, сервер DHCP будет доверять значению ciaddr и использовать его при передаче отклика клиенту.

Клиент **может** обновить или продлить аренду до истечения времени T1. Сервер может отказаться от продления аренды (например, в соответствии с политикой), но независимо от этого ему следует вернуть сообщение DHCPACK.

- DHCPREQUEST в состоянии REBINDING.

Поле server identifier и опцию requested IP address **недопустимо** заполнять, а в поле ciaddr **должен** быть указан IP-адрес клиента. В этой ситуации клиент полностью настроен и пытается продлить срок аренды. Это сообщение **должно** передаваться по широковещательному адресу IP 0xffffffff. Серверу DHCP **следует** проверить корректность значения ciaddr до передачи отклика на сообщение DHCPREQUEST.

Сообщение DHCPREQUEST от клиента в состоянии REBINDING предназначено для сайтов с множеством серверов DHCP и механизмом согласования состояний аренды между ними. Сервер DHCP **может** продлить клиенту аренду лишь в том случае, когда он имеет для этого административные полномочия.

4.3.3 Сообщение DHCPDECLINE

Получение сервером сообщения DHCPDECLINE говорит о том, что клиент тем или иным способом определил занятость предложенного ему сетевого адреса. Сервер **должен** пометить сетевой адрес как недоступный и **следует** уведомить локального администратора о возможных проблемах в конфигурации.

4.3.4 Сообщение DHCPRELEASE

При получении DHCPRELEASE сервер помечает сетевой адрес как свободный. Серверу **следует** сохранять запись с параметрами инициализации клиента для возможного повторного использования по запросу того же клиента.

4.3.5 Сообщение DHCPINFORM

Сервер отвечает на DHCPINFORM передачей отклика DHCPACK по адресу, указанному в поле ciaddr сообщения DHCPINFORM. Серверу **недопустимо** передавать срок завершения аренды и **не следует** заполнять поле yiaddr. Сервер включает другие параметры в сообщение DHCPACK в соответствии с параграфом 4.3.1.

4.3.6 Сообщения клиента

В таблице 4 приведены различия между сообщениями от клиентов в разных состояниях.

Таблица 4. Клиентские сообщения для разных состояний.

	INIT-REBOOT	SELECTING	RENEWING	REBINDING
broad/unicast	broadcast	broadcast	unicast	broadcast
server-ip	Недопустимо	Требуется	Недопустимо	Недопустимо
requested-ip	Требуется	Требуется	Недопустимо	Недопустимо
ciaddr	0	0	IP-адрес	IP-адрес

4.4 Поведение клиента DHCP

На рисунке 5 приведена диаграмма состояний клиента DHCP.

Клиент может получать от сервера сообщения:

- DHCPOFFER;
- DHCPACK;
- DHCPNAK.

Сообщение DHCPINFORM не показано на рисунке 5. Клиент просто передаёт DHCPINFORM и ждёт отклика DHCPACK. После выбора клиентом своих параметров процесс настройки его конфигурации завершается.

Таблица 5. Поля и опции, используемые клиентом DHCP.

Поле	DHCPDISCOVER DHCPIFORM	DHCPREQUEST	DHCPDECLINE DHCPRELEASE
op	BOOTREQUEST	BOOTREQUEST	BOOTREQUEST
htype	Из RFC Assigned Numbers		
hlen	Размер аппаратного адреса в октетах.		
hops	0	0	0
xid	Выбирается клиентом	xid из клиентского сообщения DHCP OFFER	Выбирается клиентом
secs	0 или число секунд с начала процесса DHCP	0 или число секунд с начала процесса DHCP	0
flags	Установка флага BROADCAST, если клиенту нужно широковещательный отклик	Установка флага BROADCAST, если клиенту нужно ширококвещательный отклик	0
ciaddr	0 (DHCPDISCOVER) Сетевой адрес клиента (DHCPIFORM)	0 или сетевой адрес клиента (BOUND/RENEW/REBIND)	0 (DHCPDECLINE) Сетевой адрес клиента (DHCPRELEASE)
yiaddr	0	0	0
siaddr	0	0	0
giaddr	0	0	0
chaddr	Сетевой адрес клиента	Сетевой адрес клиента	Сетевой адрес клиента
sname	Опции, если указаны в опции sname/file, в остальных случаях не используется	Опции, если указаны в опции sname/file, в остальных случаях не используется	(не используется)
file	Опции, если указаны в опции sname/file, в остальных случаях не используется	Опции, если указаны в опции sname/file, в остальных случаях не используется	(не используется)
options	Опции	Опции	(не используется)
Опция	DHCPDISCOVER DHCPIFORM	DHCPREQUEST	DHCPDECLINE DHCPRELEASE
Requested IP address	Возможно (DISCOVER) Недопустимо (INFORM)	Требуется (SELECTING или INIT-REBOOT) Недопустимо (BOUND или RENEWING)	Требуется (DHCPDECLINE) Недопустимо (DHCPRELEASE)
IP address lease time	Возможно (DISCOVER) Недопустимо (INFORM)	Возможно	Недопустимо
Использование полей file/sname	Возможно	Возможно	Возможно
Тип сообщения DHCP	DHCPDISCOVER DHCPIFORM	DHCPREQUEST	DHCPDECLINE DHCPRELEASE
Client identifier	Возможно	Возможно	Возможно
Vendor class identifier	Возможно	Возможно	Недопустимо
Server identifier	Недопустимо	Требуется (после SELECTING) Недопустимо (после INIT- REBOOT, BOUND, RENEWING или REBINDING)	Требуется
Parameter request list	Возможно	Возможно	Недопустимо
Maximum message size	Возможно	Возможно	Недопустимо
Message	Не следует	Не следует	Следует
Site-specific	Возможно	Возможно	Недопустимо
Все прочие	Возможно	Возможно	Недопустимо

Если параметры приемлемы, клиент записывает адрес сервера из поля server identifier и помещает этот адрес в одноимённое поле DHCPREQUEST ширококвещательного сообщения. После приёма от сервера сообщения DHCPACK клиент инициализирует себя и переходит в состояние BOUND. Сообщение DHCPREQUEST содержит то же значение xid, что и сообщение DHCP OFFER. Клиент записывает время завершения аренды как сумму времени отправки исходного запроса и продолжительности аренды, указанной в сообщении DHCPACK. Клиенту **следует** проверить предложенный адрес на предмет его занятости. Например, если в сети клиента поддерживается ARP, клиент может передать запрос ARP для предложенного адреса. При отправке ширококвещательного запроса ARP для предложенного адреса, клиент должен указать свой аппаратный адрес в поле отправителя и 0 в качестве IP-адреса отправителя, для предотвращения конфликта с кэшами ARP на других хостах той же подсети. Если сетевой адрес уже занят, клиент **должен** передать серверу сообщение DHCPDECLINE. Клиенту **следует** передать ширококвещательный отклик ARP для анонсирования нового адреса IP и сброса устаревших записей в кэшах ARP хостов подсети клиента.

4.4.2 Инициализация с известным сетевым адресом

Клиент начинает с состояния INIT-REBOOT и передаёт сообщение DHCPREQUEST. Клиент **должен** указать известный ему сетевой адрес в опции requested IP address сообщения DHCPREQUEST. Клиент может запросить конкретные параметры конфигурации, перечислив их в опции parameter request list. Клиент генерирует и записывает случайное значение идентификатора транзакции, а затем помещает его в поле xid. Клиент записывает локальное время для последующего контроля срока аренды. Клиенту **недопустимо** включать server identifier в сообщение DHCPREQUEST. Клиент передаёт сообщение DHCPREQUEST по локальному аппаратному ширококвещательному адресу в порт UDP DHCP server.

Когда от сервера приходит сообщение DHCPACK с полем xid, соответствующим значению в клиентском запросе DHCPREQUEST, клиент инициализирует себя и переходит в состояние BOUND. Клиент записывает время завершения

аренды как сумму времени отправки исходного запроса DHCPREQUEST и продолжительности аренды, указанной в сообщении DHCPACK.

4.4.3 Инициализация с назначенным изменением сетевого адресом

Клиент создаёт и записывает случайное значение идентификатора транзакции, а затем помещает его в поле `xid`, а свой сетевой адрес в поле `ciaddr`. Клиент передаёт сообщение DHCPINFORM и может запросить в нём конкретные параметры конфигурации, указав их в опции `parameter request list`. Клиенту **не следует** запрашивать срок аренды.

Клиент передаёт сообщение DHCPINFORM серверу DHCP по индивидуальному адресу, если тот известен, или по адресу ограниченного широковещания (все 1). Сообщение DHCPINFORM **должно** направляться в порт UDP DHCP server.

После получения от сервера сообщения DHCPACK с полем `xid`, совпадающим с одноимённым полем в DHCPINFORM, клиент инициализирует самого себя.

Если клиент не получил сообщения DHCPACK в течение разумного срока ожидания (60 секунд или 4 попытки при использовании тайм-аута, предложенного в параграфе 4.1), ему **следует** вывести сообщение, информирующее пользователя о проблеме, а также **следует** начать работу в сети, используя подходящие значения из Приложения А.

4.4.4 Использование широковещания и индивидуальной адресации

Клиент DHCP передаёт сообщения DHCPDISCOVER, DHCPREQUEST и DHCPINFORM, пока ему не известен адрес сервера DHCP. Сообщение DHCPRELEASE клиент передаёт по индивидуальному адресу сервера. Сообщение DHCPDECLINE передаётся в широковещательном режиме, поскольку клиент отвергает использование предложенного сервером адреса IP. Когда клиент DHCP в состоянии INIT или REBOOTING знает адрес сервера DHCP, он может использовать этот адрес в сообщении DHCPDISCOVER или DHCPREQUEST вместо широковещательного адреса IP. Клиент может также использовать индивидуальный адрес для передачи сообщения DHCPINFORM известному серверу DHCP. Если клиент не получает откликов на сообщения DHCP, отправленные по известному IP-адресу сервера DHCP, ему следует вернуться к использованию широковещательного адреса IP.

4.4.5 Завершение и повторная аренда

Клиент поддерживает параметры T1 и T2, определяющие момент, когда он пытается продлить свою аренду сетевого адреса. T1 указывает время, при котором клиент переходит в состояние RENEWING и пытается связаться с сервером, который назначил ему сетевой адрес. T2 указывает время, когда клиент переходит в состояние REBINDING и пытается связаться с любым сервером. Момент T1 **должен** наступать раньше T2, который, в свою очередь, **должен** наступать раньше завершения срока аренды.

Для предотвращения необходимости синхронизации часов значения T1 и T2 выражаются в опциях интервалами, а не абсолютным временем [2].

В момент T1 клиент переходит в состояние RENEWING и передаёт (по индивидуальному адресу) сообщение DHCPREQUEST серверу для расширения срока аренды. Клиент устанавливает в поле `ciaddr` сообщения DHCPREQUEST свой текущий сетевой адрес и записывает локальное время передачи сообщения DHCPREQUEST для вычисления срока завершения аренды. Клиенту **недопустимо** включать `server identifier` в сообщении DHCPREQUEST.

Любое сообщение DHCPACK, в котором поле `xid` не совпадает с одноимённым полем в отправленном клиентом запросе DHCPREQUEST, отбрасывается без уведомления. При получении от сервера сообщения DHCPACK клиент рассчитывает срок завершения аренды, складывая срок аренды из сообщения DHCPACK со временем отправки DHCPREQUEST. После успешного обновления аренды сетевого адреса клиент возвращается в состояние BOUND и может продолжать работу в сети.

Если сообщение DHCPACK не приходит до момента T2, клиент переходит в состояние REBINDING и передаёт (по широковещательному адресу) сообщение DHCPREQUEST для продления срока аренды, устанавливая в поле `ciaddr` свой текущий сетевой адрес. Клиенту **недопустимо** включать `server identifier` в сообщении DHCPREQUEST.

Значения T1 и T2 настраиваются сервером с помощью опций. Для T1 по умолчанию используется значение в половину срока аренды ($0,5 * duration_of_lease$), для T2 - ($0,875 * duration_of_lease$). При выборе значений T1 и T2 следует добавлять случайное отклонение (`fuzz`) для предотвращения синхронизации разных клиентов.

Клиент **может** обновить или продлить аренду до истечения времени T1. Сервер **может** принять решение о продлении аренды для клиента в соответствии с заданной сетевым администратором политикой. Серверу **следует** возвращать T1 и T2, а их значения **следует** подстраивать с учётом оставшегося времени аренды.

В состояниях RENEWING и REBINDING при отсутствии отклика на сообщение DHCPREQUEST клиенту **следует** выждать половину времени, оставшегося до T2 (RENEWING) или завершения срока аренды (REBINDING), но не менее 60 секунд до того, как повторить сообщение DHCPREQUEST.

Если срок аренды завершается до получения клиентом сообщения DHCPACK, клиент переходит в состояние INIT и **должен** незамедлительно прекратить все сетевые операции, а также запросить параметры инициализации, как будто он ещё не инициализирован. Если клиент получает сообщение DHCPACK, назначающее снова имеющийся у клиента сетевой адрес, ему **следует** продолжать работу в сети. Если клиенту назначен новый сетевой адрес, для него **недопустимо** продолжение работы с прежним адресом и **следует** уведомить об этом локальных пользователей.

4.4.6 DHCPRELEASE

Если клиенту больше не нужен назначенный ему сетевой адрес (например, при выключении хоста), он передаёт серверу сообщение DHCPRELEASE. Отметим, что корректная работа DHCP не зависит от передачи сообщений DHCPRELEASE.

5. Благодарности

Автор признателен множеству (слишком много для перечисления!) участников рабочей группы DHC за их неустанную работу по развитию DHCP и подготовке этого документа.

Спасибо J Allard, Mike Carney, Dave Lapp, Fred Lien и John Mendonca за организацию тестирования функциональной совместимости DHCP.

Разработка этого документа частично поддерживалась в рамках гранта Corporation for National Research Initiatives (CNRI), Bucknell University и Sun Microsystems.

6. Литература

- [1] Acetta, M., "Resource Location Protocol", RFC 887, CMU, December 1983.
- [2] Alexander, S., and R. Droms, "DHCP Options and BOOTP Vendor Extensions", [RFC 1533](#), Lachman Technology, Inc., Bucknell University, October 1993.
- [3] Braden, R., Editor, "Requirements for Internet Hosts – Communication Layers", STD 3, [RFC 1122](#), USC/Information Sciences Institute, October 1989.
- [4] Braden, R., Editor, "Requirements for Internet Hosts – Application and Support", STD 3, [RFC 1123](#), USC/Information Sciences Institute, October 1989.
- [5] Brownell, D, "Dynamic Reverse Address Resolution Protocol (DRARP)", Work in Progress¹.
- [6] Comer, D., and R. Droms, "Uniform Access to Internet Directory Services", Proc. of ACM SIGCOMM '90 (Special issue of Computer Communications Review), 20(4):50--59, 1990.
- [7] Croft, B., and J. Gilmore, "Bootstrap Protocol (BOOTP)", [RFC 951](#), Stanford and SUN Microsystems, September 1985.
- [8] Deering, S., "ICMP Router Discovery Messages", [RFC 1256](#), Xerox PARC, September 1991.
- [9] Droms, D., "Interoperation between DHCP and BOOTP", RFC 1534, Bucknell University, October 1993.
- [10] Finlayson, R., Mann, T., Mogul, J., and M. Theimer, "A Reverse Address Resolution Protocol", [RFC 903](#), Stanford, June 1984.
- [11] Gray C., and D. Cheriton, "Leases: An Efficient Fault-Tolerant Mechanism for Distributed File Cache Consistency", In Proc. Of the Twelfth ACM Symposium on Operating Systems Design, 1989.
- [12] Mockapetris, P., "Domain Names -- Concepts and Facilities", STD 13, [RFC 1034](#), USC/Information Sciences Institute, November 1987.
- [13] Mockapetris, P., "Domain Names -- Implementation and Specification", STD 13, [RFC 1035](#), USC/Information Sciences Institute, November 1987.
- [14] Mogul J., and S. Deering, "Path MTU Discovery", [RFC 1191](#), November 1990.
- [15] Morgan, R., "Dynamic IP Address Assignment for Ethernet Attached Hosts", Work in Progress.
- [16] Postel, J., "Internet Control Message Protocol", STD 5, [RFC 792](#), USC/Information Sciences Institute, September 1981.
- [17] Reynolds, J., "BOOTP Vendor Information Extensions", RFC 1497, USC/Information Sciences Institute, August 1993.
- [18] Reynolds, J., and J. Postel, "Assigned Numbers", STD 2, [RFC 1700](#), USC/Information Sciences Institute, October 1994.
- [19] Jeffrey Schiller and Mark Rosenstein. A Protocol for the Dynamic Assignment of IP Addresses for use on an Ethernet. (Available from the Athena Project, MIT), 1989.
- [20] Sollins, K., "The TFTP Protocol (Revision 2)", RFC 783, NIC, June 1981.
- [21] Wimer, W., "Clarifications and Extensions for the Bootstrap Protocol", RFC 1542, Carnegie Mellon University, October 1993.

7. Вопросы безопасности

DHCP работает непосредственно на основе протоколов UDP и IP, которые по сути не защищены. Кроме того, DHCP в общем случае предназначен для упрощения поддержки удалённых и бездисковых станций. Хотя использование паролей и ключей при такой настройке возможно, оно создаёт сложности и неудобства. Поэтому протокол DHCP в современном состоянии не является защищённым.

Можно легко организовать не уполномоченный сервер DHCP. Такие серверы могут передавать клиентам непригодные данные, такие как недействительные или дублирующиеся адреса IP, некорректные маршруты (включая обманные маршрутизаторы и т. п.), некорректные адресов серверов имён (например, обманных DNS) и т. д. Очевидно, что после этого атакующий может создать дополнительный риск для подвергшихся его влиянию систем.

Враждебные клиенты DHCP могут прикидываться легитимными и получать информацию, предназначенную для тех. При использовании динамического распределения ресурсов враждебные клиенты могут захватывать все ресурсы для себя, блокируя их выделение легитимным клиентам.

8. Адрес автора

Ralph Droms
Computer Science Department
323 Dana Engineering
Bucknell University

¹Работа опубликована в RFC 1931. Прим. перев.

Lewisburg, PA 17837
 Phone: (717) 524-1145
 EMail: droms@bucknell.edu

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

А. Конфигурационные параметры хоста

<i>Параметр</i>	<i>Значение</i>	<i>Документ</i>
Параметры уровня IP, на хост		
Быть маршрутизатором	on/off	RFC 1122, параграф 3.1
Нелокальная маршрутизация от источника	on/off	RFC 1122, параграф 3.3.5
Фильтры правил для нелокальной маршрутизации от отправителя	on/off	RFC 1122, параграф 3.3.5
Максимальный размер сборки (фрагментов)	integer	RFC 1122, параграф 3.3.2
Значение TTL по умолчанию	integer	RFC 1122, параграф 3.2.1.7
Таймаут старения PMTU	integer	RFC 1191, параграф 6.6
Таблица MTU (plateau)	(список)	RFC 1191, параграф 7
Параметры уровня IP, на интерфейс		
Адрес IP	(адрес)	RFC 1122, параграф 3.3.1.6
Маска подсети	(маска адреса)	RFC 1122, параграф 3.3.1.6
MTU	integer	RFC 1122, параграф 3.3.3
MTU для всех подсетей	on/off	RFC 1122, параграф 3.3.3
Вариант широковещательного адреса	0x00000000/0xffffffff	RFC 1122, параграф 3.3.6
Выполнять определение маски	on/off	RFC 1122, параграф 3.2.2.9
Служить поставщиком маски	on/off	RFC 1122, параграф 3.2.2.9
Выполнять обнаружение маршрутизаторов	on/off	RFC 1256, параграф 5.1
Адрес запроса маршрутизатора	(адрес)	RFC 1256, параграф 5.1
Используемый по умолчанию маршрутизаторы, список		
адресов маршрутизаторов	(адрес)	RFC 1122, параграф 3.3.1.6
уровней предпочтения	integer	RFC 1122, параграф 3.3.1.6
Статические маршруты, список		
получателей	(хост/подсеть/сеть)	RFC 1122, параграф 3.3.1.2
масок получателей	(маска адреса)	RFC 1122, параграф 3.3.1.2
типов обслуживания	integer	RFC 1122, параграф 3.3.1.2
первых маршрутизаторов	(адрес)	RFC 1122, параграф 3.3.1.2
игнорирование перенаправления	on/off	RFC 1122, параграф 3.3.1.2
PMTU	integer	RFC 1191, параграф 6.6
Выполнять определение PMTU	on/off	RFC 1191, параграф 6.6
Параметры канального уровня, на интерфейс		
Трейлеры	on/off	RFC 1122, параграф 2.3.1
Тайм-аут кэша ARP	integer	RFC 1122, параграф 2.3.2.1
Инкапсуляция Ethernet	(RFC 894/RFC 1042)	RFC 1122, параграф 2.3.3
TCP_parameters, на хост		
TTL	integer	RFC 1122, параграф 4.2.2.19
Интервал Keep-alive	integer	RFC 1122, параграф 4.2.3.6
Размер данных Keep-alive	0/1	RFC 1122, параграф 4.2.3.6